CONTENTS

KNC 301 / KNC 401 : Computer System Security

1 UNIT

Introduction

CONTENTS

PART-1

Introduction, What is Computer Security and What to Learn ?

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.1. Explain briefly computer security system. How you will design the policies for information security within an organization ?

Answer

1. Computer security (cyber security or IT security) is the protection of information systems from theft or disruption. It is used :
   a. To prevent theft of hardware.
   b. To prevent theft of information.
   c. To prevent disruption of service.
2. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, intentionally or accidentally.
3. Confidentiality, Integrity and Availability (CIA triad), is a model designed to guide policies for information security within an organization.
   a. **Confidentiality :** Confidentiality is a set of rules that limits access to information.
   b. **Integrity :** Integrity is the assurance that the information is trustworthy and accurate.
   c. **Availability :** Availability is a guarantee of reliable access to the information by authorized people.

Que 1.2. Which components of the computer system need to be secure ?

Answer

The components of a computer system that needs to be protected are :

1. Hardware is the physical part of the computer, like the system memory and disk drive.
2. Firmware is the permanent software that runs the processes of the computer and is mostly invisible to the user, like the start-up functions that make elements of the hardware work together.

3. Software is the program that offers service to the user and administrator. The operating system, word processor, computer games, and Internet browser are all examples of software commonly found on a computer.

Que 1.3. Discuss the goals of computer security system.

Answer

Following are the goals of computer security system :

1. **Integrity :**
   a. The objects in the system must not be accessed by any unauthorized user and any user not having sufficient rights should not be allowed to modify the important system files and resources.
2. **Secrecy :**
   a. The objects of the system must be accessible only to a limited number of authorized users.
   b. Not everyone should be able to view the system files.
3. **Availability :**
   a. All the resources of the system must be accessible to all the authorized users *i.e.*, only one user/process should not have the right to dominate all the system resources.
   b. If such kind of situation occurs, denial of service could happen.
   c. In this kind of situation, a malware might dominate the resources for itself and thus preventing the legitimate processes from accessing the system resources.

Que 1.4. Describe the problems related with computer security.

Answer

Problems related with computer security are :

1. **Phishing :** Phishing is an attempt to obtain users sensitive information, including credit card details and banking information, by disguising as a trustworthy entity in an online communication (e-mail, social media, etc).
2. **Vishing :** Vishing (voice phishing) is an attempt of fraudsters to persuade the victim to deliver personal information or transfer money over the phone.
3. **Smishing :** Smishing (SMS phishing) is any case where sent text messages attempt to make potential victims pay money or click on suspicious links.
4. **Pharming :**
   a. Pharming is a cyber attack meant to redirect a website's traffic to another, fake one.

   b. Pharming can be done either by changing the hosts file on a victim's machine or by exploiting a flaw in DNS server software.
   c. Pharming is extremely dangerous because it can affect a large number of computers simultaneously.
   d. In pharming, no conscious user interaction is required.
5. **Vulnerability :**
   a. Vulnerability is a software mistake that enables a bad actor to attack a system or network by directly accessing it.
   b. Vulnerabilities can permit an attacker to act as a super-user or even a system admin and granting them full access privileges.
6. **Exposures :**
   a. It provides a malicious actor with indirect access to a system or a network.
   b. An exposure could enable a hacker to harvest sensitive information in a secret manner.

Que 1.5. Explain security measure taken to protect the system.

Answer

To protect the system, security measures can be taken at the following levels :

1. **Physical :**
   a. The sites containing computer systems must be physically secured against armed and malicious intruders.
   b. The workstations must be carefully protected.
2. **Human :**
   a. Only appropriate users must have the authorization to access the system.
   b. Phishing (collecting confidential information) and dumpster diving (collecting basic information so as to gain unauthorized access) must be avoided.
3. **Operating system :** The system must protect itself from accidental or purposeful security breaches.
4. **Networking system :**
   a. Almost all of the information is shared between different systems via a network.
   b. Intercepting these data could be just as harmful as breaking into a computer.
   c. Henceforth, Network should be properly secured against such attacks.

Que 1.6. **How can an organization protect its computer system hardware ?**

Answer

Five steps to protect computer system hardware are :

1. **Install firewall :**
   a. A firewall enacts the role of a security guard.
   b. A firewall is the first step to provide security to the computer. It creates a barrier between the computer and any unauthorized program trying to come in through the Internet.
2. **Install antivirus software :**
   a. Antivirus is a software that helps to protect the computer from any unauthorized code or software that creates a threat to the system.
   b. Unauthorized software includes viruses, keyloggers, Trojans etc.
   c. This might slow down the processing speed of our computer, delete important files and access personal information.
3. **Install anti-spyware software :**
   a. Spyware is a software program that collects personal information or information about an organization without their approval.
   b. This information is redirected to a third party website.
   c. Spyware is designed in such a way that they are not easy to be removed.
   d. Anti-Spyware software is solely dedicated to combat spyware.
   e. Anti-spyware software offers real time protection.
   f. It scans all the incoming information and helps in blocking the threat once detected.
4. **Use complex and secure passwords :**
   a. For maintaining system security we have to use strong and complex passwords.
   b. Complex passwords are difficult for the hackers to find.
5. **Check on the security settings of the browser :**
   a. Browsers have various security and privacy settings that we should review and set to the level we desire.
   b. Recent browsers give us ability to tell websites to not track our movements, increasing our privacy and security.

Que 1.7. **What are the advantages and disadvantages of computer security ?**

Answer

Advantages of computer security :

1. Protects system against viruses, worms, spyware and other unwanted programs.
2. Protection against data from theft.
3. Protects the computer from being hacked.
4. Minimizes computer freezing and crashes.
5. Gives privacy to users.

Disadvantages of computer security :

1. Firewalls can be difficult to configure correctly.
2. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
3. Makes the system slower.
4. Need to keep updating the new software in order to keep security up to date.
5. Could be costly for average user.

Que 1.8. **Write short note on security policy used for computer systems.**

Answer

1. A security policy comprises of a set of objectives for the company, rules of behaviour for users and administrators, and requirements for system and management that collectively ensure the security of network and computer systems in an organization.
2. A security policy is a living document, meaning that the document is never finished and is continuously updated as technology and employee requirements change.
3. The security policy translates, clarifies, and communicates the management position on security as defined in high-level security principles.
4. The security policy acts as a bridge between management objectives and specific security requirements.
5. It informs users, staff, and managers of their obligatory requirements for protecting technology and information assets.
6. It should specify the mechanisms that we need to meet these requirements.
7. It also provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the security policy.

Que 1.9. **Discuss different security models in details.**

Answer

Following are the various security models :

1. **Lattice models :**
   a. A lattice is a mathematical construct that is built upon the notion of a group.
   b. A lattice is a mathematical construction with :
      i. A set of elements.
      ii. A partial ordering relation.
      iii. The property that any two elements must have unique least upper bound and greatest lower bound.
   c. A security lattice model combines multilevel and multilateral security.
   d. Lattice elements are security labels that consist of a security level and set of categories.
2. **State machine model :**
   a. In the state machine model, the state of a machine is captured in order to verify the security of a system.
   b. A given state consists of all current permissions and instances of subjects accessing the objects. If the subject can access objects only by means that are concurrent with the security policy, the system is secure.
   c. The model is used to describe the behavior of a system to different inputs. It provides mathematical constructs that represent sets (subjects, objects) and sequences. When an object accepts an input, this modifies a state variable thus transiting to a different state.
   d. Implementation tips :
      i. The developer must define what and where the state variables are.
      ii. The developer must define a secure state for each state variable.
      iii. Define and identify the allowable state transition functions.
      iv. The state transition function should be tested to verify that the overall machine state will not compromise and the integrity of the system is maintained.
3. **Non-interference models :**
   a. The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.
   b. It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it cannot change the state for the entity at the lower level.
   c. The model also addresses the inference attack that occurs when someone has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.
4. **Bell-LaPadula confidentiality model :**
   a. It was the first mathematical model with a multilevel security policy that is used to define the concept of a secure state machine and models of access and outlined rules of access.
   b. It is a state machine model that enforces the confidentiality aspects of access model.
   c. The model focuses on ensuring that the subjects with different clearances (top secret, secret, confidential) are properly authenticated by having the necessary security clearance, need to know, and formal access approval-before accessing an object that are under different classification levels.
   d. The rules of Bell-LaPadula model :
      i. **Simple security rule (no read up rule) :** It states that a subject at a given security level cannot read data that resides at a higher security level.
      ii. **Star property rule (no write down rule) :** It states that a subject in a given security level cannot write information to a lower security levels.
5. **Biba integrity model :**
   a. It uses a lattice of integrity levels unlike Bell - LaPadula which uses a lattice of security levels.
   b. It is also an information flow model like the Bell - LaPadula because they are most concerned about data flowing from one level to another.
   c. The rules of Biba model :
      i. **Simple integrity rule (no read down) :** It states that a subject cannot read data from a lower integrity level.
      ii. **Star integrity rule (no write up) :** It states that a subject cannot write data to an object at a higher integrity level.
      iii. **Invocation property :** It states that a subject cannot invoke (call upon) a subject at a higher integrity level.
6. **Clark-Wilson integrity model :**
   a. This model separates data into one subject that needs to be highly protected, referred to as a Constrained Data Item (CDI) and another subset that does not require high level of protection, referred to as Unconstrained Data Items (UDI).

b. Components of Clark-Wilson model :

i. **Subjects (users) :** These are active agents.

ii. **Transformation Procedures (TPs) :** The software procedures such as read, write, modify that perform the required operation on behalf of the subject (user).

iii. **Constrained Data Items (CDI) :** Data that can be modified only by TPs.

iv. **Unconstrained Data Items (UDI) :** Data that can be manipulated by subjects via primitive read/write operations.

v. **Integrity Verification Procedure (IVP) :** Programs that run periodically to check the consistency of CDIs with external reality. These integrity rules are usually defined by vendors.

Que 1.10. **What are the advantages and disadvantages of security model ?**

Answer

Advantages of security model :

1. Protection from malicious attacks on our network.
2. Deletion and guaranteeing malicious elements within a pre-existing network.
3. Prevents users from unauthorized access to the network.
4. Deny programs from certain resources that could be infected.
5. Securing confidential information.

Disadvantages of security model :

1. Strict regulations
2. Difficult to work with non-technical users
3. Restrictive to resources
4. Constantly needs patching
5. Constantly being attacker

Que 1.11. **Discuss the security mechanism used to provide security in computer system.**

Answer

Security mechanisms used to provide security in computer system are :

1. **Encipherment :**

a. Encipherment is an algorithm used for performing encryption or decryption by converting information from plaintext to ciphertext.

b. Cryptography and steganography are used for enciphering.

2. **Data integrity :**

a. Data integrity is the maintenance and the assurance of the accuracy of the data over its entire life-cycle.

b. Data integrity is preserved by comparing check value received to the check value generated.

3. **Digital signature :**

a. A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

b. Public and private keys can be used.

4. **Authentication exchange :** In authentication exchange, two entities exchange some messages to prove their identity to each other.

5. **Traffic padding :** Traffic padding means inserting some fake data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

6. **Routing control :** Routing control means selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.

7. **Notarization :**

a. Notarization means selecting a third trusted party to control the communication between two entities.

b. The receiver can involve a trusted third party to store the sender request in order to prevent the sender from later denying that they made a request.

8. **Access control :** Access control used methods to prove that a user has access right to the data or resources owned by a system.

Que 1.12. **What are the components of security policy ?**

Answer

Following are security policies components :

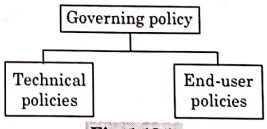

Fig. 1.12.1.

1. **Governing policy :**

a. This policy is a high-level treatment of security concepts that are important to the company.

b. Managers and technical are the intended audience.
c. The governing policy controls all security-related interaction among business units and supporting departments in the company.

2. **End-user policies :**
   a. End-user policy is a set of directives that describes what actions employees must take in order to protect corporate assets.
   b. An end-user policy can be an informal set of guidelines handed out to employees in public place.
3. **Technical policies :**
   a. Security staff members use technical policies as they carry out their security responsibilities for the system.
   b. These policies are more detailed than the governing policy and are system or issue specific.

PART-2

Sample Attacks, The Marketplace For Vulnerabilities, Error 404 Hacking Digital India Part 1 Chase.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.13. Discuss various attacks in computer security.

Answer

Various attacks in computer security :

1. **Malware :**
   a. Malware is used to describe malicious software, including spyware, ransomware, viruses and worms.
   b. Malware breaches a network through vulnerability typically when a user clicks a dangerous link or email attachment that then installs risky software.
2. **Macro viruses :**
   a. These viruses infect applications such as Microsoft Word or Excel.
   b. Macro viruses attach to an application's initialization sequence.
   c. When the application is opened, then virus executes instructions before transferring control to the application.
   d. The virus replicates itself and attaches to other code in the computer system.

3. **File infectors :**
   a. File infector viruses usually attach themselves to executable code, such as .exe files.
   b. The virus is installed when the code is loaded.
4. **System or boot-record infectors :**
   a. A boot-record virus attaches to the master boot record on hard disks.
   b. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.
5. **Stealth viruses :**
   a. Stealth viruses take over system functions to conceal themselves.
   b. They do this by compromising malware detection software so that the software will report an infected area as being uninfected.
   c. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.
6. **Trojans :**
   a. A Trojan is a program that hides in a useful program and has a malicious function.
   b. A major difference between viruses and Trojans is that Trojans do not self-replicate.
7. **Logic bombs :** A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
8. **Worms :**
   a. Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers.
   b. Worms are commonly spread through email attachments, opening the attachment activates the worm program.
9. **Droppers :**
   a. A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus scanning software.
   b. A dropper can also connect to the Internet and download updates to virus software that is resident on a compromised system.
10. **Ransomware :**
    a. Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid.

b. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.

11. Denial of service attack :

a. A denial of service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth.

b. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack.

c. This is known as a Distributed Denial of Service (DDoS) attack.

Que 1.14. Write short note on server-side attack and insider attack.

Answer

Server-side attacks :

1. Server-side attacks are launched directly from an attacker (the client) to a listening service.
2. Server-side attacks seek to compromise and breach the data and applications that are present on a server.
3. Server-side attacks exploit vulnerabilities in installed services.

Insider attacks :

1. An insider attack is a malicious attack executed on a network or computer system by a person with authorized system access.
2. Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures.
3. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

Que 1.15. Differentiate between active and passive attack.

Answer

Basis for comparison	Active attack	Passive attack
Basic	Active attack tries to change the system resources or affect their operation	Passive attack tries to read or make use of information from the system but does not influence system resources
Modification in the information	Occurs	Does not take place
Harm to the system	Always causes damage to the system	Do not cause any harm
Threat to	Integrity and availability	Confidentiality
Attack awareness	The entity (victim) gets informed about the attack	The entity is unaware of the attack
Task performed by the attacker	The transmission is captured by physically controlling the portion of a link	Just need to observe the transmission
Emphasis is on	Detection	Prevention

Que 1.16. Write a short note on marketplace for vulnerabilities.

Answer

1. Vulnerability is a cyber security term that refers to a flaw in a system that can leave it open to attack.
2. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
3. Software vulnerabilities and exploits are used to get remote access to both stored information and information generated in real time.
4. When most people use the same software, then one specific vulnerability can be used against thousands of people. In this context, criminals have become interested in such vulnerabilities.
5. As a result, both national security agencies and criminals hide certain software vulnerabilities from both users and the original developer. This type of vulnerability is known as a zero-day exploit.

Que 1.17. **How can we defend zero-day vulnerabilities ?**

Answer

1. Use virtual local area networks to segregate some areas of the network or use dedicated physical or virtual network segments to isolate sensitive traffic flowing between servers.
2. Implement IPsec, the IP security protocol, to apply encryption and authentication to network traffic.
3. Deploy an IDS or IPS. Although signature-based IDS and IPS security products may not be able to identify the attack, they may be able to alert defenders to suspicious activity that occurs as a side effect to the attack.
4. Use network access control to prevent rogue machines from gaining access to crucial parts of the enterprise environment.
5. Lock down wireless access points and use a security scheme such as Wi-Fi Protected Access 2 (WPA2) for maximum protection against wireless-based attacks.
6. Keep all systems patched and up to date. Although patches will not stop a zero-day attack, keeping network resources fully patched may make it more difficult for an attack to succeed. When a zero-day patch does become available, apply it as soon as possible.
7. Perform regular vulnerability scanning against enterprise networks and lock down any vulnerabilities that are discovered.

Que 1.18. **Discuss error 404 hacking digital India part 1 chase.**

Answer

1. In error 404 hacking digital India part 1 chase, the cyber crime and cyber attacks hack the information of users like bank detail and personal information.
2. It is real time incident. In this, attacker or hacker creates an attractive video so that victim gets attracted and plays that video into system.
3. When we clicked on video to play then at the time of buffering, hacker can know our current location and GPS history but also have complete access to our contacts, text messages, Facebook, Whatsapp and most importantly our bank details, including our CVV number.
4. Hackers are creating a kind Trojan file, and android apk files. The apk files that will be distributed all over the internet. Those who download this file will be hacked easily. They are always bound by some games like candy crush many others.
5. Potential cyber attacks that is most common in error 404 hacking :

a. Web application attack :

i. A web application is a client-server computer program which uses web browsers and web technology to allow its visitors to store and retrieve data to/from the database over the internet.

ii. If there is flaw in the web application, it allows the attacker to manipulate data using SQL injection attack.

b. Network security attacks :

i. Network security attacks are unauthorized actions against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data.

ii. As more enterprises invite employees to access data from mobile devices, networks become vulnerable to data theft or total destruction of the data or network.

c. Mobile security attacks :

i. Mobile security, or more specifically mobile device security, has become increasingly important in mobile computing.

ii. Of particular concern is the security of personal and business information now stored on smartphones.

iii. More and more users and businesses use smartphones to communicate, but also to plan and organize their users' work and also private life.

iv. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks.

v. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

PART-3

Control Hijacking, More Control Hijacking Attacks Integer Overflow, More Control Hijacking Attacks Format String Vulnerability.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.19. **Discuss control hijacking in computer security.**

Answer

1. Hijacking is a type of network security attack in which the attacker takes control of a communication.
2. In hijacking (also known as a man in the middle attack), the perpetrator takes control of an established connection while it is in progress.
3. The attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly.
4. The attacker uses a program that appears to be the server to the client and appears to be the client to the server.
5. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them.
6. Attacker's goal in control hijacking :
   a. Takeover target machine (for example web server)
   b. Execute arbitrary code on target by hijacking application control flow
7. There are three types of control hijacking in computer security :
   a. Buffer overflow attacks
   b. Integer overflow attacks
   c. Format string vulnerabilities

Que 1.20. Describe briefly buffer overflow attack.

Answer

1. A buffer is a temporary area for data storage. When more data gets placed by a program or system process, the extra data overflows.
2. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.
3. In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user.
4. For example, the data could trigger a response that damages files, changes data or unveils private information.
5. Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input.
6. There are two types of buffer overflows:
   a. **Heap-based buffer overflow :** A heap-based overflow condition is a buffer overflow, where the buffer is allocated in the heap portion of memory.

   b. **Stack-based buffer overflow :** A stack-based buffer overflow is a condition where the buffer is allocated on the stack.

Que 1.21. How to prevent buffer overflow attack ?

Answer

We can prevent buffer overflow by using :

1. **Non-executable stack :**
   a. In this method, the stack is configured not to hold any executable code.
   b. Kernel patches are available for both Linux and Solaris for configuring a non-executable stack.
   c. Data execution prevention in Windows XP protects the stack against buffer overflow.
   d. This method protects stack-based buffer overflow attacks.
   e. Heap-based overflows and static data segment overflows cannot be prevented by this technique.
2. **Static analysis :**
   a. In static analysis the source code is parsed for dangerous library calls and race conditions to detect potential buffer overflows.
   b. Functions like strcpy and sprintf are vulnerable to buffer overflows, so source code scanners are used to look for incorrect use of these functions.
3. **Dynamic run-time protection :** Buffer. overflow conditions are detected during the actual running of the program in this method, and an attack thwarted. Different techniques of dynamic run-time analysis are :
   a. **Canary :**
      i. When a function call is made, a canary is added to the return address; if a buffer overflow occurs, the canary will be corrupted.
      ii. So, before returning to the parent function, the canary is checked again to see if it has been modified.
   b. **Copying return address :**
      i. In this method, the return address is saved separately.
      ii. So even when a buffer overflow exploit overwrites the return address on the stack, it is set back to the original value when the function returns.
   c. **Array bounds checking :**
      i. When an array is read from or written to, this technique double-checks whether the boundaries are being violated.

d. **Memory access checking :**
   i. Here, verification code is added to the binary when the prog... is compiled.
   ii. It checks access violations in real time.

4. **Use safer versions of functions :**
   a. Safer alternatives are available for all the traditional functio... beset by buffer overflows.
   b. For instance, strncpy and snprintf are safer than the older str... and sprint.
   c. When new applications are being developed, ensure that only ... safer variants are used.

Que 1.22. **Explain integer overflow attack.**

Answer

1. An integer overflow attack occurs when an attacker causes a value ... the program to be large enough to overflow unexpectedly.
2. A common form of this attack is to cause a buffer to be allocated that ... too small to hold data copied into it later, thus enabling a buffer overflo... attack.
3. We are able to detect buffer overflow attacks in the same way as ... normal buffer overflow attack.
4. An integer overflow is the condition that occurs when the result of ... arithmetic operation, such as multiplication or addition, exceeds th... maximum size of the integer types used to store it.
5. When an integer overflow occurs, the interpreted value will appear ... have wrapped around the maximum value and started again at the ... minimum value, similar to a clock that represents 13 : 00 by pointing ... 1 : 00.

Que 1.23. **How can we prevent integer overflow attack.**

Answer

Integer overflow can be prevented by :

1. **Avoidance :**
   a. By allocating variables with data types that are large enough to ... contain all values that may possibly be computed and stored in ... them, it is always possible to avoid overflow.
   b. Static analysis tools and formal verification techniques can be used ... to ensure that overflow does not occur.

2. **Handling :**
   a. If it is anticipated that overflow may occur, then tests can be inserted into the program to detect when it happens and do other processing to mitigate it.
3. **Propagation :**
   a. If a value is too large to be stored it can be assigned a special value indicating that overflow has occurred.
   b. This is useful so that the problem can be checked for once at the end of a long calculation rather than after each step.
   c. This is often supported in floating point hardware called FPUs.

Que 1.24. **What do you understand by format string vulnerabilities ?**

Answer

1. Format string vulnerabilities are a class of bug that takes advantage of an easily avoidable programmer error.
2. If the programmer passes an attacker-controlled buffer as an argument to a printf (or any of the related functions, including sprintf, fprintf, etc), the attacker can perform writes to, operation arbitrarily.
3. Format string vulnerabilities arise when user-controllable input is passed as the format string parameter to a function that takes format specifiers that may be misused, as in printf family of functions in C.
4. These functions take a variable number of parameters, which may consist of different data types such as numbers and strings.
5. The format string passed to the function contains specifiers, which tell it what kind of data is contained in the variable parameters, and in what format it should be rendered.

Que 1.25. **How can we prevent format string vulnerabilities ?**

Answer

To prevent format string vulnerabilities :

1. Always specify a format string as part of program, not as an input.
2. Most format string vulnerabilities are solved by specifying "%s" as format string and not using the data string as format string.
3. If possible, make the format string a constant. Extract all the variable parts as other arguments to the call.
4. Difficult to do with some internationalization libraries.
5. Use defenses such as format guard, rare at design time.
6. Perhaps a way to keep using a legacy application and keep costs down.

7. Increase trust that a third-party application will be safe.

PART-4

Defense Against Control Hijacking-Platform Defense, Defense Against Control Hijacking-Run-Time Defense, Advanced Control Hijacking Attacks.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.26. How can we control hijacking attack ?

Answer

Hijacking attack is controlled through :

i. **Platform defense :** Through platform defense we can prevent target machine by using :

1. **Fixed the bug :**
   a. Audit software through automated tools.
   b. Rewrite software in a safe language.
   c. Concede overflow, but prevent code execution.
   d. Add run-time code to detect overflows exploits.
      i. Halt process when overflow exploit detected
      ii. Stackguard
2. **Marking memory as non-execute :**
   a. Prevent attack code execution by marking stack and heap as non-executable.

ii. **Run-time defense :**

1. In run-time defense, we tests for stack integrity.
2. We embed "canaries" in stack frames and verify their integrity prior to function return. There are two types of canaries :

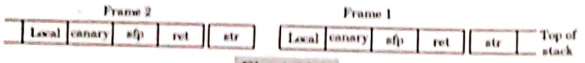

Fig. 1.26.1.

a. Random canary :

i. In random canary, random string is chosen at program startup.

ii. Insert canary string into every stack frame.
iii. Verify canary before returning from function :
   a. Exit program if canary changed.
   b. Turns potential exploit into DoS.
iv. To corrupt, attacker must learn current random string.

b. Terminator canary :

i. String functions will not copy beyond terminator.
ii. Attacker cannot use string functions to corrupt stack.

iii. Heap protection :

a. It protects function pointers and setjump buffers by encrypting them.
b. It has less effective and more noticeable performance effects.

Que 1.27. Explain heap spray attack with its techniques ?

Answer

a. Heap spraying is a technique used in exploits to facilitate arbitrary code execution.
b. In heap spray attack, we put number of copy of exploit(shell) code in various places of heaps.
c. It is reliable method for exploiting heap overflows as shown :

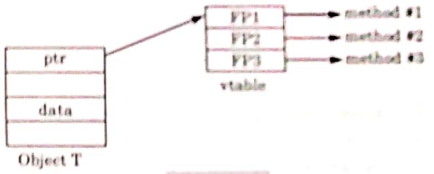

Fig. 1.27.1.

d. After overflow of buf (buffer).

Fig. 1.27.2.

e. Here, attacker does not know where browser places shell code on the heap.

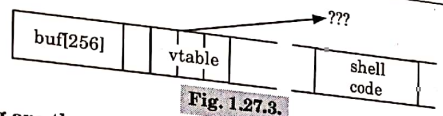

Fig. 1.27.3.

Following are the techniques used in heap spray attack :

1. **Heap spraying :**
   a. Use javascript to spray heap will shell code.
   b. Then point vtable ptr anywhere in spray area.
   c. Pointing func-ptr almost anywhere in heap will cause shell code to execute.
2. **Vulnerable buffer placement :**
   a. Placing vulnerable buf[256] next object O :
      i. By sequence of javascript allocations and frees make heap look as follows :

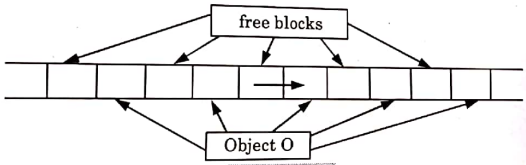

Fig. 1.27.4.

      ii. Allocate buffer in javascript and cause overflow.
      iii. Successfully used against a safari PCRE overflow.

Heap spray control hijacking can be prevented as :

1. Protect heap function pointers.
2. Better browser architecture :
   a. Store javascript strings in a separate heap from browser heap.
   b. Open BSD heap overflow protection.
   c. Detect sprays by prevalence of code of heap.

☺☺☺

2 UNIT

Confidentiality Policies

CONTENTS

PART-1

Confidentiality Policies, Confinement Principle.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.1. Define the term confidentiality policies. Explain confidentiality model.

Answer

i. A confidentiality policy is intended to protect secrets. Specifically, it is intended to prevent unauthorized disclosure of information.

ii. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

iii. One model of a confidentiality policy is the Bell-LaPadula (BLP) security model :

1. The Bell-LaPadula confidentiality model is a state machine-based multilevel security policy.
2. The model was originally designed for military applications.
3. State machine models define states with current permissions and current instances of subjects accessing the objects.
4. The security of the system is satisfied by the fact that the system transitions from one secure state to the other with no failures.
5. The model uses a layered classification scheme for subjects and a layered categorization scheme for objects.
6. The classification level of the objects and the access rights of the subjects determine which subject will have authorized access to which object. This layered structure forms a lattice for manipulating access.
7. The Bell-LaPadula confidentiality model is a static model, which assumes static states.
8. It implements Mandatory Access Control (MAC) and Discretionary Access Control (DAC).

Que 2.2. What are the issues related Bell-LaPadula model ?

Answer

Issues with Bell-LaPadula model :

1. The transfer of information from a high-sensitivity document to lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects.
2. Trusted subjects are not restricted by the property.
3. This model only addresses confidentiality, control of writing (one form of integrity).
4. Covert channels such as Trojan horses and requesting system resources to learn about other users that are mentioned but are not addressed comprehensively
5. The tranquility principle (The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced) limits its applicability to systems where security levels do not change dynamically.

Que 2.3. Explain Discretionary Access Control (DAC).

Answer

1. Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects.
2. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password.
3. In DAC, each system object has an owner, and each initial object owner is the subject that causes its creation.
4. DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

Que 2.4. Explain the issues related with DAC.

Answer

Issues related with DAC are :

1. Difficult to enforce a system-wide security policy *i.e.*, a user can leak classified documents to an unclassified users.
2. Only support course-grained privileges *i.e.*, CGA is the top-level authorization decision that is made at the perimeter of a system. This decision will be based upon the requested resource and action being tied to the user.
3. Unbounded privilege escalation.
4. Only based on users identity and ownership, ignoring security relevant information such as :

a. Users role
b. Function of the program
c. Trustworthiness of the program :
   i. Compromised program can change access to the user object.
   ii. Compromised program inherit all the permission granted to the user.
d. Sensitivity of the data
e. Integrity of the data

Que 2.5. Describe Mandatory Access Control (MAC).

Answer

1. Mandatory Access Control (MAC) is a type of access control by which the operating system constraints the ability of a subject to access or perform some sort of operation on an object.
2. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users.
3. Mandatory access control works by assigning a classification label to each file system object. Classifications include confidential, secret and top secret.
4. Each user and device on the system is assigned a similar classification and clearance level.
5. When a person or device tries to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted.
6. While it is the most secure access control setting available, MAC requires careful planning and continuous monitoring to keep all resource objects and users classifications up to date.
7. As the highest level of access control, MAC can be contrasted with lower-level Discretionary Access Control (DAC), which allows individual resource owners to make their own policies and assign security controls.

Que 2.6. What are the problems related with MAC ?

Answer

Following are the different problems in MAC :

1. **Requirement of new security levels :**
   a. In MAC, there is no security level for common people (people outside organization) where they can access certain data or information to know organization or business and hence marketing of organization or business is not possible in traditional MAC.

   b. Hence, an organization cannot reach apex heights in business by adopting MAC.
   c. Hence, an update is required to alter the security levels and include this functionality in proposed model which is an alternate to MAC.
2. **Filtration :**
   a. The security levels are assigned to both subjects and objects.
   b. These levels are assigned to values inside each attribute.
   c. The Bell-LaPadula model form the basis of MAC.
3. **Polyinstantization :**
   a. In polyinstantizition, multiple instances of a tuple are created.
   b. Consider the example, where user with security level confidential can view attributes which are at lower level or equal level as compared to this user.
   C. Other values are displayed as NULL. These values can be accesses and changed by this user by taking a key which is at lowest level in this relation and any attribute can be accessed using this key or value.

Que 2.7. What are the advantage and disadvantages of DAC and MAC ?

Answer

Advantages of Discretionary Access Control (DAC) :

a. Intuitive
b. Easy to implement

Disadvantages of Discretionary Access Control (DAC) :

a. Inherent vulnerability
b. Maintenance of ACL (Access Control List) of capability lists
c. Maintenance of Grant/Revoke.
d. Limited power of negative authorized.

Advantages of Mandatory Access Control (MAC) :

a. Ensure a high degree of protection, prevent any illegal flow of information.
b. Suitable for military and high security types of applications.

Disadvantages of Mandatory Access Control (MAC) :

a. Require strict classification of subjects and objects.
b. Applicable to few environments.

Que 2.8. Differentiate between DAC and MAC.

Answer

S.No.	DAC	MAC
1.	A type of access control in which the owner of a resource restricts access to the resource based on the identity of the users.	A type of access control that restricts the access to the resources based on the clearance of the subjects.
2.	Stands for discretionary access control.	Stands for mandatory access control.
3.	Access is determined by owner.	Access is determined by the system.
4.	More flexible.	Less flexible.
5	Not as secure as MAC.	More secure.

Que 2.9. Describe briefly confinement principle.

Answer

1. The confinement principle is the principle of preventing a server from leaking information that the user of the service considers confidential.
2. The confinement principle deals with preventing a process from taking disallowed actions.
3. Consider a client/server situation: the client sends a data request to the server; the server uses the data, performs some function, and sends the results (data) back to the client.
4. In this case the confinement principle deals with preventing a server from leaking information that the user of that service considers confidential.
5. In confinement principle, access control affects the function of the server in two ways :
   a. **Goal of service provider :** The server must ensure that the resources it accesses on behalf of the client include only those resources that the client is authorized to access.
   b. **Goal of the service user :** The server must ensure that it does not reveal the client's data to any other entity which is not authorized to see the client's data.

PART-2

Detour Unix User IDs Process IDs and Privileges, More on Confinement Techniques, System Call Interposition, Error 404 Digital Hacking in India Part 2 Chase.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.10. Describe detour used in Unix user ids and process ids.

Answer

1. Detour is defined as few words about Unix user IDs and IDs associated with Unix processes.
2. Every user in Unix like operating system is identified by different integer number, this unique number is called as UserID.
3. There are three types of UID defined for a process, which can be dynamically changed as per the privilege of task.
4. The three different types of UIDs defined are :
   a. **Real UserID :** It is account of owner of this process. It defines which files that this process has access to.
   b. **Effective UserID :** It is normally same as real UserID, but sometimes it is changed to enable a non-privileged user to access files that can only be accessed by root.
   c. **Saved UserID :** It is used when a process is running with elevated privileges (generally root) needs to do some under-privileged work, this can be achieved by temporarily switching to non-privileged account.
5. A subject is a program (application) executing on behalf of some principal(s). A principal may at any time be idle, or have one or more subjects executing on its behalf.
6. An object is anything on which a subject can perform operations (mediated by rights) usually objects are passive, for example :
   a. File
   b. Directory (or folder)
   c. Memory segment.
7. Each user account has a unique UID. The UID 0 means the super user (System admin). A user account belongs to multiple groups. Subject are processes, associated with uid/gid pairs.

8. There should be a one-to-many mapping from users to principals. A user may have many principals, but each principal is associated with a unique user. This ensures accountability of a user action.

Que 2.11. Explain basic permission bits on non-directories and directories files.

Answer

Basic permission bits on non-directories files :

1. Read controls reading the content of a file *i.e.*, the read system call.
2. Write controls changing the content of a file *i.e.*, the write system call.
3. Execute controls loading the file in memory and execute *i.e.*, the execute system call.

Permission bits on directories files :

1. Read bit allows to show file names in a directory.
2. The execution bit controls traversing a directory.
3. Write control and execution control creates or delete files in the directory.
4. Deleting a file under a directory requires no permission on the file
5. Accessing a file identified by a path name requires execution to all directories along the path.

Que 2.12. Define SUID, SGID and sticky bits with basic difference.

Answer

1. There are three special permission that are available for executable files and directories.
2. These permissions allow the file being executed to be executed with the privileges of the owner or the group. These are :
   a. **SUID permission :**
      i. SUID is set user identification. SUID is a special permission assigned to a file.
      ii. These permissions allow the file being executed to be executed with the privileges of the owner.
   b. **SGID permission :**
      i. SGID is set group identification.
      ii. When the Set Group ID bit is set, the executable is run with the authority of the group.
   c. **Sticky bit :**
      i. When the sticky bit is set on a directory, only the root user, the owner of the directory, and the owner of a file can remove files within said directory.

Difference :

Basic	SUID	SGID	Sticky bit
Non-executable files	no effect	affect locking (unimportant for us)	not used anymore
Executable files	change euid when executing the file	change egid when executing the file	not used anymore
Directories	no effect	new files inherit group of the directory	only the owner of a file can delete

Que 2.13. Discuss confinement techniques in details.

Answer

Following are the various confinement techniques :

1. **Chroot (change root) :**
   a. A chroot on Unix operating systems is an operation that changes the apparent root directory for the current running process and its children.
   b. The programs that run in this modified environment cannot access the files outside the designated directory tree. This essentially limits their access to a directory tree and thus they get the name chroot jail.
   c. The idea is that we create a directory tree where we copy or link in all the system files needed for a process to run.
   d. We then use the chroot system call to change the root directory to be at the base of this new tree and start the process running in that chrooted environment.
   e. Since it cannot actually reference paths outside the modified root, it cannot maliciously read or write to those locations.
2. **Jailkits :**
   a. Jailkit is a set of utilities to limit user accounts to specific files using chroot() and or specific commands.
   b. Setting up a chroot shell, a shell is limited to some specific command and can be automated using these utilities.
   c. Jailkit is a specialized tool that is developed with a focus on security.
   d. It will abort in a secure way if the configuration is not secure, and it will send useful log messages that explain what is wrong to system log.

e. Jailkit is known to be used in network security appliances from several leading IT security firms.

3. **FreeBSD jail :**
   a. FreeBSD is a popular free and open source operating system that is based on the Berkeley Software Distribution (BSD) version of the Unix operating system.
   b. It runs on processors such as the Pentium that are compatible with Intel's x86.
   c. FreeBSD is an alternative to Linux that will run Linux applications.
   d. The jail mechanism is an implementation of FreeBSD's OS-level virtualisation that allows system administrators to partition a FreeBSD-derived computer system into several independent mini-systems called jails, all sharing the same kernel, with very little overhead.
   e. The need for the FreeBSD jails came from a small shared-environment hosting provider's desire to establish a clean, clear-cut separation between their own services and those of their customers, mainly for security and ease of administration.

4. **System call interposition :**
   a. System call interposition is a powerful technique for regulating and monitoring program behaviours.
   b. It gives security systems the ability to monitor all of the application's interaction with network, file system and other sensitive system resources.
   c. This approach brings with it a host of pitfalls for the unwary implementer that if overlook can allow his tool to be easily circumvented.

Que 2.14. **Explain error 404 digital hacking in India part 2 chase.**

Answer

1. In error 404 digital hacking in India part 2 chase experts discuss about some attack related to cyber attack and the attacker can control the overall system if proper security is not provided to the system.
2. Some attacks discuss in error 404 digital hacking India part 2 chase are :
   a. Israel's power grid hit by a big hack attack. It is being called one of the worst cyber attack ever.
   b. In 2014 a hydropower plant in upstate New York got hacked.
   c. Iran's infrastructure including its main nuclear power plant is being targeted by a new and dangerous powerful cyber worm.
   d. Bangladesh best group hacked into nearly 20000 Indian website including the Indian Border Security Force.

   e. First virus that could crash power grid or destroy pipeline is available online for anyone to download and tinker with.
   f. India's biggest data breach when the SBI debit card branch happens. When this happened bank where initially in a state of denial but subsequently they had to own up cyber security breach that took place in Indian history.

PART-3

VM Based Isolation, Confinement Principle, Software Fault Isolation, Rootkits, Intrusion Detection Systems.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.15. **What do you understand by VM based isolation ?**

Answer

1. Virtualization technology allows the sharing of the same physical resources among several users.
2. This enables the consolidation of servers and a multitude of user machines into a very small set of physical servers, by replacing the physical machines with virtual machines, running on the same physical servers.
3. Temporal isolation or performance isolation among virtual machine (VMs) refers to the capability of isolating the temporal behaviour (or limiting the temporal interferences) of multiple VMs among each other, despite them running on the same physical host and sharing a set of physical resources such as processors, memory, and disks.
4. Virtual Machines are software abstractions of real machines. They provide a virtual platform for running tasks.
5. Virtual machines have been employed to provide various features like emulation, optimization, translation, isolation, replication etc.
6. A virtual machine can support individual processes or a complete system depending on the abstraction level where virtualization occurs.
7. Some VMs support flexible hardware usage and software isolation, while others translate from one instruction set to another.

Que 2.16. **Explain confinement principles with its techniques.**

Answer

Confinement principle : Refer Q. 2.9, Page 2–6W, Unit-2.
Confinement principles techniques : Refer Q. 2.13, Page 2–9W, Unit-2.

Que 2.17. Describe the types of VM based isolation.

Answer

Following are the types of Virtual Machine based isolation :

a. Process virtual machines :

1. Process virtual machines support individual processes or a group of processes and enforce isolation between the processes and operating system environment.
2. Process virtual machines can run processes compiled for the same Instruction Set Architecture based (ISA) or for a different ISA as long as the virtual machine runtime supports the translation.
3. Isolation policies are provided by a runtime component which runs the processes under its control.
4. Isolation is guaranteed because the virtual machine runtime does not allow direct access to the resources.

b. System virtual machines (Hypervisor virtual machines) :

1. System virtual machines provide a full replica of the underlying platform and thus enable complete operating systems to be run within it.
2. The virtual machine monitor (also called the hypervisor) runs at the highest privilege level and divides the platforms hardware resources amongst multiple replicated guest systems.
3. All accesses by the guest systems to the underlying hardware resources are then mediated by the virtual machine monitor.
4. This mediation provides the necessary isolation between the virtual machines.
5. System virtual machines can be implemented in a pure-isolation mode in which the virtual systems do not share any resources between themselves or in a sharing-mode in which the VM Monitor multiplexes resources between the machines.
6. Pure-isolation mode virtual machines are as good as separate physical machines.

c. Hosted virtual machines :

1. Hosted Virtual Machines are built on top of an existing operating system called the host.
2. The virtualization layer sits above the regular operating system and makes the virtual machine look like an application process.

3. We then install complete operating systems called guest operating systems within the host virtual machines.
4. The VM can provide the same instruction set architecture as the host platform or it may also support a completely different Instruction Set Architecture (ISA), like running Windows IA-32 OS on a Mac running on the PowerPC platform.
5. VMware GSX Server is an example where the host ISA and guest ISA are same.
6. Isolation in hosted virtual machines is as good as the isolation provided by the hypervisor approach except that the virtual machine monitor in the case of the hosted VM does not run at the highest privilege.
7. The processes running inside the virtual machine cannot affect the operation of processes outside the virtual machine.
8. System emulators are also loosely classified under hosted virtual machines.

d. Hardware virtual machines :

1. Hardware virtual machines are virtual machines built using virtualization primitives provided by the hardware like processor or I/O.
2. The advantage of hardware level virtualization is tremendous performance improvements over the software based approaches and guarantees better isolation between machines.
3. The isolation provided by the hardware assisted virtualization is more secure than that provided by its software counterpart for obvious reasons.

Que 2.18. Discuss briefly the term rootkit.

Answer

1. A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence.
2. Rootkit is a collection of tools that enabled administrator-level access to a computer or network.
3. Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool.
4. Rootkits are generally associated with malware such as Trojans, worms, viruses that conceal their existence and actions from users and other system processes.
5. A rootkit allows us to maintain command and control over a computer without the computer user/owner knowing about it.

6. Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine.
7. A rootkit on an infected computer can also access log files and spy on the legitimate computer owner's usage.
8. Rootkits can be detected using detection methods which include :
   a. Behavioural-based methods
   b. Signature scanning
   c. Memory dump analysis

Que 2.19. **Explain the purpose of rootkit. What are the examples of rootkits ?**

Answer

Purpose of rootkits :

1. The purpose of a rootkit is for a malware to give its owner, a (often) permanent, hidden remote access to our computer.
2. To avoid detection, they tamper with the system to conceal the presence of the malware (for example, hide files) and its activities (for example, running processes).

Examples of rootkits :

1. **NTRootkit :** One of the first malicious rootkits targeted at Windows OS.
2. **HackerDefender :** This early Trojan altered/augmented the OS at a very low level of functions calls.
3. **Machiavelli :** The first rootkit targeting Mac OS X. This rootkit creates hidden system calls and kernel threads.
4. **Greek wiretapping :** This rootkit targeted Ericsson's AXE PBX.

Que 2.20. **Explain various types of rootkits.**

Answer

Types of rootkits :

1. **Hardware or firmware rootkit :**
   a. This type of malware could infect our computer's hard drive or its system BIOS.
   b. It can even infect our router. Hackers can use these rootkits to intercept data written on the disk.
2. **Bootloader rootkit :**
   a. It loads our computer's operating system when we turn the machine on.

   b. A bootloader toolkit, then, attacks our system, replacing our computer's legitimate bootloader with a hacked one.
   c. This means that this rootkit is activated even before our computer's operating system turns on.
3. **Memory rootkit :**
   a. This type of rootkit hides in our computer's RAM (Random Access Memory).
   b. These rootkits will carry out harmful activities in the background.
   c. These rootkits have a short lifespan.
   d. They only live in our computer's RAM and will disappear once we reboot our system.
4. **Application rootkit :**
   a. Application rootkits replace standard files in our computer with rootkit files.
   b. They might also change the way standard applications work.
   c. These rootkits might infect programs such as Word, Paint, or Notepad.
   d. Every time we run these programs, we will give hackers access to our computer.
   e. The challenge here is that the infected programs will still run normally, making it difficult for users to detect the rootkit.
5. **Kernel mode rootkits :**
   a. These rootkits target the core of our computer's operating system.
   b. Cybercriminals can use these to change how our operating system functions. They just need to add their own code to it.
   c. This can give them easy access to our computer and make it easy for them to steal our personal information.

Que 2.21. **How can we prevent rootkits ?**

Answer

Following are the method to prevent rootkits :

1. **Avoid opening suspicious emails :**
   a. Statistics shows that malware, including rootkits, are distributed through emails.
   b. This means that the chances of getting infected with a rootkit via email are high.

c. Using another type of malware, hackers collect email addresses on the internet, which they flood with spam emails.

d. The rootkit installs silently in the background when the user opens the infected email.

e. To prevent rootkits from infiltrating our computer, avoid opening suspicious emails, especially if the sender is unfamiliar to us.

2. **Avoid downloading cracked software :**

a. Cracked software may be free but it is also unsafe.

b. Cracked software is commonly used by hackers to install rootkits on victims' computers.

c. Cracked software is sometimes bundled with Adware (a software), which generates stubborn and annoying pop-ups on the computer.

d. To prevent rootkits and other types of malware, download legitimate software only.

3. **Install software updates :**

a. Through system vulnerabilities, a rootkit can get through to our computer.

b. System vulnerabilities are inevitable. In fact, programmers are often only able to discover a bug after the software is released. The solution is a software update.

c. Unfortunately, some users ignore the importance of software updates. But the fact is that installing software updates enhances our cyber security, preventing malware like rootkits from getting onto our computer.

d. When software updates become available, donot delay their installation.

4. **Anti-malware software with rootkit detection :**

a. Anti-malware software prevents varieties of malware. But advanced anti-malware software with rootkit detection is required to stop rootkits from getting on the computer.

b. Anti-malware software equipped with a Host Intrusion Prevention System as a feature is specifically designed to monitor computer memory.

c. It prevents any malicious software from loading on the kernel of the operating system, which prevent rootkits using anti-malware software.

Que 2.22. **What is Intrusion Detection System (IDS) ?**

Answer

1. An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.
2. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies.
3. An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information.
4. IDS solutions will often take advantage of a SPAN (Switched Port Analyzer) port to analyze a copy of the inline traffic stream
5. The IDS monitors traffic and report its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system.
6. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device.

Que 2.23. **Explain the types of intrusion detection system.**

Answer

Following are the types of intrusion detection system :

1. **Network Intrusion Detection System (NIDS) :**

a. It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts.

b. It gains access to network traffic by connecting to a network hub, a network switch configured for port mirroring, or a network tap.

c. In a NIDS, sensors are placed at choke points in the network to monitor, often in the Demilitarized Zone (DMZ) or at network borders.

d. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic.

e. An example of a NIDS is Snort.

2. **Host-based Intrusion Detection System (HIDS) :**
   a. It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state.
   b. In a HIDS, sensors usually consist of a software agent.
   c. Intrusion detection systems can also be system-specific using custom tools and honeypots.
   d. In the case of physical building security, IDS is defined as an alarm system designed to detect unauthorized entry.
   e. An example of a HIDS is OSSEC (Open source HIDS Security).
3. **Perimeter Intrusion Detection System (PIDS) :**
   a. Detects and pinpoints the location of intrusion attempts on perimeter fences of critical infrastructures.
   b. Using either electronics or more advanced fiber optic cable technology fitted to the perimeter fence, the PIDS detects disturbances on the fence, and if an intrusion is detected and deemed by the system as an intrusion attempt, an alarm is triggered.
4. **VM based Intrusion Detection System (VMIDS) :**
   a. It detects intrusions using virtual machine monitoring.
   b. By using this, we can deploy the Intrusion Detection System with Virtual Machine Monitoring.
   c. It is the most recent type and it is still under development.
   d. There is no need for a separate intrusion detection system since by using this, we can monitor the overall activities.

Que 2.24. **Discuss the need of intrusion detection system.**

Answer

1. A network intrusion detection system (NIDS) is crucial for network security because it enables us to detect and respond to malicious traffic.
2. The primary purpose of an intrusion detection system is to ensure IT personnel is notified when an attack or network intrusion might be taking place.
3. A network intrusion detection system (NIDS) monitors both inbound and outbound traffic on the network, as well as data traversing between systems within the network.

4. The network IDS monitor network traffic and triggers alerts when suspicious activity or known threats are detected, so IT personnel can examine more closely and take the appropriate steps to block or stop an attack.

Que 2.25. **Explain advantages and disadvantages of different types of IDS.**

Answer

Advantages of HIDS :

1. HIDS can analyze encrypted data and communications activity.
2. HIDS tells us if an attack is successful or no.
3. Easy to deploy because it does require additional hardware.
4. It does not affect the current architecture.

Disadvantages of HIDS :

1. HIDS breakdown if the OS break down by the attack.
2. HIDS are not able to detect network scans or DOS attack.
3. HIDS tend to be resource intensive.

Advantages of NIDS :

1. Operating environment independent, therefore NIDS will not affect the performances of host.

Disadvantages of NIDS :

1. Does not indicate whether the attack was successful or not.
2. Cannot analyze encrypted traffic.
3. NIDS has very limited visibility inside the host machine

Advantages of VMIDS :

1. More flexible
2. More efficient
3. VMIDS take advantage of the strengths of the combined type.

Disadvantages of VMIDS :

1. High overhead load on the monitored system depending on the combined methodologies.
2. Processor utilization of the hybrid agent is much great.

Advantages of PIDS :

1. More accurate.

2. It can manage wireless protocol activity.

Disadvantages of PIDS :

1. Sensors have limited computational resource and limited energy.

Que 2.26. What are the features of intrusion detection system ?

Answer

Features of an intrusion detection system are :

1. It monitors and analyzes the user and system activities.
2. It performs auditing of the system files and other configurations and the operating system.
3. It assesses the integrity of system and data files.
4. It conducts analysis of patterns based on known attacks.
5. It detects errors in system configuration.
6. It detects and cautions if the system is in danger.

Que 2.27. What are the components of IDS ?

Answer

Components of intrusion detection system are :

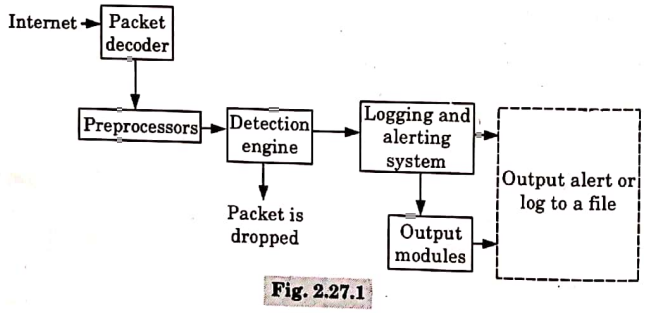

Fig. 2.27.1

1. **A packet decoder :** It takes packets from different networks and prepares them for preprocessing or any further action. It basically decodes the coming network packets.

2. **A preprocessor :** It prepares and modifies the data packets and also performs defragmentation of data packets, decodes the TCP streams.
3. **A detection engine :** It performs the packet detection on basis of Snort rules. If any packet matches the rules, appropriate action is taken, else it is dropped.
4. **Logging and alerting system :** The detected packet is either logged in system files or incase of threats, the system is alerted.
5. **Output modules :** They control the type of output from the logging and alert system.

☺☺☺

3 UNIT

Secure Architecture Principles Isolation and Leas

CONTENTS

PART- 1

Assess Control Concepts, Unix and Windows Access Control Summary, Other Issues in Access Control.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.1. Explain briefly the term access control.

Answer

1. Access control is a method of limiting access to a system, physical or virtual resources.
2. It is a process by which users can access and are granted certain prerogative to systems, resources or information.
3. Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment.
4. It is a fundamental concept in security that reduces risk to the business or organization.
5. Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors.
6. There is multi-factor authentication which requires two or more authentication factors which is an important part of the layered defense to protect access control systems.

Que 3.2. Describe different models of access control.

Answer

Different access control models are :

1. **Attribute-based Access Control (ABAC) :** In this model, access is granted or declined by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.
2. **Discretionary Access Control (DAC) :** In DAC the owner of data determines who can access specific resources.
3. **History-Based Access Control (HBAC) :** In this model, access is granted or declined by evaluating the history of activities of the inquiring

party that includes behaviour, the time between requests and content of requests.

4. **Identity-Based Access Control (IBAC) :** By using this model, network administrators can more effectively manage activity and access, based on individual requirements.
5. **Mandatory Access Control (MAC) :** A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.
6. **Organization-Based Access control (OrBAC) :** This model allows the policy designer to define a security policy independently of the implementation.
7. **Role-Based Access Control (RBAC) :** RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.
8. **Rule-Based Access Control (RAC) :** RAC method is largely context based. For example, this would be only allowing students to use the labs during a certain time of day.

Que 3.3. Discuss implementation of access control.

Answer

Implementation of access control :

1. **Administrative access control :**
   a. Administrative access control sets the access control policies and procedures for the whole organization, defines the implementation requirements of both physical and technical access control, and what the consequences of non-compliance will be.
   b. Examples are supervisory structure, staff and contractor controls, information classification, training, auditing, and testing.
2. **Physical access control :**
   a. Physical access control is critical to an organizations security and applies to the access or restriction of access to a place such as property, building or room.
   b. Examples are fences, gates, doors, turnstiles, etc., using locks, badges, bio-metrics (facial recognition, fingerprints), video surveillance cameras, security guards, motion detectors, mantrap doors, etc., to allow access to certain areas.
3. **Technical or logical access control :**
   a. Technical or logical access control limits connections to computer networks, system files, and data.

   b. It enforces restrictions on applications, protocols, operating systems, encryptions mechanisms, etc.
   c. Examples are access control lists, intrusion detection systems, and antivirus software.

Que 3.4. Briefly explain the uses of access control system.

Answer

1. Access control system is used to control access into certain areas located within the interior of buildings.
2. The purpose of an access control system is to provide quick, convenient access to those persons who are authorized, while at the same time, restricting access to unauthorized people.
3. Access control is used to minimize the risk of unauthorized access to physical and logical systems.
4. Access control is a fundamental component of security compliance programs that ensures security technology.
5. Access control policies are in place to protect confidential information, such as customer data.
6. Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services.
7. After high-profile breaches, technology vendors have shifted away from single sign-on systems to unified access management, which offers access controls for on-premises and cloud environments.

Que 3.5. What are the components of access control system ?

Answer

Basics components of access control system are :

1. **Access cards :**
   i. The access card may be thought of as an electronic key.
   ii. The access card is used by persons to gain access through the doors secured by the access control system.
   iii. Each access card is uniquely encoded. Most access cards are approximately the same size as a standard credit card, and can easily be carried in a wallet or purse.
2. **Card readers :**
   i. Card readers are the devices used to electronically read the access card.
   ii. Card readers may be of the insertion type (which requires insertion of the card into the reader).

iii. Card readers are usually mounted on the exterior (non-secured) side of the door that they control.

3. **Access control keypads :**
   i. Access control keypads are devices which may be used in addition to or in place of card readers.
   ii. The access control keypad has numeric keys which look similar to the keys on a touch-tone telephone.
   iii. The access control keypad requires that a person desiring to gain access must enter a correct numeric code.
   iv. When access control keypads are used in addition to card readers, both a valid card and the correct code must presented before entry is allowed.
   v. Where access control keypads are used in place of card readers, only a correct code is required to gain entry.
4. **Electric lock hardware :**
   i. Electric lock hardware is the equipment that is used to electrically lock and unlock each door that is controlled by the access control system.
   ii. The specific type and arrangement of hardware to be used on each door is determined based on the construction conditions at the door.
   iii. In almost all cases, the electric lock hardware is designed to control entrance into a building or secured space. To comply with building and fire codes, the electric lock hardware never restricts the ability to freely exit the building at any time.
5. **Access control field panels :**
   i. Access control field panels (also known as Intelligent Controllers) are installed in each building where access control is to be provided.
   ii. Card readers, electric lock hardware, and other access control devices are all connected to the access control field panels.
   iii. The access control field panels are used to process access control activity at the building level.
   iv. The number of access control field panels to be provided in each building depends on the number of doors to be controlled.
   v. Access control field panels are usually installed in telephone, electrical, or communications closets.
6. **Access control server computer :**
   i. The access control server computer is the brain of the access control system.
   ii. The access control server computer serves as the central database and file manager for the access control system and is responsible for recording system activity, and distributing information to and from the access control field panels.

   iii. A single access control server computer is used to control a large number of card-reader controlled doors.
   iv. The access control server computer is usually a standard computer which runs special access control system application software.
   v. In most cases, the computer is dedicated for full-time use with the access control system.

Que 3.6. Discuss access control principle and security principle used for access control.

Answer

Access control principles :

1. **Principle of least privilege :** It states that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource *i.e.*, default no access.
2. **Separation of duties :** Separating any conflicting areas of responsibility so as to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets and/or information.
3. **Need to know :** It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their duties.

Security principles used for access control :

1. **Identification :** Identification describes a method of ensuring that a subject is the entity it claims to be. For example, a user name or an account number.
2. **Authentication :** Authentication is the method of proving the subjects identity. For example, password, passphrase, PIN.
3. **Authorization :** Authorization is the method of controlling the access of objects by the subject. For example, a user cannot delete a particular file after logging into the system.
4. **Non-repudiation :** Non-repudiation is the assurance that someone cannot deny something. Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Que 3.7. What are the characteristics and features of Unix ?

Answer

Characteristics of Unix :

1. **Memory allocation :** It keeps tracks of primary memory *i.e.*, which part of it is in use or not and by whom, as well as it allocates memory when a program requests.

2. **Processor management :** It allocates the CPU for a process or deallocates if not required.
3. **Device management :** It keeps tracks of all devices it decides for how much time and to whom should be given the priority.
4. **File management :** It allocates and deallocates the resources, it also decides to whom should the resources be given.
5. **Security :** By means of password and some other techniques, preventing unauthorized access to program and data.

Features of Unix :

1. **Portable :** Unix can be installed on many hardware platforms.
2. **Multi-user :** The Unix users allow multiple users to concurrently share hardware and software.
3. **Multi-tasking :** Unix allows a user to run more than one program at a time. In fact more than one program are running at the background while user is working on the foreground.
4. **Networking :** While Unix was developed to an interactive, multi-user, multi-tasking system, networking is incorporated in the heart of the operating system.
5. **Organized file system :** Unix has organized file and directory system that allows users to organize and maintain files.
6. **Device independence :** Unix treats input output devices as ordinary files. The destination of file input and output is easily controlled through Unix design feature called redirection.
7. **Utilities :** Unix provides a rich library of utilities that can increase user's productivity.

Que 3.8. Differentiate between Unix and Windows.

Answer

S. No.	Unix	Windows
1.	It is an open source.	It is a close source.
2.	It has very high security system.	It has low security system.
3.	It is a command based operating system.	It is a not command based operating system.
4.	The file system is arranged in hierarchical manner.	The file system is arranged in a parallel manner.
5.	Unix is not user friendly.	It is user friendly.

Que 3.9. What are the various issues in access control ?

Answer

Issues related to access control are :

1. **Appropriate role-based access :**
   i. Users should only be given access to systems that they need to access, and at a level that's appropriate to their role.
   ii. Good practice is to ensure that access privileges (and changes) are approved by a sufficiently senior director or manager.
   iii. Finally, access privileges should be reviewed regularly and amended as part of a process of security governance.
2. **Poor password management :**
   i. Password management is most common mistakes when it comes to access control.
   ii. When there are a lot of different systems that require a password to access then it is not uncommon for employees and even business owners to use the same password across the board.
   iii. Even when employees are required to change their password regularly though, there is still the problem of using passwords that are weak and easy to crack.
   iv. It is logical why people would do this since remembering multiple passwords can often be impractical.
3. **Poor user education :**
   a. One of the most important aspects of improving the security of company data is educating employees about risk.
   b. Employees could easily be doing things that are putting our data at risk.
   c. Human error is always one of the biggest security risks for company so we should be aware of this and take steps we can educate our employees, including risk-training programs.

PART-2

Introduction to Browser Isolation.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.10. **Describe browser isolation.**

Answer

1. Browser isolation is a cyber security model for web browsing that can be used to physically separate an internet user's browsing activity from their local machine, network and infrastructure.
2. With this model, individual browser sessions are abstracted away from hardware and direct internet access, trapping harmful activity inside the disposable environment.
3. Browser isolation may also be referred to as remote browser isolation, web isolation or remote browsing.
4. A major weakness in popular security tools is protection from web or browser-based attacks, malware and ransomware.
5. By separating browsing activity from endpoint hardware, the device's attack surface is reduced, sensitive data is protected and malware or other known and unknown security threats are minimized.
6. This is an evolution of the cyber security concepts of security through physical isolation and air-gapping.

Que 3.11. **Explain working of browser isolation.**

Answer

1. Browser isolation works by providing users with a disposable, non-persistent environment for browsing.
2. This can be executed through a variety of methods but involves virtualization, containerization or cloud browsing.
3. When a user closes the browsing session or the session is timed out, the isolated environment is reset or discarded.
4. Any malicious code or harmful traffic is discarded as well, preventing it from ever reaching the endpoint device or network.
5. The browser isolation method treats all websites, files and content equally by labelling them as untrusted or blacklisted unless otherwise specified.
6. Within the isolated environment, files can be rendered remotely or sanitized without the need to download them.
7. This is different from other security methods that do not treat information equally and filter content based on potential threatening signs.

Que 3.12. **Define browser isolation technology. What are browser isolation vendors ?**

Answer

Browser isolation technology : Browser isolation technology is a technology delivered to customers through a cloud browser, a container, a virtual machine or browser isolation technology hosted on a server.

Following are the browser isolation vendors :

i. Apozy
ii. Authentic
iii. Ericom
iv. Menlo security
v. Symantec
vi. WEBGAP

Que 3.13. **What are the advantages and disadvantages of browser isolation ?**

Answer

Advantages of browser isolation :

1. The primary benefit to browser isolation is reducing the spread of malware through web browsers.
2. It is more effective than other anti-virus application methods since it does not need to be programmed to find specific threats or risks.

Disadvantages of browser isolation :

1. The installation of browser isolation can be complex or expensive.
2. Browser isolation may cause users to experience slight delay or lag times when browsing.

PART-3

Web Security Definitions Goals and Threat Models, HTTP Content Rendering, Browser Isolation.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.14. **Define web security with its goals.**

Answer

1. Web security is the process of securing confidential data stored online from unauthorized access and modification.
2. This is accomplished by enforcing strict policy measures.
3. Websites are scanned for any possible vulnerabilities and malware through website security software. This software can scan for backdoor hacks, redirect hacks, Trojans, and many other threats.
4. A website security software notifies the user if the website has any issue and provides solutions to address them.
5. It is the cumulative phrase for all of the methods and measure that we can use and enforce to keep the files behind our website and any data of our customers safe.
6. Security should be built into our website from beginning, but certain systems, the likes of WordPress, allow us to easily install security measures at any time at little or no cost.
7. The goal of web security is to identify the following :
   i. Critical assets of the organization
   ii. Genuine users who may access the data
   iii. Level of access provided to each user
   iv. Various vulnerabilities that may exist in the application
   v. Data criticality and risk analysis on data exposure.
   vi. Appropriate remediation measures.

Que 3.15. Explain threat modelling. What is its purpose ?

Answer

1. Threat modelling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining counter measures to prevent, or mitigate the effects of threats to the system.
2. In this context, a threat is a potential or actual adverse event that may be malicious (such as a denial-of-service attack) or incidental (such as the failure of a storage device), and that can compromise the assets of an enterprise.
3. The key to threat modelling is to determine where the most effort should be applied to keep a system secure.
4. Threat modelling is an iterative process that consists of defining enterprise assets, identifying what each application does with respect to these assets, creating a security profile for each application, identifying potential threats, prioritizing potential threats, and documenting adverse events and the actions taken in each case.

5. Threat modelling is a structured approach to identifying, quantifying, and addressing threats.
6. It allows system security staff to communicate the potential damage of security flaws and prioritize remediation efforts.

Purpose of threat modelling :

1. The purpose of threat modelling is to identify, communicate, and understand threats and mitigation to the organisation's stakeholder's as early as possible.
2. Documentation from this process provides system analyst and defenders with a complete analysis of probable attacker profile.

Que 3.16. Discuss threat modelling methodologies.

Answer

Following are the threat modelling methodologies :

1. **STRIDE :** STRIDE is a methodology that provides a mnemonic for security threats in six categories :
   a. **Spoofing :** An adversary posing as another user, component, or other system that has an identity in the system being modelled.
   b. **Tampering :** The modification of data within the system to achieve a malicious goal.
   c. **Repudiation :** The ability of an adversary to deny performing some malicious activity in absence of sufficient proof.
   d. **Information disclosure :** The exposure of protected data to a user that is not otherwise allowed access to that data.
   e. **Denial of service :** It is an attack where the attackers attempt to prevent legitimate users from accessing the service.
2. **DREAD :** DREAD was proposed for threat modelling but due to inconsistent ratings it was dropped by Microsoft in 2008. It is currently used by open stack and many other corporations. It provides a mnemonic for risk rating security threats using five categories :
   a. **Damage potential :** Ranks the extent of damage that would occur if vulnerability is exploited.
   b. **Reproducibility :** Ranks how easy it is to reproduce attack.
   c. **Exploitability :** Assigns a number to the effort required to launch the attack.
   d. **Affected users :** A value characterizing how many people will be impacted if an exploit become widely available.
   e. **Discoverability :** Measures the likelihood how easy it is to discover the threat.

3. **PASTA :**
   i. The Process for Attack Simulation and Threat Analysis (PASTA) is risk-centric methodology.
   ii. The purpose is to provide a dynamic threat identification, enumeration, and scoring process.
   iii. Upon completion of threat model security, subject matter experts develop a detailed analysis of the identified threats.
   iv. Finally, appropriate security controls can be enumerated. This helps developer to develop a asset-centric mitigation strategy by analyzing attacker-centric view of application.
4. **Trike :**
   i. The focus is in using threat models as risk management tool.
   ii. Threat models are based on requirement model.
   iii. The requirements model establishes the stakeholder-defined acceptable level of risk assigned to each asset class.
   iv. Analysis of the requirements model yields a threat model from which threats are identified and assigned risk values.
   v. The completed threat model is used to build a risk model on the basis of asset, roles, actions, and calculated risk exposure.
5. **VAST :**
   i. VAST is an acronym for Visual, Agile, and Simple Threat modelling.
   ii. This methodology provides actionable outputs for the unique needs of various stakeholders like application architects and developers, cyber security personnel etc.
   iii. It provides a unique application and infrastructure visualisation scheme such that the creation and use of threat models do not require specific security subject matter expertise.
6. **Attack tree :**
   i. Attack trees are the conceptual diagram showing how an asset, or target, might be attacked.
   ii. These are multi-level diagram consisting of one root node, leaves and children nodes.
   iii. Bottom to top, child nodes are conditions which must be satisfied to make the direct parent node true.
   iv. An attack in considered complete when the root is satisfied. Each node may be satisfied only by its direct child nodes.
7. **Common Vulnerability Scoring System (CVSS) :**
   i. It provides a way to capture the principal characteristics of vulnerability and produce a numerical score depicting its severity.

   ii. The score can then be translated into a qualitative representation to help organizations properly assess and prioritize their vulnerability management processes.
8. **T-MAP :**
   i. T-MAP is an approach which is used in Commercial Off The Shelf (COTS) systems to calculate the weights of attack paths.
   ii. This model is developed by using UML class diagrams, access class diagrams, vulnerability class diagrams, target asset class diagrams and affected value class diagrams.

Que 3.17. Explain tools used for threats modelling.

Answer

Tools used for threat modelling :

1. **Microsoft's threat modelling tool :** This tool identifies threats based on STRIDE threat classification scheme and it is based on Data Flow Diagram (DFD).
2. **My App security :**
   a. It offers the first commercially available threat modeling tool *i.e.*, Threat Modeler.
   b. It uses VAST threat classification scheme and it is based on Process Flow Diagram (PFD).
3. **IriuRisk :**
   a. It offers both a community and a commercial version of the tool.
   b. This tool is primarily used to create and maintain live threat model through the entire SDLC.
   c. It connects with other several different tools like OWASP ZAP, BDD-Security etc., to facilitate automation and involves fully customizable questionnaires and risk pattern libraries.
4. **securiCAD :**
   a. It is a threat modelling and risk management tool.
   b. Risk are identified and quantified by conducting automated attack simulations to current and future IT architectures, and provides decision support based on the findings.
   c. SecuriCAD is offered in both commercial and community editions.
5. **SD elements by security compass :** It is a software security requirements management platform that includes automated threat modelling capabilities.
6. **Modelling attack trees :** Commercial tools like SecurITree, AttackTree+ and open source tools like ADTool, SeaMonster are used to model attack trees.

7. **Tiramisu :**
   a. This tool is used for T-MAP approach.
   b. It is used to calculate a list of all attack paths and produce overall threats in terms of total weight of attack paths.

Que 3.18. How to create a threat model ?

Answer

All threat modelling process start with creating visual representation of application or system being analyzed. There are two ways to create visual representation :

a. Visual representation using data flow diagram :

1. The Microsoft methodology, PASTA and Trike each develop a visual representation of the application-infrastructure utilizing data flow diagrams (DFD).
2. DFDs are used to provide a high-level visualization of how an application works within a system to move, store, and manipulate data.
3. The concept of trust boundaries was added by security professionals in an attempt to make them applicable for threat modelling.
4. DFDs are used to identify broad categories usually using STRIDE threat classification scheme.
5. The list of threats identifies through such methods is limited and thus a poor starting point for the modelling.
6. DFD based approach uses three main steps :
   i. View system as an adversary
   ii. Characterize the system
   iii. Determine the threats
7. DFD based approach has certain weakness :
   i. DFD does not accurately represent design and flow of application.
   ii. They analyse how data is flowing rather than how user interacts with system.
   iii. DFD based threat modelling has no standard approach due to which different people create threat models with different output for the same scenario or problem.

b. Visual representation using process flow diagram :

1. To deal with the limitations of DFD based threat modelling Process Flow Diagrams were introduced as a tool to allow Agile software development teams to create threat models based on the application design process.

2. These were designed to illustrate how attacker thinks.
3. Attacker does not analyze data flow. Rather, they try to figure out how they can move through application which was not supported in DFD based threat modelling.
4. Their analysis lays emphasis on how to abuse ordinary use cases to access assets or other targeted goals.
5. Threat models based on PFD view application from the perspective of user interactions.
6. Following are the steps for PFD based threat modelling :
   i. Designing application's use cases.
   ii. The communication protocols by which individuals move between use cases are defined.
   iii. Including the various technical controls such as a forms, cookies etc.
7. PFD based threat modelling has following advantages :
   i. PFD based threat models are easy to understand that do not require any security expertise.
   ii. Creation of process map-showing how individuals move through an application. Thus, it is easy to understand application from attacker's point of view.

Que 3.19. What is rendering ? Discuss rendering engine. List some rendering engine in web browser.

Answer

i. Rendering or image synthesis is the automatic process of generating a photorealistic or non-photorealistic image from a 2D or 3D model by means of computer programs. Also, the result of displaying such a model is called a render.

ii. A rendering engine is often used interchangeably with browser engines. It is responsible for the layout of our website on our audience's screen.

iii. A rendering engine is responsible for the paint, and animations used on our website.

iv. It creates the visuals on the screen or brightens the pixels exactly how they are meant to be to give the feel of the website like how it was made to be.

v. Steps for what happens when we surf the web :
   1. We type an URL into address bar in our preferred browser.
   2. The browser parses the URL to find the protocol, host, port, and path. It forms a HTTP request.

3. To reach the host, it first needs to translate the human readable host into an IP number, and it does this by doing a DNS lookup on the host.
4. Then a socket needs to be opened from the user's computer to that IP number, on the port specified (most often port 80).
5. When a connection is open, the HTTP request is sent to the host.
6. The host forwards the request to the server software configured to listen on the specified port.
7. The server inspects the request and launches the server plugin needed to handle the request.
8. The plugin gets access to the full request, and starts to prepare a HTTP response.
9. The plugin combines that data with some meta data and sends the HTTP response back to the browser.
10. The browser receives the response, and parses the HTML in the response. A DOM tree is built out of the broken HTML.
11. New requests are made to the server for each new resource that is found in the HTML source (typically images, style sheets, and JavaScript files).
12. Stylesheets are parsed, and the rendering information in each gets attached to the matching node in the DOM tree.
13. Javascript is parsed and executed, and DOM nodes are moved and style information is updated accordingly.
14. The browser renders the page on the screen according to the DOM tree and the style information for each node.
15. We see the page on the screen.

List of rendering engines produced by major web browser vendors:

1. **Blink :** It is used in Google Chrome, and Opera browsers.
2. **WebKit :** It is used in Safari browsers.
3. **Gecko :** It is used in Mozilla Firefox browsers.
4. **Trident :** It is used in Internet Explorer browsers.
5. **EdgeHTML :** It is used in Edge browsers.
6. **Presto :** Legacy rendering engine for Opera.

Que 3.20. Explain browser isolation in detail.

Answer

Refer Q. 3.10, Page 3–9W, Unit-3.

PART-4

Security Interface, Cookies Frames and Frame Busting, Major Web Server Threats.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.21. Explain security interface framework.

Answer

1. The security interface framework is a set of Objective-C classes that provide user interface elements for programs that implement security features such as authorization, access to digital certificates, and access to items in keychains.
2. User Interface (UI) defines the way humans interact with the information systems.
3. User Interface (UI) is a series of pages, screens, buttons, forms and other visual elements that are used to interact with the device. Every app and every website has a user interface.
4. User Interface (UI) design is the creation of graphics, illustrations, and use of photographic artwork and typography to enhance the display and layout of a digital product within its various device views.
5. Interface elements consist of input controls (buttons, drop-down menus, data fields), navigational components (search fields, slider, icons, tags), informational components (progress bars, notifications, message boxes).

Que 3.22. Describe cookies and frame busting.

Answer

1. A cookie is a text file that a web browser stores on a user's machine.
2. Cookies are a way for web applications to maintain application state.
3. They are used by websites for authentication, storing website information/preferences, other browsing information and anything else that can help the web browser while accessing web servers.
4. HTTP cookies are known by many different names, including browser cookies, web cookies or HTTP cookies.
5. Frame busting refers to code or annotation provided by a web page intended to prevent the web page from being loaded in a sub-frame.

6. Frame busting is the recommended defense against click-jacking and is also required to secure image-based authentication such as the sign-in seal used by Yahoo.
7. Sign-in seal displays a user-selected image that authenticates the Yahoo login page to the user.
8. Without frame busting, the correct image is displayed to the user, even though the top page is not the real Yahoo login page.
9. New advancements in click jacking techniques using drag and drop to extract and inject data into frames makes frame busting even more critical.

Que 3.23. Discuss web server threats in details.

Answer

Major web server threats are :

1. **Injection flaws :**
   a. Injection flaws, such as SQL, OS injection occur when untrusted data is sent to an interpreter as part of a command or query.
   b. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2. **Broken authentication :** Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users identities.
3. **Sensitive data exposure :**
   a. Many web applications and APIs do not properly protect sensitive data such as financial, healthcare.
   b. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.
   c. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. **XML external entities :**
   a. Many older or poorly configured XML processors evaluate external entity references within XML documents.
   b. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial-of-service attacks.
5. **Broken access control :**
   a. Restrictions on what authenticated users are allowed to do are often not properly enforced.

   b. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users accounts, view sensitive files, modify other users, data, change access rights, etc.
6. **Security misconfiguration :**
   a. Exploits application stack vulnerabilities such as unpatched software, zero-day threats, and undeleted default accounts.
   b. Also exploits misconfigured HTTP headers and verbose error messages that contain sensitive information.
7. **Cross-Site Scripting (XSS) :**
   a. Injects malicious code from a trusted source to execute scripts in the victim's browser that can hijack user sessions or redirect the user to malicious sites.
   b. Cross-site scripting is a common vector that inserts malicious code into a web application found to be vulnerable.
   c. Unlike other web attack types, such as SQL, its objective is not our web application. Rather, it targets its users, resulting in harm to our clients and the reputation of our organization.
8. **Reflected XSS :**
   a. Reflected XSS use a malicious script to reflect traffic to a visitor's browser from web application.
   b. Initiated via a link, a request is directed to a vulnerable website.
   c. Web application is then manipulated to activate harmful scripts.
9. **Cross-Site Request Forgery (CSRF) :**
   a. It is also known as XSRF, Sea Surf, or session riding, cross-site request forgery deceives the user's browser-logged into our application-to run an unauthorized action.
   b. A CSRF can transfer funds in an authorized manner and change passwords, in addition to stealing session cookies and business data.
10. **Man in the Middle Attack (MITM) :**
    a. A man in the middle attack can occur when a bad actor positions himself between application and an unsuspecting user.
    b. MITM can be used for eavesdropping or impersonation.
    c. Meanwhile, account credentials, credit card numbers, and other personal information can easily be harvested by the attacker.
11. **Phishing attack :**
    a. Phishing can be set up to steal user data, such as credit card and login information.
    b. The perpetrator, posing as a trustworthy entity, fools their prey into opening an email, text memo, or instant message.
    c. Then attract to click a link that hides a payload.

d. Such an action can cause malware to be covert installed.

e. It is also possible for ransomware to freeze the user's PC, or for sensitive data to be passed.

12. Remote File inclusion (RFI) :

a. Remote File Inclusion (RFI) exploits weaknesses in those web applications that dynamically call external scripts.

b. Taking advantage of that function, an RFI attack uploads malware and takes over the system.

13. Insecure deserialization :

a. Insecure deserialization often leads to remote code execution.

b. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

14. Using components with known vulnerabilities : It occurs when attackers are able to take control of and exploit vulnerable libraries, frameworks, and other modules running with full privileges.

15. Insufficient logging and monitoring :

a. Insufficient logging and monitoring, allows attackers to attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

16. Backdoor attack :

a. Being a form of malware, a backdoor circumvents login authentication to enter a system.

b. Many organizations offer employees and partners remote access to application resources, including file servers and databases.

c. This enables bad actors to trigger system commands in the compromised system and keep their malware updated.

d. The attacker's files are usually heavily cloaked, making detection problematic.

PART-5

Cross Site Request Forgery, Cross Site-Scripting, Defenses and Protection Against XSS, Finding Vulnerabilities, Secure Development.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.24. Describe cross-site request forgery in details.

Answer

1. Cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.
2. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.
3. With the help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.

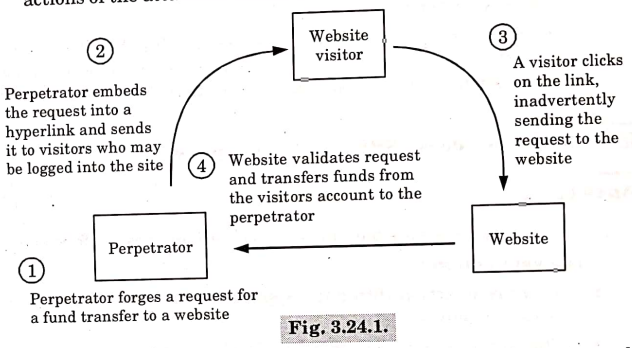

Fig. 3.24.1.

4. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth.
5. If the victim is an administrative account, CSRF can compromise the entire web application.
6. Cross-Site Request Forgery (CSRF) is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in.
7. A successful CSRF attack can be devastating for both the business and user. It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft-including stolen session cookies.
8. As the unsuspecting user is authenticated by their application at the time of the attack, it is impossible to distinguish a legitimate request from a forged one.

Que 3.25. How can we prevent CSRF attack ?

Answer

We can prevent CSRF attack in two ways :

1. **On user side :** User side prevention is very inefficient in terms of browsing experience, prevention can be done by browsing only a single tab at a time and not using the remember-me functionality.
2. **On server side :**
   a. There are many proposed ways to implement CSRF protection on server side, among which the use of CSRF tokens is most popular.
   b. A CSRF token is a string that is tied to a user's session but is not submitted automatically.
   c. A website proceeds only when it receives a valid CSRF token along with the cookies, since there is no way for an attacker to know a user specific token, the attacker cannot perform actions on user's behalf.

Que 3.26. When does CSRF attack takes place ?

Answer

For a CSRF attack to be possible, three key conditions must be followed :

1. **A relevant action :**
   a. There is an action within the application that the attacker has a reason to induce.
   b. This might be a privileged action (such as modifying permissions for other users) or any action on user-specific data (such as changing the user's own password).
2. **Cookie-based session handling :**
   a. Performing the action involves issuing one or more HTTP requests, and the application relies solely on session cookies to identify the user who has made the requests.
   b. There is no other mechanism in place for tracking sessions or validating user requests.
3. **No unpredictable request parameters :**
   a. The requests that perform the action do not contain any parameters whose values the attacker cannot determine or guess.
   b. For example, when causing a user to change their password, the function is not vulnerable if an attacker needs to know the value of the existing password.

Que 3.27. Write short note on cross-site scripting.

Answer

1. Cross-site scripting (XSS) is vulnerability in a web application that allows a third party to execute a script in the user's browser on behalf of the web application.
2. Cross-site scripting is one of the most prevalent vulnerabilities present on the web.
3. The exploitation of XSS against a user can lead to various consequences such as account compromise, account deletion, privilege escalation, malware infection and many more.
4. It was called CSS (Cross Site Scripting). The definition changed when Netscape introduced the Same Origin Policy and cross-site scripting was restricted from enabling cross-origin response reading.
5. Soon it was recommended to call this vulnerability as XSS to avoid confusion with Cascading Style Sheets (CSS).

Que 3.28. Describe the types of cross-site scripting.

Answer

Depending on the context, there are two types of XSS :

1. **Reflected XSS :**
   i. If the input has to be provided each time to execute, such XSS is called reflected.
   ii. These attacks are mostly carried out by delivering a payload directly to the victim.

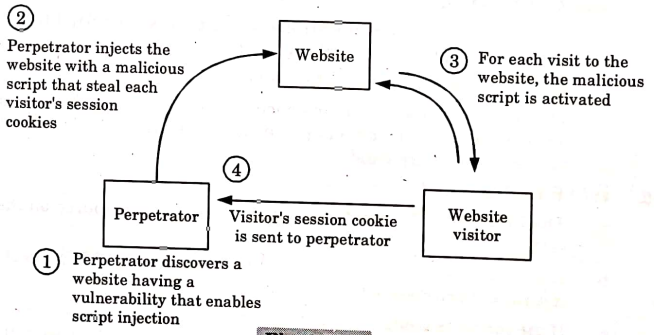

Fig. 3.28.1.

iii. Victim requests a page with a request containing the payload and the payload comes embedded in the response as a script.

iv. An example of reflected XSS is XSS in the search field.

2. **Stored XSS :**

a. When the response containing the payload is stored on the server in such a way that the script gets executed on every visit without submission of payload, then it is identified as stored XSS.

b. An example of stored XSS is XSS in the comment thread.

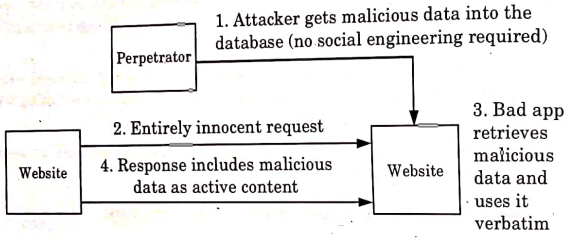

Fig. 3.28.2.

Que 3.29. Explain protection methods used for CSRF.

Answer

The protection methods used for CSRF are :

1. **Anti CSRF Token :**

a. This is a cryptographically strong string that is submitted to the website separately from cookies.

b. This can be sent as a request parameter or as an HTTP header.

c. The server checks for the presence and correctness of this token when a request is made and proceeds only if the token is correct and the cookies are valid.

2. **HTTP PUT method :**

a. The PUT method is used to create instances of a resource on the server.

b. It is similar to POST except that sending the same PUT requests multiple times does not do anything extra.

c. If the server is using PUT method for sensitive actions then there is no need for any additional CSRF protection (unless Cross-Origin Resource Sharing is enabled) at that endpoint.

d. It is because the PUT request cannot be duplicated through a web page like POST request (HTTP forms do not allow PUT requests).

3. **HTTP bearer authentication :**

a. This is a type of HTTP authentication where the user is identified through a token that is submitted in authorization header of each request.

b. This mechanism solves CSRF because unlike cookies it is not submitted by the browser automatically.

c. There are problems and potential bypasses to each of these methods.

d. Anti CSRF tokens do not have a fixed standard so their generation mechanism and use depends solely on how developers intended it to be.

e. Due to this lack of a standard, a lot of implementation specific loopholes exist in web applications.

Que 3.30. Explain different ways used to prevent XSS.

Answer

Different ways used to prevent XSS are :

1. **Escaping :**

a. The first method used to prevent XSS vulnerabilities from appearing in our applications is by escaping user input.

b. Escaping data means taking the data an application has received and ensuring it is secure before rendering it for the end user.

c. By escaping user input, key characters in the data received by a web page will be prevented from being interpreted in any malicious way.

d. In essence, we are censoring the data our web page receives in a way that will disallow the characters especially <and> characters from being rendered, which otherwise could cause harm to the application and/or users.

2. **Validating input :**

a. Validating input is the process of ensuring an application is rendering the correct data and preventing malicious data from doing harm to the site, database, and users.

b. While whitelisting and input validation are more commonly associated with SQL injection, they can also be used as an additional method of prevention for XSS.

c. Whereas blacklisting, or disallowing certain, predetermined characters in user input, disallows only known bad characters,

whitelisting only allows known good characters and is a better method for preventing XSS attacks as well as others.

d. Input validation is especially helpful and good at preventing XSS in forms, as it prevents a user from adding special characters into the fields, instead refusing the request.

e. However, input validation is not a primary prevention method for vulnerabilities such as XSS and SQL injection, but instead helps to reduce the effects should an attacker discover such vulnerability.

3. Sanitizing :

a. A third way to prevent cross-site scripting attacks is to sanitize user input.

b. Sanitizing data is a strong defense, but should not be used alone to battle XSS attacks.

c. Sanitizing user input is especially helpful on sites that allow HTML markup, to ensure data received can do no harm to users as well as our database by scrubbing the data clean of potentially harmful markup, changing unacceptable user input to an acceptable format.

Que 3.31. **Describe XSS vulnerabilities.**

Answer

Following are XSS vulnerabilities :

1. Stored XSS vulnerabilities :

a. Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc.

b. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also referred to as Persistent or Type-I XSS.

2. Reflected XSS vulnerabilities :

a. Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request.

b. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other website.

c. When a user is tricked into clicking on a malicious link, submitting a specially crafted form, or even just browsing to a malicious site, the injected code travels to the vulnerable web site, which reflects the attack back to the user's browser.

d. The browser then executes the code because it came from a trusted server.

e. Reflected XSS is also referred to as Non-Persistent or Type-II XSS.

3. Server-side versus DOM-based vulnerabilities :

a. XSS vulnerabilities were first found in applications that performed all data processing on the server side.

b. User input (including an XSS vector) would be sent to the server, and then sent back to the user as a web page.

c. The need for an improved user experience resulted in popularity of applications that had a majority of the presentation logic working on the client-side that pulled data, on-demand, from the server using AJAX.

d. As the JavaScript code was also processing user input and rendering it in the web page content, a new sub-class of reflected XSS attacks started to appear that was called DOM-based cross-site scripting.

e. In a DOM-based XSS attack, the malicious data does not touch the web server. Rather, it is being reflected by the JavaScript code, fully on the client side.

☺☺☺

4

UNIT

Basic Cryptography

CONTENTS

PART-1

Public Key Cryptography, RSA Public Key Crypto.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.1. **Discuss public key cryptography.**

Answer

1. In public key cryptography, there are two keys : a private key and a public key.
2. The private key is kept by the receiver. The public key is announced to the public.
3. In Fig. 4.1.1 imagine Aaditya wants to send a message to Jyoti. Aaditya uses the public key to encrypt the message. When the message is received by Jyoti, the private key is used to decrypt the message.
4. In public key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption.

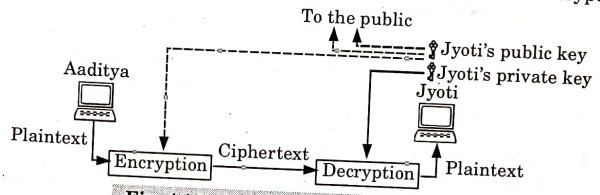

Fig. 4.1.1. Asymmetric key cryptography.

Que 4.2. **What is the principle of public key cryptography ? Discuss the applications for public key cryptography.**

Answer

Principle of public key cryptography :

1. The concept of public key cryptography evolved from an attempt to solve the most difficult problems associated with symmetric encryption :
   i. Two communicants already share a key, which has been distributed to them.

ii. The use of a key distribution center.

2. The second problem negates the very essence of cryptography *i.e.*, the ability to maintain total secrecy over the communication.

Applications for public key cryptography : The use of public key cryptography is classified into three categories :

a. **Encryption/decryption :** The sender encrypts a message with the recipient's public key.

b. **Digital signature :** The sender signs a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

c. **Key exchange :** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private keys of one or both parties.

Que 4.3. Difference between symmetric and asymmetric key cryptography.

Answer

S. No.	Symmetric-key cryptography	Asymmetric-key cryptography
1.	It uses a single key for both encryption and decryption of data.	It uses two different keys—public key for encryption and private key for decryption.
2.	Both the communicating parties share the same algorithm and the key.	Both the communicating parties should have atleast one of the matched pair of keys.
3.	The processes of encryption and decryption are very fast.	The encryption and decryption processes are slower as compared to symmetric-key cryptography.
4.	Key distribution is a problem.	Key distribution is not a problem.
5.	The size of encrypted text is same or less than the original text.	The size of encrypted text is more than the size of the original text.

Que 4.4. Describe RSA algorithm. In RSA, given $e = 07$ and $n = 3$. Encrypt the message "ME" using 00 to 25 for letters A to Z.

Answer

RSA algorithm :

1. RSA is a public key encryption algorithm, named for its inventors (Rivest, Shamir and Adleman).
2. The RSA algorithm is based on the mathematical part that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.
3. The RSA algorithm is shown as :
   a. Choose two large prime numbers p and q.
   b. Calculate $n = p \times q$.
   c. Select the public key (*i.e.*, the encryption key) e such that it is not a factor of $(p - 1)$ and $(q - 1)$.
   d. Select the private key (*i.e.*, the decryption key) d such that the following equation is true :
   $$(d \times e) \bmod (p - 1) \times (q - 1) = 1$$
   e. For encryption, calculate the cipher text C from the plain text M as follows :
   $$C = M^e \bmod n$$
   f. Send C as the cipher text to the receiver.
   g. For decryption, calculate the plain text C from the cipher text C as follows :
   $$M = C^d \bmod n$$

Numerical :

1. Translate the numbers into letters : $M = 12$ and $E = 4$
2. Encrypt each block M using, $C \equiv M^7 \pmod 3$
3. For $M = 12$

$$C = 12^7 \pmod 3$$
$$= 12^4 \times 12^3 \pmod 3$$
$$= (12^2)^2 \times 12^2 \times 12 \pmod 3 = 0$$

For $E = 4$

$$C = E^7 \pmod 3$$
$$= 4^7 \pmod 3$$
$$= 4 \pmod 3 = 1$$

∴ The encrypted ciphertext is : 0 and 1.

Que 4.5. Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for $p = 11$, $q = 13$, $e = 7$, $m = 9$.

OR

Explain RSA using example.

Answer

RSA algorithm : Refer Q. 4.4, Page 4–3W, Unit-4.

Numerical :

Step 1 : $p = 11, q = 13$

Step 2 : $n = p \times q = 11 \times 13 = 143$

Step 3 : Calculate

$$\phi(n) = (p-1)(q-1)$$
$$= (11-1)(13-1) = 10 \times 12 = 120$$

Step 4 : Determine d such that $de \equiv 1 \pmod{160}$

$$d = e^{-1} \bmod 160$$

Using extended Euclidean algorithm we calculate d.

q	r_1	r_2	r	t_1	t_2	t
17	120	7	1	0	1	– 17
7	7	1	0	1	– 17	120
	1	0		– 17	120	

$$= -17 \bmod 120$$

$$d = 103$$

Public key = {7, 143}

Private key = {103, 143}

Encryption $(C) = M^e \pmod{n}$

$$M = 9$$

$$C = 9^7 \bmod 143$$

$$= [(9^4 \bmod 143) \times (9^2 \bmod 143)$$
$$(9^1 \bmod 143)] \bmod 14$$

$$= (126 \times 81 \times 9) \bmod 143$$

$$= 91854 \bmod 143 = 48$$

Decryption $(M) = 13^{103} \bmod 143$

Que 4.6. **Discuss public key cryptography. Explain RSA algorith with suitable steps. Let $p = 17$, $q = 11$, $e = 7$ and d = 23. Calculate th public key and private key and show encryption and decryption fo plain text $M = 88$ by using RSA algorithm.**

Answer

Public key cryptography : Refer Q. 4.1, Page 4–2W, Unit-4.

RSA algorithm : Refer Q. 4.4, Page 4–3W, Unit-4.

Numerical :

Step 1 : $p = 17, q = 11$

Step 2 : $n = p \times q = 17 \times 11 = 187$

Step 3 : Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

Step 4 : $d = 23$ and $e = 7$

Public key is {7, 187}

Private key is {23, 187}

Encryption : Ciphertext is

$C = M^e \bmod n = 88^7 \bmod 187 = (88^2 \bmod 187)\ (88^5 \bmod 187)$

$= [77 \times (77 \times 77) \times 88] \bmod 187 = 11$

$C = 11$

Decryption : Plaintext is

$M = C^d \bmod n = 11^{23} \bmod 187 = (11^5 \bmod 187)\ (11^{18} \bmod 187)$

$= [44 \times (44 \times 44 \times 44)\ (11^3 \bmod 187)] \bmod 187$

$= [44^4 \times 22] \bmod 187 = 88$

Que 4.7. **What are the advantages and disadvantages of RSA ?**

Answer

Advantages of RSA :

1. **Convenience :** It solves the problem of distributing the key for encryption.
2. **Provides message authentication :** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is from a particular sender.
3. **Detection of tampering :** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
4. **Provides non-repudiation :** Digitally signing a message is related to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

Disadvantages of RSA :

1. **Public keys should/must be authenticated :** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.
2. **Slow :** Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.
3. **Uses more computer resources :** It requires a lot more computer supplies compared to single-key encryption.
4. **Widespread security compromise is possible :** If an attacker determines a person's private key, his or her entire messages can be read.
5. **Loss of private key may be irreparable :** The loss of a private key means that all received messages cannot be decrypted.

Que 4.8. **What are the securities of RSA ? Perform encryption and decryption using RSA algorithm for $p = 17$, $q = 11$, $e = 7$, $m = 88$.**

Answer

Three possible approaches and securities of the RSA algorithm are :

1. **Brute force :**
   a. This involves trying all possible private keys.
   b. The defense against the brute force approach is to use a large key space.
2. **Mathematical attacks :**
   a. There are several approaches used for factoring the product of two primes.
   b. The defense against mathematical attacks is to use factoring performance as a benchmark against which to evaluate the security of RSA.
3. **Timing attacks :** These depend on the running time of the decryption algorithm. Counter-measures that can be used, includes the following :
   a. **Constant exponentiation time :** Ensure that all exponentiation take the same amount of time before returning a result. This is a simple fix but does degrade performance.
   b. **Random delay :** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.
   c. **Blinding :** Multiply the ciphertext by a random number before performing exponentiation. This process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack.

Numerical : Refer Q. 4.6, Page 4–5W, Unit-4.

Que 4.9. **Write a short note on hybrid cryptosystem.**

Answer

i. A hybrid cryptosystem is a protocol using multiple ciphers of different types together.

ii. In hybrid cryptosystem, we generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key.

iii. The message itself is then encrypted using the symmetric cipher and the secret key.

iv. Both the encrypted secret key and the encrypted message are then sent to the recipient.

v. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message.

vi. The steps of hybrid encryption are :

1. Generate a symmetric key. The symmetric key needs to be kept a secret.
2. Encrypt the data using the secret symmetric key.
3. The person to whom we wish to send a message will share her public key and keep the private key a secret.
4. Encrypt the symmetric key using the public key of the receiver.
5. Send the encrypted symmetric key to the receiver.
6. Send the encrypted message text.
7. The receiver decrypts the encrypted symmetric key using her private key and gets the symmetric key needed for decryption.
8. The receiver uses the decrypted symmetric key to decrypt the message, getting the original message.

PART-2

Digital Signature Hash Functions, Public Key Distribution.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.10. **Describe briefly the term digital envelope.**

Answer

1. A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication.
2. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.
3. Rivest, Shamir and Adleman (RSA) Public-Key Cryptography Standard (PKCS) governs the application of cryptography to data for digital envelopes and digital signatures.
4. A digital envelope is also known as a digital wrapper.
5. Following methods may be used to create a digital envelope :
   a. Secret key encryption algorithms, for message encryption.
   b. Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

6. An example of a digital envelope is Pretty Good Privacy (PGP), a popular data cryptography software that provides cryptographic privacy and data communication authentication.

Que 4.11. Explain the digital signatures.

Answer

1. Digital signature is a mathematical scheme used for verifying the authenticity of digital message or documents.
2. Digital signature uses three algorithms :

a. Key generation : This algorithm selects a private key uniformly at random from a set of possible private keys. Output of this algorithm is private key and its corresponding public key.

b. Signing algorithm : It produce signature by using message and private key.

c. Signature verifying algorithm : For a given message, signature and public key, either accepts or rejects the messages claim to authenticity.

3. Fig. 4.11.1 shows the concept of digital signature.

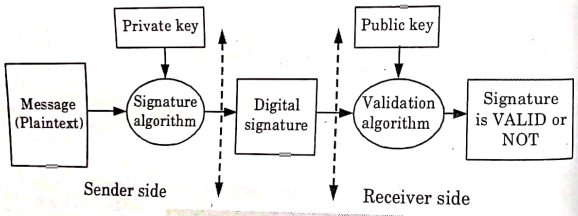

Fig. 4.11.1. Digital signature.

Que 4.12. Explain key generation algorithm, signing algorithm, signature verification algorithm in digital signature.

Answer

1. **Key generation algorithms :**
   a. Digital signatures are electronic signatures, which assures that the message was sent by a particular sender.
   b. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.

2. **Signing algorithms :**
   a. To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed.
   b. The signing algorithm then encrypts the hash value using the private key (signature key).
   c. This encrypted hash along with other information like the hashing algorithm is the digital signature.
   d. This digital signature is appended with the data and sent to the verifier.
   e. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value.
   f. This saves time as instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature verification algorithms :**
   a. Verifier receives digital signature along with the data.
   b. It then uses verification algorithm to process on the digital signature and the public key (verification key) and generates some value.
   c. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

Que 4.13. Describe the steps used in creating digital signature.

Answer

The steps followed in creating digital signature are :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender. (This assures authenticity as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).

6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Que 4.14. Write a short note on Message Digest (MD) hash function.

Answer

1. The MD hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed length digest value to be used for authenticating the original message.
2. The MD hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures.
3. MD has been deprecated for uses other than as a non-cryptographic checksum to verify data integrity and detect unintentional data corruption.
4. MD hashing is no longer considered reliable for use as a cryptographic checksum because researchers have demonstrated techniques capable of easily generating MD collisions on commercial off-the-shelf computers.
5. The goal of any message digest function is to produce digests that appear to be random.
6. To be considered cryptographically secure, the hash function should meet two requirements :
   i. It is impossible for an attacker to generate a message matching a specific hash value.
   ii. It is impossible for an attacker to create two messages that produce the same hash value.

Que 4.15. Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA ?

Answer

Digital Signature Algorithm (DSA) : DSA is an asymmetric encryption algorithm that works on two different key *i.e.*, one public and one private to produce digital signature.

1. The sender generates a random number k, which is less than q.
2. The sender now calculates :
   a. $r = (g^k \bmod p) \bmod q$
   b. $s = (K^{-1}(H(m) + xr)) \bmod q$

   The values r and s are the signatures of the sender.
3. The sender sends these values to the receiver. To verify the signature, the receiver calculates :

   $w = s^{-1} \bmod q$

$u1 = (H(m) * w) \bmod q$

$u2 = (rw) \bmod q$

$v = ((g^{u1*} y^{u2}) \bmod p) \bmod q$

If $v = r$, the signature is said to be verified. Otherwise, it is rejected.

where,

p = A prime number of length L bits

q = A 160-bits prime factor of $(p - 1)$

$g = h^{(p-1)/q} \bmod p$

x = A number less than q.

$y = g^x \bmod p$.

H = Message Digest algorithm.

If same secret $(k1, k2)$ is used for signing two different messages, it will generate two different signatures $(r1, s1)$ and $(r1, s2)$:

1. $s1 = k1^{-1}(h1k2 + d(r1 + r2))$
2. $s2 = k1^{-1}(h2k2 + d(r1 + r2))$

   where $h1 = \text{SHA512}(m1)$ and $h2 = \text{SHA512}(m2)$
3. $k1s1 - k1s2 = h1k2 + dr - h2k2 - dr$
4. $k1(s1 - s2) = k2(h1 - h2)$
5. We cannot obtain $k1$, $k2$ from this equation and so this scheme is more secure than original ECDSA (Elliptical Curve Digital Signature Algorithm) scheme.

Que 4.16. What are the properties and requirements for a digital signature ?

Answer

Properties of digital signature :

1. It must be able to verify the author, the date and time of the signature.
2. It must be able to authenticate the contents of the message at the time of the signature.
3. There must be third (trusted) party who can verify the digital signature to resolve disputes between the sender and receiver.

Requirements for a digital signature :

1. The signature must be in the form of a bit pattern and relative to the message being signed.
2. The signature must contain information that is unique to the sender, so that forgery and denial can be avoided.
3. The process of creating, recognizing and verifying the digital signature must also be comparatively easy.

4. A high computational effort must be required to forge a digital signature.
6. The copy of a digital signature must be retained in storage mechanism.

Que 4.17. Explain the variants of digital signatures ?

Answer

Variants of digital signature are :

1. **Timestamped signature :**
   a. Timestamped digital signatures include a timestamp value in order to prevent replay attack.
   b. In a replay attack, the documents can be replayed by a third party.
2. **Blind signature :**
   a. Blind signature is used when the sender does not want to reveal the contents of the message to the signer and just wishes to get the message signed by the signer.
   b. Blind signatures are used in situations where the signer message authors are completely different parties.
   c. Blind signatures scheme can be implemented by using a number of public-key digital signature schemes such as RSA and DSS.
3. **Undeniable digital signature :**
   a. This scheme is a non self-authenticating signature scheme in which no signatures can be verified without the signer's cooperation and notification.
   b. This scheme has three components :
      i. **Signing algorithm :** This allows the signer to sign a message.
      ii. **Verification (or confirmation) protocol :** This allows the signer to limit the users who can verify his or her signature.
      iii. **Disavowal (or denial) protocol :** Since the verification process requires the involvement of the signer, it is quite possible that the signer can freely decline the request of the verifier. This protocol prevents the signer from proving that a signature is invalid when it is valid and vice-versa.

Que 4.18. What is hash function ? Discuss SHA-512 with all required steps, round function and block diagram.

Answer

Hash function :

1. A cryptographic hash function is a transformation that takes an input and returns a fixed-size string, which is called the hash value.
2. A hash value h is generated by a function H of the form :

$$h = H(M)$$

where M is the variable length message and H(M) is the fixed length hash value.

3. The hash value is appended to the message at the source at a time when message is assumed or known to be correct.
4. The receiver authenticates the message by recomputing the hash value.
5. The ideal hash function has three main properties :
   a. It is extremely easy to calculate a hash for any given data.
   b. It is extremely difficult to calculate a text that has given hash.
   c. It is extremely unlikely that two different messages, however close, will have the same hash.

Working of Secure Hash Algorithm (SHA) : The algorithm takes as input a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks. The processing consists of following steps :

Step 1 : Padding : The first step in SHA is to add padding to the end of the original message in such a way that the length of the message is 64-bits short of a multiple of 512.

Step 2 : Append length : The length of the message excluding the length of the padding is calculated and appended to the end of the padding as a 64-bit block.

Step 3 : Divide the input into 512-bit blocks : The input message is divided into blocks, each of length 512-bits. These blocks become the input to the message digest processing logic.

Step 4 : Initialize chaining variables : Five chaining variables *A* through *E* are initialized. In SHA, we want to produce a message digest of length 160-bits. Therefore, we need to have five chaining variables.

Step 5 : Process blocks : Main algorithm is executed in process block.

Round Functions :

1. The round function computes a new value for variable A and shifts all working variable once per round.
2. The computation for variable A is a five operand addition modulo 2^{32} where the operands depend on all input words, the round-dependent constant K_t, and the current message word W_t.

Block diagram of SHA-512 :

1. The core is composed of two main units, the SHA1 Engine and the padding unit.
2. The SHA1 Engine applies the SHA1 loops on a single 512-bit message block, while the padding unit splits the input message into 512-bit blocks and performs the message padding on the last block of the message.

3. The processing of one 512-bit block is performed in 82 clock cycles and the bit-rate achieved is 6.24 Mbps / MHz on the input of the SHA1 core.

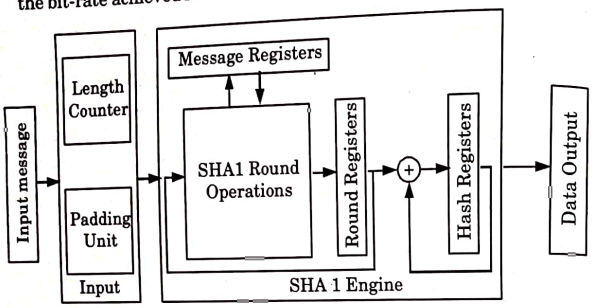

Fig. 4.18.1.

Que 4.19. What are the characteristics of SHA function ?

Answer

Characteristics (requirements) of secure hash function :

1. The hash function should be applicable on a block of data of any size.
2. The output produced by the hash function should always be of fixed length.
3. For any given message or block of data, it should be easier to generate the hash code.
4. Given a hash code, it should be nearly impossible to determine the corresponding message or block of data.
5. Given a message or block of data, it should not be computationally feasible to determine another message or block of data generating the same hash code as that of the given message or block of data.
6. No two messages or blocks of data, even being almost similar, should be likely to have the same hash code.

Que 4.20. Discuss public key distribution. Describe the various schemes used for public key distribution.

Answer

1. In public key cryptography, the key distribution of public keys is done through public key servers.
2. When a person creates a key-pair, they keep one key private and the other known as the public-key is uploaded to a server where it can be accessed by anyone to send the user a private, encrypted, message.

Schemes used for the distribution of public keys are as follows :

1. **Public announcement :**
   a. The main focus of public key encryption is that the public key should be public; that is, a user can send his or her public key to any other user of broadcast it to a large community.
   b. The main problem is that of forgery. That is, anyone can forge the key while it is being transmitted.
2. **Public directory :**
   a. Public directory is a dynamic directory the name and public key entry for each user is maintained and distributed by some trusted authority.
   b. This approach assumes that the public key of the authority is known to everyone, however the corresponding private key is known only to the authority.
   c. Each user has to register his or her public key with the directory authority.
   d. The user can replace its existing key with a new one as per his or her choice.
3. **Public key authority :**
   a. In public directory scheme, if the private key of the authority is stolen, then it may result in loss of data.
   b. Thus, to achieve stronger security for public key distribution, a tighter control needs to be provided over the distribution of public keys from the directory.
   c. It this case, a central authority maintains the dynamic directory of the public keys of all the users. The user knows only the public key of the authority, while the corresponding private key is secret to the authority.

Que 4.21. Discuss X.509 certificates in detail. What is the role of X.509 certificates in cryptography ?

Answer

X.509 certificates :

1. In cryptography, X.509 is an ITU-T standard for a Public Key Infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI).
2. X.509 specifies, standard formats for public key certificates, certificate revocation lists, attribute certificates and a certification path validation algorithm.
3. X.509 defines a framework for the provision of authentication services by the X.500 directory to its user.

4. X.509 certificate is based on the use of public key cryptography and digital signatures.
5. The standard does not dictate the use of a specific algorithm but recommends RSA.
6. X.509 certificates format is used in S/MIME, IP security and SET.

Role of X.509 certificates in cryptography :

1. To verify that a public key belong to the user, computer or service identify contained within the certificate.
2. To validate the identity of encrypted data.

Que 4.22. Discuss X.509 digital certificate format.

Answer

Format of X.509 certificate :

The general format of a X.509 digital certificate is shown in Fig. 4.22.1.

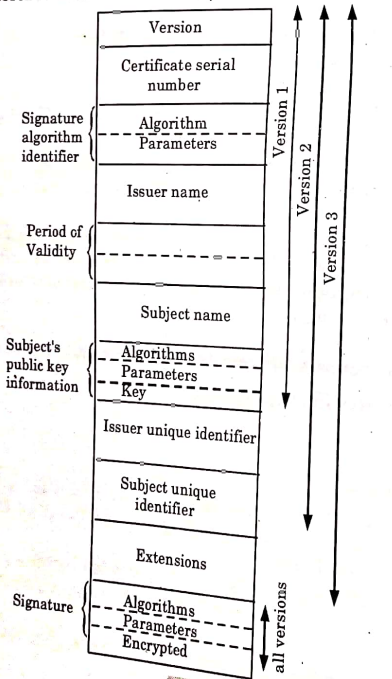

Fig. 4.22.1. X.509 format.

1. **Version :** Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, then the value must be version 2. If one or more extensions are present, the version must be version 3.
2. **Serial number :** It is a unique integer value within the issuing CA (Certification Authority) that is unambiguously associated with this certificate.
3. **Signature algorithm identifier :** This algorithm is used to sign the certificates together with any associated parameters.
4. **Issuer name :** X.500 name of the CA that created and signed the certificate.
5. **Period of validity :** Consist of two dates : the first and last on which the certificate is valid.
6. **Subject name :** The name of the user to whom this certificate refers. This certificate certifies the public key of the subject who holds the corresponding private key.
7. **Subject's public key information :** The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.
8. **Issuer unique identifier :** An optional bit string field used to identify uniquely the issuing CA.
9. **Subject unique identifier :** An optional bit string field used to identify uniquely the subject in the event that X.500 name has been reused for different entities.
10. **Extensions :** A set of one or more extension fields. Extensions were added in version 3.
11. **Signature :** Cover all other fields of the certificate. It contains the hash code of the other fields encrypted with the CA's private key. This field includes the signature algorithm identifier.

Que 4.23. What do you mean by PGP ? Discuss its application.

Answer

PGP :

1. PGP (Pretty Good Privacy) is an encryption algorithm that provides cryptographic privacy and authentication for data communication.
2. PGP uses a combination of public-key and conventional encryption to provide security services for electronic mail message and data files.
3. PGP provides five services related to the format of messages and data files : authentication, confidentiality, compression, e-mail compatibility and segmentation.

Application of PGP :

1. PGP provides secure encryption of documents and data files that even advanced super computers are not able to crack.
2. For authentication, PGP employs the RSA public-key encryption scheme and the MD5, a one-way hash function to form a digital signature that assures the receiver that an incoming messages is authentic (that it comes from the alleged send and that it has not been altered).

Que 4.24. Discuss the steps that are followed for the transmission and reception of PGP messages.

Answer

The PGP messages are transmitted from the sender to receiver using following steps :

1. If signature is required, the hash code of the uncompressed plaintext message is created and encrypted using the sender's private key.
2. The plaintext message and the signature are compressed using the ZIP compression algorithm.
3. The compressed plaintext message and compressed signature are encrypted with a randomly generated session key to provide confidentiality. The session key is then encrypted with the recipient's public key and is added to the beginning of the message.
4. The entire block is converted to radix-64 format.

On receiving the PGP message, the receiver follows the following steps :

1. The entire block is first converted back to binary format.
2. The recipient recovers the session key using his or her private key, and then decrypts the message with the session key.
3. The decrypted message is then decompressed.
4. If the message is signed, the receiver needs to verify the signature. For this, he or she computes a new hash code and compares it with the received hash code. If they match, the message is accepted; otherwise, it is rejected.

PART-3

Real World Protocols, Basic Terminologies.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.25. Explain real world protocols.

Answer

Following are the real world protocols :

1. **SSL architecture :**
   - i. The Secure Socket Layer (SSL) protocol provides exchange of information between a web browser and a web server in a secure manner.
   - ii. Its main aim is to provide entity authentication, message integrity and confidentiality.
   - iii. SSL is an additional layer located between the application layer and the transport layer of the TCP/IP protocol suite. All the major web browsers support SSL.
2. **S/MIME :**
   - i. A secure version of MIME, S/MIME (Secure/Multipurpose Internet Mail Extensions), is used to support encryption of email messages.
   - ii. It is based on the MIME standard and provides the security services for electronic messaging applications : authentication, message integrity and data security.
   - iii. S/MIME uses public key cryptography to sign and encrypt e-mail.
   - iv. Every participant has two keys :
     - a. A private key, which is kept secret.
     - b. A public key, which is available to everyone.
   - iv. The following steps are taken in order to create a signed message :
     - a. The user writes the message as clear-text.
     - b. The message digest is being calculated using SHA-1 or MD5.
     - c. The message digest is being encrypted using the signer's private key (DSS or RSA).
3. **PGP :** Refer Q. 4.23, Page 4–18W, Unit-4.
4. **SET :**
   - i. Secure Electronic Transaction (SET) is a standard protocol for securing credit card transactions over insecure networks, *i.e.*, the internet.
   - ii. SET is not a payment system but rather a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion.
   - iii. SET is based on X.509 certificates with several extensions.
   - iv. SET makes use of cryptographic techniques such as digital certificates and public key cryptography to allow parties to identify themselves to each other and exchange information securely.

v. SET uses a blinding algorithm that lets merchants to substitute a certificate for a user's credit card number.

vi. This allows traders to credit funds from client's credit cards without the need of the credit card numbers.

vii. The purpose of the SET protocol is to establish payment transactions. It provides confidentiality of payment and ordering information, and ensures the integrity of all transmitted data.

viii. SET creates a protocol that neither depends on transport security mechanisms nor prevents their use.

ix. It facilitates and encourages interoperatability among software and network providers.

5. **IPSec :**

i. IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network layer.

ii. IPSec is a capability that can be added to either version of the Internet Protocol (IPv4 or IPv6), by means of additional headers.

iii. IPSec encompasses three functional areas : authentication, confidentiality, and key management.

a. The authentication mechanism assures that a received packet was transmitted by the party identified as the source in the packet header.

b. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third party.

c. The key management facility is concerned with the secure exchange of keys.

iv. IPSec has two modes of operation :

a. **Transport mode :** It is the default mode of IPSec which provide end-to-end security. It can secure communication between a client and a server.

b. **Tunnel mode :** Tunnel mode is used between two routers, between a host and a router, or between a router and a host. It is used when either the sender or the receiver is not a host.

v. IPSec uses two protocols for message security :

a. **Authentication Header (AH) :** It covers the packet format and general issues related to the use of AH for packet authentication.

b. **Encapsulating Security Payload (ESP) :** It covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.

Que 4.26. List the basic terminology used in cryptography.

Answer

Some basic terminology used in cryptography :

1. **Plaintext :** Plaintext is a readable, plain message that anyone can read.
2. **Cipher text :** The transformed message or coded message
3. **Cipher :** An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.
4. **Key :** Some critical information used by the cipher, known only to the sender and receiver
5. **Encoding/Encryption :** The process of converting plaintext to cipher text using a cipher and a key.
6. **Decoding/Decryption :** The process of converting cipher text back into plaintext using a cipher and a key.
7. **Cryptanalysis (code breaking) :** The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.
8. **Cryptology :** The combination of cryptography and cryptanalysis.
9. **Code :** An algorithm for transforming an intelligible message into an unintelligible one using a code-book.
10. Symmetric algorithms use the same key for encryption and decryption. These algorithms require that both the sender and receiver agree on a key before they can exchange messages securely.
11. **Public key algorithms :** It also known as asymmetric algorithms uses two different keys (a key pair) for encryption and decryption. The keys in a key pair are mathematically related, but it is computationally infeasible to deduce one key from the other. These algorithms are called "public-key" because the encryption key can be made public. Anyone can use the public key to encrypt a message, but only the owner of the corresponding private key can decrypt it.
12. **Substitution :** Replacing one entity with other.
13. **Transposition :** Shuffling the entities.
14. **Block cipher :** Processes the input one block element and produce one output block.
15. **Stream Cipher :** Processes the one input element and outputs one element at a time.

Que 4.27. Discuss the functionality of S/MIME.

Answer

The basic functionalities of S/MIME are :

1. **Enveloped data :** S/MIME supports enveloped data, which consists of the message containing any type of contents in encrypted form and the encryption key encrypted with receiver's public key.
2. **Signed data :** This consists of the message digest encrypted using the sender's private key. This signed message can only be viewed by the receivers who have S/MIME capability.
3. **Clear-signed data :** This functionality is similar to the signed data that allows the receivers to view the contents of the message even if they do not have S/MIME capability. However, they cannot verify the signature.
4. **Signed and enveloped data :** In this, S/MIME allows nesting of signed-only and encrypted-only entities, so that the encrypted data can be signed, and signed or clear-signed data can be encrypted.

PART-4

Email Security Certificates, Transport Layer Security TLS, IP Security.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.28. What is email security ?

Answer

1. Email security refers to the collective measures used to secure the access and content of an email account or service.
2. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.
3. Email security is a term that encompasses multiple techniques used to secure an email service.
4. It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.
5. SSL, TLS refers to the standard protocol used to secure email transmission.
6. Transport Layer Security (TLS) provides a way to encrypt a communication channel between two computers over the internet.

Que 4.29. What is an email certificate ?

Answer

1. Email certificates (S/MIME certificates), are digital certificates that can be used to sign and encrypt email messages.
2. When we encrypt an email using an email certificate, only the person that we sent it to can decrypt and read the email. The recipient can also be sure that the email has not been changed in any way.
3. An email certificate is a digital file that is installed to our email application to enable secure email communication.
4. These certificates are known by many names email security certificates, email encryption certificates, S/MIME certificates, etc. S/MIME, Stands for Secure/Multipurpose Internet Mail Extension, is a certificate that allows users to digitally sign their email communications as well as encrypt the content and attachments included in them.
5. Not only does this authenticate the identity of the sender to the recipient, but it also protects the integrity of the email data before it is transmitted across the internet.
6. An S/MIME email certificate allows we to :
   a. Encrypt our emails so that only our intended recipient can access the content of the message.
   b. Digitally sign our emails so the recipient can verify that the email was, in fact, sent by you and not a phisher posing as you.

Que 4.30. What is Transport Layer Security (TLS) ?

Answer

1. Transport Layer Security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet.
2. It enables privacy, integrity and protection for the data that is transmitted between different nodes on the Internet.
3. TLS is a successor to the Secure Socket Layer (SSL) protocol.
4. Transport Layer Security (TLS) is a protocol that provides authentication, privacy, and data integrity between two communicating computer applications.
5. It is the most widely-deployed security protocol used for web browsers and other applications that require data to be securely exchanged over a network, such as web browsing sessions, file transfers, VPN connections, remote desktop sessions, and Voice over IP (VoIP).
6. TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.

7. TLS primarily enables secure Web browsing, applications access, data transfer and most Internet-based communication.
8. It prevents the transmitted/transported data from being eavesdropped or tampered.
9. TLS is used to secure Web browsers, Web servers, VPNs, database servers and more.
10. TLS protocol consists of :
    a. **TLS handshake protocol :** It enables the client and server to authenticate each other and select an encryption algorithm prior to sending the data.
    b. **TLS record protocol :** It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services.

Que 4.31. **What are the components of TLS ? Explain the working of TLS.**

Answer

1. TLS is used on top of a transport layer security protocol like TCP.
2. There are three main components to TLS :
    a. **Encryption :** It hides the data being transferred from third parties.
    b. **Authentication :** It ensures that the parties exchanging information are who they claim to be.
    c. **Integrity :** It verifies that the data has not been forged or tampered with.

Working of TLS :

1. A TLS connection is initiated using a sequence known as the TLS handshake.
2. The TLS handshake establishes a cipher suite for each communication session.
3. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session.
4. TLS is able to set the matching session keys over an unencrypted channel known as public key cryptography.
5. The handshake also handles authentication, which usually consists of the server proving its identity to the client. This is done using public keys.

6. Public keys are encryption keys that use one-way encryption, meaning that anyone can unscramble data encrypted with the private key to ensure its authenticity, but only the original sender can encrypt data with the private key.
7. Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC).
8. The recipient can then verify the MAC to ensure the integrity of the data.

Que 4.32. **Explain internet protocol security (IPSec) in detail.**

Answer

Refer Q. 4.25, Page 4–20W, Unit-4.

Que 4.33. **Write a short note on the applications of IP security.**

Answer

Applications of IP security :

1. **Secure remote Internet access :** Using IPSec, we can make a local call to our Internet Service Provider (ISP) so as to connect to our organization's network in a secure manner from our home or hotel.
2. **Secure branch office connectivity :** Rather than subscribing to an expensive borrow line for connecting its branches across cities/countries an organization can set up an IPSec-enabled network to securely connect all its branches over the Internet.
3. **Set up communication with other organizations :** IPSec allows connectivity between various branches of an organization, and it can also be used to connect the networks of different organizations together in a secure and inexpensive fashion.

Que 4.34. **What are the advantages of IPSec ?**

Answer

1. IPSec is transparent to the end users. There is no need for user training, key revocation.
2. When IPSec is configured to work with a firewall, it becomes the only entry-exit point for all traffic making it extra secure.
3. IPSec works at the network layer. Hence, no changes are needed to the upper layers *i.e.*, application and transport.

4. When IPSec is implemented in a firewall or a router, all the outgoing and incoming traffic gets protected. However, the internal traffic does not have to use IPSec. Thus, it does not add any overheads for the internal traffic.
5. IPSec can allow traveling staff to have secure access to the corporate network.
6. IPSec allows interconnectivity between branches/offices in a very inexpensive manner.

Que 4.35. What are the uses of IP security ?

Answer

IPsec can be used :

1. To encrypt application layer data.
2. To provide security for routers sending routing data across the public internet.
3. To provide authentication without encryption, like to authenticate that the data originates from a known sender.
4. To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network (VPN) connection.

Que 4.36. Discuss components of IP Security.

Answer

Components of IP security :

1. **Encapsulating Security Payload (ESP) :** It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header AH :**
   a. It also provides data integrity, authentication and anti-replay and it does not provide encryption.
   b. The anti-replay protection protects against unauthorized transmission of packets. It does not protect data's confidentiality.
3. **Internet Key Exchange (IKE) :**
   a. It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between two devices.

   b. The Security Association (SA) establishes shared security attributes between two network entities to support secure communication.
   c. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange.
   d. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
   e. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5.

Que 4.37. Explain the working of IP Security.

Answer

Working of IP security :

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the IKE Phase I starts in which the two hosts (using IPsec) authenticate themselves to each other to start a secure channel. It has two modes. The main mode which provides the greater security and the aggressive mode which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

PART-5

DNS Security.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.38. Describe briefly Domain Name Server (DNS).

Answer

1. Domain Name Server is a prominent building block of the Internet. It is developed as a system to convert alphabetical names into IP addresses, allowing users to access websites and exchange emails.
2. DNS is organized into a tree-like infrastructure where the first level contains topmost domains, such as .com and .org.
3. The second level nodes contain general, traditional domain names.
4. The leaf nodes on this tree are known as hosts.
5. DNS works similar to a database which is accessed by millions of computer systems in trying to identify which address is most likely to solve a user's query.
6. In DNS attacks, hackers will target the servers which contain the domain names.
7. In other cases, these attackers will try to determine vulnerabilities within the system itself and exploit them for their own benefits.

Que 4.39. How DNS security works ?

Answer

1. The DNS turns domain names, or website names, into internet protocol (IP) addresses.
2. These are unique identifiers that help computers around the world access the information quickly.
3. DNS security adds a set of extensions for increased protection.
4. These security extensions include :
   a. **Origin authentication of DNS data :** This ensures that the recipient of the data can verify the source.
   b. **Authenticated denial of existence :** This tells a resolver (responsible for translating the domain name into an IP address) that a certain domain name does not exist.

   c. **Data integrity :** This assures the data recipient that the data has not been changed in transit.

Que 4.40. Explain the DNS security threats.

Answer

Common DNS security threats are :

1. **Distributed Denial of service (DDoS) :**
   a. The attacker controls an overwhelming amount of computers (hundreds or thousands) in order to spread malware and flood the victim's computer with unnecessary and overloading traffic.
   b. Eventually, unable to harness the power necessary to handle the intensive processing, the systems will overload and crash.
2. **DNS spoofing (also known as DNS cache poisoning) :**
   a. Attacker will drive the traffic away from real DNS servers and redirect them to a pirate server, unbeknownst to the users.
   b. This may cause in the corruption/theft of a user's personal data.
3. **Fast flux :**
   a. Fast flux is a technique to constantly change location-based data in order to hide where exactly the attack is coming from.
   b. This will mask the attacker's real location, giving him the time needed to exploit the attack.
   c. Flux can be single or double or of any other variant. A single flux changes address of the web server while double flux changes both the address of web server and names of DNS serves.
4. **Reflected attacks :**
   a. Attackers will send thousands of queries while spoofing their own IP address and using the victim's source address.
   b. When these queries are answered, they will all be redirected to the victim himself.
5. **Reflective amplification DoS :**
   a. When the size of the answer is considerably larger than the query itself a flux is triggered, causing an amplification effect.
   b. This generally uses the same method as a reflected attack, but this attack will overwhelm the user's system's infrastructure further.

Que 4.41. Discuss measures against DNS attacks.

Answer

Measures against DNS attacks :

1. Use digital signatures and certificates to authenticate sessions in order to protect private data.
2. Update regularly and use the latest software versions, such as BIND. BIND is open source software that resolves DNS queries for users. It is widely used by a good majority of the DNS servers on the Internet.
3. Install appropriate patches and fix faulty bugs regularly.
4. Replicate data in a few other servers, so that if data is corrupted/ lost in one server, it can be recovered from the others. This could also prevent single point failure.
5. Block redundant queries in order to prevent spoofing.
6. Limit the number of possible queries.

☺☺☺

UNIT 5

Internet Infrastructure

CONTENTS

PART-1

Internet Infrastructure, Basic Security Problems.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.1. Define internet infrastructure. What are different internet infrastructures ?

Answer

Internet infrastructures are the frameworks or architectures that the internet systems are made of.

Various internet infrastructures are :

1. **TCP/IP :**
   a. TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).
   b. The entire internet protocol suite is a set of rules and procedures and is commonly referred to as TCP/IP, though others are included in the suite.
   c. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination.
   d. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.
2. **DNS :** Refer Q. 4.38, Page 4–29W, Unit-4.
3. **BGP :**
   a. Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among Autonomous Systems (AS) on the Internet.
   b. The protocol is classified as a path vector protocol.
   c. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

   d. BGP may be used for routing within an autonomous system. In this application it is referred to as Interior Border Gateway Protocol, Internal BGP, or iBGP.
   e. In contrast, the Internet application of the protocol may be referred to as Exterior Border Gateway Protocol, External BGP, or eBGP.

Que 5.2. Explain the advantages and disadvantages of in TCP/IP model.

Answer

Advantages of TCP/IP model are :

1. It is an industry-standard model that can be effectively deployed in practical networking problems.
2. It is interoperable, *i.e.*, it allows cross-platform communications among heterogeneous networks.
3. It is an open protocol suite. It is not owned by any particular institute and so can be used by any individual or organization.
4. It is a scalable, client-server architecture. This allows networks to be added without disrupting the current services.
5. It assigns an IP address to each computer on the network, thus making each device to be identifiable over the network. It assigns each site a domain name. It provides name and address resolution services.

Disadvantages of the TCP/IP model are :

1. It is not generic in nature. So, it fails to represent any protocol stack other than the TCP/IP suite. For example, it cannot describe the Bluetooth connection.
2. It does not clearly separate the concepts of services, interfaces, and protocols. So, it is not suitable to describe new technologies in new networks.
3. It does not distinguish between the data link and the physical layers, which has very different functionalities. The data link layer should concern with the transmission of frames. On the other hand, the physical layer should lay down the physical characteristics of transmission.
4. It was originally designed and implemented for wide area networks. It is not optimized for small networks like LAN (Local Area Network) and PAN (Personal Area Network).

Que 5.3. What are functions of internet protocol (IP) ?

Answer

Following are the functions of internet protocols :

1. **Addressing :**
   a. In order to perform the job of delivering datagrams, IP must know where to deliver them to. For this reason, IP includes a mechanism for host addressing.
   b. Since IP operates over internetworks, its system is designed to allow unique addressing of devices across arbitrarily large networks.
   c. It also contains a structure to facilitate the routing of datagrams to distant networks if required.
   d. Since most of the other TCP/IP protocols use IP, understanding the IP addressing scheme is of vital importance to understand TCP/IP.
2. **Data encapsulation and formatting / packaging :**
   a. As the TCP/IP network layer protocol, IP accepts data from the transport layer protocols UDP and TCP.
   b. It then encapsulates this data into an IP datagram using a special format prior to transmission.
3. **Fragmentation and reassembly :**
   a. IP datagrams are passed down to the data link layer for transmission on the local network.
   b. However, the maximum frame size of each physical/data link network using IP may be different.
   c. For this reason, IP includes the ability to fragment IP datagrams into pieces so that they can each be carried on the local network.
   d. The receiving device uses the reassembly function to recreate the whole IP datagram again.

PART-2

Routing Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.4. **Define routing protocols.**

Answer

1. A routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.

2. Routers perform the traffic directing functions on the Internet, data packets are forwarded through the networks of the internet from router to router until they reach their destination computer.
3. Routing algorithms determine the specific choice of route. Each router has a prior knowledge only of networks attached to it directly.
4. A routing protocol shares this information first among immediate neighbours, and then throughout the network. This way, routers gain knowledge of the topology of the network.
5. The ability of routing protocols to dynamically adjust to changing conditions such as disabled data lines and computers and route data around obstructions is what gives the Internet its survivability and reliability.
6. The specific characteristics of routing protocols include :

i. The manner in which they avoid routing loops.
ii. The manner in which they select preferred routes, using information about hop costs.

Que 5.5. **What are the types of routing protocols ?**

Answer

Various types of routing protocols are :

1. **Routing Information Protocols (RIP) :**
   a. RIP is dynamic routing protocol which uses hop count as a routing metric to find best path between the source and destination network.
   b. RIP (Routing Information Protocol) is a forceful protocol type used in local area network and wide area network.
   c. RIP is categorized as an interior gateway protocol within the use of distance vector algorithm.
   d. It prevents routing loops by implementing a limit on the number of hops allowed in the path.
2. **Interior Gateway Routing Protocol (IGRP) :**
   a. It is distance vector Interior Gateway Routing Protocol (IGRP).
   b. It is used by router to exchange routing data within an independent system.
   c. Interior gateway routing protocol created in part to defeat the confines of RIP in large networks.
   d. It maintains multiple metrics for each route as well as reliability, delay load, and bandwidth.
   e. It measured in classful routing protocol, but it is less popular because of wasteful of IP address space.

3. **Open Shortest Path first (OSPF) :**
   a. Open Shortest Path First (OSPF) is an active routing protocol used in internet protocol.
   b. It is a link state routing protocol and includes into the group of interior gateway protocol.
   c. Open Shortest Path First (OSPF) operates inside a distinct autonomous system.
   d. The Open Shortest Path First (OSPF) is used in the network of big business companies.
4. **Exterior Gateway Protocol (EGP) :**
   a. The absolute routing protocol for internet is exterior gateway protocol.
   b. EGP (Exterior Gateway Protocol) is a protocol for exchanging routing table information between two neighbour gateway hosts.
   c. The Exterior Gateway Protocol (EGP) is unlike distance vector and path vector protocol.
5. **Enhanced Interior Gateway Routing Protocol (EIGRP) :**
   a. Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing that is used in a computer network for automating routing decisions and configuration.
   b. It works on network layer protocol of OSI model and uses the protocol number 88.
6. **Border Gateway Protocol (BGP) :** Refer Q. 5.1, Page 5–2W, Unit-5.
7. **Intermediate System-to-Intermediate System (IS-IS) :**
   a. Intermediate System-to-Intermediate System (IS-IS) is a protocol used by network devices to determine the best packet switched network route for data through.
   b. It is an interior gateway protocol designed for use within an administrative network.

Que 5.6. **Discuss the advantages and disadvantages of different routing protocols.**

Answer

Advantages of RIP :

1. Easy to configure and use.
2. Supported by all routers.
3. Support load balancing.

Disadvantages of RIP :

1. Limited to a hop count of 15 *i.e.*, it can transmit packet through 15 routers only.
2. Does not support a Variable-Length Subnet Mask (VLSM), which means that it sends routing updates based only on a fixed-length subnet mask (FLSM) or routes that fall on classful boundaries.
3. Converges slowly, especially on large networks.
4. Does not have knowledge of the bandwidth of a link.
5. Does not support multiple paths for the same route.
6. Routing updates can require significant bandwidth, as the entire routing table is sent when a link's status changes.
7. Prone to routing loops.

Advantages of IGRP :

1. Easy to configure and use.
2. Uses the delay, bandwidth, reliability, and load of a link as its metric. This makes it very accurate in selecting the proper route.

Disadvantages of IGRP :

1. It is not an Internet standard, all routers must be from Cisco Systems.
2. Converges slowly, slower than RIP.
3. Does not support VLSM.
4. Prone to routing loops.

Advantage of EIGRP :

1. It provides very quick convergence and a loop-free network.
2. It supports different version of IP.
3. It requires less CPU than OSPF.
4. It requires little bandwidth for routing updates.
5. It supports VLSM.

Disadvantages of EIGRP :

1. It is not an Internet standard, all routers must be from Cisco Systems.

Advantages of OSPF :

1. It converges quickly, compared to a distance vector protocol.
2. Its routing update packets are small, as the entire routing table is not sent.
3. It is not prone to routing loops.
4. It scales very well to large networks.
5. It recognizes the bandwidth of a link, taking this into account in link selection.
6. It supports VLSM.

7. It supports a long list of optional features that many of the other protocols do not support.

Disadvantages of OSPF V2 :

1. More complex to configure and understand than a distance vector protocol.

PART-3

DNS Revisited, Summary of Weakness of Internet Security.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.7. What do you mean by DNS ? Explain DNS rebinding attack.

Answer

DNS : Refer Q. 4.38, Page 4–29W, Unit-4.

DNS rebinding attack :

1. DNS rebinding is a form of computer attack.
2. In this attack, a malicious web page causes visitors to run a client-side script that attacks machines elsewhere on the network.
3. In this attacks, the same-origin policy prevents this from happening, client-side scripts are only allowed to access content on the same host that served the script.
4. Comparing domain names is an essential part of enforcing this policy, so DNS rebinding circumvents this protection by misusing the Domain Name System (DNS).
5. This attack can be used to breach a private network by causing the victim's web browser to access computers at private IP addresses and return the results to the attacker.
6. It can also be employed to use the victim machine for spamming, distributed denial-of-service attacks, or other malicious activities.

Que 5.8. How DNS rebinding work ?

Answer

DNS rebinding works as :

1. The attacker registers a domain (such as attacker.com) and delegates it to a DNS server that is under the attacker's control.

2. The server is configured to respond with a very short Time-To-Live (TTL) record, preventing the DNS response from being cached. When the victim browses to the malicious domain, the attacker's DNS server first responds with the IP address of a server hosting the malicious client-side code.
3. For instance, they could point the victim's browser to a website that contains malicious JavaScript or Flash scripts that are intended to execute on the victim's computer.
4. The malicious client-side code makes additional accesses to the original domain name (such as attacker.com).
5. These are permitted by the same-origin policy. However, when the victim's browser runs the script it makes a new DNS request for the domain, and the attacker replies with a new IP address.
6. For instance, they could reply with an internal IP address or the IP address of a target somewhere else on the Internet.

Que 5.9. Discuss the features of DNS rebinding attack.

Answer

Features of DNS rebinding attacks :

1. Custom DNS server that allows rebinding the DNS name and IP address of the attacker's web server to the target victim machine's address.
2. HTTP server serves HTML pages and JavaScript code to targeted users and to manage the attacks.
3. Several sample attack payloads, ranging from grabbing the home page of a target application to performing remote code execution. These payloads can be easily adapted to perform new and custom attacks.
4. Supports concurrent users.
5. Provides several DNS rebinding strategies, including sequential mapping from the attacker to the target IP address and random mapping, to minimize the impact of IDS/IPS interfering with the attack.
6. A number of technical controls to maximize the reliability and speed of attacks :
   a. Disabling HTTP keep alive, caching, DNS prefetching.
   b. Aggressive DNS response TTLs.
7. Ability to allocate HTTP servers at startup or dynamically thereafter :
   a. A convenience feature to avoid restarting singularity to listen on a different HTTP port.
   b. To lay the ground work to attack vulnerable ports discovered after a scan.

Que 5.10. **How can we prevent DNS rebinding attack ?**

Answer

1. DNS rebinding attacks can be prevented by validating the Host HTTP header on the server-side to only allow a set of whitelisted values.
2. For services listening on the loopback interface, this set of whitelisted host values should only contain localhost and all reserved numeric addresses for the loopback interface, including 127.0.0.1.
3. For instance, let's say that a service is listening on address 127.0.0.1, TCP port 3000. Then, the service should check that all HTTP request Host header values strictly contain "127.0.0.1 : 3000" and/or "localhost : 3000".
4. If the host header contains anything else, then the request should be denied.
5. Depending on the application deployment model, we may have to whitelist other or additional addresses such as 127.0.0.2, another reserved numeric address for the loopback interface.
6. For services exposed on the network (and for any services in general), authentication should be required to prevent unauthorized access.
7. Filtering DNS responses containing private, link-local or loopback addresses, both for IPv4 and IPv6, should not be relied upon as a primary defense mechanism against DNS rebinding attacks.
8. Singularity can bypass some filters in certain conditions, such as responding with a localhost record when targeting an application via the Google Chrome browser.

Que 5.11. **Explain key management protocol.**

Answer

1. Key management protocol refers to the collection of processes used for the generation, storage, installation, transcription, recording, change, disposition, and control of keys that are used in cryptography.
2. It is essential for secure ongoing operation of any cryptosystem.
3. The various functions of key management protocol are :
   a. **Generation :** This process involves the selection of a key that is used for encrypting and decrypting the messages.
   b. **Distribution :** This process involves all the efforts made in carrying the key from the point where it is generated to the point where it is to be used.
   c. **Installation :** This process involves getting the key into the storage of the device or the process that needs to use this key.

   d. **Storage :** This process involves maintaining the confidentiality of stored or installed keys while preserving the integrity of the storage mechanism.
   e. **Change :** This process involves ending with the use of the key and starting with the use of another key.
   f. **Control :** This process refers to the ability to implement a directing influence over the content and use of the key.

Que 5.12. **What are the advantages and disadvantages of key management protocol ?**

Answer

Advantages :

1. In key management protocol, less than $N - 1$ keys are stored.
2. It is scalable.

Disadvantages :

1. It lacks authentication process and does not clearly define any process for revoking or refreshing keys.
2. The dynamic handshaking process prevents any form of data aggregation.
3. No support for collaborative operations.
4. No node is guaranteed to have common key with all of its neighbours there is a chance that some nodes are unreachable.
5. Fails to satisfy security requirement authentication and operational requirement accessibility.

Que 5.13. **What are the security and operational requirements for key management protocol ?**

Answer

Security and operational requirements for key management protocol :

1. **Confidentiality :** Nodes should not reveal data to any unintended recipients.
2. **Integrity :** Data should not be changed between transmissions due to environment or malicious activity.
3. **Data freshness :** Old data should not be used as new.
4. **Authentication :** Data used in decision making process should originate from correct source.
5. **Robustness :** When some nodes are compromised, the entire network should not be compromised.

6. **Self-organization :** Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).
7. **Availability :** Network should not fail frequently.
8. **Time synchronization :** These protocols should not be manipulated to produce incorrect data.
9. **Secure localization :** Nodes should be able to accurately and securely acquire location information.
10. **Accessibility :** Intermediate nodes should be able to perform data aggregation by combining data from different nodes.

Que 5.14. **Write a short note on VPN and tunnel mode.**

Answer

Virtual Private Network (VPN) :

1. A Virtual Private Network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
2. It is a way to extend a private network using a public network such as internet.
3. The name only suggests that it is Virtual private network *i.e.*, user can be the part of local network sitting at a remote location.
4. It makes use of tunneling protocols to establish a secure connection.

Tunnel mode :

1. In IPSec tunnel mode, the original IP packet (IP header and the Data payload) is encapsulated within another packet.
2. In IPSec tunnel mode, the original IP Datagram is encapsulated with an Authentication Header (AH) (provides no confidentiality by encryption) or Encapsulating Security Protocol (ESP) (provides encryption) header and an additional IP header.
3. The traffic between the two VPN Gateways appears to be from the two gateways (in a new IP datagram), with the original IP datagram is encrypted (in case of ESP) inside IPSec packet.

PART-4

Link Layer Connectivity and TCP/IP Connectivity, Packet Filtering Firewall, Intrusion Detection.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.15. **Discuss link layer connection in TCP/IP model.**

Answer

1. The link layer in the TCP/IP model is a descriptive field networking protocols that operate only on the local network segment (link) that a host is connected to. Such protocol packets are not routed to other networks.
2. The link layer includes the protocols that define communication between local (on-link) network nodes which fulfill the purpose of maintaining link states between the local nodes, such as the local network topology, and that usually use protocols that are based on the framing of packets specific to the link types.
3. The core protocols specified by the Internet Engineering Task Force (IETF) in this layer are the Address Resolution Protocol (ARP), the Reverse Address Resolution Protocol (RARP), and the Neighbour Discovery Protocol (NDP), which is a facility delivering similar functionality as ARP for IPv6.
4. The link layer of the TCP/IP model is often compared directly with the combination of the data link layer and the physical layer in the Open Systems Interconnection (OSI) protocol stack. Although they are congruent to some degree in technical coverage of protocols, they are not identical.
5. In general, direct or strict comparisons should be avoided, because the layering in TCP/IP is not a principal design criterion and in general is considered to be harmful.

Que 5.16. **Write short note on firewall.**

Answer

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
2. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
3. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

4. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
5. A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Que 5.17. What is packet filtering firewall ? Explain its advantage and disadvantage.

Answer

Packet filtering firewall :

1. Packet filtering firewall is a technique used to control network access by monitoring outgoing and incoming packets.
2. Packet filtering firewall allows packet to pass or halt based on the source and destination Internet Protocol (IP) address, Protocols and ports.

Advantages :

1. They are simple, since a single rule is enough to indicate whether to allow or deny the packet.
2. They are transparent to the users *i.e.*, the users need not know the existence of packet filters.
3. They operate at a fast speed as compared to other techniques.
4. The client computers need not be configured specially while implementing packet-filtering firewalls.
5. They protect the IP addresses of internal hosts from the outside network.

Disadvantages :

1. They are unable to inspect the application layer data in the packets and thus, cannot restrict access to FTP services.
2. It is a difficult task to set up the packet-filtering rules correctly.
3. They lack support for authentication and have no alert mechanisms.
4. Being stateless in nature, they are not well suited to application layer protocols.

Que 5.18. Write short note on telnet.

Answer

1. Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers.
2. Through Telnet, an administrator or another user can access someone else's computer remotely.

3. With Telnet, we log on as a regular user with whatever privileges we may have been granted to the specific application and data on that computer.
4. At the Telnet client, a character that is typed on the keyboard is not displayed on the monitor, but, instead, is encoded as an ASCII character and transmitted to a remote Telnet server.
5. At the server, the ASCII character is interpreted as if a user had typed the character on the keyboard of the remote machine. If the keystroke results in any output, this output is encoded as (ASCII) text and sent to the Telnet client, which displays it on its monitor.
6. The output can be just the (echo of the) typed character or it can be the output of a command that was executed at the remote Telnet server.

Que 5.19. Explain briefly fragmentation at network layer.

Answer

1. Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held a frame *i.e.*, its Maximum Transmission Unit (MTU).
2. The network layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.
3. It is done by network layer at the destination side and is usually done at routers.
4. Source side does not require fragmentation due to segmentation by transport layer *i.e.*, the transport layer looks at datagram data limit and frame data limit and does segmentation in such a way that resulting data can easily fit in a frame without the need of fragmentation.
5. Receiver identifies the frame with the identification (16 bits) field in IP header. Each fragment of a frame has same identification number.
6. Receiver identifies sequence of frames using the fragment offset (13 bits) field in IP header.
7. An overhead at network layer is present due to extra header introduced due to fragmentation.

Que 5.20. Write short note on proxy firewall.

Answer

1. Proxy firewalls are the most secure types of firewalls, but this comes at the expense of speed and functionality, as they can limit which applications our network can support.
2. The enhanced security of a proxy firewall is because, information packets do not pass through a proxy. Instead the proxy acts as an intermediary, computers make a connection to the proxy which then initiates a new

network connection based on the request, effectively a mirror of the information transfer.

3. This prevents direct connections and packet transfer between either sides of the firewall, which makes it harder for intruders to discover where the location of the network is from packet information.
4. A firewall proxy provides internet access to computers on a network but is mostly deployed to provide safety or security by controlling the information going in and out of the network.
5. Firewall proxy servers filter, cache, log, and control requests coming from a client to keep the network secure and free of intruders and viruses.

Que 5.21. Write short note on intrusion detection.

Answer

1. Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.
2. An intrusion detection system is a software/hardware designed to detect unwanted attempts at accessing of target application or system.
3. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
4. Even if the detection is not sufficiently time to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and more quickly recovery can be achieved.
5. An effective intrusion detection system can serve as a deterrent to intrusions.
6. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Que 5.22. Briefly describe approaches for intrusion detection.

Answer

Two approaches for intrusion detection are :

1. **Statistical anomaly detection :** In this category, the behaviour of legitimate users is evaluated over some time interval. It can be achieved by two way :
   - **a. Threshold detection :**
     - i. In threshold detection, thresholds are defined for all users as a group, and the total numbers of events that are attributed to the user are measured against these threshold values.

     - ii. The number of events is assumed to round upto a number that is most likely to occur, and if the event count exceeds this number, then intrusion is said to have occurred.
   - **b. Profile-based detection :**
     - i. In profile-based detection, profiles for all users are created, and then matched with available statistical data to find out if any unwanted action has been performed.
     - ii. A user profile contains several parameters. Therefore, change in a single parameter is not a sign of alert.
2. **Rule-based detection :** In this category, certain rules are applied on the actions performed by the users. It is classified into two types :
   - **a. Anomaly-based detection :**
     - i. In anomaly-based detection, the usage patterns of users are collected, and certain rules are applied to check any deviation from the previous usage patterns.
     - ii. The collected patterns are defined by the set of rules that includes past behaviour patterns of users, programs, privileges, time-slots, terminals, etc.
     - iii. The current behaviour patterns of the user are matched with the defined set of rules to check whether there is any deviation in the patterns.
   - **b. Penetration identification :**
     - i. In penetration identification, an expert system is maintained that looks for any unwanted attempts.
     - ii. This system also contains rules that are used to identify the suspicious behaviour and penetrations that can exploit known weaknesses.

☺☺☺

1 UNIT

Introduction (2 Marks Questions)

1.1. What do you understand by computer security ?

Ans. Computer security (cyber security or IT security) is the protection of information systems from theft or disruption.

1.2. What are the problems related with computer security ?

Ans. **Problems related with computer security are :**

1. Phishing
2. Vishing
3. Smishing
4. Pharming

1.3. What are the advantages and disadvantages of computer security ?

Ans. **Advantages :**

i. Protection from malicious attacks on our network.
ii. Prevents users from unauthorized access to the network.

Disadvantages :

i. Strict regulations.
ii. Difficult to work with non-technical users.

1.4. What are various security mechanisms ?

Ans. **Various security mechanisms to provide security are :**

1. Encipherment
2. Digital integrity
3. Digital signature

1.5. Define the term security policy.

Ans. Security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situation when they do occur.

1.6. What is not considered in security system centric design ?

Ans. Agreement is not considered in security system centric design.

1.7. Where did storm botnet is used ?

Ans. Storm botnet is used in spamming.

1.8. How computer vulnerabilities and exploits database are maintained ?

Ans. Computer vulnerabilities and exploits database are maintained by MITRE corporation.

1.9. What are various computer security attacks ?

Ans. **Various computer security attacks are :**

i. Malware
ii. Macro virus
iii. File infector
iv. Boot record infector
v. Worm
vi. Trojan

1.10. Define vulnerabilities.

Ans. Vulnerability is a cyber-security term that refers to a flaw in a system or refers to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

1.11. Name the software whose vulnerability is exploited the most.

Ans. Android is the software whose vulnerability is exploited the most.

1.12. What is a buffer ?

Ans. A buffer is a temporary area for data storage. When more data gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.

1.13. Define buffer overflow attack.

Ans. Buffer-overflow attack is the overflow attack where extra data holds specific instructions for actions intended by a hacker or malicious user.

1.14. How can we prevent buffer overflow attack ?

Ans. **We can prevent buffer overflow attack using :**

1. Non-executable stack
2. Static analysis
3. Dynamic run-time protection
4. Use safer versions of functions

1.15. What is integer overflow attack ?

Ans. An integer overflow is an attack that occurs when an arithmetic operation attempts to create a numeric value that is outside of the range.

1.16. How can we prevent integer overflow attack ?

Ans: Integer overflow attack can be prevented through :

1. Avoidance
2. Handling
3. Propagation

1.17. Define hijacking.

Ans: Hijacking is a type of network security attack in which the attacker takes control of a communication.

1.18. How can we control hijacking attacks ?

Ans: Hijacking attack is controlled through :

1. Platform defense
2. Run-time defense
3. Heap protection

1.19. Name the techniques used in heap spray attacks.

Ans: Techniques used in heap spray attacks are:

1. Heap spraying.
2. Vulnerable buffer placement.

1.20. How can we prevent heap spray control hijacking ?

Ans: We can prevent heap spray control hijacking :

1. Protect heap function pointer.
2. Better browser architecture.

1.21. What was the percentage increase in zero-day vulnerabilities in the year 2015 ?

Ans: 50 % is the percentage increase in zero-day vulnerability in the year 2015.

1.22. Name the buffer overflow which is common among attackers.

Ans: Stack-based buffer overflow is most common among attackers.

1.23. Which goal is not considered in the security system design ?

Ans: Vulnerability is not considered in the security system design.

1.24. Which thing is important in design of secure system ?

Ans: Two things are important in designing secure system :

i. Assessing vulnerability.
ii. Changing or updating system according to vulnerability.

1.25. Name the programming languages which are having buffer-overflow error.

Ans: C, C++ are the programming language having buffer-overflow error.

1.26. What is the price for selling windows as vulnerability in black market ?

Ans: $60K-$100K is the price for selling windows as vulnerability in black market.

1.27. What is the price for selling firefox or safari browser vulnerability in the black market ?

Ans: $60K-$150K is the price for selling firefox or safari browser vulnerability in the black market.

1.28. What is the range of port number used by client port ?

Ans: Client port uses the port number between 1024 and 16383.

☺☺☺

2 UNIT

Confidentiality Policies (2 Marks Questions)

2.1. Define confidentiality policy.

Ans. A confidentiality policy is intended to protect secrets and prevent unauthorized disclosure of information. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

2.2. Name the security model used in confidentiality policy.

Ans. Security model used in confidentiality policy is Bell-LaPadula confidentiality model.

2.3. Define Bell-LaPadula confidentiality model.

Ans. The Bell-LaPadula confidentiality model is a state machine-based multi-level security policy. This model was originally designed for military applications.

2.4. Define the term access control.

Ans. Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.

2.5. What are the types of access control ?

Ans. **Following are the types of access control :**

1. Discretionary Access Control (DAC)
2. Mandatory Access Control (MAC)

2.6. Define DAC.

Ans. Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner.

2.7. What are the advantages of DAC ?

Ans. **Following are the advantages of DAC :**

1. User may transfer object ownership to another users.
2. User may determine the access type of other users.

2.8. What are the disadvantages of DAC ?

Ans. **Following are the disadvantages of DAC :**

1. Inherent vulnerabilities (Trojan horse).
2. Access control list maintenance.
3. Grant and revoke permissions maintenance.

2.9. What are the issues related with DAC ?

Ans. **Issues related with DAC are :**

1. Difficult to enforce a system-wide security policy *i.e.*, a user can leak classified documents to a unclassified users.
2. Only support coarse-grained privileges.
3. Unbounded privilege escalation.

2.10. What is MAC ?

Ans. Mandatory access control is a type of access control by which the operating system constraints the ability of a subject to access or perform some sort of operation on an object.

2.11. What are the advantages of MAC ?

Ans. **Advantages of MAC are :**

1. It ensures a high degree of protection, prevent illegal flow of information.
2. It is suitable for military and high security types of applications.

2.12. What are the disadvantages of MAC ?

Ans. **Disadvantages of MAC are :**

1. It requires strict classification of subjects and objects.
2. It is applicable to few environments.

2.13. Define confinement problem.

Ans. The confinement problem is the problem of preventing a server from leaking information that the user of the service considers confidential. The confinement problem deals with preventing a process from taking disallowed actions.

2.14. What are the types of Unix user ID ?

Ans. **Types of Unix user ID are :**

1. Real user ID
2. Effective user ID
3. Saved user ID

2.15. Define real user ID.

Ans. Real user ID defines that which files the process has access to. It is account of owner of the process.

2.16. Define effective user ID.

Ans. Effective user ID is same as real user ID, but sometimes it is changed to enable a non-privileged user to access files that can only be accessed by root.

2.17. Define saved user ID.

Ans. Saved user ID is a user ID used when a process is running with elevated privileges (generally root) needs to do some under-privileged work, this can be achieved by temporarily switching to non-privileged account.

2.18. What are confinement techniques ?

Ans. Following are the various confinement techniques :

1. Chroot (change root)
2. Jailkits
3. FreeBSD jail
4. System call interposition

2.19. What are the types of VM based isolation ?

Ans. Following are the types of Virtual Machine based isolation :

1. Process virtual machines
2. System virtual machines (Hypervisor virtual machines)
3. Hosted virtual machines
4. Hardware virtual machine

2.20. Define rootkit.

Ans. A rootkit is a computer program designed to provide continued privileged access to a computer while hiding its presence. Rootkit is a collection of tools that enabled administrator-level access to a computer or network.

2.21. What is the purpose of rootkits ?

Ans. The purpose of a rootkit is for a malware to give its owner, a permanent, hidden remote access to our computer. To avoid detection, they tamper with the system to conceal the presence of the malware and its activities.

2.22. What is intrusion detection system ?

Ans. An Intrusion Detection System (IDS) is a network security technology built for detecting vulnerability exploits against a target application or computer.

2.23. What are the types of intrusion detection system ?

Ans. Following are the types of intrusion detection system :

1. Network Intrusion Detection System (NIDS)
2. Host-based Intrusion Detection System (HIDS)
3. Perimeter Intrusion Detection System (PIDS)
4. VM based Intrusion Detection System (VMIDS)

2.24. What are the components of intrusion detection system?

Ans. Components of intrusion detection system are :

1. Packet decoder
2. Preprocessor
3. Detection engine
4. Logging and alerting system
5. Output modules

2.25. What are the difficulties in anomaly detection ?

Ans. Difficulties in anomaly detection are :

i. Lack of training data
ii. Data drift
iii. False identification is very costly.

2.26. Which is not the component of snort ?

Ans. Hypervisor is not the component of snort.

2.27. What are the features offered by snort ?

Ans. Features offered by snort are :

i. IDS
ii. Packet logger
iii. Shiffer

2.28. What are the disadvantages of snort ?

Ans. Disadvantages of snort are :

i. Snort spends 80 % of time doing string.
ii. Probability of detection is low.

☺☺☺

3 UNIT

Secure Architecture Principles Isolation and Leas (2 Marks Questions)

3.1. What do you understand by access control ?

Ans: Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

3.2. Define physical and logical access control.

Ans: **Physical access control :** Physical access control limits access to campuses, buildings, rooms and physical IT assets.
Logical access control : Logical access control limits connections to computer networks, system files and data.

3.3. What are the types of access control ?

Ans: **Types of access control are :**
1. Mandatory Access Control (MAC)
2. Discretionary Access Control (DAC)
3. Role-Based Access Control (RBAC)
4. Rule-Based Access Control
5. Attribute-Based Access Control (ABAC)

3.4. What are the best practices for access control ?

Ans: **Access control practices are :**
1. It denies access to systems by undefined users.
2. It limits and monitors the usage of administrator.
3. It suspends or delay access capability.
4. It removes obsolete user accounts as soon as the user leaves the company.
5. It suspends inactive accounts after 30 to 60 days.

3.5. Discuss security principle for access control.

Ans: **Security principles for access control are :**
1. Identification
2. Authentication
3. Authorization
4. Non-repudiation

3.6. Define the term identification, authentication, authorization, non-repudiation.

Ans: **Identification :** Identification describes a method of ensuring that a subject is the entity it claims to be.
Authentication : Authentication is the method of proving the subjects identity.
Authorization : Authorization is the method of controlling the access of objects by the subject.
Non-repudiation : Non-repudiation is the assurance that someone cannot deny something.

3.7. What are the various issues in access control ?

Ans: **Various issues in access control are :**
1. Appropriate role-based access
2. Poor password management
3. Poor user education

3.8. What do you understand by browser isolation ?

Ans: Browser isolation is a cyber security model for web browsing that can be used to physically separate an internet user's browsing activity from their local machine, network and infrastructure.

3.9. List some browser isolation vendors.

Ans: **Browser isolation vendors include :**
1. Apozy
2. Authentic
3. Ericom
4. Menlo Security

3.10. What is threat modelling ?

Ans: Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining counter measures to prevent, or mitigate the effects of, threats to the system.

3.11. What are the elements of threat modelling ?

Ans: **Three main elements of threat modelling are :**
1. Assets
2. Threats
3. Vulnerabilities

3.12. What are the layers used in threat modelling.

Ans: **Layers used in threat modelling are :**
1. Network layer
2. Host layer
3. Application layer

3.13. What are the steps used for threat modelling ?

Ans. Steps used for threat modelling are :

1. Identify the assets
2. Describe the architecture
3. Break down the applications
4. Identify the threats
5. Document and classify the threats
6. Rate the threats

3.14. What are major web server threats ?

Ans. Major web server threats are :

1. Injection flaws
2. Broken authentication
3. Sensitive data exposure
4. Cross-Site Request Forgery (CSRF)
5. Man in the Middle Attack (MITM)
6. Phishing attack

3.15. What are the methods of CSRF mitigation ?

Ans. Methods of CSRF mitigation are :

1. Logging off web applications when not in use.
2. Securing usernames and passwords.
3. Not allowing browsers to remember passwords.
4. Avoiding simultaneously browsing while logged into an application.

3.16. How can we secure development of software ?

Ans. Secure software can be developed by :

1. Sanitize inputs at the client side and server side.
2. Encode request/response.
3. Use HTTPS for domain entries.
4. Use only current encryption and hashing algorithms.
5. Do not allow for directory listing.

3.17. What is the cost of launching Denial of service attack on a website ?

Ans. $100/day is the cost of launching Denial of service attack on a website.

3.18. Web security mechanism relies on which protocol.

Ans. Web security mechanism relies on DNS, TCP/IP, BGP protocols.

3.19. How to avoid limitation in threat models ?

Ans. We can avoid limitation in threat models by :

1. Making more explicit and formalized threat models to understand possible weaknesses.
2. Making simpler and more general threat models.
3. Making less assumption to design a better threat model.

3.20. For what IKE creates Security Association (SAs).

Ans. IKE (Internet Key Exchange) creates SAs for IPsec.

3.21. What is the reward amount for Pwn2Own competition ?

Ans. $ 1500 is the reward amount for Pwn2Own competition.

3.22. What is penetration testing ?

Ans. Penetration testing is an internal inspection of applications and operating systems for security flaws. It is an authorized simulated cyber-attack on a computer system, performed to evaluate the security of the system.

☺☺☺

4 UNIT

Basic Cryptography (2 Marks Questions)

4.1. What do you mean by cryptography ?

Ans. Cryptography is defined as the conversion of data into a scrambled code that can be decrypted and sent across a public or private network. It is the science and art of creating secret codes.

4.2. What are the different factors on which cryptography depends ?

Ans. **Following are the different factors on which cryptography depends :**

1. Plaintext
2. Encryption algorithm
3. Ciphertext
4. Decryption algorithm

4.3. What are the different security attacks ?

Ans. **Following are the two types of security attacks :**

1. **Passive attacks :** Passive attacks are those attacks where the attacker indulges in monitoring of data transmission.
2. **Active attacks :** Active attacks are those attacks where the attackers attempt to make change to data.

4.4. Distinguish between an active and passive attack.

Ans.

S. No.	Active attack	Passive attack
1.	Access and modify information.	Access information.
2.	System is harmed.	No harm to system.
3.	Easy to detect than prevent.	Difficult to detect than prevent.
4.	Threat to integrity, availability.	Threat to confidentiality.

4.5. What are the requirements for the use of a public key certificates scheme ?

Ans. **Requirements for the use of a public key certificates scheme are :**

1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not fake.
3. Only the certificate authority can create and update certificates.
4. Any participant can verify the currency of the certificate.

4.6. Give the ingredients of public key encryption scheme.

Ans. **Ingredients of public key encryption scheme are :**

i. Plain text
ii. Encryption algorithm
iii. Public and private keys
iv. Ciphertext
v. Decryption algorithm

4.7. What do you mean by RSA ?

Ans. RSA is asymmetric cryptography algorithm where the encryption key is public and it is different from the decryption key which is kept secret.

4.8. What requirements should a digital signature scheme satisfy ?

Ans. **Following are the requirements for digital signature are :**

1. The signature must be a bit pattern that depends on the message being signed.
2. The signature must use some information unique to the sender, to prevent both forgery and denial.
3. Production of digital signature must be easy.

4.9. Explain briefly the two different approaches of digital signature.

Ans. **Two different approaches of digital signature are :**

1. **RSA :** RSA is used for encryption and decryption.
2. **DSA :** DSA (Digital Signature Algorithm) is used for signing/ verification.

4.10. Define hash algorithm.

Ans. A hash algorithm is a function that converts a data string of variable length into a numeric output string of fixed length. Hash algorithms are designed to be collision-resistant, hence there is a very low probability that the same string would be created for different data.

4.11. Write down the security services provided by a digital signature.

Ans: Security services provided by digital signature are :
i. Message authentication
ii. Message integrity
iii. Non-repudiation
iv. Confidentiality

4.12. What are the drawbacks of digital signature ?
Ans: Drawbacks of digital signature are :
i. Association of digital signature and trusted time stamping.
ii. Non-repudiation.

4.13. Define symmetric key cryptography.
Ans: Symmetric key cryptography is a shared secret key between two parties. It is more efficient for enciphering large messages. Its strength rests with the key distribution technique.

4.14. Define S/ MIME.
Ans: S/MIME is a standard for public key encryption and signing of MIME data. S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the RSA encryption system.

4.15. What do you mean by mail security ?
Ans: Mail security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.

4.16. Write down the different ways the public key can be distributed.
Ans: Different ways the public key can distributed are :
i. Public announcement
ii. Publically available directory
iii. Public key authority

4.17 What do you understand by Pretty Good Privacy algorithm ?
Ans: PGP is an encryption algorithm that provides cryptographic privacy and authentication for data communication.

4.18. Give the services provided by PGP.
Ans: Service provided by PGP :
i. Authentication
ii. Confidentiality
iii. Compression
iv. Segmentation and reassembly
v. Signature component
vi. Message component

4.19. Differentiate between public key and private key.
Ans:

S. No.	Public key	Private key
1.	It is use to encrypt the message.	It is use to decrypt the message.
2.	Distributed freely and openly.	Protected by owner.
3.	It is used to verify signatures.	It is used to sign signatures.

4.20. What is IP security ?
Ans: IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network layer.

4.21. Explain intrusion detection.
Ans: Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access. An intrusion detection system is a software/hardware designed to detect unwanted attempts at accessing of target application or system.

4.22. What are the functional areas of IPsec ?
Ans: Functional areas of IPSec are :
i. Authentication
ii. Confidentiality
iii. Key management

4.23. What are the services provided by IPSec ?
Ans: Services provided by IPSec are :
i. Access control
ii. Connectionless integrity
iii. Data origin authentication
iv. Confidentiality
v. Limited traffic flow confidentiality

4.24. Describe briefly the security policy database.
Ans: Security policy database specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or a security gateway.

4.25. Give a list of main entities in SET.
Ans: There are four main entities in SET :
i. Card holder (customer)
ii. Merchant (web server)
iii. Merchant's Bank (payment gateway, acquirer)
iv. Issuer (cardholder's bank)

4.26. Describe briefly the purpose of SET protocol.

Ans: Purpose of SET protocol :

i. Provide confidentiality of payment and ordering information.
ii. It facilitates and encourages interoperability among software and network providers.
iii. It ensures the integrity of all transmitted data.

4.27. What are the major transactions supported by SET ?

Ans: The major transactions supported by SET are purchase request, payment authorization and payment capture.

4.28. What is the function of DNS rebinding defense ?

Ans: Function of DNS rebinding defense are :

i. Browser mitigation
ii. Server-side defenses
iii. Firewall defenses

4.29. What is VPNs ?

Ans: VPNs is a remote access client connection.

4.30. What are string library functions used for buffer ?

Ans: String library functions used for buffer :

i. gets (char * str)
ii. strcat (char destination, const char source)
iii. strcpy (char destination, const char source)

4.31. What is the other name of bug bounty program ?

Ans: Google vulnerability program is the other name for bug bounty program.

4.32. What is ransomware ?

Ans: It is a form of malware that encrypts the whole hard drive of the computer, essentially locking the user out of the entire system.

4.33. What can be poisoned if it is having an erroneous entry where the invader gets to organize the DNS server and change different kinds of information on it ?

Ans: Domain name is poisoned if it is having an erroneous entry where the invader gets to organize the DNS server and change different kinds of information on it.

4.34. What is silent banker ?

Ans: It is a Trojan horse. It records keystrokes, captures screens and steals confidential banking credentials and sends them to remote attacker.

4.35. What is target attack ?

Ans: It is an example of server-side attack. More than 140 million credit card information was stolen in the attack happened in 2011.

4.36. Name the protocol defined by IPSec.

Ans: Protocols defined by IPSec are :

1. Authentication Header (AH)
2. Encapsulating Security Payload (ESP)

4.37. What do IPSec do in tunnel mode ?

Ans: IPSec protects the entire IP packets in tunnel mode.

☺☺☺

5 UNIT

Internet Infrastructure (2 Marks Questions)

5.1. What is internet infrastructure ?

Ans. Internet infrastructure is a collective term for all hardware and software systems that constitute essential components in the operation of the Internet.

5.2. What are the components of network infrastructure ?

Ans. **Network infrastructure includes :**

1. Network hardware
2. Network software
3. Network services

5.3. What is routing ?

Ans. Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Routing is performed in many types of networks, including circuit-switched networks, such as the Public Switched Telephone Network (PSTN), and computer networks, such as the Internet.

5.4. What are the impacts of attack on router ?

Ans. **Impact of attacks on routers are :**

1. Traffic redirection
2. Traffic sent to a routing black hole
3. Router denial-of-service (DoS)
4. Routing protocol DoS
5. Unauthorized route prefix origination

5.5. What are the main functions of link layer ?

Ans. **The data link layer has three main functions :**

1. It handles problems that occur as a result of bit transmission errors.
2. It ensures data flows at a pace that does not overwhelm sending and receiving devices.
3. It permits the transmission of data to upper layer, the network layer, where it is addressed and routed.

5.6. What do you understand by TCP/IP ?

Ans. Transmission Control Protocol/Internet Protocol (TCP/IP) is the language a computer uses to access the internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the internet.

5.7. What is firewall ?

Ans. Firewall is a network device that isolates organization's internal network from larger outside network/Internet. It can be hardware, software, or combined system that prevents unauthorized access to or from internal network.

5.8. What are various types of firewall ?

Ans. **Types of firewall are :**

1. Packet filtering
2. Stateful packet filtering
3. Application level gateways (Proxy)

5.9. What is packet filtering ?

Ans. A firewall filters the IP packets. The IP headers of all the packets that enter or exit the network firewall are inspected. Firewall makes an explicit decision on each packet that enters as to whether to allow the packet or deny the packet.

5.10. What is application level gateway ?

Ans. Application level gateway is a firewall which is capable of inspecting application level protocols. This requires the firewall to understand certain specific application protocols.

5.11. Write disadvantages of packet filtering.

Ans. **Disadvantages of packet filtering are :**

1. The packet filtering rules tend to be hard to configure. We need a lot of expertise and proper strategy to configure it right.
2. Once it is configured, it is difficult to comprehensively test and verify whether it is working correctly or not.
3. It is a stateless machine. It does not remember the state of the previous packet. Stateless packet filters are vulnerable to attacks.

5.12. Write advantages of packet filtering.

Ans. **The main advantage of the packet filtering :**

1. A strategically placed packet filtering firewall can protect the entire network.
2. Packet filtering is available in routers.

5.13. At which layer packet filter firewall filters the packet.

Ans. Packet filter firewall filters packets at network layer.

5.14. What is the other name of stateful packet filtering ?

Ans. Stateful packet filtering is also known as dynamic packet filtering.

5.15. What is the full form of DNS ?

Ans. Domain Name System.

5.16. How does server handles requests for other domains ?

Ans. Server handles requests for other domains by contacting remote DNS server.

5.17. What are the basic issues in packet filtering ?

Ans. **The basic issues in packet filtering are :**

1. Stateful filtering
2. Encapsulation
3. Fragmentation

5.18. Name intrusion detection model.

Ans. **Intrusion detection model are :**

i. Misuse detection model
ii. Anomaly detection model

5.19. How does network layer firewall work ?

Ans. Network layer firewall works as packet filter.

5.20. What are the issues related with TCP/IP ?

Ans. **Issues related with TCP/IP are :**

i. Cache poisoning
ii. Rebinding
iii. Packet shifting

5.21. What is stuxnet ?

Ans. Stuxnet is a malicious computer worm.

5.22. Which protocol is designed to create security association both inbound and outbound ?

Ans. IKE (Internet Key Exchange) is designed to create inbound and outbound security association.

5.23. What is included in standard network defenses ?

Ans. Firewall and intrusion detection are included in standard network defenses.

5.24. What is the full form of CVE ?

Ans. Common vulnerability and exposures.

5.25. Which protocol is not used in operation of a VPN ?

Ans. YMUM.