Review Questions & Answers from Slide Content

Operating System Security

1. **What does the concept "defense in depth" mean?**
   Answer: It means implementing multiple layers of security controls (both hardware and software) so that if one layer fails, additional layers still protect the system.

2. **What is a DMZ in the context of firewalls?**
   Answer: A DMZ (Demilitarized Zone) is a network segment that sits between the external (untrusted) network and the internal (trusted) network. It hosts external-facing services while protecting the internal network from direct exposure.

3. **What is an IDS and what is the difference between an IDS and an IPS?**
   Answer:
   - An IDS (Intrusion Detection System) monitors network or host activity and alerts administrators about suspicious behavior.
   - An IPS (Intrusion Prevention System) not only detects but also actively blocks or prevents potentially malicious traffic.

4. **What is Wireshark and what can you do with it?**
   Answer: Wireshark is a network protocol analyzer that captures and displays live network traffic. It lets you inspect packet details across various OSI layers to troubleshoot or analyze network behavior.

5. **Why should we use SFTP/SCP instead of FTP?**
   Answer: SFTP and SCP encrypt data during transit, protecting credentials and transferred data from interception, whereas FTP transmits data in plaintext.

6. **What is the difference between a packet filter firewall and a stateful firewall?**
   Answer:
   - A packet filter firewall makes decisions solely based on static header information (source/destination IP addresses and ports).
   - A stateful firewall monitors the state of active connections (such as established TCP sessions) and makes decisions based on both header information and connection context.

7. **Which one is easier to implement? Which one might provide additional security benefits?**
   Answer: Packet filtering is easier to implement, but stateful firewalls offer additional security benefits by tracking the state of connections.

Network Security

1. **What is the IP address of caslab.case.edu?**
   Answer: The IP address is determined by DNS resolution (using tools like `host` or `dig`). (Students are expected to run these commands to obtain the current address.)

2. **What ports are open on caslab.case.edu?**
   Answer: Commonly, ports such as 22 (SSH), 80 (HTTP), and 443 (HTTPS) are open. Exact ports should be verified with a scan (e.g., using nmap).

3. **What versions of software may be running on caslab.case.edu?**
   Answer: By using service version detection (with nmap's `-sV` flag), you may identify versions of services (e.g., the Apache web server, SSH daemon, etc.) running on that host.

4. **If nmap does not work, can you use an alternative method to scan?**
   Answer: Yes. Alternatives include using tools like tcpdump, netcat (nc), or other port-scanning utilities.

5. **(Vulnerability Exercise)**

   - **Question:** Perform a search for "xz utils vulnerability" and read the Ars Technica article. Which service is affected, and how can you check if your VM is vulnerable?
     Answer: The vulnerability affects the xz-utils (a compression utility). To check if your VM is vulnerable, run:

```
apt-cache policy xz-utils
```

   Then compare the installed version with the vulnerable version detailed in the article.

Cryptography & Certificates

1. **How is a hash different from both symmetric and asymmetric encryption?**
   Answer: A hash is a one-way function that produces a fixed-length output from data; it cannot be reversed to reveal the original data, whereas encryption (symmetric or asymmetric) is reversible with the proper key.

2. **How can a hash be used for integrity?**
   Answer: By comparing the hash of the original data to the hash computed after transmission, you can verify that the data has not been altered.

3. **How can a hash be used for confidentiality?**
   Answer: Although hashing is not used directly for confidentiality (since it is one-way), it is used in digital signatures to ensure that data has not been tampered with and can indirectly support confidentiality measures when combined with encryption.

4. **(True/False) In order to reset someone's password, we should store it in the database so we can email it to them.**
   Answer: False. Passwords should be stored as salted hashes; they should never be stored in cleartext for email retrieval.

5. **Which hash function is stronger: MD5 or SHA-256?**
   Answer: SHA-256 is stronger than MD5.

6. **In the Java example, what was one of the issues in creating our key?**
   Answer: One issue was ensuring the key met the required length (e.g., a 16-byte key for AES-128)

and properly handling the salt to derive a consistent cryptographic key.

Cryptography – Intro

1. **What command would show the current directory?**
   Answer: `pwd`

2. **What command allows you to change directories?**
   Answer: `cd`

3. **What command shows the files in a directory?**
   Answer: `ls` (commonly with the `-l` flag for a detailed list)

4. **What command will show the contents of a file?**
   Answer: `cat filename`

5. **Which command allows you to change the permissions of a file?**
   Answer: `chmod`

6. **What is the difference between `>` and `|`?**
   Answer:

   - `>` redirects the output of a command to a file (overwriting or creating it).
   - `|` (pipe) passes the output of one command directly as input to another command.

7. **Given the command `chmod 640 filename`:**

   - **What permissions does the owner have?**
     Answer: Read and write.
   - **What permissions does the group have?**
     Answer: Read only.
   - **What permissions does everyone else have?**
     Answer: No permissions.

Certificates – Continued

1. **What is the DN (Distinguished Name) property on a certificate?**
   Answer: The DN is the full, unique identifier for the certificate holder, including details such as country, organization, and common name.

2. **How is the DN different from the CN (Common Name)?**
   Answer: The CN is one attribute (often the primary domain name), whereas the DN includes all identifying attributes.

3. **What is a certificate authority?**
   Answer: It is an entity that issues and digitally signs certificates, thereby verifying the identity of certificate requesters.

4. **Why include a public key in a certificate?**
   Answer: To allow others to encrypt messages for the certificate holder and to verify digital signatures.

5. **What would happen if you visit a site and the certificate has expired?**
   Answer: Your browser will warn you that the certificate is invalid, which may prevent you from accessing the site unless you bypass the warning.

6. **What is X.509?**
   Answer: X.509 is the international standard that defines the format of public key certificates.

7. **What is "Let's Encrypt"?**
   Answer: It is a free, automated certificate authority that provides digital certificates to enable HTTPS on websites.

Additional Quiz Questions (from quiz review.md)

1. **A salt can be stored along with the hashed password. (True/False)**
   Answer: True.

2. **A single salt should be used for all users in a database table. (True/False)**
   Answer: False. Each user should have a unique salt.

3. **Certificates provide the following functionality:**

   - A mechanism to verify the subject presenting the certificate.
   - A mechanism to share the public key.
     Answer: Both are correct; certificates verify identity and share public keys.

4. **Which of the following is not an encryption algorithm?**
   Options: DES, AES, 3DES, Base64
   Answer: Base64 (it is an encoding scheme, not an encryption algorithm).

5. **Asymmetric encryption tends to be faster than symmetric since two keys are used. (True/False)**
   Answer: False. Symmetric encryption is faster.

6. **Assume Jane wants to send John an encrypted message, which of the following methods is correct?**
   Answer: Jane uses John's public key to encrypt the message; John uses his private key to decrypt it.

7. **When using a larger symmetric key size, the following two things tend to happen:**
   Answer: The message becomes more difficult to brute-force (more secure), and the time to perform the encryption is longer.

8. **Only information security professionals should study computer security. (True/False)**
   Answer: False. Secure coding and security practices are important for all software engineers and IT professionals.

9. **What is the operating system that we will be practicing with in this course?**
   Answer: Ubuntu.

10. **Which of the following topics will we look at in this course? (Select all that apply)**
    Options: Web Application Penetration Testing, Privacy, Operating System Security, Cryptography
    Answer: All of the above.

11. **In this course, we will learn about best practices in writing secure code. (True/False)**
    Answer: True.

12. **Which of the following best describes how a TCP SYN flood attack works?**
    Answer: By spoofing the source IP address, another host sends SYN-ACK packets to a target.

13. **Assume a non-privileged user account attempts to run the following command:**

    ```
    sudo chown me:me somefile
    ```

    Answer: The command will fail (or be denied) because the user is not authorized to execute sudo commands if not in the sudoers list.

!