BARI ANKIT (56)

Exp 9: Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark.

Detecting ARP Spoofing Using Nmap, ARPWATCH, and Wireshark

ARP Spoofing (also known as ARP Poisoning) is a type of cyberattack where an attacker sends fake ARP (Address Resolution Protocol) messages onto a network. This results in associating the attacker's MAC address with the IP address of a legitimate device (such as a router or another host). As a result, traffic meant for the legitimate device is intercepted by the attacker, potentially leading to a man-in-the-middle attack.

To detect ARP Spoofing, you can use various tools such as Nmap, ARPWatch, and Wireshark.

---

1. Detecting ARP Spoofing with Nmap

Nmap doesn't have a direct "ARP Spoofing" detection feature, but it can help you identify discrepancies in the ARP cache by performing host discovery or by using the ARP scan.

ARP Scan with Nmap

Nmap can detect changes in ARP tables using the -PR option, which sends ARP requests on a local network to identify devices and their MAC addresses. By checking for inconsistent IP-MAC pairings, you can identify potential ARP spoofing attacks.

1. Perform an ARP Scan:

Run the following command to scan a subnet for devices and their IP-MAC associations:

```
nmap -sn -PR 192.168.1.0/24
```

This command tells Nmap to perform an ARP discovery scan (-PR) on the IP range 192.168.1.0/24. It will display the IP-MAC pairings of the devices found in that range.

2. Compare Results:

   - If you notice duplicate IP addresses mapping to different MAC addresses, it is a strong indication that ARP spoofing might be occurring.
   - Alternatively, if multiple IPs are resolving to a single MAC address, it could point to a spoofing attempt where a malicious actor has made multiple devices point to their MAC address.

---

2. Detecting ARP Spoofing with ARPWATCH

ARPWatch is a tool specifically designed to monitor ARP activity on a network. It listens for ARP replies and can detect any changes in the ARP cache, such as when a host changes its MAC address or when an IP-MAC mapping is duplicated.

Installing ARPWatch

On Linux (Ubuntu/Debian):

1. Install ARPWatch:

```
sudo apt update
```

```
sudo apt install arpwatch
```

2. Start ARPWatch to monitor the network:

```
sudo service arpwatch start
```

ARPWatch will now monitor the local network for any changes in ARP mappings. It keeps logs of ARP changes, which you can view by accessing the log files.

Viewing ARPWatch Logs

1. Check ARPWatch Log: ARPWatch typically logs events in /var/log/arpwatch.log. You can check the log by running:

```
cat /var/log/arpwatch.log
```

The log will show events like:

   - New IP-MAC mappings
   - Changes in MAC addresses
   - Duplicate IP address warnings

2. Detecting ARP Spoofing:
   - If ARPWatch detects an IP address being associated with multiple MAC addresses, it will log an event.
   - A common sign of ARP spoofing is multiple warnings of duplicate IP addresses associated with different MAC addresses. ARPWatch will alert you to these suspicious events.

---

3. Detecting ARP Spoofing with Wireshark

Wireshark is a network protocol analyzer that allows you to capture and inspect network traffic. By analyzing ARP packets, you can detect ARP spoofing by looking for suspicious ARP replies.

Capturing ARP Packets with Wireshark

1. Start Wireshark and begin a capture on the network interface connected to the same network as the suspected device.
2. Set ARP Filter:

Apply the filter arp in Wireshark to capture only ARP packets:

This will display all ARP requests and responses on the network.

3. Look for Suspicious ARP Packets:
   - In a normal network, each IP address should have one unique MAC

address. If you see multiple ARP responses from different MAC addresses associated with the same IP, it's a potential sign of ARP spoofing.

   - Specifically, ARP replies (not requests) are the key indicators of ARP spoofing. You should see legitimate devices respond to ARP requests with their MAC address. If an attacker spoofs ARP replies, it will show as an IP address being mapped to a different MAC address.

4. Identify ARP Spoofing by Looking for Duplicate Entries:
   - Pay attention to duplicate ARP replies for the same IP address but with different MAC addresses. For example:

IP: 192.168.1.1 --> MAC: 00:11:22:33:44:55

IP: 192.168.1.1 --> MAC: 00:66:77:88:99:AA

This indicates that the same IP address (192.168.1.1) is being associated with two different MAC addresses, which could be the result of ARP spoofing.

5. Use Wireshark Statistics to Analyze ARP Packets: You can also use Wireshark's Statistics menu to analyze ARP packets:
   - Go to Statistics > Protocol Hierarchy to view the distribution of protocols on your network.
   - Look for ARP packets and analyze their frequency.
   - A high number of ARP replies from different MAC addresses for the same IP could signal a spoofing attack.

---

4. Combining These Tools for Effective ARP Spoofing Detection

While each tool can help you detect ARP spoofing independently, combining them will give you a more complete view of your network:

- Nmap provides an easy way to scan the network and look for duplicate IP-MAC pairs.
- ARPWatch offers continuous monitoring and alerts for any suspicious ARP activity.
- Wireshark gives you a real-time, detailed packet-level analysis of ARP traffic, which can help you visually spot spoofed ARP replies.

By using all three tools together, you can effectively detect and mitigate ARP spoofing attacks on your network.

---

5. Preventing ARP Spoofing

Here are a few methods to mitigate or prevent ARP spoofing attacks:

1. Static ARP Entries: Manually set static ARP entries on critical network devices (e.g., routers, switches) to prevent changes in IP-MAC associations.

```
sudo arp -s 192.168.1.1 00:11:22:33:44:55
```

This will bind the IP address 192.168.1.1 to the specified MAC address and prevent changes.

2. ARP Spoofing Detection Tools: Implement intrusion detection systems (IDS) like Snort or use dedicated ARP monitoring tools like ARPWatch or XArp.
3. VLAN Segmentation: Segment your network into virtual LANs (VLANs) to limit the scope of ARP spoofing attacks.
4. Encryption and Authentication: Use HTTPS, SSH, or other encrypted protocols to secure communication, preventing attackers from successfully intercepting data even if they are able to spoof ARP.