By Maha Rana

CS627 Finalterm subjective Solved

Short Questions

1. **When Nmap is uncertain about port state, it may provide two possible options in its report. Name those options?**
    - **Open | filtered** (the port is either open or filtered)
    - **Closed | filtered** (the port is either closed or filtered)

2. **Purpose of SSH**

• SSH (Secure Shell) is a cryptographic network protocol that provides secure remote access and file transfer between two systems.

• It offers a secure alternative to traditional remote access protocols like Telnet and FTP.

• SSH ensures the confidentiality, integrity, and authenticity of data exchanged between client and server.

3. **"Coordination function" in Wireless LAN?**

Coordination function in WLAN refers to the **method of controlling access to the wireless medium**. It ensures that multiple devices communicate efficiently without collisions. IEEE 802.11 defines two coordination functions:

DCF (Distributed Coordination Function): Uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

PCF (Point Coordination Function): Uses a centralized approach with polling.

4. **Mention the name of the security standard specifically designed to ensure that all components that accept, process, store, and transmit credit card information maintain a secure environment?**
   PCI DSS (Payment Card Industry Data Security Standard)

5. **Role of access control in operating system security and example?**

   Security mechanisms

   - Authentication; Access Control
   - Secure Communication (using cryptography)
   - Logging & Auditing o Intrusion Prevention and Detection

Example:

Discretionary Access Control (DAC): A file owner sets permissions for other users.

Mandatory Access Control (MAC): Security levels define who can access classified data.

6. **Define Trojan Horse?**

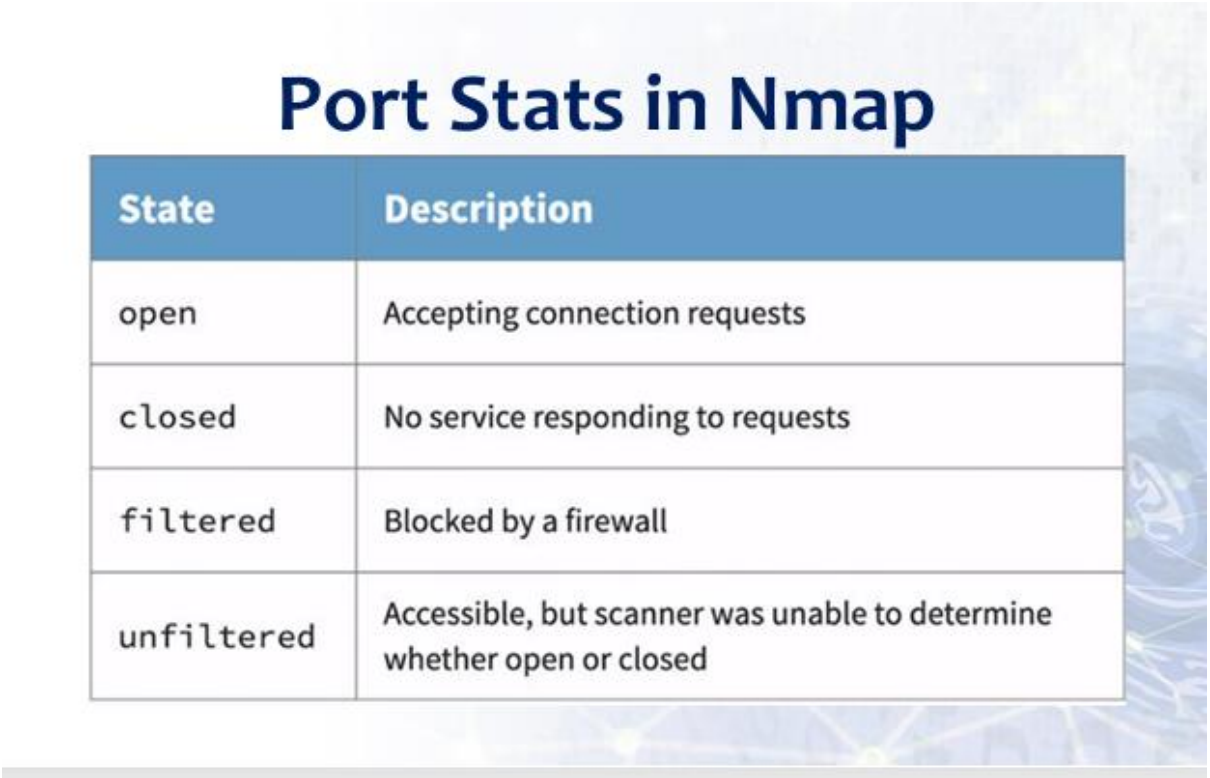
   • In computing, a Trojan horse is any malware that misleads users of its true intent by disguising itself as a standard program.

   • The term is derived from the ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

• Once installed, Trojans may perform a range of malicious actions.
• Many tend to contact one or more Command and Control (C2) servers across the Internet and await instruction.

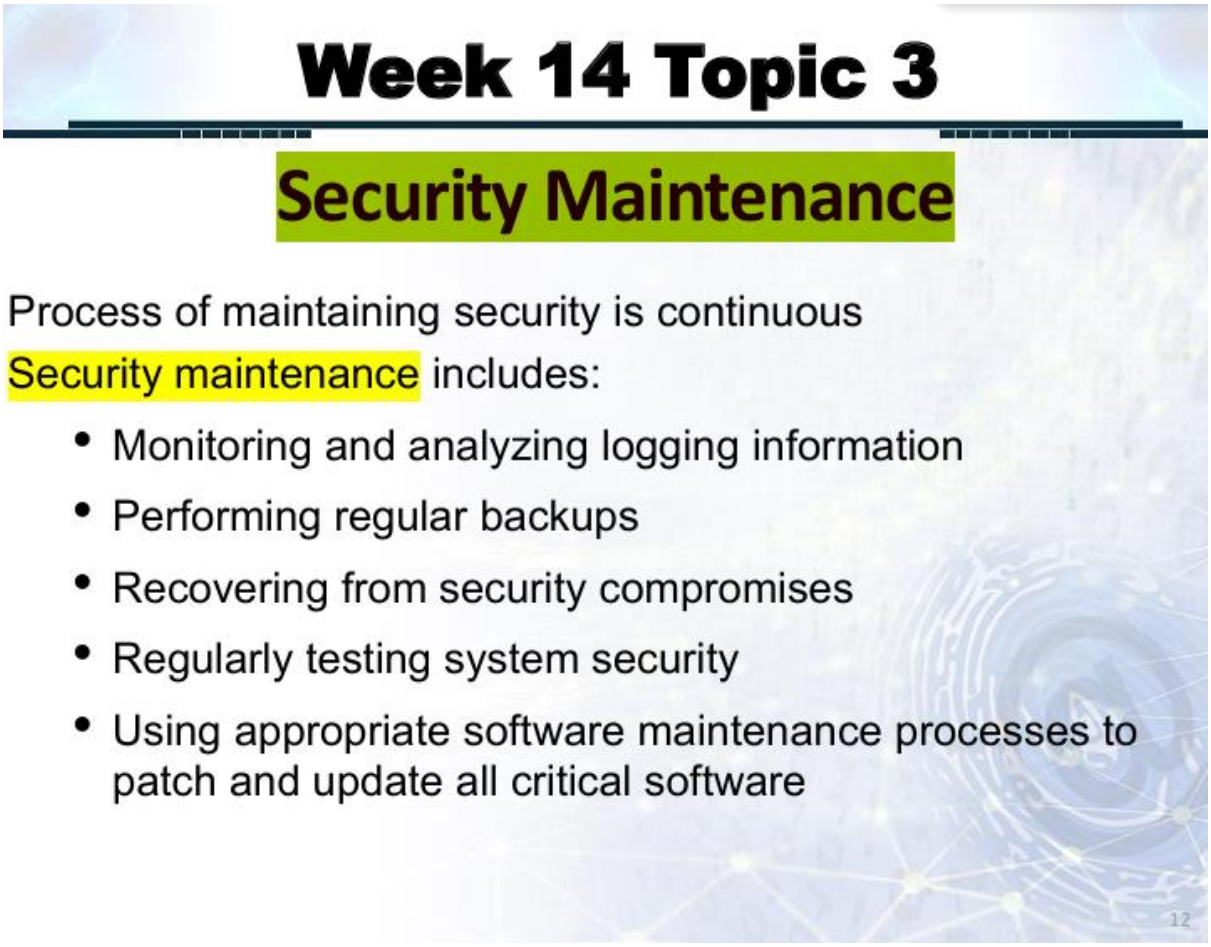
Long Questions

7. **Port names in Nmap**



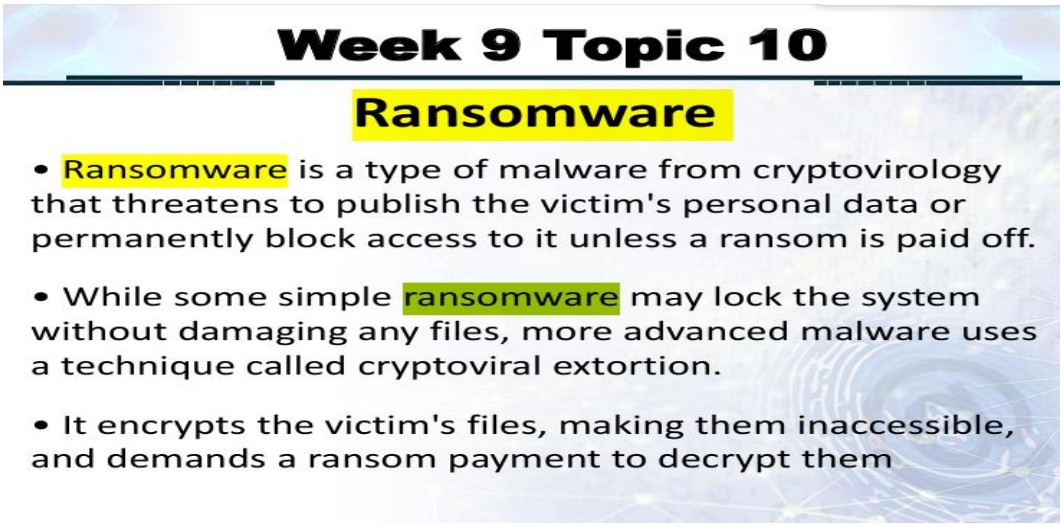
8. **Shellcode role in buffer overflow attack**
    - **Shellcode** is a small, malicious piece of code used by attackers in a **buffer overflow attack**.
    - When an attacker overflows a buffer, they **overwrite the return address** of a function to point to their shellcode, allowing them to execute arbitrary commands, often gaining **unauthorized access** to a system.
9. **Security Maintenance Plan Tasks**

By Maha Rana



Short Questions

10. **What is Ransomware?**



11. **How many default ports does Nmap scan?**

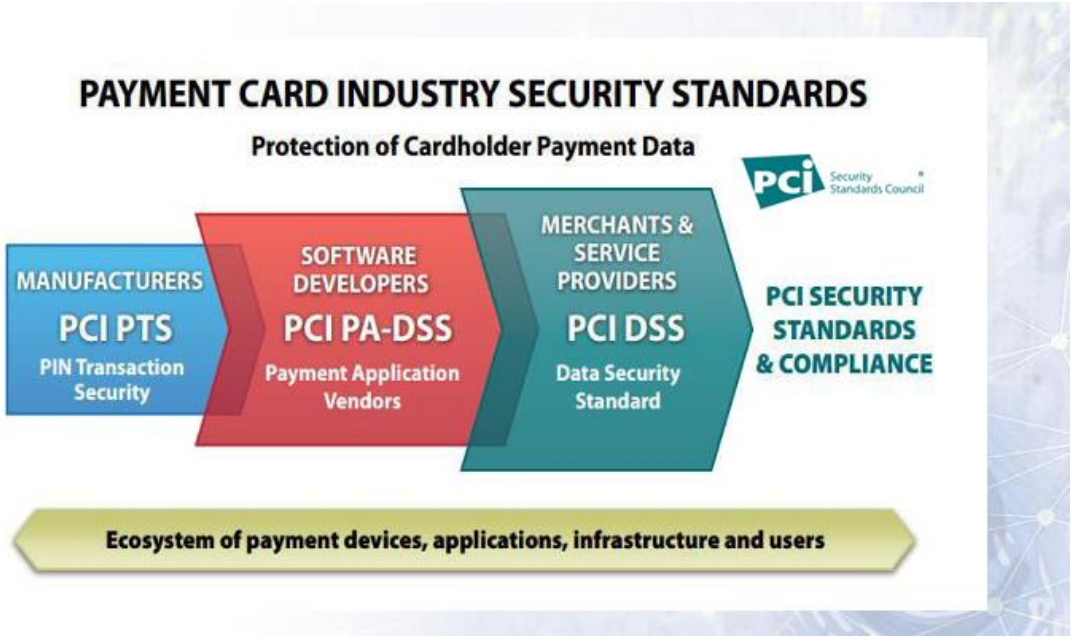
Nmap scans **1,000 most commonly used TCP ports** by default.

12. **What is SSH, and why do we use it?**

SSH (Secure Shell) is a cryptographic network protocol used for **secure remote login, encrypted file transfers, and secure command execution** over an unsecured network.

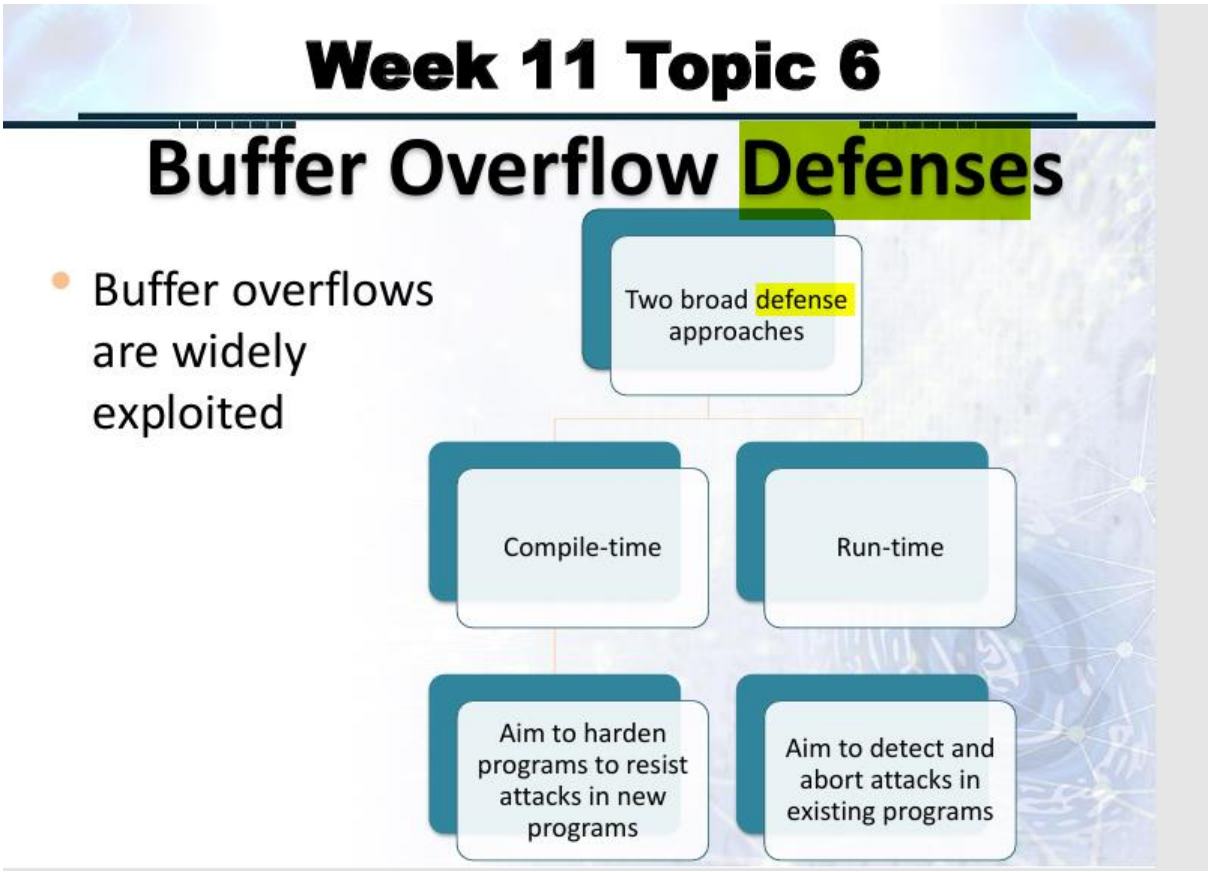
Usage: Remote server management, encrypted communications, tunneling, and authentication.

13. **Three Payment Card Industry (PCI) Standards?**

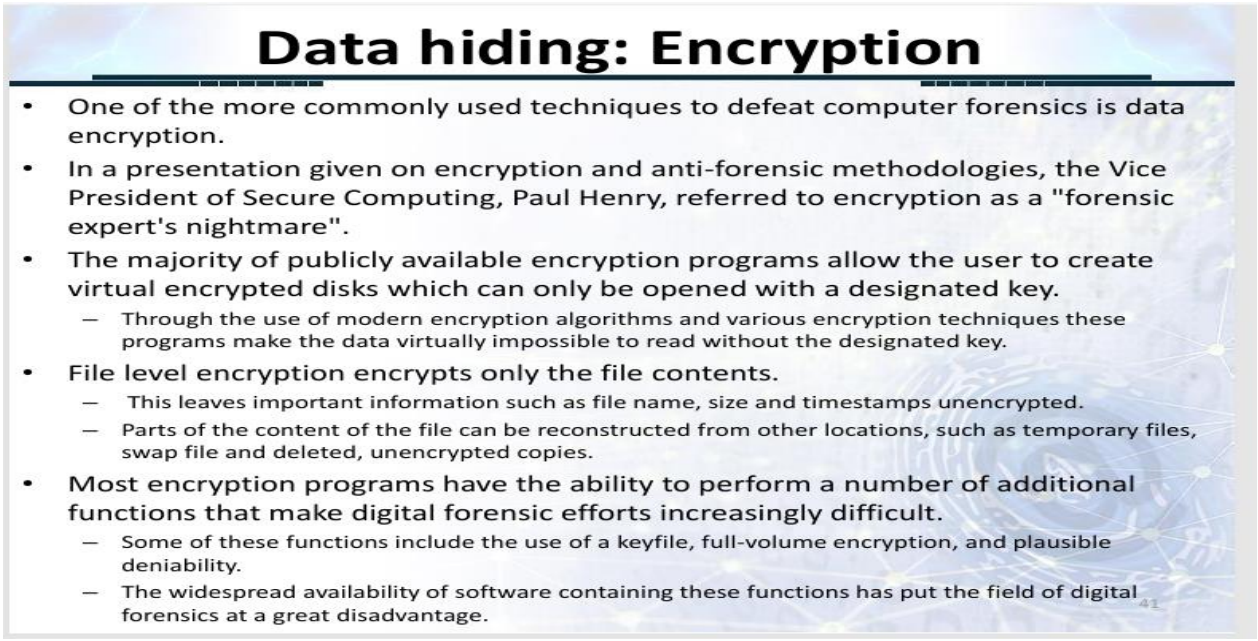


14. **Which defense systems are used against Buffer Overflow?**

By Maha Rana



15. **Data Hiding Techniques + Real-World Cases?**



By Maha Rana

Data hiding: Steganography

- Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight.
- "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph)."
- While some experts have argued that the use of steganography techniques is not very widespread and therefore the subject shouldn't be given a lot of thought, most experts agree that steganography has the capability of disrupting the forensic process when used correctly.
- According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current steganalysis programs. It did this through the use of steganography in conjunction with file compression

42

Data hiding: Other forms of data hiding

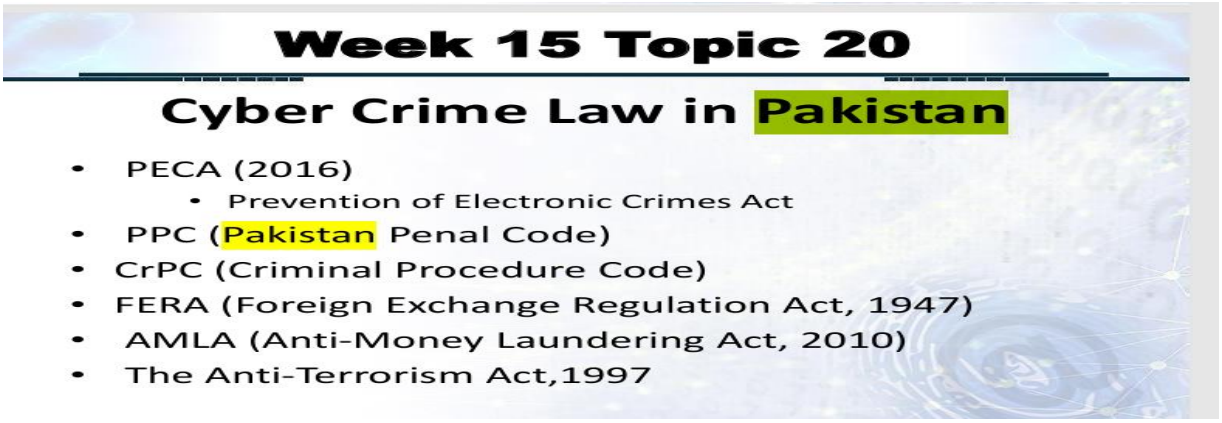
- Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system.
    - Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."
- One of the more well known tools that is often used for data hiding is called Slacker (part of the Metasploit framework).
    - Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software.
- Another data hiding technique involves the use of bad sectors.
    - To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster.
    - The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents

Long Questions

16. **What are White, Black, and Grey Risks in OS Security?**
    - **White Risk:** Known and documented security vulnerabilities that can be mitigated using standard security measures (e.g., outdated software with available patches).
    - **Black Risk:** Unknown and unpredictable vulnerabilities that can be exploited without prior knowledge (e.g., zero-day exploits).
    - **Grey Risk:** Semi-known vulnerabilities where some aspects are understood but not fully mitigated (e.g., partial security patches, misconfigurations).

17. **CIS Benchmark Control Content Categories?**
    - **Profile Applicability**
    - **Description**
    - **Rationale**
    - **Audit**
    - **Remediation**
    - **Impact**
    - **Default Value**
    - **References**

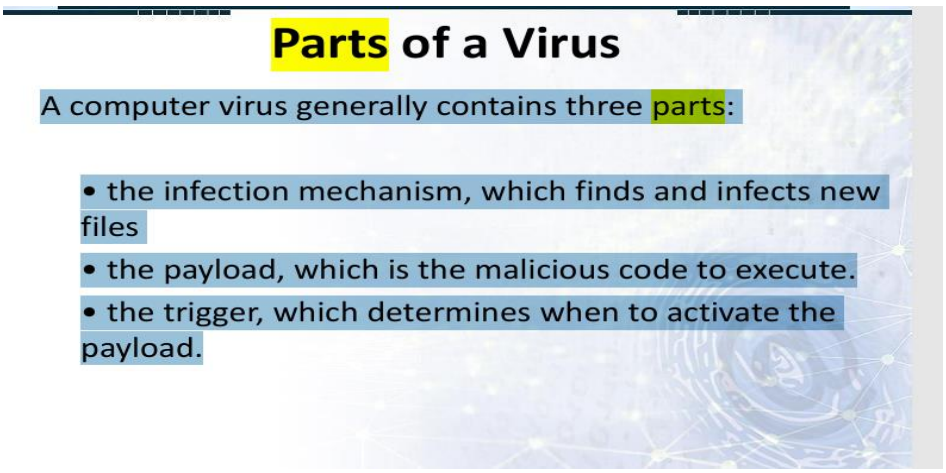
18. **What are the Cybercrime Laws in Pakistan?**



19. **IEEE 802.11x Objectives and Ports**
    - **Objectives:**
        - Provides authentication and access control for wireless networks.
        - Implements **EAP (Extensible Authentication Protocol)** for secure authentication.
        - Prevents unauthorized access to WLANs.
        - Uses **RADIUS (Remote Authentication Dial-In User Service)** for centralized authentication.
        - Helps prevent **rogue access points** and unauthorized devices.
    - **Ports Used:**
        - **Port 1812 (RADIUS Authentication)**
        - **Port 1813 (RADIUS Accounting)**
        - **Port 1645/1646 (Legacy RADIUS Ports)**

Short Questions

20. **Parts of a Virus**



21. **Nmap Syntax for Given IP Addresses (192.168.3.1, 192.168.3.2, 192.168.3.3)**

- To scan these specific IPs in Nmap, the correct command is:

```
nmap 192.168.3.1 192.168.3.2 192.168.3.3
```

- If scanning a range:

```
nmap 192.168.3.1-3
```

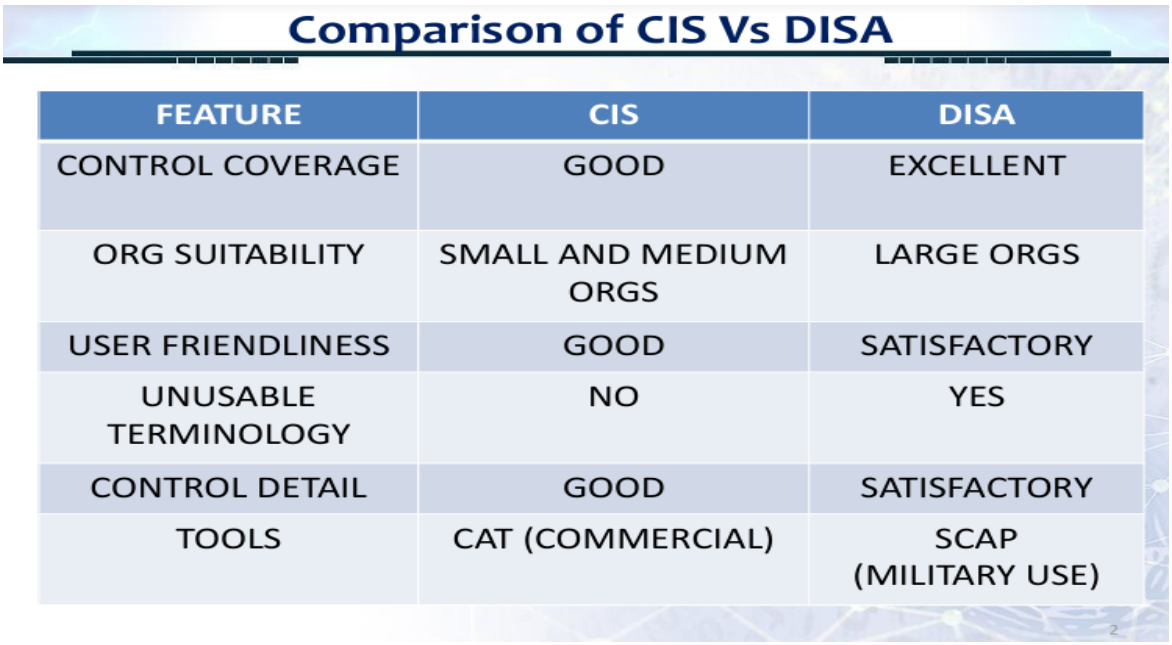
- If scanning an entire subnet:

```
nmap 192.168.3.0/24
```

22. **Two Modes of IPsec**

- **Transport Mode:** Encrypts only the data payload of the packet (used in end-to-end communication).
- **Tunnel Mode:** Encrypts the entire IP packet (used for VPNs).

23. **CIS vs DISA - Comparison Table**



FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

24. **Three Security Risks of Wireless LAN Compared to Wired LAN**

- **Eavesdropping:** Wireless signals can be intercepted by attackers.
- **Unauthorized Access:** Open or weakly protected Wi-Fi networks allow attackers to join the network.
- **Denial of Service (DoS) Attacks:** Attackers can flood the network with traffic to disrupt communication.

25. **Linux Syntax for "Togarate...txt" and Nmap Scan Command**

- To create a file in Linux:

```
touch togarate.txt
```

- To scan this file using Nmap (if referring to scanning a host with the name "togarate.txt" or checking an IP from a file):

```
nmap -iL togarate.txt
```

- If scanning a host named "togarate":

```
nmap togarate
```

- If checking the open ports of a system:

```
nmap -p- <IP-ADDRESS>
```

26. **IEEE 802.1x Activities**

- **Authentication:** Uses EAP (Extensible Authentication Protocol) for verifying devices.
- **Authorization:** Grants network access to authenticated users.
- **Accounting:** Logs network activity for security monitoring.
- **Port-Based Network Access Control:** Prevents unauthorized devices from accessing LAN/WLAN.

Integration with RADIUS: Uses RADIUS for centralized authentication and user management.

27. **Hiding Techniques Challenges in Forensic Security + Real Implemented Examples**

Challenges in Forensic Security:

- **Encryption:** Attackers use encryption to hide files and communications.
- **Steganography:** Malicious data can be hidden inside images or videos.
- **Obfuscation:** Malware uses obfuscation techniques to evade detection.
- **Fileless Malware:** Runs directly in memory without leaving a trace on disk.

Real Implemented Examples:

- **Steganography:** Terrorist groups hiding messages inside image files.
- **Encryption:** Ransomware encrypting user files to demand ransom.
- **Obfuscation:** Malware modifying its code to avoid antivirus detection.
- **Rootkits:** Advanced persistent threats (APTs) using rootkits to maintain access to compromised systems.

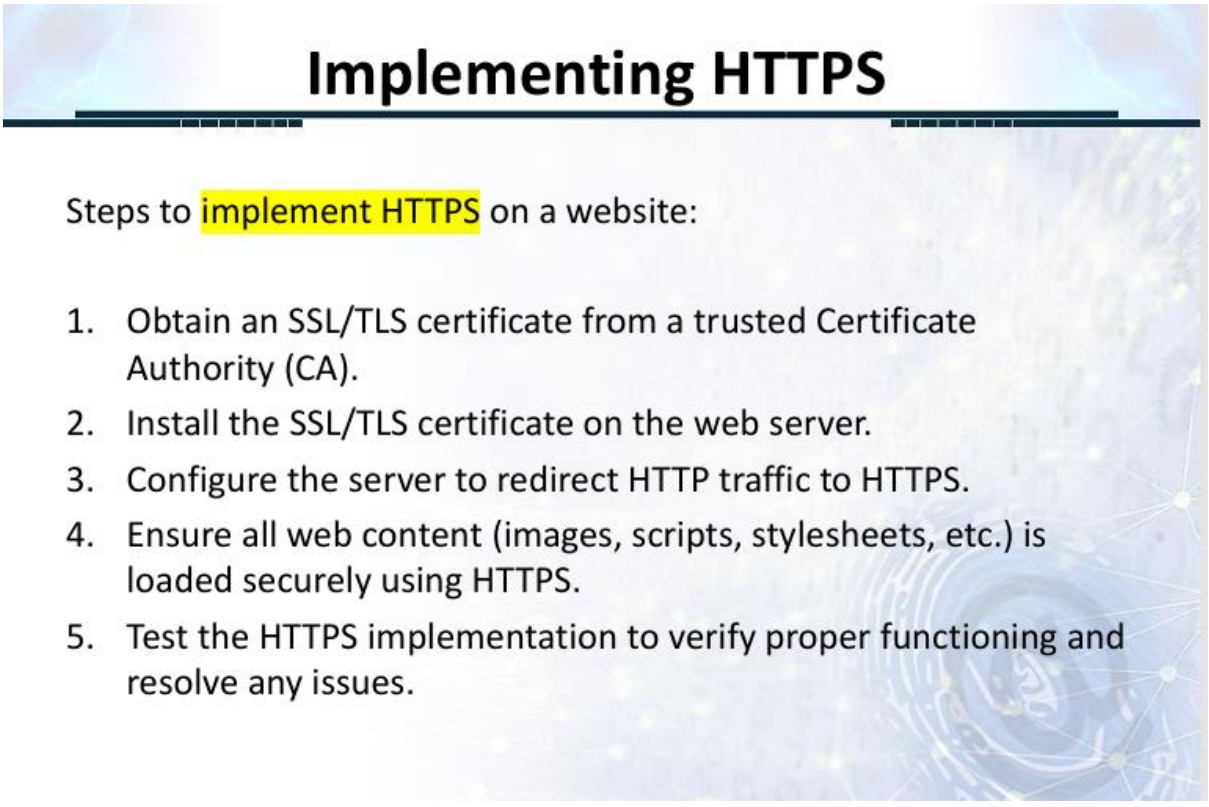
28. **Which security standard is used for card transactions?**

- **PCI DSS (Payment Card Industry Data Security Standard)** ensures that all systems that **accept, process, store, or transmit credit card information** maintain a secure environment.

29. **Which IEEE standard is used for wired and wireless networks?**
    - **Wired LAN: IEEE 802.3** (Ethernet Standard)
    - **Wireless LAN: IEEE 802.11** (Wi-Fi Standard)

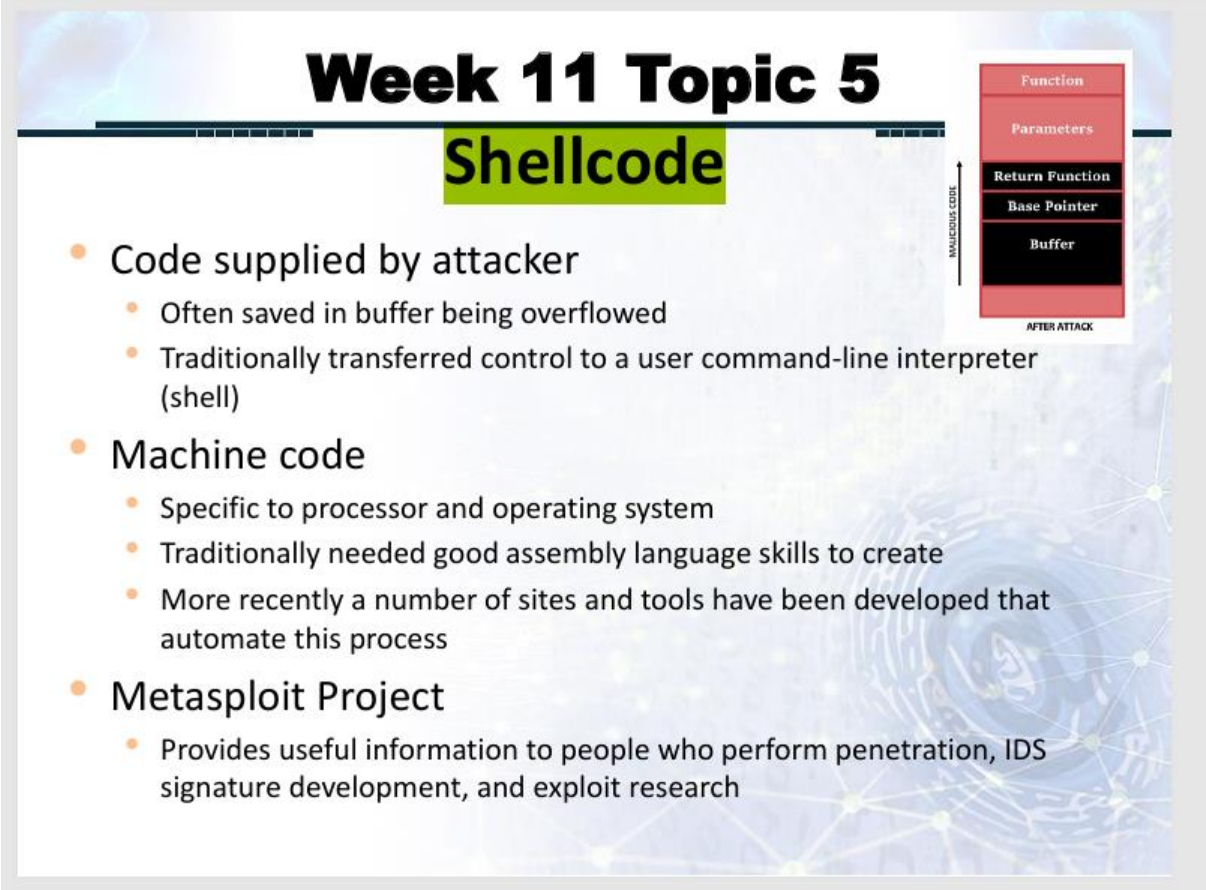
30. **What is a Trojan Horse?**
    - A **Trojan Horse** is a type of **malware** that disguises itself as legitimate software but secretly performs malicious actions, such as stealing data or providing unauthorized access to hackers.

31. **Steps to Implement HTTPS**



32. **What is Shell Code?**

By Maha Rana



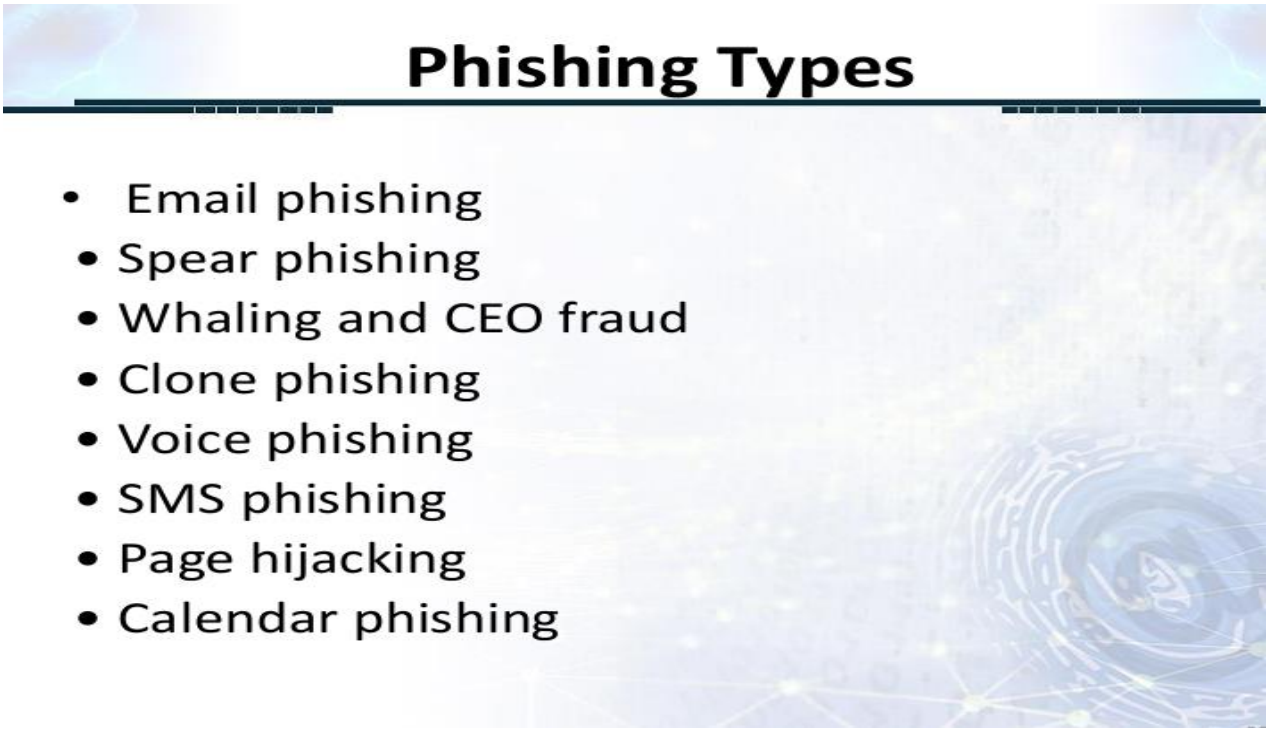
33. **CIS Security Benchmark Content - Any 5**
    - **Profile Applicability** (Which systems the control applies to).
    - **Description** (Overview of the control).
    - **Rationale** (Why the control is needed).
    - **Audit** (Steps to verify control implementation).
    - **Remediation** (How to fix non-compliance issues).
34. **Nmap Command to Scan Three IP Addresses at Once**
    - To scan **multiple IPs simultaneously**, the correct command is:

      ```
      nmap -p- 192.168.1.1 192.168.1.2 192.168.1.3
      ```

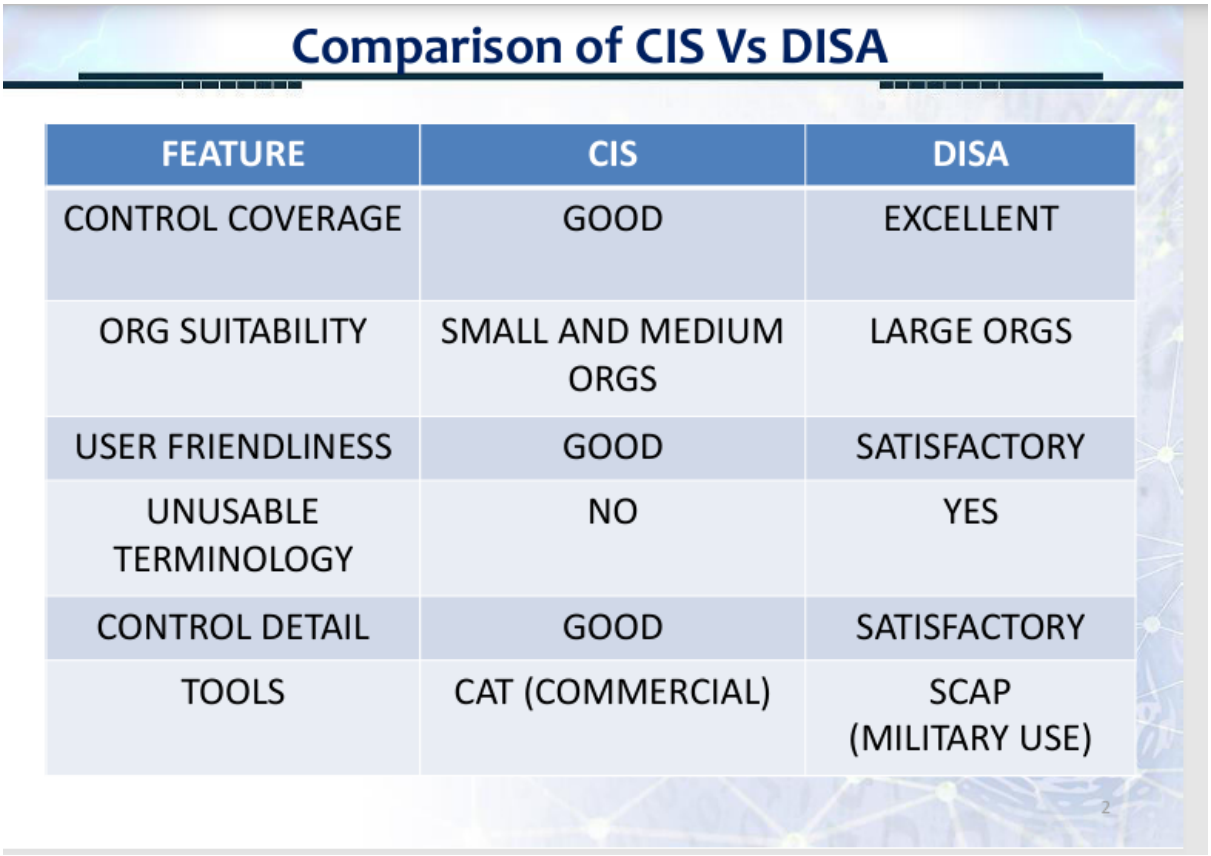
    - **Explanation:**
      - **`-p-`** → Scans **all** 65,535 ports of the given IPs.
      - **Multiple IPs can be listed one after another.**

35. **Purpose of SSL (Secure Sockets Layer)**

1. **Three Types of Phishing Attacks**



36. **CIS CAT Question**



Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

2

Long Questions

37. **Five Phases of IEEE 802.11i Operation**
    - **Phase 1: Discovery**
    - **Phase 2: Authentication**
    - **Phase 3: Key Management**
    - **Phase 4: Protected Data Transfer**
    - **Phase 5: Connection Termination**

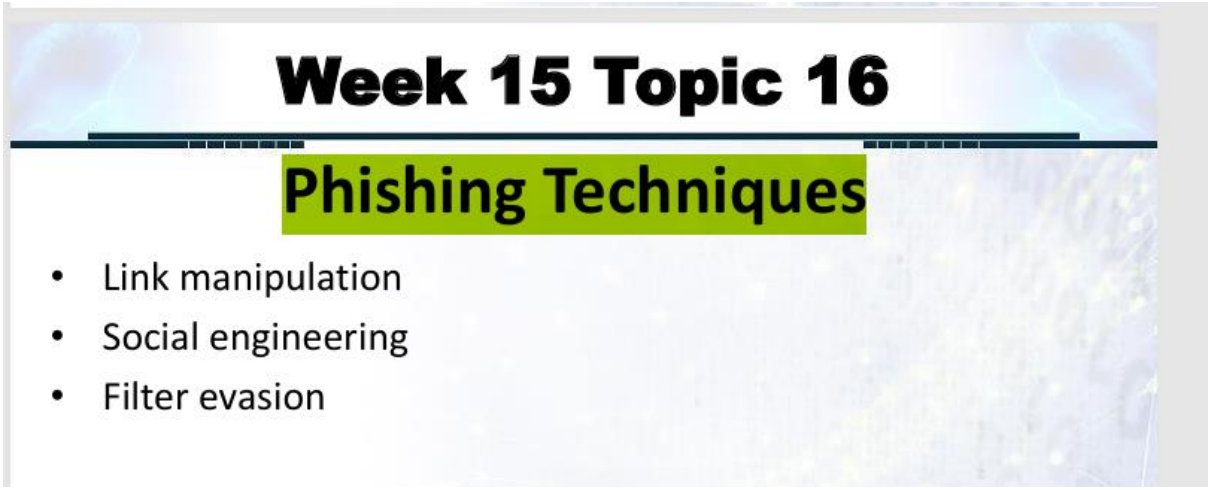
38. **What is Defensive Method? How does it differ from Traditional Methods? Purpose?**

- **Defensive Method:** A proactive cybersecurity strategy that **identifies, detects, and mitigates** attacks **before they cause damage**.
- **Difference from Traditional Methods:**

Defensive Security	Traditional Security
Focuses on **preventing** attacks	Focuses on **reacting** after attacks
Uses **AI, automation, and threat intelligence**	Uses **firewalls, antivirus, and manual monitoring**
More **adaptive and predictive**	More **static and rule-based**

- **Purpose of Defensive Methods:**
  - Reduce attack surfaces.
  - Improve real-time threat detection.
  - Automate security responses.

39. **How Criminals Use Phishing Techniques?**



Short Questions

40. **Nmap Command**
    - **Basic Scan of an IP Address:**

By Maha Rana

- Basic Scan of an IP Address:

```bash
nmap 192.168.1.1
```

- Scan Multiple IPs:

```bash
nmap 192.168.1.1 192.168.1.2 192.168.1.3
```

- Scan All Ports of an IP Address:

```bash
nmap -p- 192.168.1.1
```

- Aggressive Scan (OS, version detection, script scanning, traceroute):

```bash
nmap -A 192.168.1.1
```

41. **Security Standards**
    - **ISO 27001:** Information Security Management System (ISMS).
    - **PCI DSS:** Payment Card Industry Data Security Standard (protects cardholder data).
    - **NIST Cybersecurity Framework:** Risk management framework for cybersecurity.
    - **CIS Benchmarks:** Security best practices for various platforms.
    - **HIPAA:** Protects healthcare data privacy and security.

42. **Software Errors**
    - **Syntax Errors:** Mistakes in code structure (e.g., missing semicolons).
    - **Logical Errors:** Code runs but produces incorrect output.

- **Runtime Errors:** Errors that occur during program execution (e.g., division by zero).
- **Buffer Overflow Errors:** When a program writes more data to a buffer than its allocated memory.
- **Memory Leaks:** When allocated memory is not freed, causing excessive resource use.

43.Nmap Flags (Important Flags & Their Uses)

Flags (options) modify the behavior of Nmap scans. Some commonly used ones include:

Flag	Use	Example
`-p`	Specify a port or range	`nmap -p 80 192.168.1.1`
`-p-`	Scan **all** 65,535 ports	`nmap -p- 192.168.1.1`
`-A`	**Aggressive scan** (OS, versions, scripts, traceroute)	`nmap -A 192.168.1.1`
`-sS`	**Stealth Scan** (SYN Scan)	`nmap -sS 192.168.1.1`
`-sV`	**Service Version Detection**	`nmap -sV 192.168.1.1`
`-O`	**Detect OS of the target**	`nmap -O 192.168.1.1`
`-Pn`	**Disable ping check (scan even if host appears down)**	`nmap -Pn 192.168.1.1`
`-F`	**Fast scan (top 100 ports only)**	`nmap -F 192.168.1.1`

44. Famous Hackers & Attackers

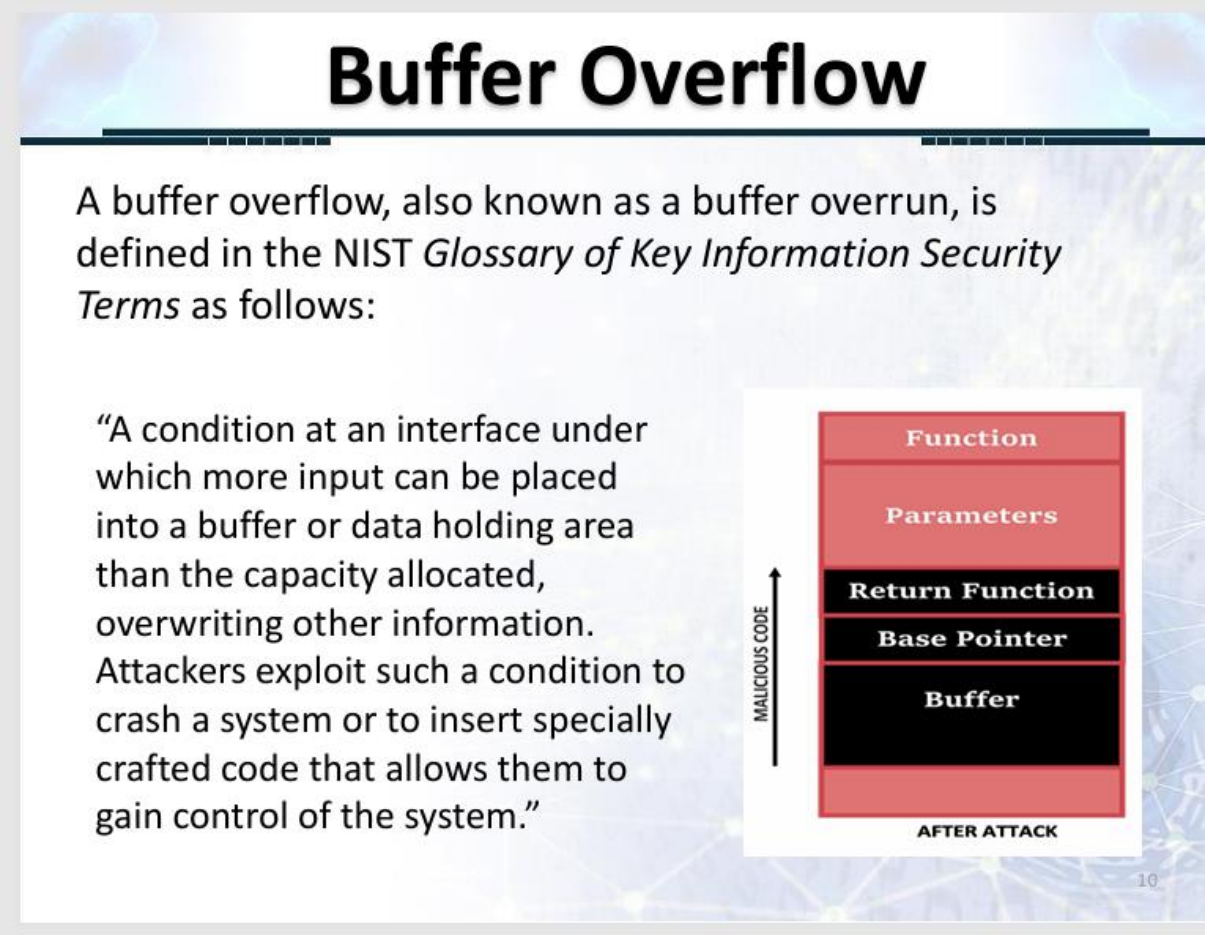
Some well-known cyber attackers and hackers in history:

1. **Kevin Mitnick** – Social engineering expert, hacked into government and corporate systems.
2. **Anonymous** – Decentralized hacking group known for DDoS attacks.
3. **Edward Snowden** – Former NSA contractor who leaked classified surveillance data.
4. **Adrian Lamo** – Hacker who reported Chelsea Manning's leaks.

5. **Gary McKinnon** – British hacker who broke into NASA and Pentagon systems.

45.Buffer Overflow (Concept & Explanation)

- **What is Buffer Overflow?**



46.Nmap-Related

Nmap is used for **network scanning, vulnerability detection, and security auditing**.

- **Basic Nmap Scan:**

By Maha Rana

- **Basic Nmap Scan:**

```
bash

nmap 192.168.1.1
```

- **Scan Multiple IPs:**

```
bash

nmap 192.168.1.1 192.168.1.2 192.168.1.3
```

- **Full Port Scan:**

```
bash

nmap -p- 192.168.1.1
```

- **Aggressive Scan:**

```
bash

nmap -A 192.168.1.1
```

- **Detect OS & Services:**

```
bash

nmap -O -sV 192.168.1.1
```

---

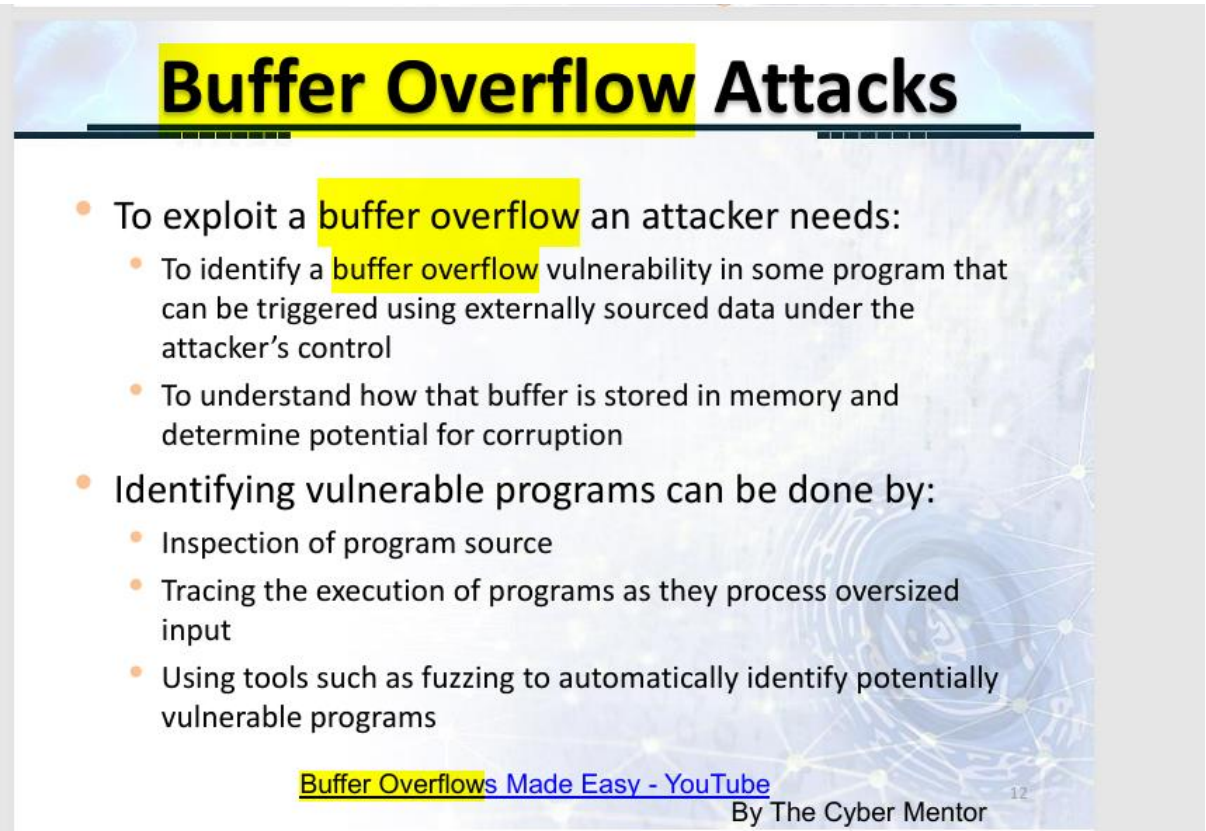
47. Zenmap Profiles

Zenmap is the **GUI version of Nmap**, used for network scanning.

Zenmap Scan Profiles:

Profile	Description
Intense Scan	Scans all ports + OS & service detection
Regular Scan	Basic Nmap scan
Quick Scan	Faster scan using a limited number of packets
Quick Scan Plus	Fast scan with version detection
Quick Traceroute	Identifies network routes
Slow Comprehensive Scan	Deep scan with aggressive options

48. Buffer Overflow Attacks



49.SSH & SSL

SSH (Secure Shell)

- Used for **secure remote login and command execution**.
- Provides **encryption, authentication, and integrity**.
- Ports: **22 (default)**

By Maha Rana

SSL (Secure Sockets Layer)

- Encrypts **web communications** between browser and server.
- Uses **HTTPS (port 443)** to protect **user credentials, transactions, and sensitive data**.

Key Difference Between SSH & SSL

Feature	SSH	SSL
Purpose	Secure remote access	Secure web traffic
Protocol	Used in shell commands	Used in HTTPS
Ports	22	443
Encryption	RSA, AES	TLS, SSL

50. OS Security

- **Security Layers in OS:**

  ✅**Authentication** – Verifies user identity.

  ✅**Authorization** – Controls access to system resources.

  ✅**Integrity Checks** – Ensures system files are not altered.

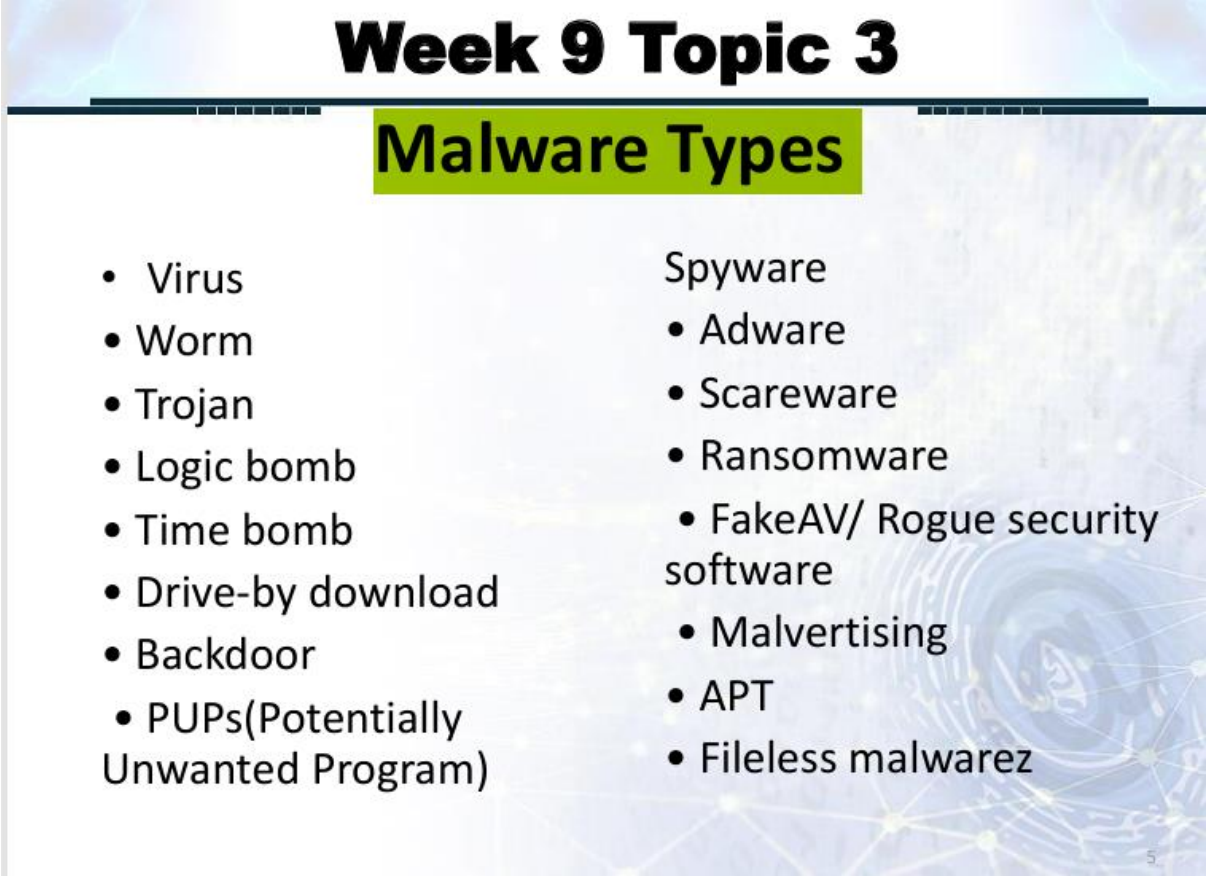
  ✅**Patch Management** – Regular OS updates to fix security flaws.
- **Common OS Attacks:**
  - Privilege Escalation
  - Rootkits
  - Kernel Exploits

51.Cyber Crimes

Types of Cyber Crimes:

Type	Example
Hacking	Unauthorized system access
Identity Theft	Using stolen credentials for fraud
Phishing	Fake emails to steal sensitive data
Cyberstalking	Online harassment
DDoS Attacks	Overloading servers to crash websites

52.Malware Types



53.Difference Between Computer Forensics & Network Forensics (Long Question)

Aspect	Computer Forensics	Network Forensics
Focus	Investigates files, disks, and OS logs	Analyzes network traffic, packets, and logs
Data Source	Hard drives, RAM, registry	Firewalls, routers, Wireshark captures
Purpose	Recover deleted data, analyze malware	Detect intrusions, track cybercriminals
Example Tools	FTK, EnCase, Autopsy	Wireshark, Snort, Suricata

54. Nmap Default Ports (Short Question)

- By default, **Nmap scans the 1,000 most commonly used TCP ports** on a target system.
- **Full port scan (all 65,535 ports):**

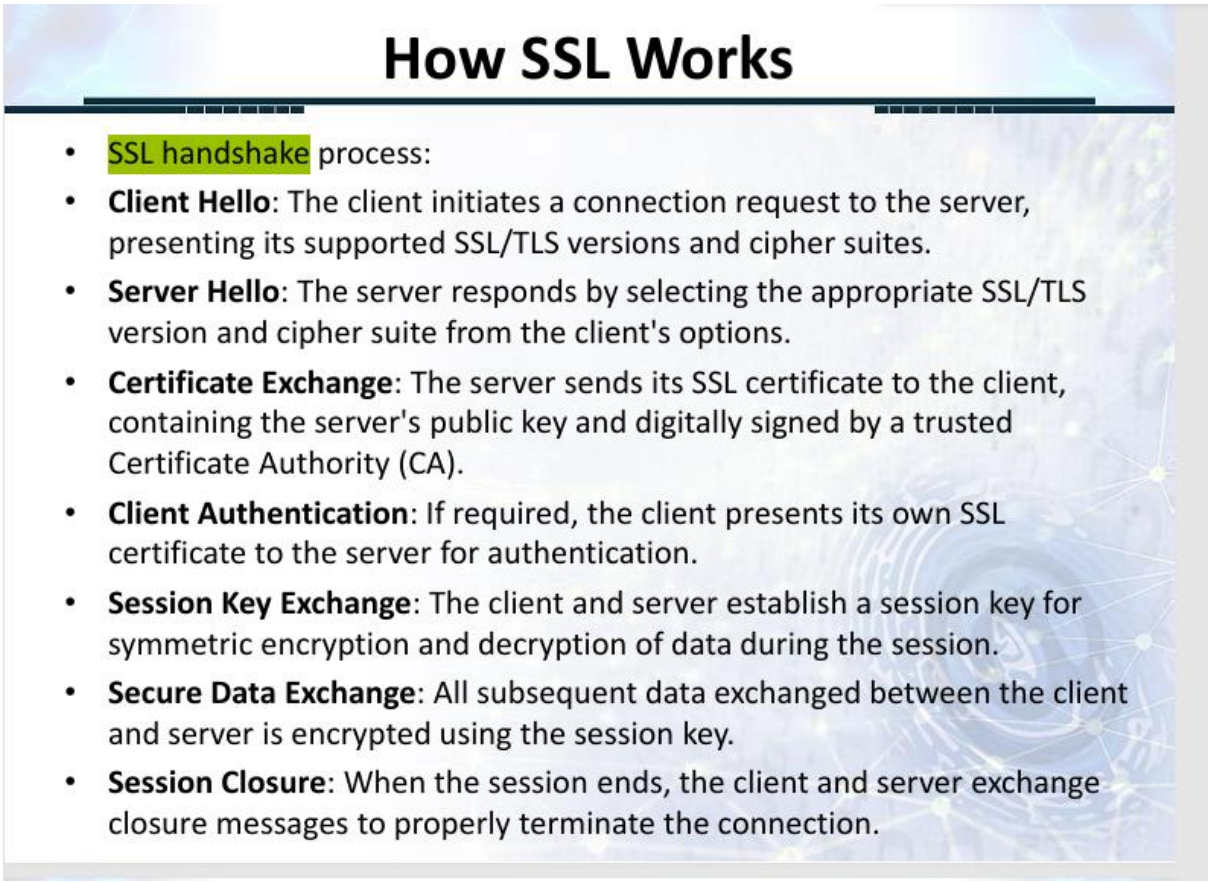
```
nmap -p- 192.168.1.1
```

- **Commonly scanned ports include:**
  - **80 (HTTP)**
  - **443 (HTTPS)**
  - **22 (SSH)**
  - **53 (DNS)**
  - **25 (SMTP)**
  - **3389 (RDP)**

55.Demerits of ISO 27001:2013 (Short Question)

- **Broad & Generalized:** Does not specify detailed implementation steps.
- **Costly & Resource-Intensive:** Requires dedicated teams for compliance.
- **Time-Consuming:** Full implementation takes **months to years**.
- **Not Industry-Specific:** Lacks specific controls for certain industries.
- **Complex Certification Process:** Involves regular audits and documentation.
- **SSL Handshake Steps (Short Question)**
- **SSL Handshake Process (Between Client & Server):**

By Maha Rana



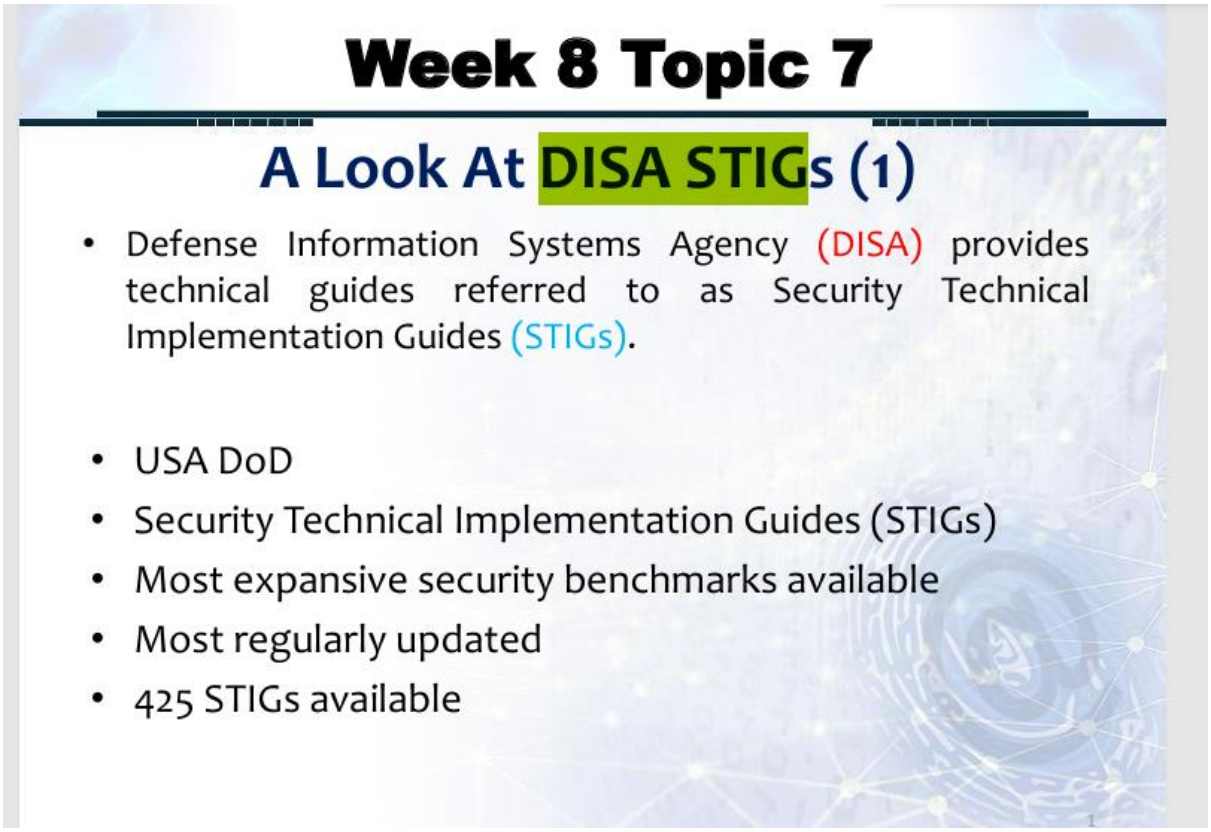
56. ISO 27001:2013 Contents (4-Way Handshake & Security Controls)

 Key Sections in ISO 27001:

1. **Information Security Policies** – Guidelines for data protection.
2. **Risk Assessment & Treatment** – Identifies and mitigates threats.
3. **Access Control** – Restricts unauthorized access to systems.
4. **Cryptography** – Encrypts sensitive data for security.
5. **Network Security** – Secures networks from intrusions.
6. **4-Way Handshake (Wireless Security - IEEE 802.11i):**
    - Step 1: Client & AP exchange keys.
    - Step 2: Generate Pairwise Master Key (PMK).
    - Step 3: Secure data encryption setup.
    - Step 4: Confirm & finalize connection.

By Maha Rana

57. DISA STIG (Security Technical Implementation Guide) - Five Content Names



By Maha Rana

May Allah grant you success, ease your efforts, and bless you with wisdom and perseverance. Keep your faith strong, for with prayer, every challenge becomes an opportunity. And please remember me in your prayers.

I hope this file helps you a lot; I have tried my best to find the most relevant and authenticated answers for the questions. However, in some cases, the questions might slightly differ from the ones in your slides. I recommend that every student kindly verify the answers on their own before using them. I am not responsible for any discrepancies.

Best wishes for Finals!