ARP SPOOFING DETECTION AND PREVENTION

CO-ORDINATORS

Mr.N.Srinivasa Reddy

PRESENTED BY

M PRAVEEN NAIK

21311A04BB

paloalto® NETWORKS

EduSkills

Nation Building Through Skills

SNIST

Sreenidhi Institute of Science and Technology

Because, Life is all about taking the right decisions

ABSTRACT

- As Wi-Fi networks become integral to our daily lives, the security of these networks becomes vital and the persistent threat of Address Resolution Protocol (ARP) spoofing within Wi-Fi environments and presents an in-depth analysis of advanced detection and prevention techniques. ARP spoofing, a technique exploited by attackers to compromise network integrity, demands innovative and robust countermeasures to ensure the confidentiality and integrity of transmitted data.

- By addressing the complexities associated with ARP spoofing, this work aims to fortify Wi-Fi networks against these pervasive threats, ultimately enhancing the overall security posture of wireless communication infrastructures that includes the Attacks as MIMA,DOS Attack.

Hardware & Software Requirements

Hardware requirements:

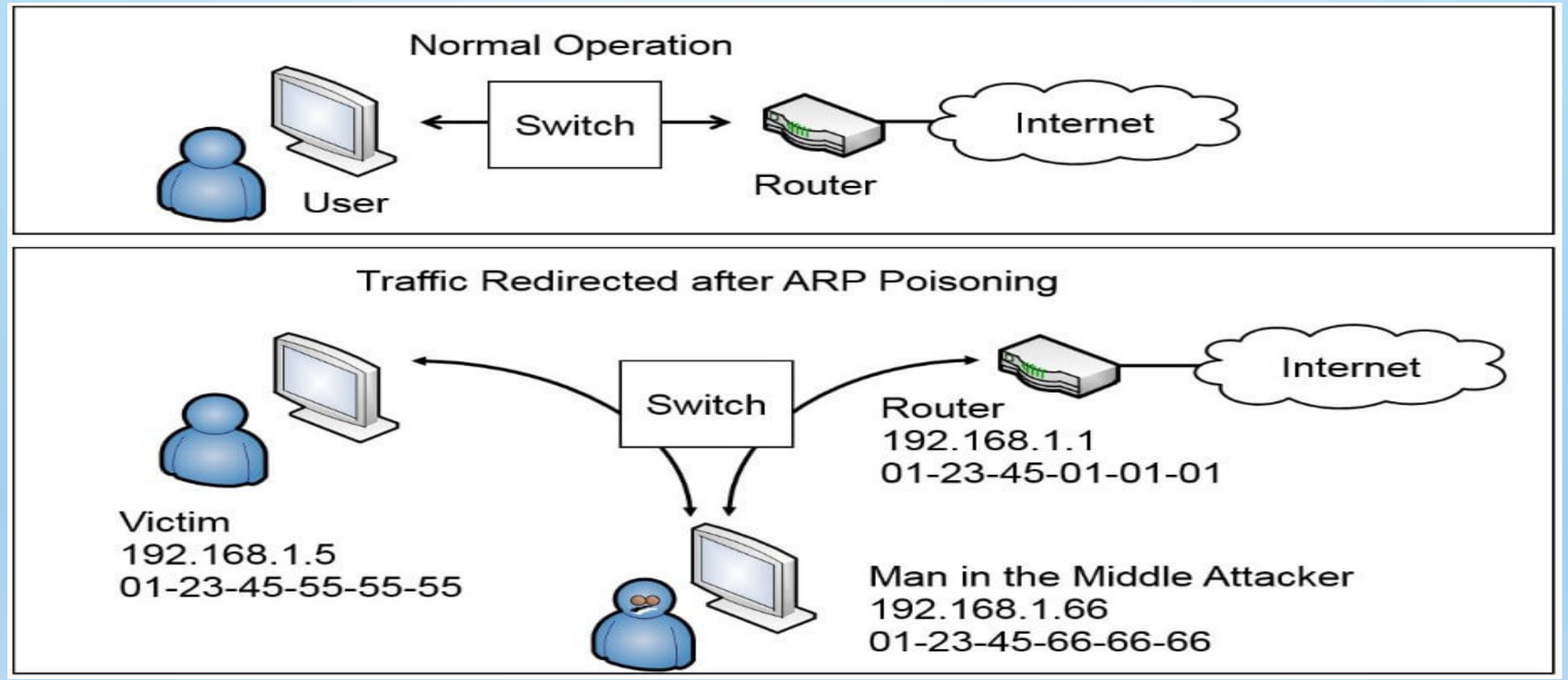
1) Kali Linux - Attackers OS.
2)Windows 10 - Victim’ s OS.
3) Wi-Fi Router - Local Area Network

Software requirements:

1) Wireshark
2) Ettercap
3) Command Prompt

PROBLEM STATEMENT

When a person connects to the public wifi network and working on their sensitive data , it will be vulnerable and have high risk of data breach by the intruder who is connected to the same local network .



Broad overview of Solution

Prevention of ARP Spoofing :

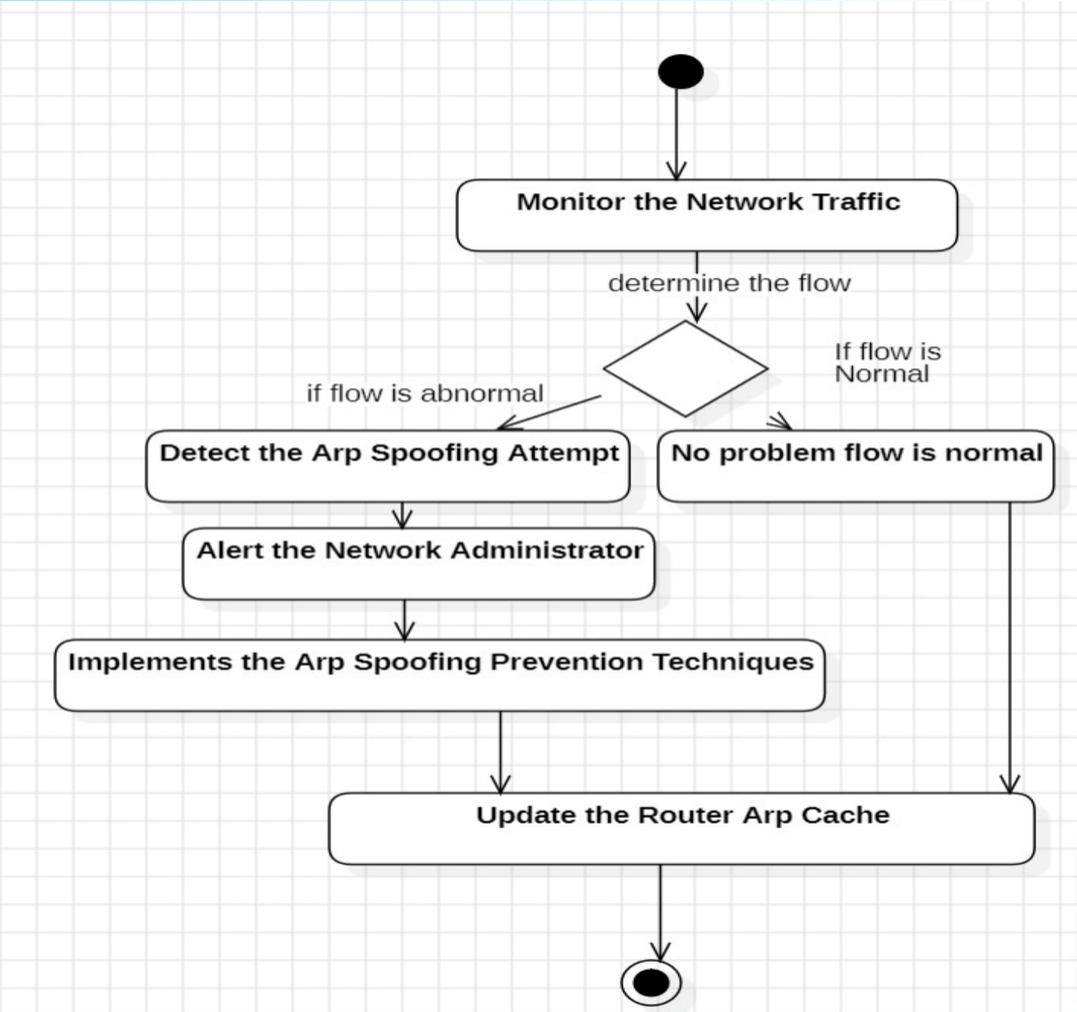
1) Static ARP: In static ARP configuration, network administrators manually enter ARP mappings into the ARP cache of a device.
2) Physical Security : Limit access to network closets or data centers where switches are housed.
3) Network isolation: It involves separating different segments of a network to enhance security and control.
4) Encryption :Encryption is a security measure that transforms plaintext into an ciphertext using algorithms and keys.
5) Switch security : It typically involves configuring features like port security, VLANs to protect against unauthorized access and network attacks.

Change Defaults: Modify default credentials and disable unused ports.

Implement Port Security: Use features like port security and VLANs to control access .

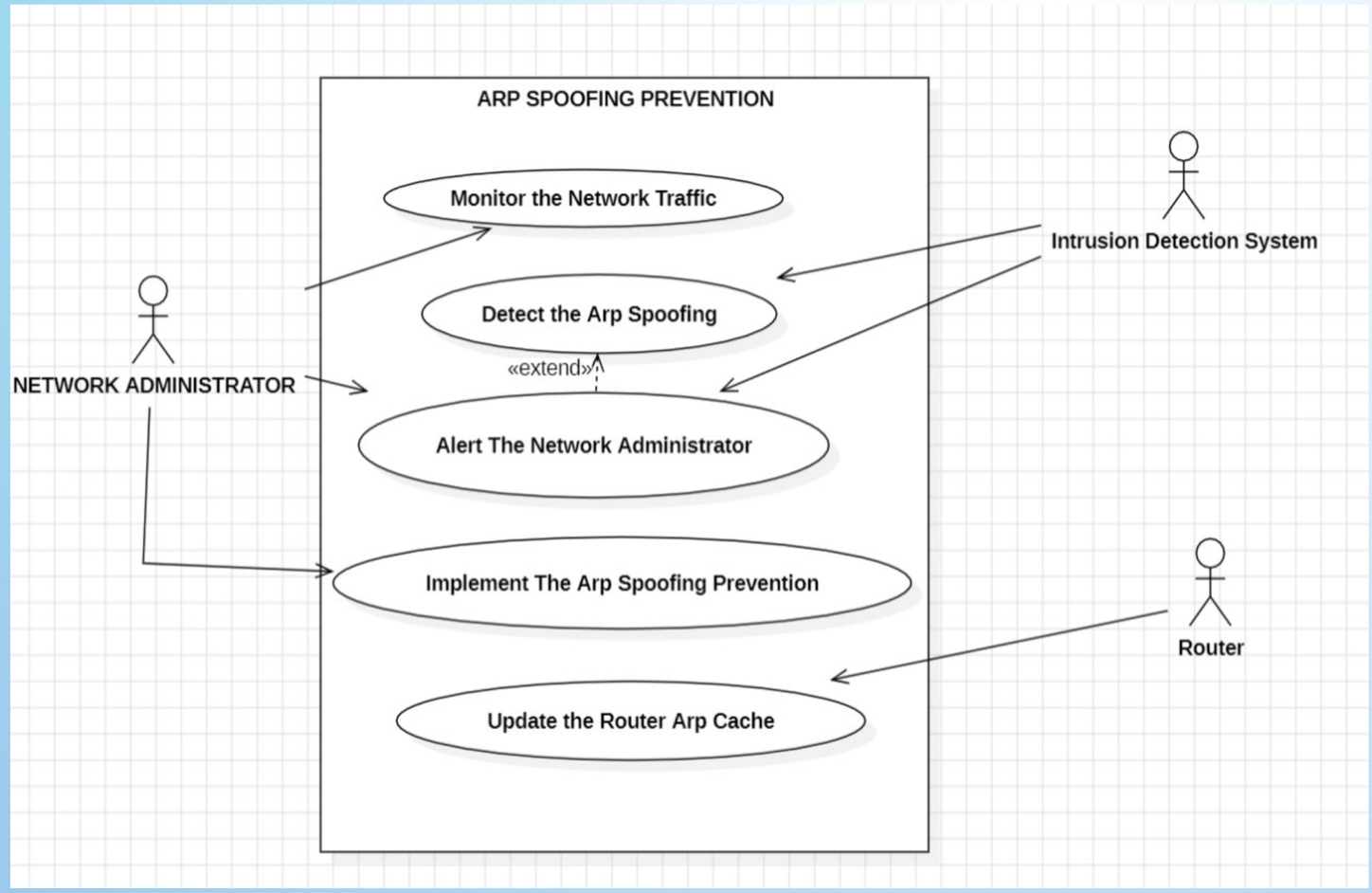
Regular Updates and Monitoring: Keep firmware updated, enable logging, and monitor for security events.

Activity Diagram of ARP Spoofing



An activity diagram is a type of UML (Unified Modeling Language) diagram that visually represents the dynamic aspects of a system or business process. It is particularly useful for modeling workflows and the flow of activities within a system.

Use case Diagram of ARP Spoofing

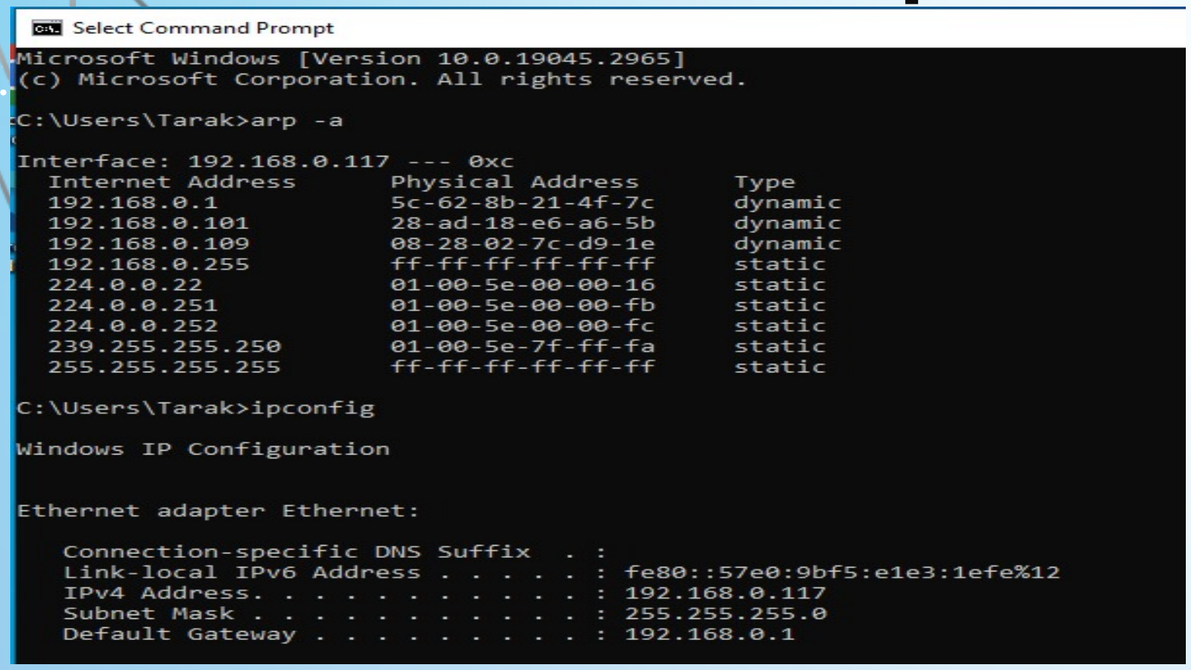


A use case diagram is a visual representation in the Unified Modeling Language (UML) that illustrates the interactions between users (actors) and a system.

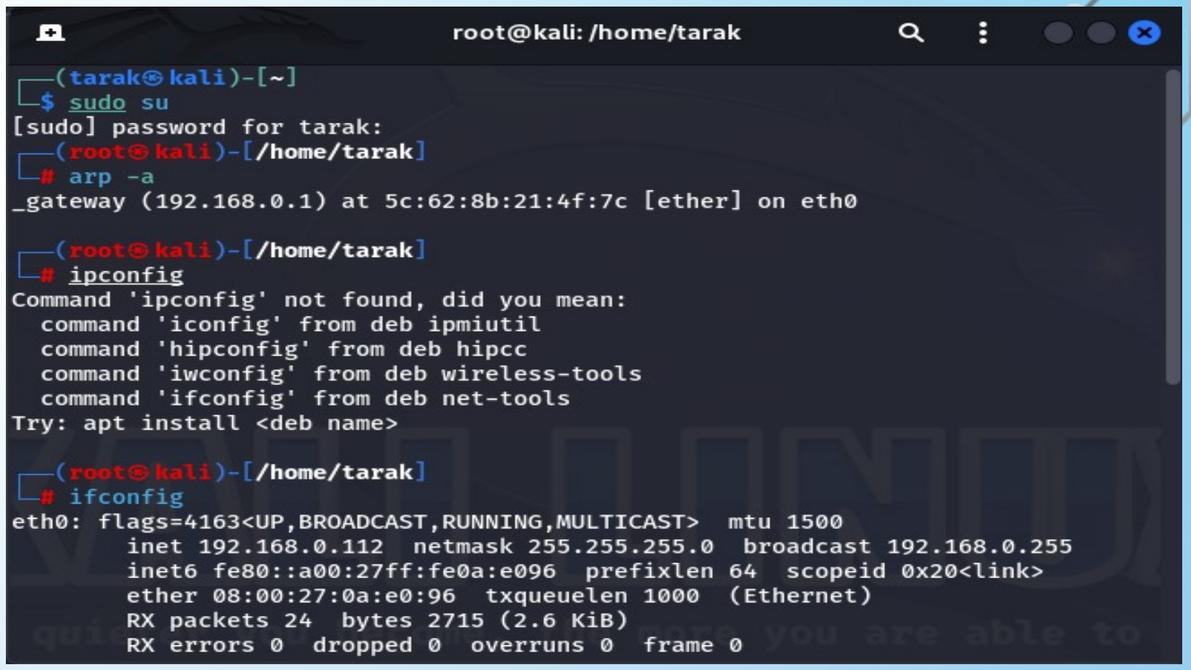
1)Actor
2)Use case
3)Relationship between use case and actor.

ARP spoofing detection

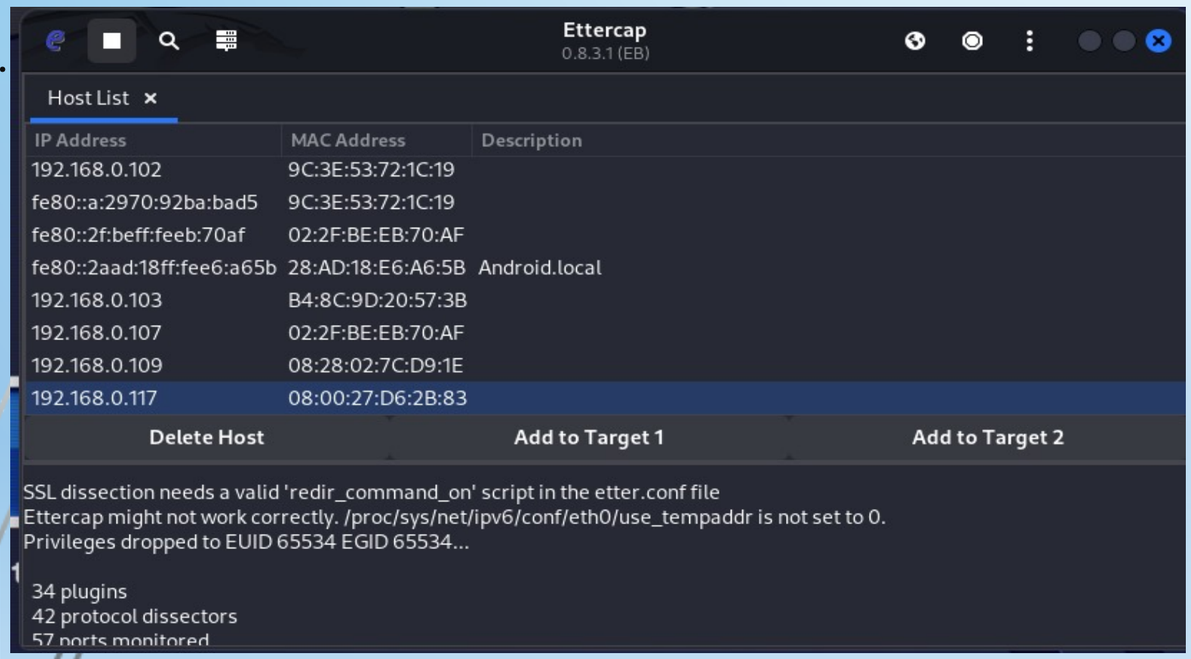
1.



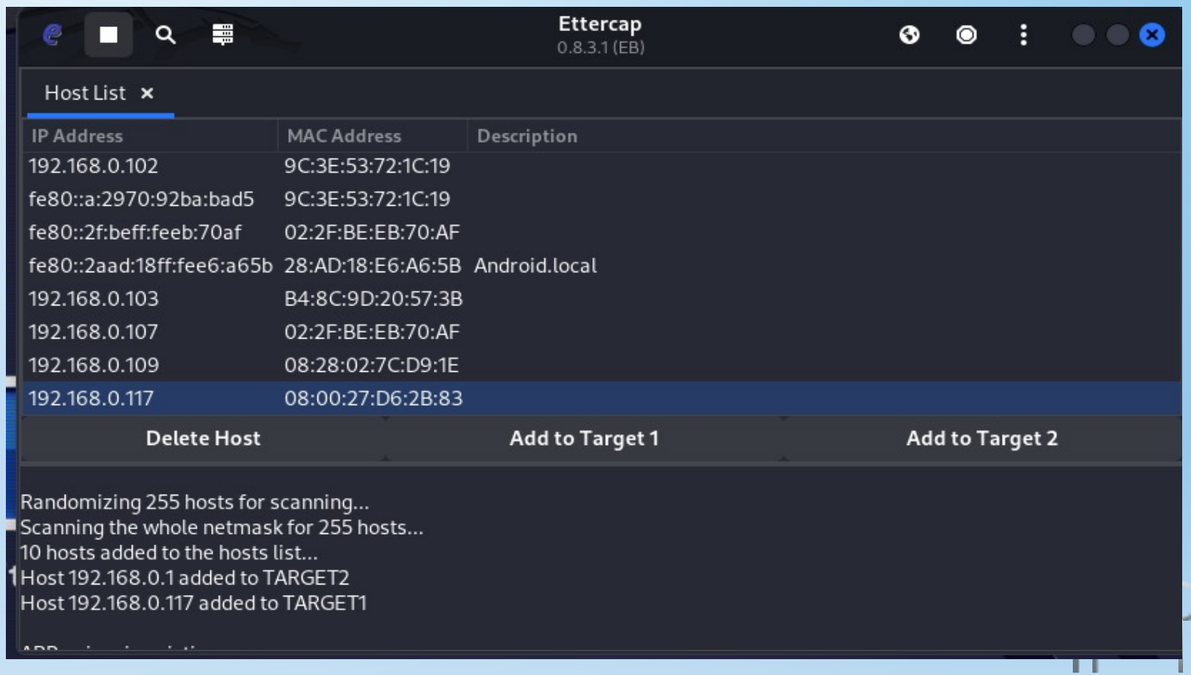
2.



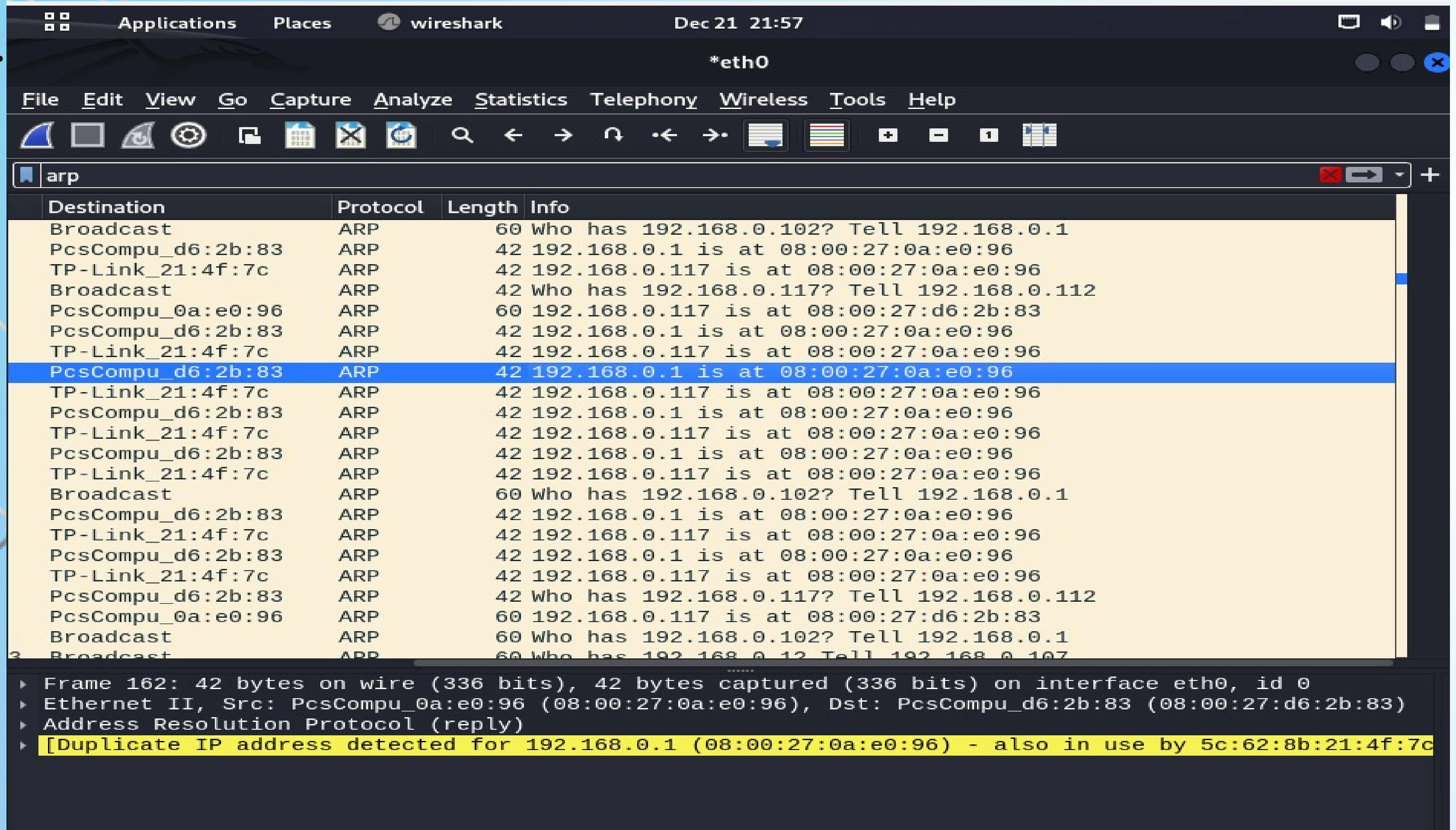
3.



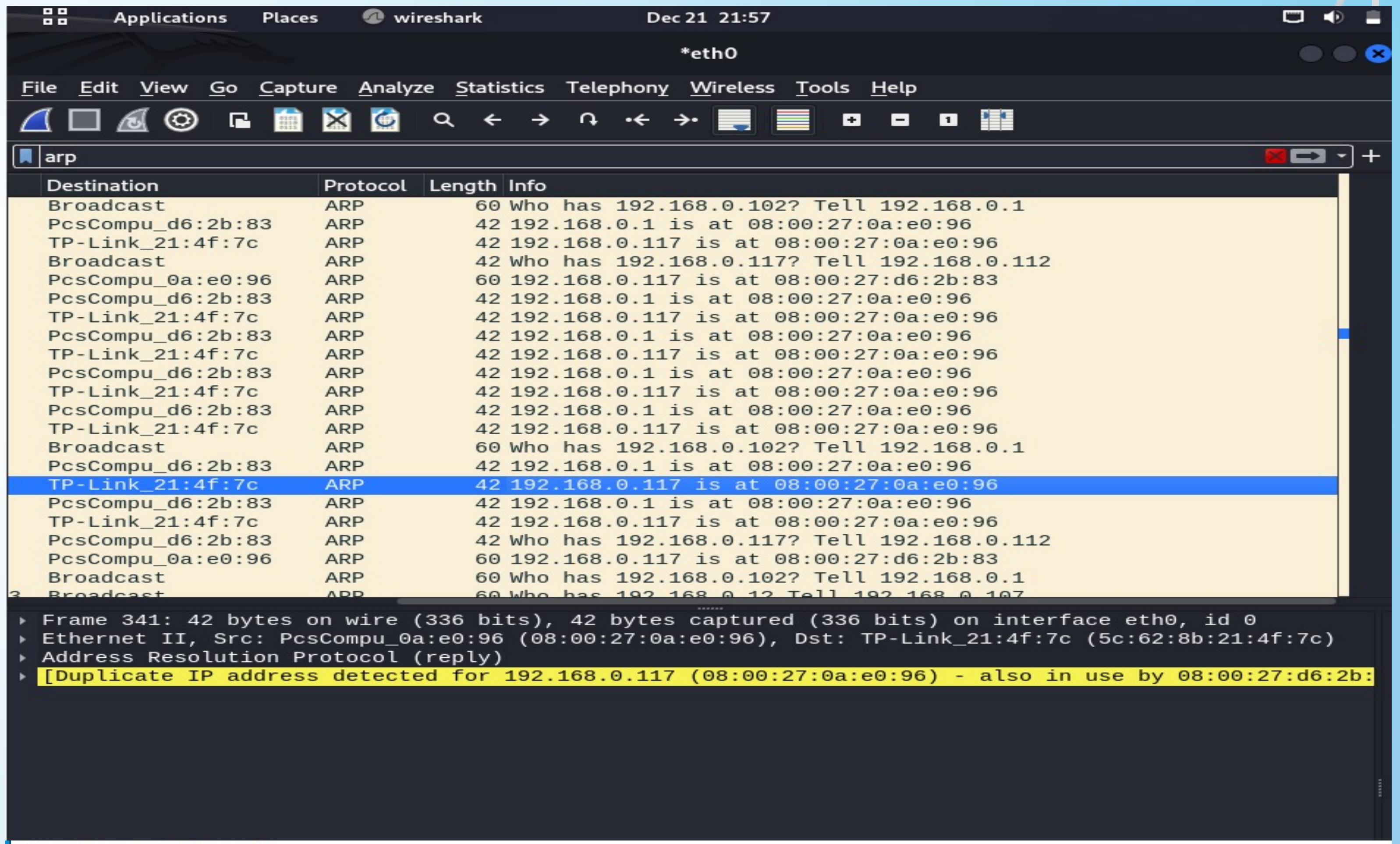
4.



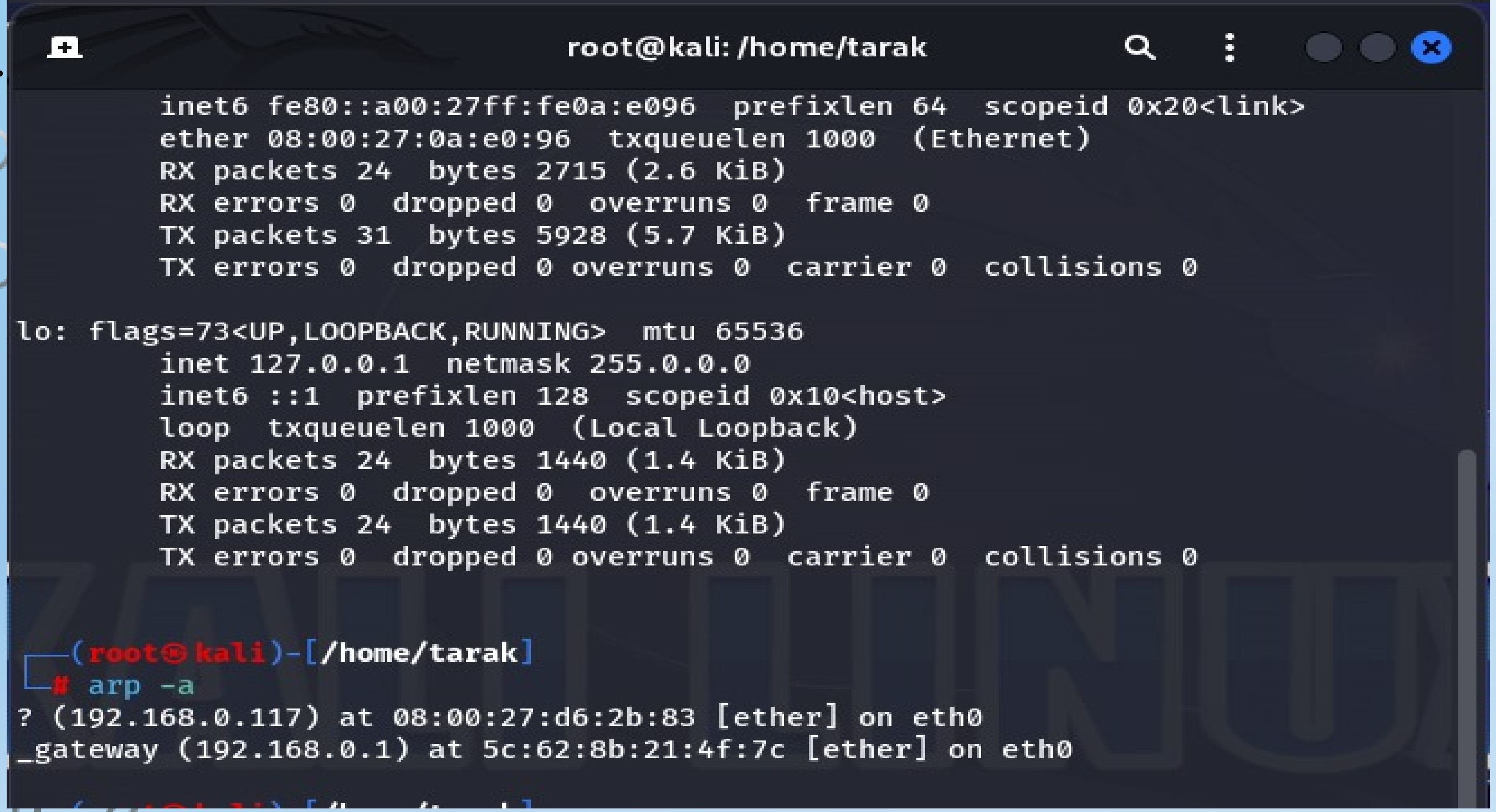
5.


Applications Places wireshark Dec 21 21:57
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Destination Protocol Length Info
Broadcast ARP 60 Who has 192.168.0.102? Tell 192.168.0.1
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
Broadcast ARP 42 Who has 192.168.0.117? Tell 192.168.0.112
PcsCompu_0a:e0:96 ARP 60 192.168.0.117 is at 08:00:27:d6:2b:83
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
Broadcast ARP 60 Who has 192.168.0.102? Tell 192.168.0.1
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 Who has 192.168.0.117? Tell 192.168.0.112
PcsCompu_0a:e0:96 ARP 60 192.168.0.117 is at 08:00:27:d6:2b:83
Broadcast ARP 60 Who has 192.168.0.102? Tell 192.168.0.1
Frame 162: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0a:e0:96 (08:00:27:0a:e0:96), Dst: PcsCompu_d6:2b:83 (08:00:27:d6:2b:83)
Address Resolution Protocol (reply)
[Duplicate IP address detected for 192.168.0.1 (08:00:27:0a:e0:96) - also in use by 5c:62:8b:21:4f:7c

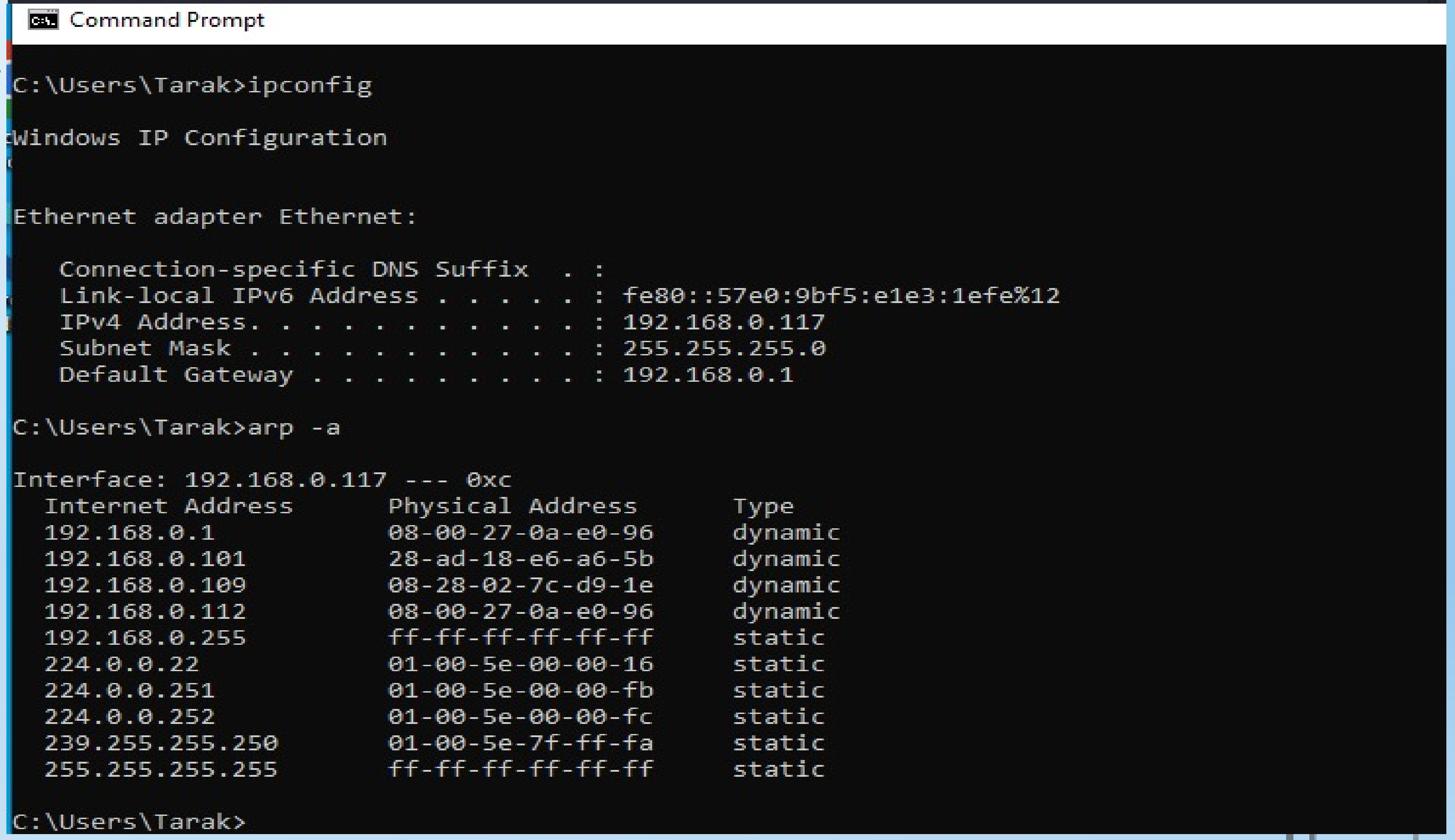
6.


Applications Places wireshark Dec 21 21:57
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Destination Protocol Length Info
Broadcast ARP 60 Who has 192.168.0.102? Tell 192.168.0.1
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
Broadcast ARP 42 Who has 192.168.0.117? Tell 192.168.0.112
PcsCompu_0a:e0:96 ARP 60 192.168.0.117 is at 08:00:27:d6:2b:83
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
Broadcast ARP 60 Who has 192.168.0.102? Tell 192.168.0.1
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 192.168.0.1 is at 08:00:27:0a:e0:96
TP-Link_21:4f:7c ARP 42 192.168.0.117 is at 08:00:27:0a:e0:96
PcsCompu_d6:2b:83 ARP 42 Who has 192.168.0.117? Tell 192.168.0.112
PcsCompu_0a:e0:96 ARP 60 192.168.0.117 is at 08:00:27:d6:2b:83
Broadcast ARP 60 Who has 192.168.0.102? Tell 192.168.0.1
Frame 341: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0a:e0:96 (08:00:27:0a:e0:96), Dst: TP-Link_21:4f:7c (5c:62:8b:21:4f:7c)
Address Resolution Protocol (reply)
[Duplicate IP address detected for 192.168.0.117 (08:00:27:0a:e0:96) - also in use by 08:00:27:d6:2b:

7.


root@kali: /home/tarak
inet6 fe80::a00:27ff:fe0a:e096 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:0a:e0:96 txqueuelen 1000 (Ethernet)
RX packets 24 bytes 2715 (2.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31 bytes 5928 (5.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 24 bytes 1440 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1440 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(root㉿kali)-[/home/tarak]
arp -a
? (192.168.0.117) at 08:00:27:d6:2b:83 [ether] on eth0
_gateway (192.168.0.1) at 5c:62:8b:21:4f:7c [ether] on eth0

8.


Command Prompt
C:\Users\Tarak>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::57e0:9bf5:e1e3:1efe%12
IPv4 Address. . . . . : 192.168.0.117
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : 192.168.0.1
C:\Users\Tarak>arp -a
Interface: 192.168.0.117 --- 0xc
Internet Address Physical Address Type
192.168.0.1 08-00-27-0a-e0-96 dynamic
192.168.0.101 28-ad-18-e6-a6-5b dynamic
192.168.0.109 08-28-02-7c-d9-1e dynamic
192.168.0.112 08-00-27-0a-e0-96 dynamic
192.168.0.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\Tarak>

Prevention methods:

1) Using Static ARP

Creating a static ARP entry in your server can help reduce the risk of spoofing. If you have two hosts that regularly communicate with one another, setting up a static ARP entry creates a permanent entry in your ARP cache that can help add a layer of protection from spoofing.A CISCO router can help examine the ARP information to monitor whether or not an ARP spoofing event is occurring. It may take some advanced knowledge to really understand how to use a static ARP and set it up appropriately. Make sure whatever method you’ re using is executed correctly or you could end up with a false sense of security about your ARP.

2) Encryption

Encryption

Protocols such as HTTPS and SSH can also help to reduce the chances of a successful ARP poisoning attack. When traffic is encrypted, the attacker would have to go to the additional step of tricking the target’ s browser into accepting an illegitimate certificate. However, any data transmitted outside of these protocols will still be vulnerable.

VPNs

A VPN can be a reasonable defense for individuals, but they are generally not suitable for larger organizations. If it is just a single person making a potentially dangerous connection, such as using public wifi at an airport, then a VPN will encrypt all of the data that travels between the client and the exit server. This helps to keep them safe, because an attacker will only be able to see the ciphertext.
It’ s a less-feasible solution at the organizational level, because VPN connections would need to be in place between each computer and each server. Not only would this be complex to set up and maintain, but encrypting and decrypting on that scale would also hinder the network’ s performance.

3) Switch Security:

Most Ethernet switches have features that can help mitigate ARP Poisoning attacks. These features are also known as Dynamic ARP Inspection(DAI) and help in validating the ARP messages and drop packets that show any kind of malicious activity. This also allows one to limit the rate at which ARP messages can pass through the switch. DAI and other such features are now not only available on high-end networking gear but also on all business-grade switches. Usually, DAI is enabled on all ports but the ones connected to other switches. Port security on a switch helps in reducing ARP Cache Poisoning attacks. While using port security, there is no chance that an attacker may take multiple identities over the network. This is because, using port security, a single MAC address can be configured on a switch port.

4) Physical Security:

A very simple way to mitigate ARP Poisoning attacks is to control the physical space of your business. Routing of ARP messages takes place only within a local network. Thus, probable attackers are in physical proximity to the network of the victim. Also, in the case of wireless systems, an attacker might be present in a street or a parking lot. The use of technologies like 802.1x can help in removing any threats to the devices and the network.

5) Network Isolation:

Since ARP messages don’ t have a scope greater than the local subnet, a well-segmented network is better than a normal network. This way, even if the attack occurs, a part of the network will only be affected and the other parts will be safe. Attack in one subnet does not impact the devices in any other subnet. Thus, important resources can be placed in a dedicated segment with high security.

CONCLUSION

► Addressing ARP spoofing is paramount in maintaining the integrity and security of computer networks. The potential for malicious actors to manipulate the ARP protocol underscores the importance of robust detection and prevention mechanisms. By implementing comprehensive security measures, organizations can significantly mitigate the risks associated with ARP spoofing.

► Key measures to ensure security from Arp Spoofing are

1.User Education

2.Use of Secure protocol etc.,