Armaan Shamsaasef

Common Threat Vectors - SY0-701 - 2.2

Definition: A path or method used by a threat actor to gain access to a system or network.

1. Direct Network Attacks

- Description: An attacker directly targets a system by scanning for and exploiting open ports and services.
- How it Works:
    1. An attacker uses a tool like Nmap to scan a network for devices with open ports (e.g., port 22 for SSH, port 3389 for RDP).
    2. They find a service with a known vulnerability or weak configuration.
    3. They launch an exploit against that service to gain access.
- Example: An attacker finds a web server (port 80/443) running an outdated version of software and uses a known exploit to get a shell on the server.

2. Malicious Email (Phishing)

- Description: A social engineering attack delivered via email.
- Common Payloads:
    - Malicious Links: Leads to a fake login page or a website that hosts malware.
    - Malicious Attachments: Files (like PDFs, Word documents, spreadsheets) that contain macros or scripts which install malware when opened.
- Example: An email pretending to be from the IT helpdesk with a link to "update your password," which actually steals your credentials.

3. Removable Media

- Description: Malware that is spread through USB drives, external hard drives, or other removable devices.
- How it Works:
  - Intentional: An attacker plants infected USB drives in a public place (e.g., a parking lot), hoping an employee will pick one up and plug it into a corporate machine (USB Drop Attack).
  - Unintentional: An employee uses an infected personal USB drive on a work computer.
- Example: The Stuxnet worm was initially propagated via USB drives to infiltrate and sabotage an air-gapped nuclear facility.

4. Wireless Networks

- Description: Attacks that target wireless communication protocols.
- Common Methods:
  - Rogue Access Points: An attacker sets up a malicious wireless network with a legitimate-sounding name (e.g., "Free Public Wi-Fi" or "Company_Guest") to trick users into connecting.
  - Evil Twin Attack: A specific type of rogue AP that mimics the SSID of a legitimate, trusted network.
  - Exploiting Weak Encryption: Attacking Wi-Fi networks using outdated protocols like WEP or WPA.

5. Cloud-Based vs. On-Premises

- Cloud-Based Threats:
  - Target misconfigured cloud services (e.g., storage buckets set to "public").
  - Exploit weaknesses in cloud access management and identities.
- On-Premises Threats:
  - Target the organization's own physical data center and network infrastructure.
- Key Point: The attack surface and methods differ, but the goal is the same. Cloud misconfigurations are a major modern vector.

6. Supply Chain Attacks

- Description: Compromising a system by targeting a less-secure element in the supply chain, such as a software vendor or hardware manufacturer.
- How it Works: The victim is infected with malware through a trusted, legitimate update or product.
- Example: The SolarWinds attack, where malicious code was inserted into a legitimate software update, which was then distributed to thousands of the company's customers.

7. Threat Vectors Summary Table

Threat Vector	How Access is Gained
Direct Network	Exploiting vulnerable services exposed to the network.
Malicious Email	Tricking users into clicking links or opening attachments.
Removable Media	Using physical devices to bypass network security.
Wireless	Tricking connections to rogue access points or cracking encryption.
Cloud/On-Prem	Targeting misconfigurations in different infrastructure models.

Supply Chain	Compromising a trusted third-party to infect the final target.

Summary

- A threat vector is the "how" an attacker gets in.
- Vectors can be technical (network exploits), social (phishing), or physical (removable media).
- Modern attackers often target the easiest path, which is frequently through people (phishing) or third-party partners (supply chain).