**LAN SECURITY CONCEPT**

Initial Compromise



**A. Layer 2 Security Threats**



Compromised

|  |  |  |
| --- | --- | --- |
|  | OSI Model | TCP/IP Protocol |
| 7 | Application | HTTP, HTTPS, POP3, IMAP, SSL, SSH, … |
| 6 | Presentation |
| 5 | Session |
| 4 | Transport | Protocols/Ports |
| 3 | Network | IP Addresses |
| 2 | Data Link | Ethernet Frames |
| 1 | Physics | Physical Links |

**B. Switch Attack Categories**

- MAC Table Attacks

- VLAN Attacks

- DHCP Attacks

- ARP Attacks

- Address Spoofing Attacks

- STP Attacks

**C. Switch Attack Mitigation Techniques (Kỹ thuật giảm thiểu tấn công chuyển đổi)**

- Port Security

- DHCP Snooping

- Dynamic ARP Inspecion (DAI)

- IP Source Guard (IPSG)

**D. MAC Address Table Flooding**

- The Problem:

* Switches use a "phone book" (MAC address table) to know where to send network messages.
* This "phone book" has limited space.

- The Attack (MAC Flooding):

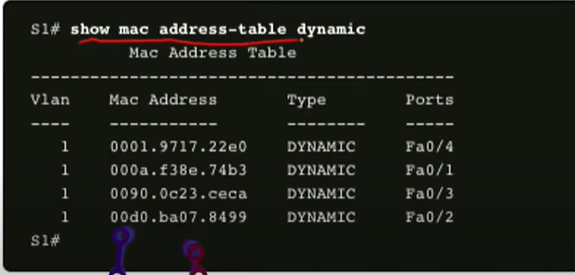
* The attacker sends tons of fake "phone numbers" (MAC addresses) really fast.
* The switch's "phone book" fills up with these fake numbers.

- What Happens:

* The switch gets confused and starts sending all messages to everyone, like a loudspeaker.
* The attacker can now see all the network traffic.

- How to Stop It:

* Limit how many "phone numbers" each port can remember.
* Use network "walls" (VLANs) to keep things separate.
* Use switches with security features.

In short: An attacker tricks a switch into forgetting who's where, so they can eavesdrop on everything.

A blue arrow with orange and black text

AI-generated content may be incorrect.- Tools like macof create MAC table overflow attack

- Mitigation – Port security

**E. VLAN Hopping (Tấn công nhảy VLAN/ vượt VLAN)**

- Attacker gains access to other VLANS on a switch through two techniques:

+ Switch spoofing

+ Double Tagging

- Switch spoofing:

|  |  |
| --- | --- |
| Attack | Switch spoofing |
| What It Is | Attacker gains access to other VLANS by leveraging Dynamic Trunking Protocol (DTP) |
| How It Works | 1. Attacker’s machine send DTP packets to switch to set up a trunk line  2. Attacker can see all VLANS that are communicating on the trunk line |
| Tools | Kali |
| Mitigation | Do not use DTP  1. Disable trunking on all access ports  2. Disable auto trunking on all trunk lines |

- Double Tagging:

|  |  |
| --- | --- |
| Attack | Double Tagging |
| What Is It | Attacker uses native VLAN to gain access to other VLANs |
| How it Works | 1. Attacker’s machine sends frames with two 802.1q tags  \* First is of the native VLAN  \* Second of the VLAN the Attacker is trying to access  2. Attacker sends packer to the switch  3. Switch looks at tag, consider it part of the Native VLAN, and removes the tag  4. Switch forwards frame across trunk line to other switches:  \* It does not remove the second tag  \* It does not add the native VLAN tag  \* Frame still has the second tag  5. Other switching see that it’s part of the second VLAN |
| Tools | Yersinia, vconfig |
| Mitigation | - Avoid using native VLAN  - Change native VLAN to something other than default  - Disable trunking on all access ports  - Specify allowed VLANs on every trunk line |

**F. Networks Attacks Today**

- Enterprise networks are frequently targeted by cyberattacks. Common attack types include:

+ Distributed Denial of Service (DDoS): Overwhelming a network with traffic from multiple compromised devices (zombies), making it unavailable to legitimate users.

+ Data Breach: Unauthorized access to and theft of sensitive information stored on an organization's servers or systems.

+ Malware: Infection of systems with malicious software, such as ransomware (like WannaCry), that can encrypt data and disrupt operations.

**G. DDoS**

- DdoS:

\* A cyber atack on a specific server or network

\* An intended purpose of disrupting normal operation

\* Flooding the target with a constant flood of traffic.

- **DDoS Attack Process:**

1. **Botnet Build:**
   * Malware infects devices, creating a botnet.
   * Attacker controls botnet via C2 server.
2. **Attack Launch:**
   * Botnet floods target with traffic (volume, protocol, or application-layer).
   * Overwhelms target's resources.
3. **Service Disruption:**
   * Target becomes inaccessible to legitimate users.
   * Results in denial of service.
4. **Attack End/Continue:**
   * Attacker stops or prolongs attack.
   * Ransom may be demanded.

**H. Data Breach**

- Definition: Unauthorized access/disclosure of sensitive data.

- Data Types: PII (personal info), financial, health, IP.

- Causes:

* Cyberattacks (hacking, malware, phishing).
* Human error (accidental leaks, lost devices).
* Insider threats (malicious employees).
* Vulnerabilities (software, network).

- Consequences:

* Individual: Identity theft, fraud, privacy loss.
* Organization: Financial loss, reputational damage, legal issues.

**I. Network Security Devices**

- VPN-Enabled Router: provides a secure connection to remote users across a public network and into the enterprise network.

- NGFW: provides stateful packet inspection, application visibility and control, a next-generation intrusion prevention system (NGIPS), advanced malware protection (AMP), and URL filtering.

- NAC: includes authentication, authorization, and accounting (AAA) services. In larger enterprises, these services might be incorporated into an appliance that can manage access policies across a wide variety of users and device types. The Cisco Identity Services Engine (ISE) is an example of a NAC device.

**J. Endpoint protection**

- What: Securing devices (laptops, phones, servers) on a network.

- Why: Endpoints = attack entry points.

- Key tools:

* Antivirus/Malware (detects threats).
* EDR (monitors & responds).
* Firewall (controls traffic).
* DLP (data loss prevention)

- Focus: Proactive defense, centralized control.