****

**YILDIZ TECHNICAL UNIVERSITY**

**FACULTY OF ELECTRICAL AND ELECTRONICS**

**SECURITY OF COMPUTER SYSTEMS**

**(BLM4011)**

**LAB 1 – ARP POISONING**

20011901 – Muhammet Kayra Bulut

19011707– Barış Can Yılmaz

kayra.bulut@std.yildiz.edu.tr

can.yilmaz8@ std.yildiz.edu.tr

**DEPARTMENT OF COMPUTER ENGINEERING**

1. **INTRODUCTION**

In an ARP poisoning attack, the attacker sends falsified ARP messages to devices on a local area network. These messages contain incorrect information about the association between the attacker's MAC address and the IP address of another device on the network. This causes the other devices to send their traffic to the attacker's device instead of the intended recipient, allowing the attacker to intercept and potentially modify the traffic. This can be used to steal sensitive information, such as login credentials and other data. ARP poisoning attacks can be difficult to detect and prevent, making them a serious threat to network security.

1. **METHOD**

Attacker must be in the same local network as the victim.

• Finds the IP of the router with the command `ip route` (Figure 1).

• Use a spoofing tool Ettercap to flood the network with forged entries.

• Scan the network for available hosts with Ettercap.

• Selects the router and victim from the host list and sets them as target 1 and

target 2.

• After the spoofing attack, the router MAC address in the ARP cache of the victim is updated with the MAC address of the attacker. So, all packets pass through attacker before being sent to the router. That is why this attack type is also called "Man-in-the-Middle attack".

• Sniff the packets by using a network analyzer tool like Wireshark.

Results can be filtered with "ip.addr == <victim\_ip> && http" filter to

reduce the network traffic down to packets coming only from victim.

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Figure 1**

**metin, ekran görüntüsü, ekran, birkaç içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**Figure 2**

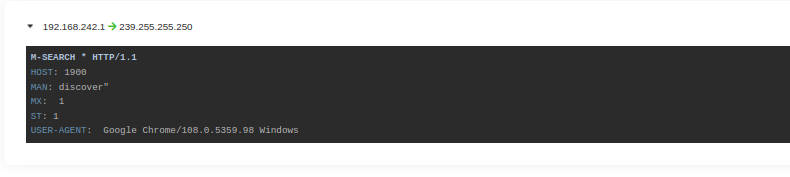
**tablo içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**Figure 3**

1. **RESULTS**

An ARP poisoning attack occurs when a perpetrator sends falsified ARP messages to devices on a local area network. These messages contain incorrect information about the association between the attacker's MAC address and the IP address of another device on the network. This causes the other devices to send their traffic to the attacker's device instead of the intended recipient, allowing the attacker to intercept and potentially modify the traffic. This can be done using a variety of techniques, such as sending a large number of spoofed ARP messages or using malware to automate the process. Once the attacker has gained access to the traffic, they can use it to steal sensitive information or perform other malicious actions.



**Figure 4**