Module 4:Attacking What We Do – IP Services

ENDPOINT SECURITY | CISCO NETWORKING ACADEMY

PREPARED BY: KUDZAISHE MAJEZA

Agenda

- Introduction to IP Services
- ARP Vulnerabilities
- ARP Cache Poisoning
- Real-Life Scenario – ARP Poisoning Attack
- DNS Attacks
- Real-Life Scenario – DHCP Attack
- DNS Tunneling
- Real-Life Scenario – DNS Tunelling
- DHCP Overview
- DHCP Attacks
- Real-Life Scenario – DHCP Attack
- Why IP Service Attacks Matter
- Summary & Key Takeaways

Introduction to IP Services

- IP services support everyday network communication
- They work on top of basic IP connectivity
- Examples include ARP, DNS, and DHCP
- Attackers target these services because they are trusted by default

ARP Vulnerabilities

- ARP stands for **Address Resolution Protocol**
- It maps IP addresses to MAC (hardware) addresses
- ARP does **not** authenticate messages
- Any device can claim to be another device
- This makes ARP easy to exploit

ARP Cache Poisoning

- Attacker sends fake ARP replies
- Devices store incorrect MAC-to-IP mappings
- Traffic is redirected through the attacker
- Enables **Man-in-the-Middle (MITM)** attacks
- Common in local area networks

Real-Life Scenario – ARP Poisoning Attack

- **Real-Life Incident: ARP Poisoning on Public Wi-Fi (2018–Present)**
- In **2018**, security researchers reported widespread **ARP poisoning attacks** on **public Wi-Fi networks** (cafés, airports, hotels).
- Attackers connected to the same Wi-Fi network as victims.
- They sent **fake ARP replies**, tricking devices into sending traffic through the attacker.
- Login credentials, emails, and session cookies were stolen.
- This attack is still common today on unsecured public networks.

DNS Attacks

- DNS stands for **Domain Name System**
- Translates domain names into IP addresses
- DNS spoofing redirects users to fake websites
- DNS cache poisoning corrupts DNS records
- DNS amplification is used in DDoS attacks

Real-Life Scenario – DNS Attack

- **Real-Life Incident: Dyn DNS DDoS Attack (October 21, 2016)**
- On **October 21, 2016**, Dyn, a major **DNS (Domain Name System)** provider, was attacked.
- Attack type: **DNS amplification DDoS attack**.
- The attack used thousands of compromised IoT devices (Mirai botnet).
- Websites like **Twitter, Netflix, GitHub, PayPal, and Spotify** went offline.
- Showed how attacking DNS can break large parts of the internet.

DNS Tunneling

- Malicious data hidden inside DNS queries
- DNS traffic is usually allowed through firewalls
- Attackers use it for data exfiltration
- Also used for command-and-control communication
- Difficult to detect without deep inspection

Real-Life Scenario – DNS Tunneling

- **Real-Life Incident: DNS Tunneling Used by Malware (2017–2023)**
- In **2017**, malware families like **Feederbot and Iodine** were discovered using DNS tunneling.
- Attackers hid stolen data inside DNS requests.
- Firewalls allowed DNS traffic, so the attack went unnoticed.
- Used for **data exfiltration** and **command-and-control communication**.
- DNS tunneling is still actively used by advanced attackers today.

DHCP Overview

- DHCP stands for **Dynamic Host Configuration Protocol**
- Automatically assigns IP addresses to devices
- Provides gateway, DNS server, and network settings
- Simplifies network management
- Trusted by default on most networks

DHCP Attacks

- Rogue DHCP servers give malicious network settings
- DHCP starvation exhausts all available IP addresses
- Attackers can redirect traffic through fake gateways
- Can cause network-wide outages

Real-Life Scenario – DHCP Attack

- **Real-Life Incident: Rogue DHCP Attacks in Corporate Networks (2020–2022)**
- Between **2020 and 2022**, multiple enterprise breaches involved **rogue DHCP servers**.
- Attackers plugged unauthorized devices into internal networks.
- Victims received **fake IP addresses, gateways, and DNS servers**.
- Network traffic was redirected to attacker-controlled systems.
- Used to launch **Man-in-the-Middle (MITM)** attacks and steal credentials.

Why IP Service Attacks Matter

- These services affect every device on the network
- Attacks are difficult to notice immediately
- Trust-based protocols are easy to exploit
- Successful attacks enable larger breaches

Summary & Key Takeaways

- IP services are essential and widely used
- ARP, DNS, and DHCP lack strong built-in security
- Attackers exploit trust and misconfiguration
- Proper monitoring and security controls are critical