VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

UNIT 02
ARP SPOOFING

By
Dr. Ravi Verma

Output of this Presentation

- Students will be able to perform different attacking activities like Man in the Middle attack for realizing the impact of ARP Spoofing and MTMA.

Contents To Be Discuss Cont….

- ARP Poisoning or Spoofing
- What Is an ARP?
- An ARP should
- ARP Attacks
- Goal
- Known ARP Vulnerabilities
- ARP Poisoning Attack Prevention
- Conclusion

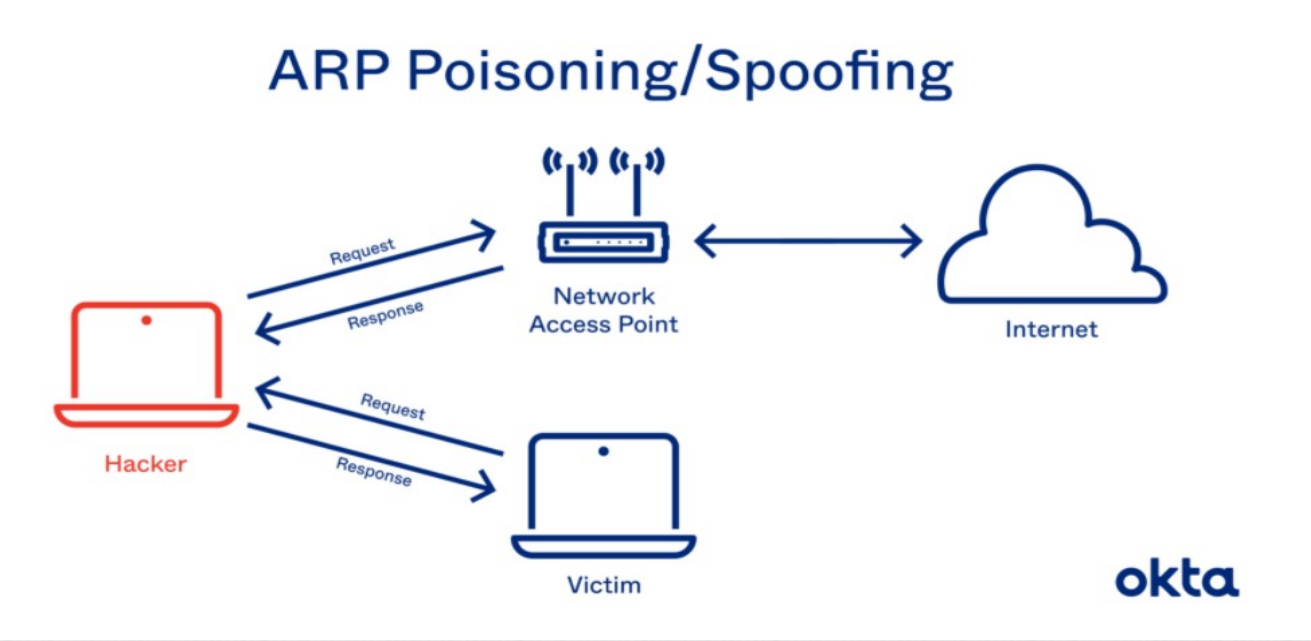
ARP Poisoning or Spoofing

- ARP poisoning (also known as ARP spoofing) is a cyber attack carried out through malicious ARP messages.
- An ARP attack is difficult to detect, and once it's in place, the impact is impossible to ignore.

ARP Poisoning or Spoofing Cont..

- A hacker that successfully implements either ARP spoofing or ARP poisoning could gain control of every document on your network. You could be subject to spying, or your traffic could grind to a halt until you give the hacker what's requested for ransom.

ARP Poisoning or Spoofing Cont..



What Is an ARP?

- In 2001, developers introduced the address resolution protocol (ARP) to Unix developers. At the time, they described it as a "workhorse" that could establish IP-level connections to new hosts.
- The work is critical, especially if your network is constantly growing, and you need a way to add new functionality without authorizing each request yourself.

What is ARP? Cont..

- The basis of ARP is media access control (MAC). As experts explain, an MAC is a unique, hardware-level address of an ethernet network interface card (NIC). These numbers are assigned at the factory, although they can be changed by software.

An ARP should:

- **Accept requests.** A new device asks to join the local area network (LAN), providing an IP address.
- **Translate.** Devices on the LAN don't communicate via IP address. The ARP translates the IP address to a MAC address.
- **Send requests.** If the ARP doesn't know the MAC address to use for an IP address, it sends an ARP packet request, which queries other machines on the network to get what's missing.

ARP Attacks: Key Definitions

- A malicious developer, hoping to gain access to important data, could expose vulnerabilities and sneak inside, and you may never know it's happening.
- Two types of ARP attacks exist.
- **ARP spoofing:** A hacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN.
- **ARP poisoning:** After a successful ARP spoofing, a hacker changes the company's ARP table, so it contains falsified MAC maps. The contagion spreads.

Goal

- The goal is to link a hacker's MAC with the LAN. The result means any traffic sent to the compromised LAN will head to the attacker instead.
- At the end of a successful ARP attack, a hacker can:
- **Hijack.** Someone may look over everything that heads to the LAN before releasing it.
- **Deny service.** Someone may refuse to release anything from the infected LAN unless some kind of ransom is paid.

Goal Cont..

- **Sit in the middle.** Someone conducting a man-in-the-middle attack can do almost anything, including altering documents before sending them out. These attacks both threaten confidentiality and reduce user confidence. They are among the most dangerous attacks anyone can perpetrate.
- If a hacker wants to take over an end host, the work must be done quickly. ARP processes expire within about 60 seconds. But on a network, requests can linger for up to 4 hours. That leaves plenty of time for a hacker to both contemplate and execute an attack.

Known ARP Vulnerabilities

- Speed, functionality, and autonomy were the goals when ARP was developed. The protocol wasn't made with security in mind, and it's proven very easy to spoof and tweak for malicious ends.
- A hacker needs just a few tools to make this work.
- **Connection:** The attacker needs control of one LAN-connected machine. Better yet, the hacker is directly connected to the LAN already.

Known ARP Vulnerabilities

- **Coding skills:** The hacker must know how to write up ARP packets that are immediately accepted or stored on the system.
- **Outside tools:** A hacker could use a spoofing tool, such as Arpspoof, to send out falsified or otherwise inauthentic ARP responses.
- **Patience.** Some hackers breeze into systems quickly. But others must send dozens or even hundreds of requests before they fool the LAN.

Known ARP Vulnerabilities

- ARP is stateless, and networks tend to cache ARP replies. The longer they linger, the more dangerous they become. One leftover reply could be used in the next attack, which leads to ARP poisoning.
- No method of identity proofing exists in a traditional ARP system. Hosts can't determine if packets are authentic, and they can't even determine where they came from.

ARP Poisoning Attack Prevention

- Hackers use a predictable series of steps to take over a LAN. They send a spoofed ARP packet, they send a request that connects to the spoof, and they take over. The request is broadcast to all computers on the LAN, and control is complete.

ARP Poisoning Attack Prevention

- Network administrators can use two techniques to detect ARP spoofing.

1. **Passive:** Monitor ARP traffic and look for mapping inconsistencies.
2. **Active:** Inject falsified ARP packets into the network. A spoofing attack like this helps you identify weak points in your system. Remediate them quickly, and you could stop an attack in progress.

Protection Tools to Consider

- Plenty of companies provide monitoring programs you can use to both oversee your network and spot ARP problems.
- These are common solutions:
- Arpwatch: Monitor ethernet activity, including changing IP and MAC addresses, via this Linux tool. Look over the log every day, and access timestamps to understand just when the attack happened.

ARP Poisoning Attack Prevention Cont..

- ARP-GUARD: Tap into a graphic overview of your existing network, including illustrations of switches and routers. Allow the program to develop an understanding of what devices are on your network and build rules to control future connections.
- XArp: Use this tool to detect attacks happening below your firewall. Get notified as soon as an attack begins, and use the tool to determine what to do next.

ARP Poisoning Attack Prevention Cont..

- **Wireshark:** Use this tool to develop a graphic understanding of all the devices on your network. This tool is powerful, but you may need advanced skills to implement it properly.
- **Packet filtering:** Use this firewall technique to manage network access by monitoring incoming and outgoing IP packets. Packets are allowed or stopped based on source and destination IP addresses, ports, and protocols.
- **Static ARP:** These ARPs are added to the cache and retained on a permanent basis. These will serve as permanent mappings between MAC addresses and IP addresses.

11 Types of Spoofing Attacks Every Security Professional Should Know About

1. ARP Spoofing

- This one is a common source of man-in-the-middle attacks. To execute it, a cybercriminal inundates a local area network with falsified Address Resolution Protocol (ARP) packets in order to tamper with the normal traffic routing process. The logic of this interference boils down to binding the adversary’s MAC address with the IP address of the target’s default LAN gateway.

11 Types of Spoofing Attacks Every Security Professional Should Know About

2.MAC Spoofing

In theory, every network adapter built into a connected device should have a unique Media Access Control (MAC) address that won't be encountered elsewhere. In practice though, a clever hack can turn this state of things upside down. An attacker may harness imperfections of some hardware drivers to modify, or spoof, the MAC address. This way, the criminal masquerades his device as one enrolled in a target network to bypass traditional access restriction mechanisms.

11 Types of Spoofing Attacks Every Security Professional Should Know About

3.IP Spoofing

- To perform this attack, the adversary sends Internet Protocol packets that have a falsified source address. This is a way to obfuscate the actual online identity of the packet sender and thereby impersonate another computer. IP spoofing is often used to set DDoS attacks in motion. The reason is that it’s hard for digital infrastructure to filter such rogue packets, given that each one appears to hail from a different address and therefore the crooks feign legitimate traffic quite persuasively.

11 Types of Spoofing Attacks Every Security Professional Should Know About

4. DNS Cache Poisoning (DNS Spoofing)

- Every tech-savvy user knows the Domain Name Server (DNS) wiki: it maps domain names to specific IP addresses so that people type easy-to-remember URLs in the browser rather than enter the underlying IP strings. Threat actors may be able to contort this mapping logic by piggybacking on known DNS server caching flaws. As a result of this interference, the victim runs the risk of going to a malicious replica of the intended domain. From a cybercriminal's perspective, that's a perfect basis for phishing hoaxes that look really true-to-life.

Conclusion

- This Presentation describes the ARP and Its various types .
- This presentation also brings the Effect of ARP or Man in the Middle Attack in Network .

Question ?