**Reflective Questions**

**Lab 3**

**REFLECTIVE QUESTIONS – TASK 1**

1. List 4 examples of hash algorithms.

* MD5
* SHA-1
* SHA-256
* SHA-3

1. What is the issue with the MD5 algorithm?

* Collision Vulnerability: MD5 is prone to producing the same hash for different inputs, compromising its security.

**REFLECTIVE QUESTIONS – TASK 2**

1. Describe the functionality of hashing encryption compared to symmetric and asymmetric encryption.

* Symmetric vs. Hashing: Hashing is one-way and tests data integrity; symmetric encrypts and decrypts with the same key to provide confidentiality.
* Asymmetric vs. Hashing: Hashing verifies integrity, but asymmetric encrypts with one key and decrypts with another for secure communication.
* Symmetric vs. Asymmetric: Symmetric uses a single shared key for speed, but secure key sharing is required. For secure communication and key exchange, asymmetric employs key pairs.

**REFLECTIVE QUESTIONS – TASK 3**

1. What is the meaning of GPG?

* GNU Privacy Guard. It's free software that keeps communication secure by encrypting and authenticating data.

1. Using your own words, explain the difference between PGP and GnuPG.

* PGP is a program for secure data exchange that uses a combination of fast and safe encryption technologies. Originally exclusive. GnuPG: An open-source version of PGP, sometimes known as GPG. Both perform comparable functions, but GnuPG is free and adheres to open-source ideals.

**REFLECTIVE QUESTIONS – TASK 5**

1. Why cryptography is important in cybersecurity?

* Cryptography keeps information safe online by making it unreadable to the wrong people. It ensures data is kept private, and untampered, and confirms the identity of users.

1. Give one example of an application that applied cryptography in our daily life.

* Online banking uses encryption to keep your personal and financial information secure during transactions.

1. Describe an example of such an application in question 2 which relates to the objectives of cryptography.

* In online banking, encryption keeps your login and transaction details private and unaltered. This protects sensitive data from unauthorized access and tampering.

1. Describe 5 differences between symmetric and asymmetric encryption for cryptography.

|  |  |  |
| --- | --- | --- |
| **Symmetric** | **Differences** | **Asymmetric** |
| Uses 1 shared key | **Key Type** | Uses a pair of keys |
| Faster | **Speed** | Slower |
| Needs a secure way to share | **Key Distribution** | Public keys can shared freely |
| Requires less power | **Computational Resources** | Demands more resources |
| Efficient for many data | **Use Cases** | Used for secure communication and key exchange |

1. List 5 differences between cryptography and steganography.

* Objective:

Cryptography: Encrypts information to keep it safe.

Steganography: The concealment of the fact that information exists.

* Visibility:

Encrypted data is visible but unintelligible due to cryptography.

Steganography: The presence of secret data is concealed.

* Detection:

Cryptography: This is determined by the algorithm's strength.

Steganography is difficult to detect because it conceals data within other data.

* Useful Information:

Cryptography encrypts and decrypts data using keys.

Steganography: May or may not utilize keys; focuses on data concealment.

* Communication:

Cryptography: A method of protecting data during transmission.

Steganography: The concealment of data within other data, such as images or audio files.

**Lab 4**

***REFLECTION QUESTIONS TASK 1***

1. Explain what is defence in-depth and how it relates to host security.

* Defense in depth means using many layers of protection to keep a system safe. Host security, which is about protecting individual computers, involves steps like physical security, controlling network access, and using secure software practices. The idea is to make it hard for attackers by having multiple layers of defense.

1. Based on your understanding, explain why host security is important.

* Data Protection: It keeps sensitive information safe.
* System Availability: It prevents disruptions to computer services.
* Compliance: It ensures adherence to rules and regulations.
* Business Continuity: It helps a company keep running smoothly.
* Threat Prevention: It guards against various types of cyber threats.
* Lateral Movement Prevention: It stops attackers from moving easily within a network.

***REFLECTION QUESTIONS TASK 2***

1. Is there any security issue with the ping command? If so explain briefly.

No.

***REFLECTION QUESTIONS TASK 3***

1. Scanning can be done without proper consent. Why?

* Scanning can happen without proper permission because someone might do it without knowing they need permission, or, in some cases, with bad intentions to find weaknesses.

1. At your organization, is there any statement in the security policy related to scanning activity? Please state it here.

***REFLECTION QUESTIONS TASK 4***

1. Why security baseline is important to be applied to a particular host in the enterprise or any company?

* Keeps security consistent across all hosts.
* Reduces the risk of cyber attacks by addressing vulnerabilities.
* Helps meet industry standards and compliance requirements.
* Makes security management more efficient.
* Enables quick responses to emerging threats.

1. Explain 5 security techniques to properly secure a virtual host machine

* **Hypervisor Security**: Secure the virtualization software to prevent unauthorized access.
* **Network Segmentation**: Isolate virtual machines to limit potential security breaches.
* **Regular Patching**: Keep the virtual host and guest operating systems updated for security.
* **Virtual Machine Isolation**: Restrict unnecessary services and access for virtual machines.
* **Secure Virtual Disk Encryption**: Encrypt virtual machine disks to protect sensitive data.

1. Explain 5 ways to manage host security

* **Regular Audits**: Check and fix vulnerabilities on the host regularly.
* **Endpoint Protection**: Use antivirus and anti-malware tools to prevent malicious activities.
* **User Education**: Train users on security practices and how to recognize threats.
* **Incident Response Planning**: Have a plan to handle security incidents effectively.
* **Access Controls**: Limit user permissions and use strong authentication methods.

**Lab 5**

REFLECTION QUESTIONS - TASK 2

1. In your own words, explain ARP poisoning.

* ARP poisoning is a cyber-attack where an intruder sends fake messages to a local network, tricking devices into sending their data to the attacker. This allows them to intercept, modify, or block communications between devices on the network.

1. How can we prevent the ARP poisoning attack?

* Use detection tools, static ARP entries, network segmentation, ARP spoofing prevention protocols

1. Why do you think telnet is not a safe way to connect to a remote machine? What is the safer way to do it?

* Telnet exposes data, including login details, making it insecure for transmitting sensitive information. Use SSH for secure remote connections. It encrypts the entire session, protecting against unauthorized access and data interception.

REFLECTION QUESTIONS - TASK 3

1. Based on your understanding, what is network security and what are the basic objectives of network security?

* Network security means protecting computer networks from unauthorized access or harm. The main goals are keeping information safe, making sure data is accurate, and ensuring networks are available when needed.

1. Differentiate between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

* IDS watches for suspicious activity and raises alerts but doesn't actively block threats. IPS actively identifies and stops potential threats, going beyond just alerting.

1. Why Virtual Private Network (VPN) is important for network security?

* VPNs are crucial for security because they create a secure, encrypted connection over untrusted networks, like the internet, ensuring that data remains confidential.

1. In what situation you might want to install a Demilitarized Zone (DMZ) on your network?

* A DMZ is used when you want controlled access to services from the internet, like web servers. It adds security by separating these servers from the internal network.

1. What is the role of Network Address Translation (NAT) on a network?

* NAT hides internal device details by mapping private IP addresses to a single public IP address, improving security and providing some anonymity.

1. To apply and manage the security principle, you must understand how the network devices and technologies operate. Explain how the proxy server operates to provide security on the network.

* A proxy server acts as a middleman between users and the internet, enhancing security by filtering content, anonymizing traffic, caching for speed, logging user activities, controlling access, and inspecting encrypted traffic. Understanding these functions helps in effectively managing network security.

**Lab 6**

REFLECTION QUESTIONS

1. In your own words, explain about Common Vulnerability Scanning System (CVSS) and Common Vulnerability Enumeration (CVE).

* CVSS - It's a system for evaluating and rating the seriousness of security vulnerabilities in software. It helps organizations prioritize responses to threats by quantifying the risk of each vulnerability.
* CVE - This is a database of known information security vulnerabilities. Each entry has a unique identifier, allowing for standardized referencing and discussion of vulnerabilities across different security tools.

1. Explain the difference(s) between CVSS and CVE.

|  |  |  |
| --- | --- | --- |
| **Aspect** | **CVSS** | **CVE** |
| Purpose and Function | Framework for assessing and rating vulnerability severity. | Database of unique identifiers for known vulnerabilities. |
| Nature | Scoring system for assigning severity scores. | Identifier system for uniquely referencing vulnerabilities. |
| Output | Numerical score (Base Score) indicating severity. | Unique identifier (CVE ID) for each vulnerability. |
| Usage | Prioritizing responses based on severity scores. | Uniquely identifying and tracking vulnerabilities. |

1. How many severity levels are there in the CVSS version 3.0?

Low, Medium, High, Critical

1. Draw a table of CVSS3.0 severity levels and their base score range.

|  |  |
| --- | --- |
| **Severity Level** | **Base Score Range** |
| Low | 0.0 - 3.9 |
| Medium | 4.0 - 6.9 |
| High | 7.0 - 8.9 |
| Critical | 1. - 10.0 |

1. Observe the information provided at vuldb.com and answer the questions below:
2. List three (3) most recent vulnerabilities and their severities.

* CVE-2020-1472 (ZeroLogon)
* CVE-2021-44228 (Log4Shell)
* CVE-2022-22536 (ICMAD)

1. List three (3) latest available exploits.

* Improper Input Validation in Apache Log4j Logging Library: In 2022, this vulnerability was exploited to allow remote code execution. Organizations and individuals using this library were at risk of potential attacks.
* Vulnerability in Fortinet SSL VPNs (CVE-2018-13379): This particular vulnerability affected Fortinet SSL VPNs and was routinely exploited. It was mentioned as one of the top routinely exploited vulnerabilities in 2020.
* Various Vulnerabilities in Confluence Server (CVEs): Atlassian Confluence Server had multiple vulnerabilities in 2022 that were exploited. The specific CVEs were not mentioned, but it highlights the importance of regularly patching and updating software to protect against potential exploits.

1. List three (3) vulnerabilities in the current CVSS Top 5.

* Unitronics Vision Series PLC all insecure default initialization of resource
* Zyxel NAS326/NAS542 WSGI Server os command injection
* Zyxel NAS326/NAS542 HTTP POST Request show\_zysync\_server\_contents os command  
  injection

**Lab 3**

1. Hash Algorithms:
   * MD5, SHA-1, SHA-256, SHA-3
2. Issue with MD5:
   * Collision Vulnerability: Same hash for different inputs.
3. Hashing vs. Encryption:
   * Hashing: One-way, tests data integrity.
   * Symmetric Encryption: Uses a shared key for confidentiality.
   * Asymmetric Encryption: Uses key pairs for secure communication.
4. GPG vs. PGP:
   * GPG (GNU Privacy Guard): Free, open-source version of PGP.
5. Importance of Cryptography:
   * Keeps information secure online.
6. Cryptography Application:
   * Online banking for secure transactions.
7. Symmetric vs. Asymmetric Encryption:
   * Table of Differences (Key type, Speed, Key Distribution, Computational Resources, Use Cases).
8. Cryptography vs. Steganography:
   * Differences: Objective, Visibility, Detection, Useful Information, Communication.

**Lab 4**

1. Defense in Depth:
   * Multiple layers of protection for system safety.
2. Importance of Host Security:
   * Data Protection, System Availability, Compliance, Business Continuity, Threat Prevention, Lateral Movement Prevention.
3. Security Issue with Ping:
   * None.
4. Scanning Without Consent:
   * Can happen unknowingly or with malicious intent.
5. Security Baseline Importance:
   * Consistency, Risk Reduction, Compliance, Efficiency, Threat Response.
6. Secure Virtual Host Techniques:
   * Hypervisor Security, Network Segmentation, Regular Patching, VM Isolation, Secure Virtual Disk Encryption.
7. Host Security Management:
   * Regular Audits, Endpoint Protection, User Education, Incident Response Planning, and Access Controls.

**Lab 5**

1. ARP Poisoning:
   * Attack tricking devices into sending data to the attacker.
2. Preventing ARP Poisoning:
   * Use detection tools, static ARP entries, network segmentation, ARP spoofing prevention protocols.
3. Telnet Insecurity:
   * Exposes data; use SSH for secure remote connections.
4. Network Security Objectives:
   * Protecting networks from unauthorized access, ensuring data accuracy, maintaining network availability.
5. IDS vs. IPS:
   * IDS alerts, IPS actively identifies and stops threats.
6. VPN Importance:
   * Creates a secure, encrypted connection over untrusted networks.
7. DMZ Purpose:
   * Controlled access to services from the internet.
8. NAT Role:
   * Hides internal device details by mapping private IPs to a single public IP.

**Lab 6**

1. CVSS and CVE:
   * CVSS: Rates vulnerability severity; CVE: Database of vulnerabilities.
2. CVSS vs. CVE:
   * CVSS is a scoring system, while CVE is an identifier system.
3. CVSS Severity Levels (3.0):
   * Low, Medium, High, Critical.
4. CVSS3.0 Severity Levels and Base Score Range:
   * Low (0.0-3.9), Medium (4.0-6.9), High (7.0-8.9), Critical (9.0-10.0).
5. Recent Vulnerabilities and Exploits:
   * ZeroLogon, Log4Shell, ICMAD; exploits for Log4j, Fortinet SSL VPNs, Confluence Server.
6. Simplified CVSS Top 5 Vulnerabilities:
   * Unitronics PLC default initialization, Zyxel NAS326/NAS542 command injection vulnerabilities.