Group 9F

Authors :
Praveen Kumar Pendyala - 2919474
Shrikanth Diwakar - 2492658
Ankush Chikhale - 2973449

Task 1.1: Is the network traffic in plaintext? Can you look into every packet which is sent through the network?

The network traffic is in plaintext. However, we can see only the broadcast traffic and the packets intended for us. Under normal circumstances, we cannot see every packet which is sent through the network.

Task 2.1: What is ARP spoofing? Describe the attack and the impact of such an attack on the network topology. What can an attacker achieve by spoofing a MAC-address of another network client?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate device on the network.

Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. The attacker could also falsify the network's Default Gateway address and thus gain access to all traffic flowing through the network.

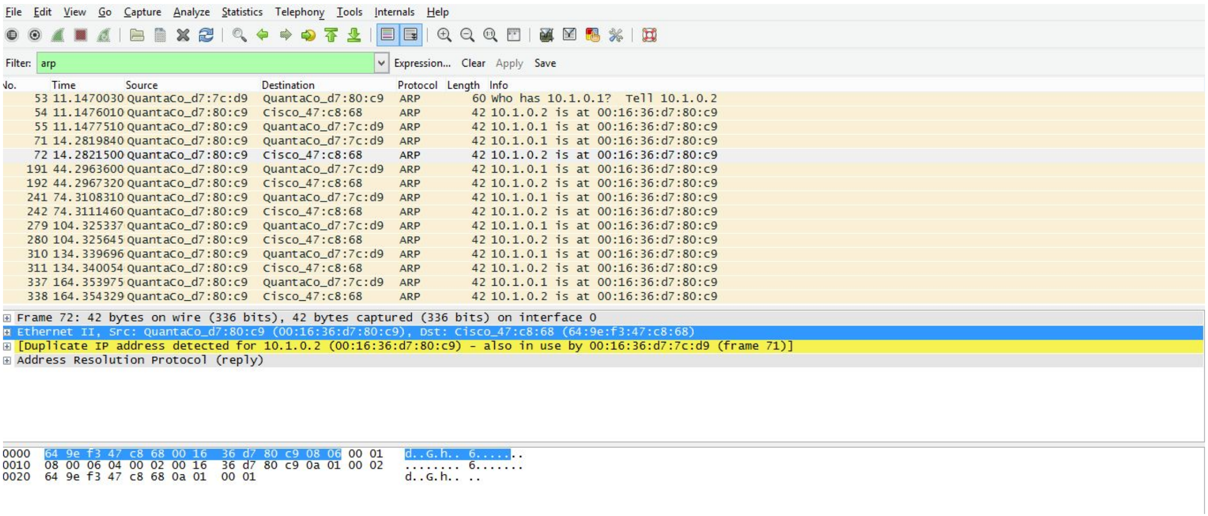
ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. A wide range of attacks such as, not limited to, Denial-of-service, Man-in-the-middle and Session hijacking are possible through ARP spoofing.

Task 2.2: Would it be also possible for an attacker to spoof the MAC-address with an ARP spoofing attack if he is connected to switch 2? Justify your answer.

No, it is not possible to perform an ARP spoofing attack on the client machines connected to switch 1. ARP messages are broadcast messages that are flooded within a broadcast domain. Here, router segregates the LAN and hence ARP request/reply from the attacker connected to switch 2 cannot get past the router 1 to reach the Victim, in this case PC0, who is connected to switch 1.

However, the attacker can still perform an ARP spoofing attack on clients that are within in his broadcast - clients connected, if any, between router 1 and 2.

Task 2.3: Try to perform an ARP spoofing attack in your network environment. Run the tool Cain & Abel on desktop 1 and try to spoof the MAC-address of router 1. Monitor this process with Wireshark from desktop 1. Append a screenshot to your solution on which the ARP spoofing attack is visible and briefly describe the attack operation by explaining the related messages.



ARP Spoofed network traffic. Filtered for ARP packets only.

In the above network log capture screenshot, we can see a warning, in yellow, which states "Duplicate IP address detected for .." This is basically hinting about ARP poisoning. The attack works by poisoning the ARP tables of the devices in the network.

Here, the attacker is interested in bidirectional traffic of a victim.

1. **For victim's Incoming traffic:** The attacker poisons the ARP table entries of every device in the network by pointing his MAC address for Victims IP address. We can see that in the highlighted ARP broadcast packet for 10.1.0.2. All traffic addressed to victim would go through attacker.

2. **For victim's Outgoing traffic:** The attacker poisons the ARP table entries of every device in the network by pointing his MAC address for Gateway IP. We can see that in the highlighted ARP broadcast packet for 10.1.0.1.

Task 2.4: If your attack is successful, contact one of the advisors to login to a service on the server (10.1.2.3) from desktop 0. Then, write down the credentials you were able to obtain via Cain & Abel.

Credentials obtained from logs on the attacker machine.
username : netsec
password : Giflor

Task 2.5: How can an ARP spoofing attack be detected in the network? List some possible indications for such an attack.

Possible ways to detect ARP spoofing.

1. By checking ARP cache to see if there are multiple IPs mapped on to same MAC address. This may however lead to false positives in some cases.
2. By raising an alert whenever an ARP cache entry is updated to a different value.
3. We can check for suspicious messages on Wireshark. As shown in an earlier screenshot, Wireshark warns about duplicate IPs for the same MAC address.

Other possible indications of ARP attack in some special scenarios :

1. Delay in receiving packets.
2. Denial-of-Service from an otherwise trustworthy link/server.

Task 2.6: What kind of countermeasures could protect against an ARP spoofing attack?

Possible countermeasures against ARP spoofing.

1. Static ARP entries : IP-to-MAC mappings in the local ARP cache may be statically entered so that hosts ignore all ARP reply packets.
2. Disabling gratuitous ARP : In this case, an alternative mechanism to update ARP entries should be employed.
3. OS security : There different tools to address ARP spoofing by patching OS at a kernel level. For example : AntiARP for Windows and ArpStar for Linux.

Task 3.1: What is the purpose of the monitor port? Is the result of using such a monitor port comparable with the ARP spoofing attack you performed in the previous task? What kind of device is usually connected to such a monitor port?

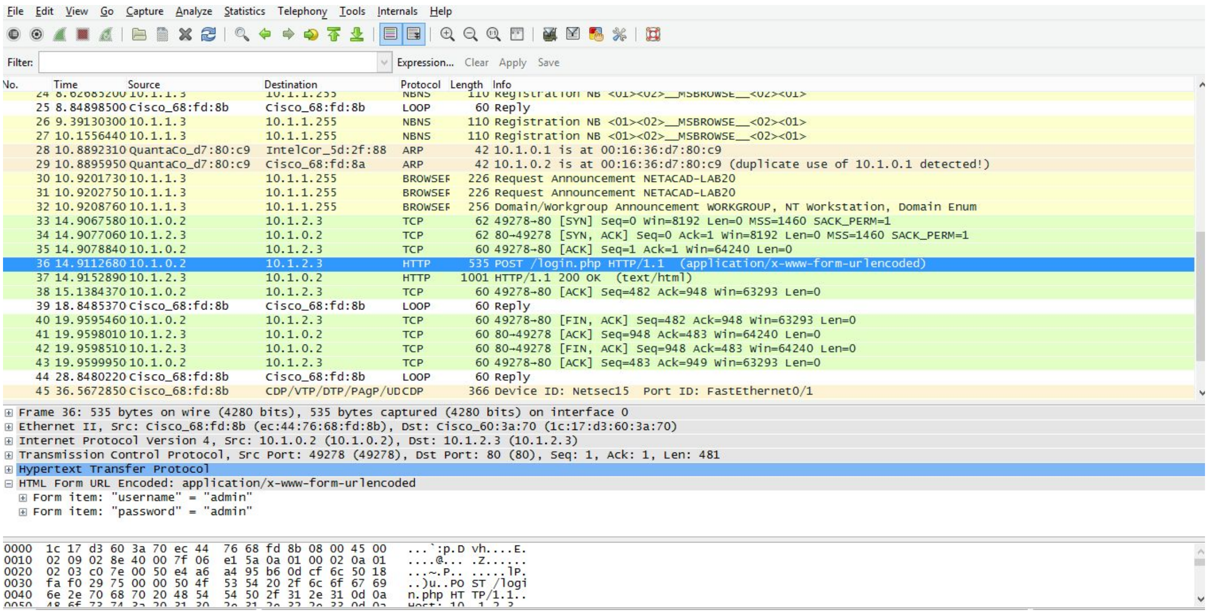
Purpose of a monitor port is to passively observe all the traffic that passes through the switch. Monitor ports are generally used for debugging and Intrusion Detection.

Yes, it is comparable to ARP spoofing (only passive) in the sense that we can sniff all the traffic between router 1 and router 2. However, we cannot modify the traffic, which is possible with ARP spoofing.

Intrusion detection systems, Desktops running tools like Wireshark to capture packets for debugging purpose are some of the devices connected to this port.

Task 3.2, 3.3

In this case, all network traffic is visible.

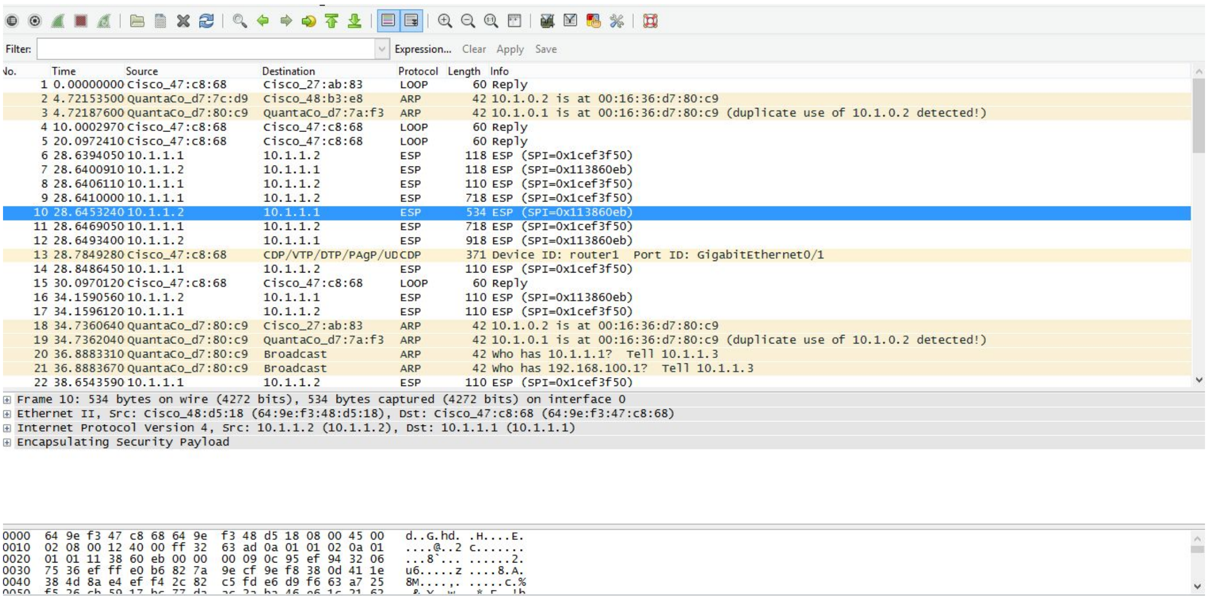


Wireshark log as seen from the Monitor port

Task 4.1: Save the monitored traffic and compare it to the one captured in Task 3.3. What kind of information is still in plain text and which information is encrypted?

We see that Ethernet and IP headers are still in plain text.

However, IP payload is encrypted - this includes all TCP headers, except IP values, and TCP payload data. We can only infer information such as the number of messages that are being exchanged between two IP addresses.



Wireshark log of IPSec traffic encrypted using ESP

Task 4.2: According to Task 4.1 some information is still in plain text and can be monitored by an attacker. Why is it not possible to encrypt this information?

Since we are using ESP protocol in tunnel mode, some part of the packet such as Ethernet and IP headers are not encrypted. This cannot be encrypted to be able to route the packet to the destination. All the intermediate network devices will lookup IP-MAC pair present in the header to route the packet to destination.

Task 4.3: Could IPSec be combined with security mechanisms on other layers? What would be advantages and disadvantages?

Yes. IPSec can be transparently combined with the security mechanisms on layers above it. For example IPSec can be using in conjugation with the Transport layer security protocols like SSH or TLS.

Advantages:
This allows the protection of the otherwise unprotected header fields of the higher layers. It also offers additional security guarantees in both the layers. In case of SSL with IPSec, security guarantees are provided at both Transport and Network layer. All header fields of the SSL protocol will be encrypted by IPSec.

Disadvantages:
Computational and temporal overhead in enforcing security on different layers. Redundant Encryption and Hashing of the same application data at different layers. The redundant work has to be performed both at server and client end.