**CTF Challenge: Scanning Networks**

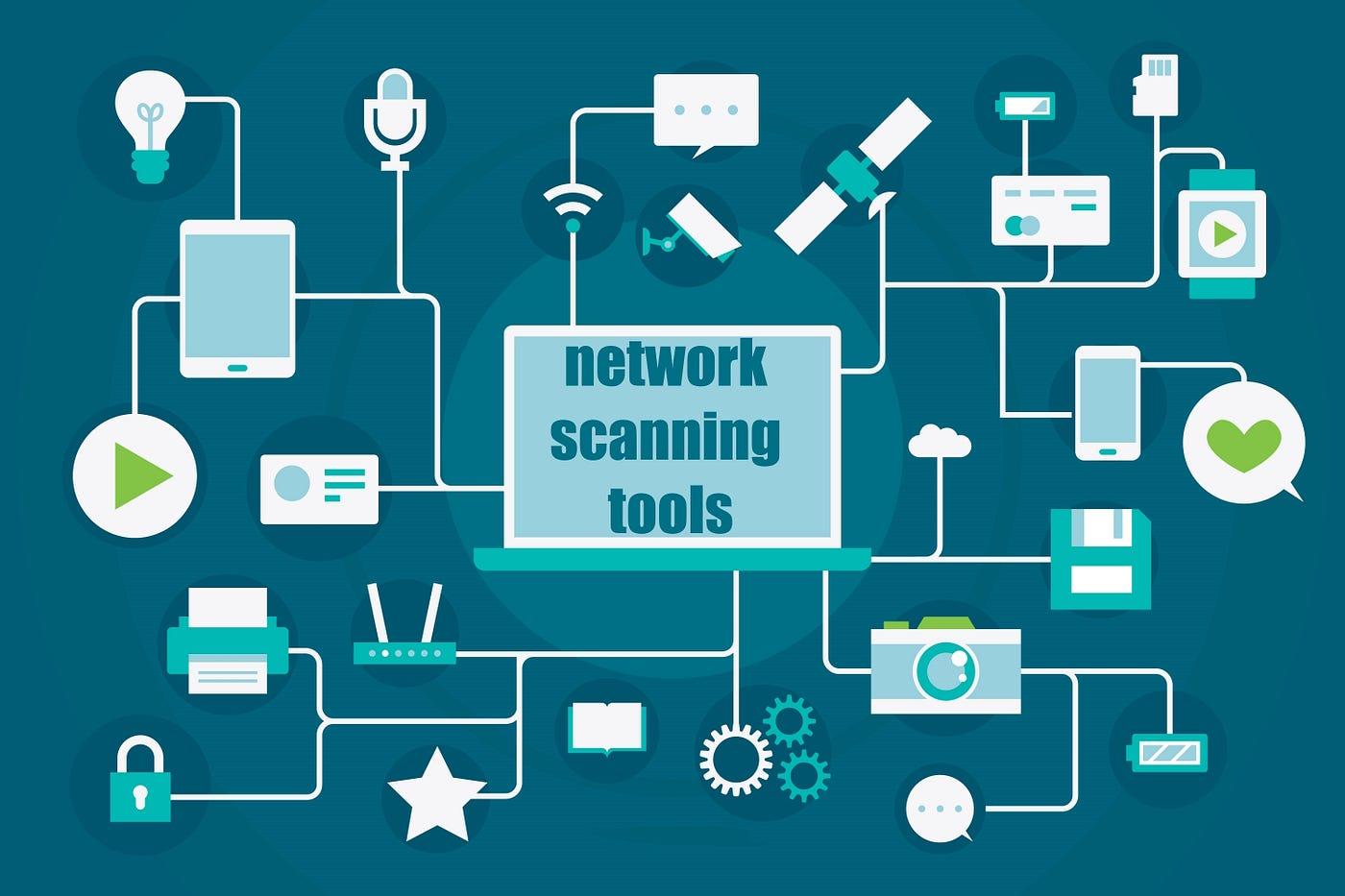
****

**Why Scan Networks?**

Network scanning serves several purposes:

* **Vulnerability Assessment:** Security professionals use scanning to identify vulnerabilities in devices and services on a network. This helps prioritize patching and remediation efforts.
* **Intrusion Detection:** Scanning can help detect unauthorized devices or suspicious activities on a network.
* **Network Inventory:** Scanning helps create an up-to-date inventory of all devices connected to a network, which is crucial for network management and security.
* **Penetration Testing:** Ethical hackers use scanning techniques during penetration testing to identify potential entry points into a network.

**Types of Network Scanning:**

****

There are various approaches to network scanning, each suited for different purposes:

* **Ping Sweeps:** A basic technique that sends ping requests to a range of IP addresses to identify active devices on the network.
* **Port Scans:** This technique scans specific ports on devices to determine if they are open or closed. Open ports might indicate running services that could be vulnerable to attacks.
* **Vulnerability Scans:** These scans use databases of known vulnerabilities to identify specific weaknesses in devices and software versions on the network.
* **Network Mapping:** Advanced scanning techniques can map the entire network layout, identifying devices, their connections, and potential security risks.

**Tools of the Trade:**There are numerous network scanning tools available, both free and paid. Some popular options include:

* Nmap
* Nessus
* OpenVAS
* SecurityScanner

**Ethical Considerations:**

It's crucial to only scan networks with proper authorization. Scanning without permission is illegal and can be considered a cyberattack.

# **Capture the Flag (CTF) Challenges**

Flag 1. Security professionals use scanning to identify what on a network?

Answer: Vulnerabilities

Flag Captured

Flag 2. Scanning can help detect what on a network?

Answer: Intrusion

Flag Captured

Flag 3. A basic technique that sends pings to identify active devices is called a what scan?

Answer: Ping Sweeps

Flag Captured

Flag 4. This technique scans ports to see if they are open or closed, potentially revealing services.

Answer: Port Scans

Flag Captured