📘 Domain 2: Threats, Vulnerabilities, and Mitigations (22%)

🔹 2.1 Common Threats and Attack Vectors

🛠️ Social Engineering Attacks

Attack Type	Description	Example
Phishing	Email pretending to be legitimate to trick the user into revealing info	Fake bank email
Spear Phishing	Targeted phishing toward a specific person or role	CEO receives fake invoice
Whaling	Phishing aimed at high-level executives	CFO targeted with legal threats
Vishing	Voice phishing over the phone	Fake tech support call
Smishing	SMS phishing	“You’ve won a prize!” text
Pretexting	Attacker builds a fake scenario to gain trust	Pretending to be from HR
Tailgating	Following someone into a restricted area	Walking behind employee at secure door
Impersonation	Pretending to be someone else	Posing as IT staff
Dumpster Diving	Searching trash for sensitive information	Looking for credentials in thrown-away papers

✅ **Tip:** Social engineering questions often require identifying **behavioral cues** or **human vulnerabilities**.

🔐 Malware Types

Type	Description	Behavior
Virus	Infects files and spreads via user action	Needs host file
Worm	Self-replicates and spreads automatically	No user action needed
Trojan Horse	Appears legitimate but hides malicious intent	Backdoor access
Ransomware	Encrypts data and demands payment	Crypto-malware is common
Spyware	Secretly collects user data	Keyloggers, screen capture
Adware	Shows unwanted ads	Sometimes bundled with freeware
Rootkit	Hides its presence and grants privileged access	Hard to detect
Botnet	Group of infected systems controlled remotely	Used in DDoS attacks

⚠️ **Note**: SY0-701 focuses more on **ransomware**, **botnets**, and **fileless malware**.

🛡️ Attack Vectors

- **Email**
- **Web browsing (drive-by downloads)**
- **Removable media**
- **Insider threats**
- **Third-party partners**
- **Unpatched software**

🔹 2.2 Network Attacks

Attack Type	Description
DoS / DDoS	Flooding a system to make it unavailable
MITM (Man-in-the-Middle)	Intercepts and alters communication between two parties
Session Hijacking	Attacker takes over a session by stealing session ID
DNS Poisoning	Redirects user to malicious sites via fake DNS records
ARP Poisoning	Links attacker's MAC address to a trusted IP
MAC Spoofing	Faking a MAC address to impersonate another device
IP Spoofing	Faking a source IP address
Replay Attack	Repeating a captured valid transmission
Smurf Attack	Spoofed ICMP requests flood the network
Ping of Death	Sending oversized ping packets to crash a system

> ✅ Many of these are best mitigated by **encryption, firewalls, and network segmentation**.

🔹 2.3 Application and Service Attacks

Attack Type	Description
SQL Injection	Malicious SQL input manipulates database queries
XSS (Cross-Site Scripting)	Injects code into websites viewed by others
XSRF / CSRF (Cross-Site Request Forgery)	Forces a user to perform unwanted actions
Command Injection	Executes commands on the host system
Directory Traversal	Gains unauthorized access to files outside web root
Privilege Escalation	Gains higher access rights than intended
Logic Bomb	Code triggered by a specific condition
Buffer Overflow	Overwrites memory, causing crashes or code execution

> 🔐 Use input validation, parameterized queries, and least privilege to **mitigate** most application attacks.

🔹 2.4 Insider Threats and Supply Chain Risks

Insider Threats

- **Intentional**: Disgruntled employee leaking data
- **Unintentional**: User falls for phishing
- **Mitigation**: Monitoring, DLP, role-based access, least privilege

Supply Chain Risks

- **Third-party vendors** may introduce vulnerabilities.
- Includes:
    - Insecure software/hardware
    - Compromised updates
    - Insider access from partners

🛑 Zero Trust helps mitigate both insider and supply chain threats.

🔹 2.5 Common Vulnerabilities

Vulnerability	Description
Unpatched systems	Known flaws not fixed yet
Default credentials	Admin/admin still used
Misconfigurations	Firewalls left open, cloud buckets exposed
Weak encryption	Using outdated algorithms (e.g., MD5)
Unsecured APIs	Lacking authentication or rate limiting
Open ports/services	Not required, potential backdoors

🔹 2.6 Vulnerability Management Process

📋 Steps:

1. **Identify Assets**
2. **Perform Vulnerability Scans**
3. **Analyze Results**
4. **Remediate or Mitigate**
5. **Rescan to Validate**

🛠️ Tools:

- **Nessus**, **OpenVAS**, **Qualys**
- **Exploit Frameworks**: Metasploit

> 🔍 Use **credentialed scans** for deeper inspection; **non-credentialed** for external view.

🔹 2.7 Threat Intelligence Sources

Source Type	Description	Example
Open-source (OSINT)	Public data	news, blogs, Shodan
Proprietary	Paid data	FireEye, Recorded Future
Government	National alerts	US-CERT, NIST
ISACs	Industry-specific sharing	FS-ISAC (Finance), H-ISAC (Healthcare)

📌 Threat intelligence feeds help with **early detection and proactive defense**.

🔹 2.8 Indicators of Compromise (IOCs)

- **Unusual outbound traffic**
- **Unusual login times or geolocations**
- **Multiple failed logins**
- **Unusual file changes**
- **Disabled logging**

⚠️ IOC detection requires **SIEM tools, logging, and alerting systems**.

📌 Key Takeaways for Domain 2

- Know **types of malware** and how they behave.
- Expect scenario questions about **social engineering**.
- Be able to map **attacks to their network layers**.
- Understand the **vulnerability management lifecycle**.
- Remember: **Prevention** (patching, MFA, firewall) + **Detection** (SIEM, IDS) = security.
