ARP Poisoning

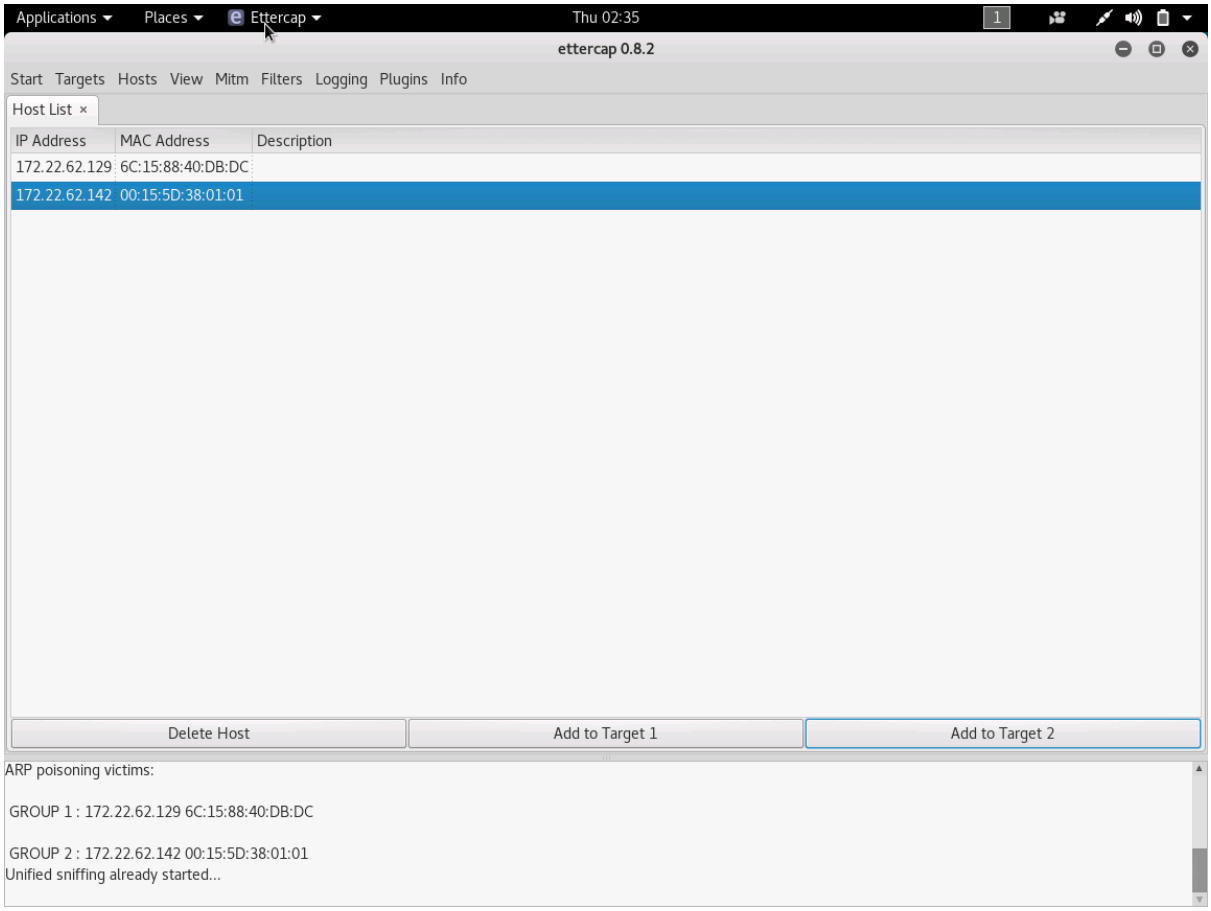
ARP Poisoning (also called ARP Spoofing) is a type of MITM attack carried on IPv4 over a LAN that involves sending malicious ARP packets to a default gateway on a LAN in order to change the ARP bindings, also known as the ARP table. The ARP protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning is very easy to be carried out, as long as the attacker has control of a machine within the target LAN or has direct access to it. An effective ARP poisoning attempt is undetectable to the user.

When an Internet Protocol (IP) datagram is sent from one host to another in a local area network, the destination IP address must be resolved to a MAC address for transmission via the data link layer.[2] When another host's IP address is known, and its MAC address is needed, a broadcast packet is sent out on the local network. This packet is known as an ARP request. The destination machine with the IP in the ARP request then responds with an ARP reply that contains the MAC address for that IP.

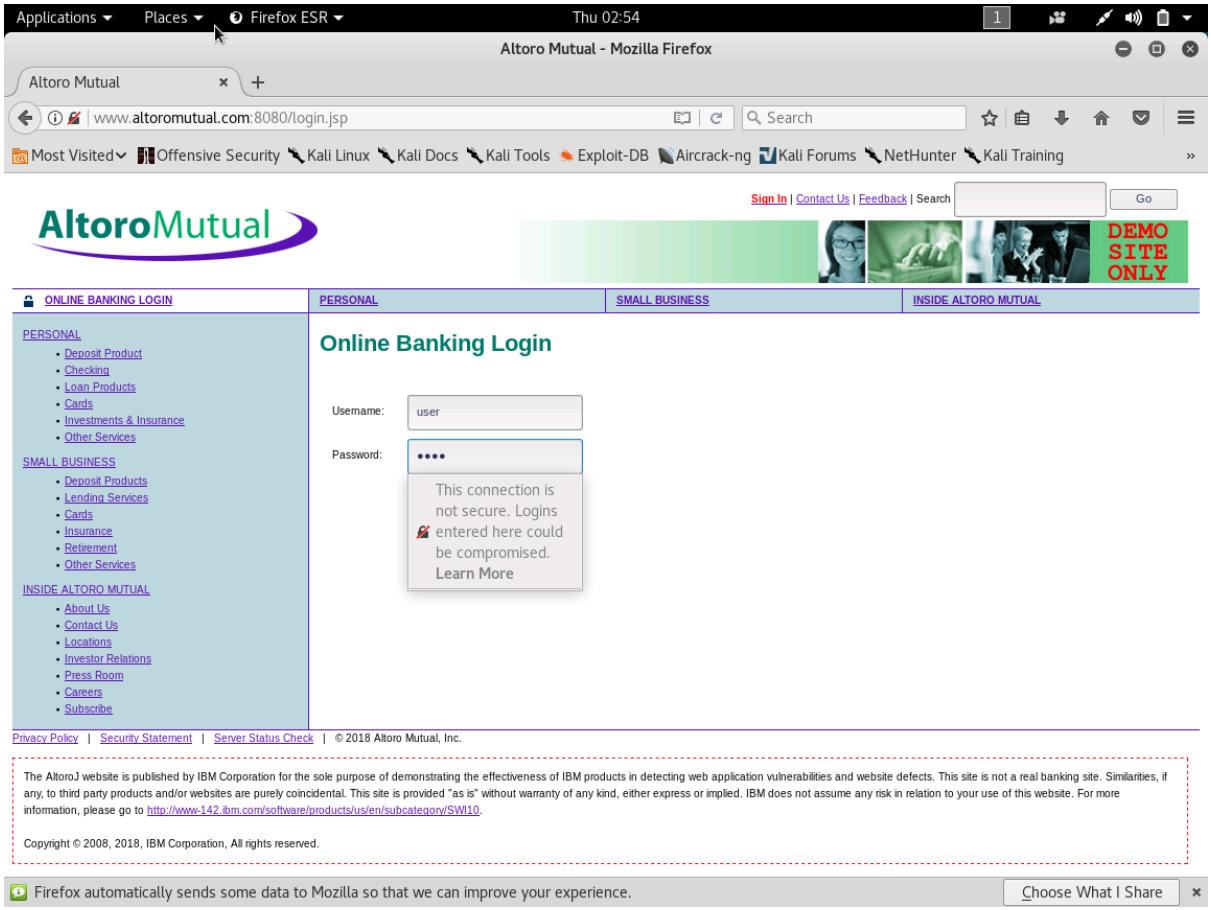
ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.

The attack itself consists of an attacker sending a false ARP reply message to the default network gateway informing it that their MAC address should be associated with his or her target's IP address, so that any traffic meant for the target will be sent to the attacker. The attacker may choose to inspect the packets, while forwarding (spying) modify the data before forwarding it or launch a Denial of service attack by causing some or all of the packets on the network to be dropped.

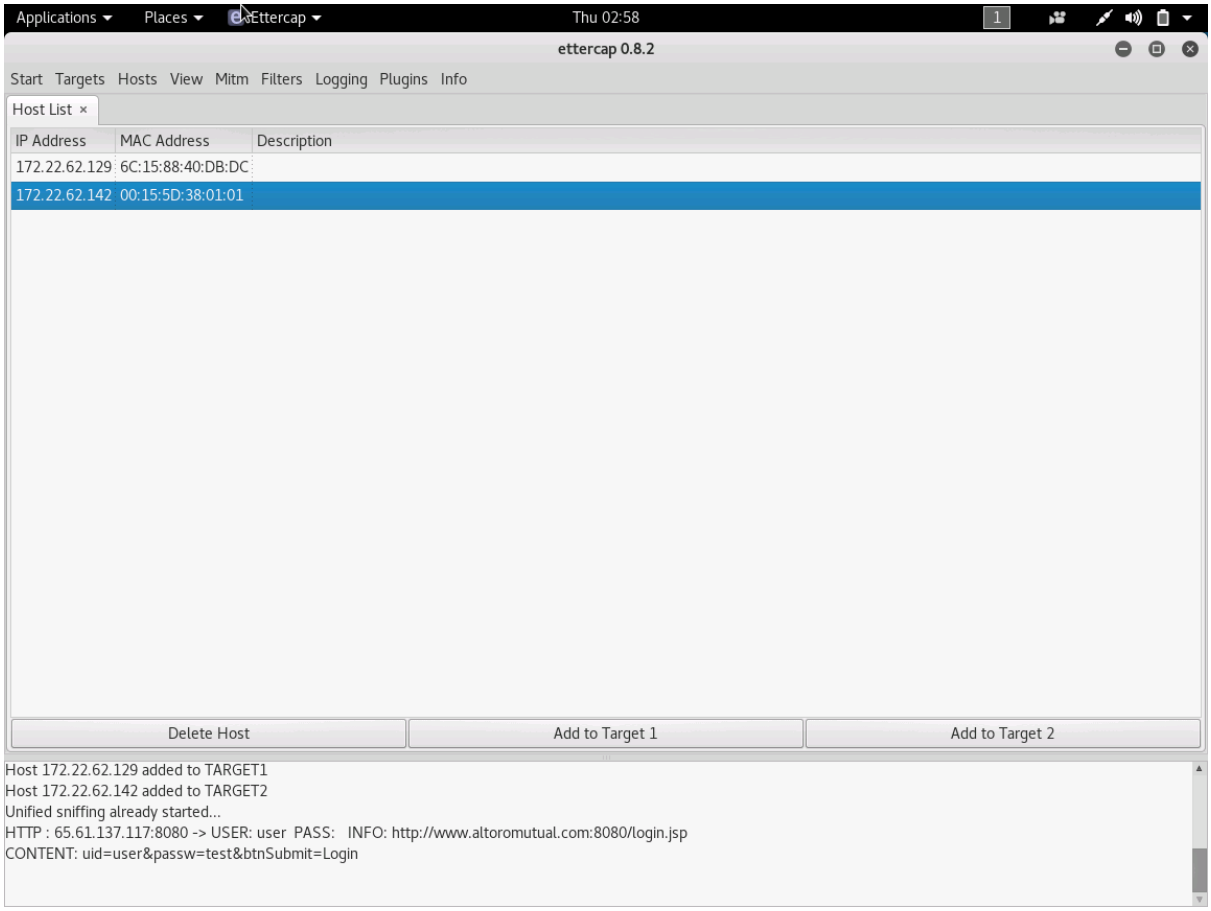
Here, we demonstrate an ARP poisoning attack using Ettercap, a spoofing tool. In this demo, we use two virtual machines on the same network.



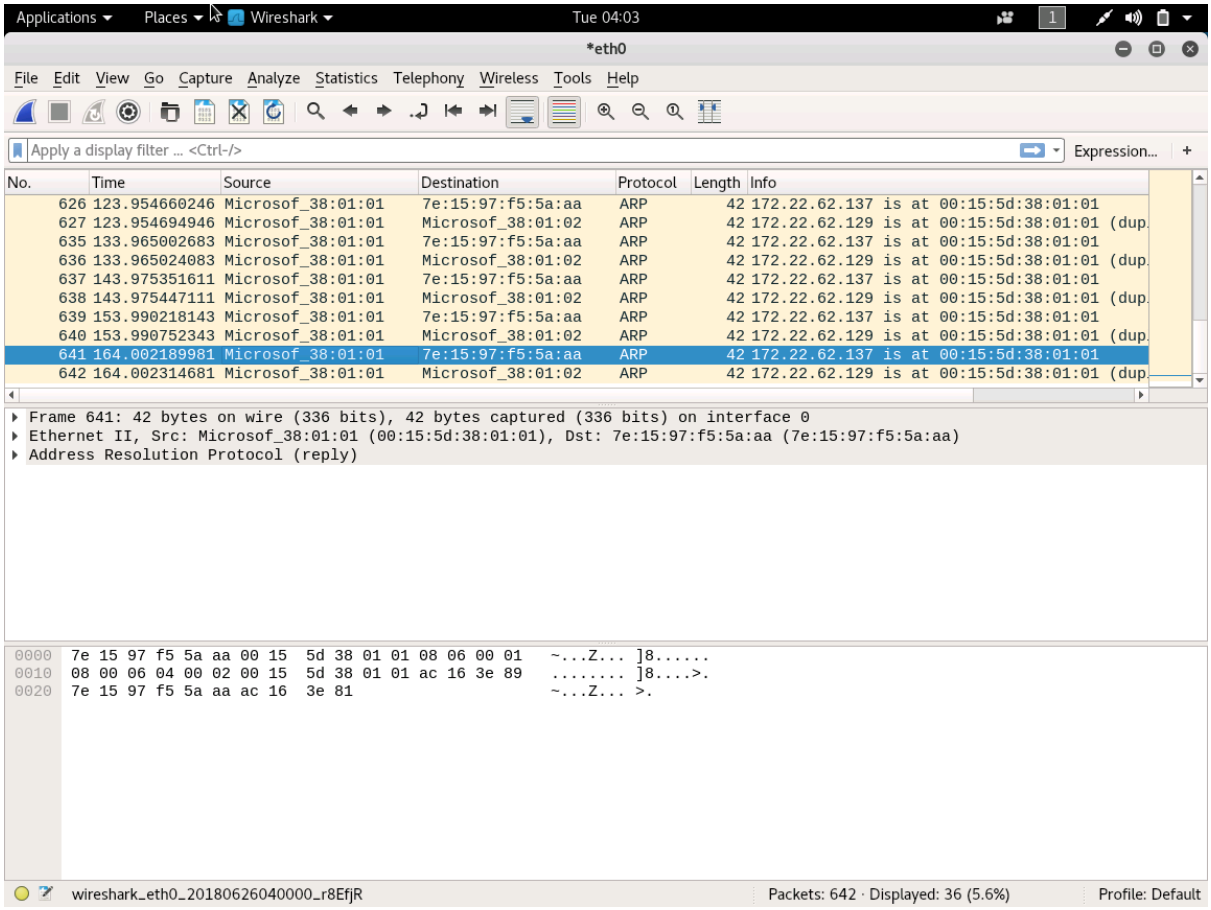
Sniffing has now started after specifying both ends of the attack, namely the target and the host.



The victim enters sensitive information on unencrypted connection, which can be detected by the attacker. Here, we use test credentials, Username: user and Password: test



The attacker's machine automatically detects the sensitive content used on the website by the victim and displays the credentials.



Wireshark on the attack machine shows the ARP packets being flooded over the Network.

How to avoid ARP Poisoning

1. Never enter credentials on unsecure connections. Always verify whether the connection is using HTTPS at the application layer or SSL/TLS at Session layer.

2. Use static ARP bindings: Static ARP bindings do not require any ARP requests over the network again, as every node has the ARP table.

3. Use ARP spoofing detection software: There are many programs available that help organizations detect ARP spoofing attacks. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.

4. Force use IPv6 which uses NDP or use S-ARP[1].

Additional Info and Conclusion

ARP (Address Resolution Protocol) Poisoning, A.K.A. Man-In-The-Middle (MITM), is a very effective attack if proper mitigation techniques have not been implemented. As the MITM attack requires the attacker to be on the same network as the intended victims, an attack would need to be initiated from the inside of the network. With the Ettercap tool being publicly available, and versions that run

[1] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.9787&rep=rep1&type=pdf

on both Windows and Linux based operating systems, most network could be susceptible to this attack if mitigation techniques were not in place.

By using the DHCP Snooping and Dynamic ARP Inspection (DAI) features, multiple types of Layer 2 attacks, including the ARP Poisoning (MITM) attack can be stopped.

DHCP Snooping is a security feature capable of intercepting DHCP messages crossing a switch and blocking bogus DHCP offers. DHCP Snooping uses the concept of trusted and untrusted ports. Typically, the trusted ports are used to reach DHCP servers or relay agents, while untrusted ports are used to connect to clients. All DHCP messages are allowed on trusted ports, while only DHCP client messages are accepted on untrusted ports. As neither servers nor relay agents are supposed to connect to untrusted ports, server messages like DHCPOFFER, DHCPACK, and DHCPNAK are dropped on untrusted ports. In addition, DHCP Snooping builds and maintains a MAC-to-IP binding table that is used to validate DHCP packets received from untrusted ports. DHCP Snooping discards all untrusted DHCP packets not consistent with the information in the binding table. For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces. The DHCP Snooping binding table contains the MAC address, IP address, lease time in seconds, and VLAN port information for the DHCP clients on the untrusted ports of a switch. The information that is contained in a DHCP-snooping binding table is removed from the binding table when its lease expires or DHCP Snooping is disabled in the VLAN

Dynamic ARP Inspection (DAI) is a security feature that helps prevent ARP poisoning and other ARP-based attacks by intercepting all ARP requests and responses, and by verifying their authenticity before updating the switch's local ARP cache or forwarding the packets to the intended destinations. The DAI verification consists primarily of intercepting each ARP packet and comparing its MAC address and IP address information against the MAC-IP bindings contained in a trusted binding table. DAI discards any ARP packets that are inconsistent with the information contained in the binding table. The trusted binding table is dynamically populated by DHCP snooping when this feature is enabled. In addition, DAI allows the configuration of static ARP ACLs to support systems that use statically configured IP addresses and that do not rely on DHCP. DAI can also be configured to drop ARP packets with invalid IP addresses, such as 0.0.0.0 or 255.255.255.255, and ARP packets containing MAC addresses in their payloads that do not match the addresses specified the Ethernet headers.

Another important feature of DAI is that it implements a configurable rate-limit function that controls the number of incoming ARP packets. This function is particularly important because all validation checks are performed by the CPU, and without a rate-limiter, there could be a DoS condition.

DAI associates a trust state with each interface on the system, similar to DHCP Snooping. Packets arriving on trusted interfaces bypass all DAI validation checks, while those arriving on untrusted interfaces go through the DAI validation process. In a typical network configuration for DAI, all ports connected to host ports are configured as untrusted, while all ports connected to switches are configured as trusted. With this configuration, all ARP packets entering the network from a given

switch will have passed the security check. By default, DAI is disabled on all VLANs, and all ports are configured as untrusted.

As discussed earlier, DAI populates its database of valid MAC address to IP address bindings through DHCP snooping. It also validates ARP packets against statically configured ARP ACLs. It is important to note that ARP ACLs have precedence over entries in the DHCP snooping database. ARP packets are first compared to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, then the packet will be denied even if a valid binding exists in the database populated by DHCP snooping.

Note that configuring DHCP Snooping is a prerequisite to configure Dynamic ARP Inspection (DAI). It is also worth noting that if you plan to use any static IP addresses are planned to be used when configuring DHCP Snooping and DAI, a static IP-to-MAC address mapping must also be entered.

References and Whitepapers

1. Most of the inspiration has been drawn from:
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

2. https://security.radware.com/ddos-knowledge-center/ddospedia/arp-poisoning

3. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/ipv6-secure-neighbor.html