Vidyavardhini's College of Engineering and Technology

Department of Artificial Intelligence & Data Science

Experiment No. 9
Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark.
Date of Performance:
Date of Submission:

Experiment No. 9

Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark

Course Outcome [CSL602.6]: Apply security basics for different attacks on network.

Aim: Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark

Objectives:

• To understand ARP spoofing.

• To understand ARPWATCH and use it to detect ARP spoofing.

Theory:

1. Nmap (Network Mapper):

While Nmap isn't specifically designed for ARP spoofing detection, it can be used indirectly. Nmap can perform a quick network scan to identify active devices and their MAC addresses. You can then compare this information with the ARP table on your machine (using arp -a on Linux/macOS) to identify any discrepancies.

For example, if Nmap identifies a device with a specific IP address but the ARP table shows a different MAC address associated with that IP, it might indicate ARP spoofing. However, this method can be unreliable as legitimate network configurations can also cause MAC address changes.

2. Arpwatch:

Arpwatch is a dedicated tool for monitoring ARP activity on your network. It keeps track of learned MAC addresses for IPs and monitors for any changes. Here's how it helps detect ARP spoofing:

Database: Arpwatch maintains a database of learned IP/MAC mappings.

Monitoring: It continuously monitors ARP packets on the network.

Alerting: If Arpwatch detects an unsolicited ARP reply (attacker trying to modify the ARP table) or a change in the MAC address associated with a known IP, it raises an alert in the system logs.

3. Wireshark:

Wireshark is a powerful network packet analyzer. While not solely for ARP spoofing detection, it can be used for in-depth analysis of network traffic. Here's how it helps:

Packet Capture: Wireshark can capture live network traffic.

Filtering: You can filter captured packets to focus specifically on ARP traffic.

Analysis: By examining ARP packets, you can identify inconsistencies. For instance, if you see multiple ARP replies for the same IP address with different MAC addresses, it might indicate ARP spoofing.

Conclusion : In conclusion, Nmap is a powerful tool for network exploration, management, and security auditing. It offers several advantages, such as open-source availability, wide range of scanning techniques, and valuable information. However, it also has some disadvantages, such as complexity and potential for false positives. Nmap has several applications in the cybersecurity field, including network exploration, security auditing, penetration testing, and network monitoring.