

Names: Yasar Azimi, Qais Haidarzada, Sohail Amiri, Sapida Muska Masood

Lab Exercise: Network sniffing and spoofing with ettercap

Dr. Ala Abdulaziz

Class: ITC 470

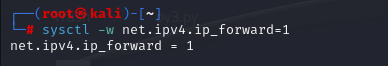
2023/10/8

***Lab Exercise: Network Sniffing and Spoofing with Ettercap***

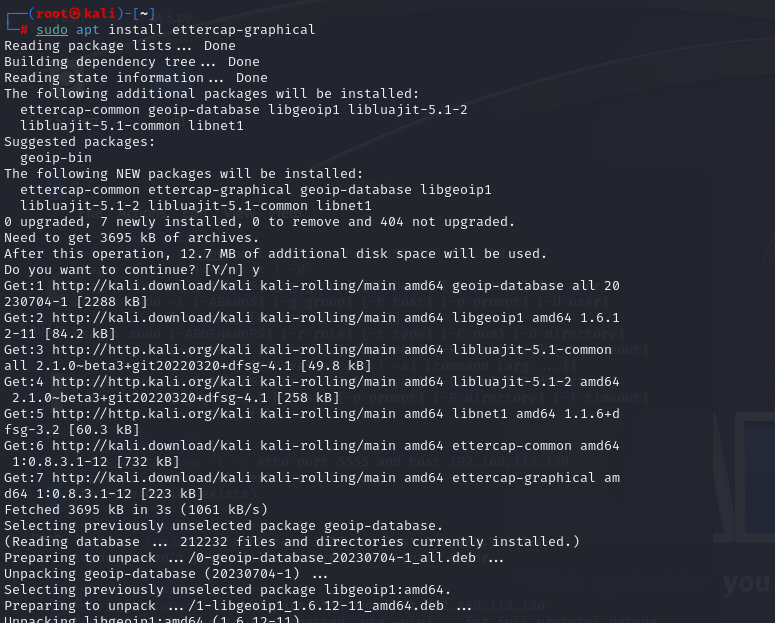
***Note: the discussion is at the end of the pictures.***

**Steps:**

**Step 1: Enabling IP Forwarding**

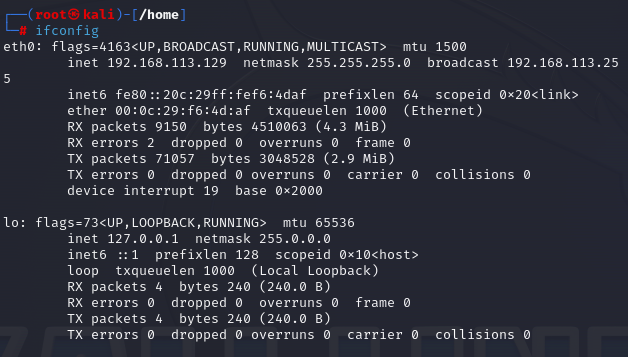


**Step 2: Launching Ettercap**

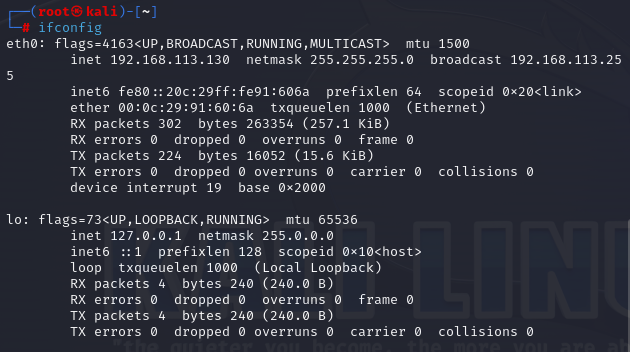


**Step 3: Identifying Targets**

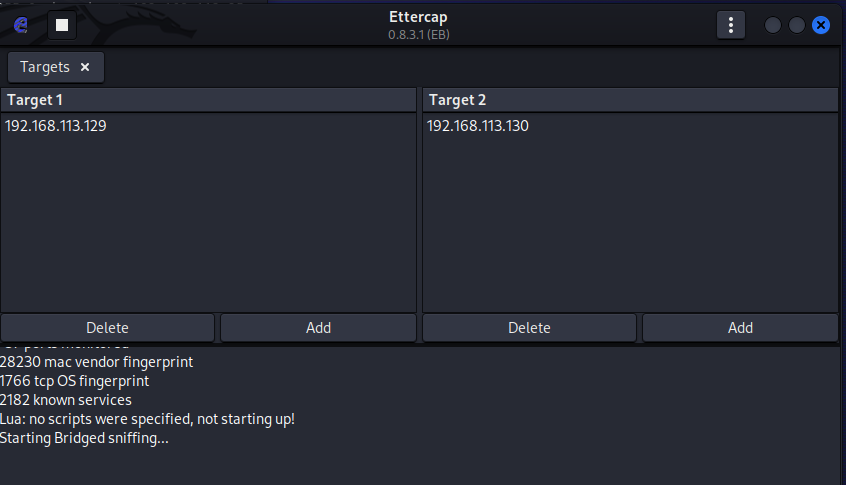
1. Target 1



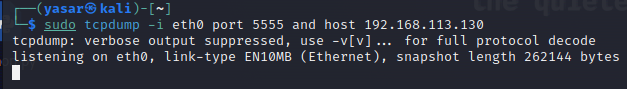
1. Target 2



**Step 4: Adding Targets in Ettercap**

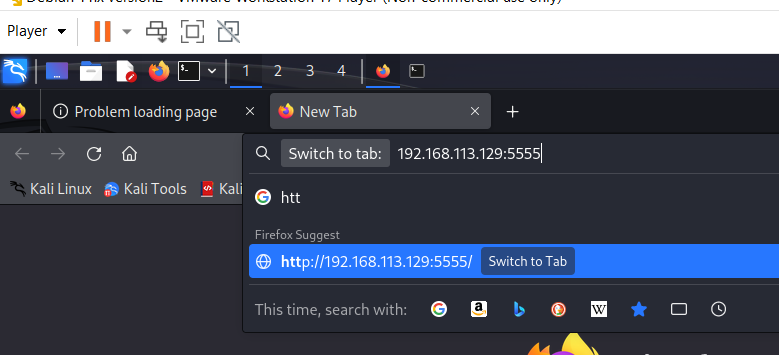


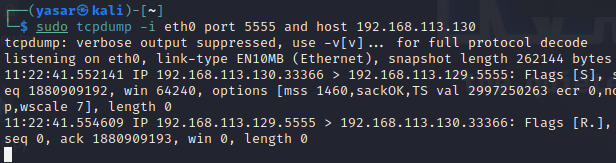
**Step 5: Using Tcpdump for Packet Capture**

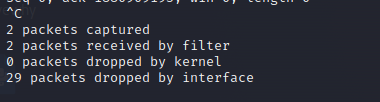


**Step 6: Observe the packet capture output for any intercepted traffic.**

Note: We performed action in the targeted linux and saw the result in the attacker, and after ending the session we can see that packets have been captured.







***Discussion and Reflection:***

1. What is the purpose of enabling IP forwarding using the sysctl command?

Answer:

It allows for the system to be able to accept the cookies/packets from another system and check if they are intended for the system and if not to forward it to the other target system, so that one PC can get to another PC.

1. How can IP forwarding impact the routing of network traffic on a Linux system?

Answer:

Allows for traffic from one interface to another interface so that one computer can reach different computer on a different network.

1. Are there any security or ethical considerations when enabling IP forwarding?

Answer:

Enabling the IP forwarding is a security risk if you don’t have proper firewall and security measures installed since if you can gain access to others system they can also gain access to your system.

1. What are the potential ethical and legal implications of network sniffing and spoofing?

Answer:

* 1. Network Sniffing:
     1. Privacy violation without authorization: it can lead to privacy violation since you get information like login accounts, password and etc.
     2. Data protection law: in countries that has protection laws it can lead to law breaking.
     3. Unauthorized Access: it can lead to gathering info without permission.
     4. Security Risk: this leads to security breaches and attacks from others as well.
  2. Network spoofing:
     1. Identity theft: Spoofing involves impersonating someone/ some device on network, which is identity theft and impersonation and both are highly illegal.
     2. Data tempering: Spoofing can lead to intercepting, modifying data without authorization.
     3. Dos attacks: Spoofing can be used to perform DOS attack by overflowing the network.
     4. Unauthorized access: Spoofing is used for gaining access to a network without the targets permission.
  3. Ethical implication:
     1. Respect of privacy: Spoofing violates the privacy of people since it leads to loss of info or other problems.
     2. Harm prevention: Using these attack should be only for pen testers in a controlled environment and nothing else.
     3. Transparency: one should be transparent about their behaviour but spoofing and such violates that by lying and harming others.

1. How can network administrators defend against ARP spoofing attacks?

Answer: Address Resolution Protocol or (ARP) are attacks used by attackers to intercept the network traffic which can lead to potential other attacks. For defence some of the ways we can use are down below:

* + 1. Static ARP Entries: It creates ARP entries which makes sure the devices only communicate using MAC addresses and prevent spoof ARP from affecting them.
    2. ARP Inspection (ARP Guard): it leads to inspections on network switches and routers. Which will allow for matching of IP to mac address.
    3. Use ARP Spoofing detection tools: tools used for detecting spoof IP’s.
    4. Port Security: this will prevent attacker’s form easily plugging in rogue devices.
    5. Network monitoring: checking network traffic for unsual patterns or unexpected ARP request.

ARP spoofing attacks can be disruptive and pose serious security risks. A combination of preventive measures, network segmentation, monitoring, and user education can help network administrators defend against these attacks effectively. Additionally, staying informed about new attack techniques and evolving security solutions is essential to maintaining network security.

1. In what situations might network sniffing and spoofing be used for legitimate purposes, such as penetration testing?

Answer: Yes it can be used for legitimate purposes, penetration testing and network security assessments. Some of the ways it can be used include:

* + 1. Penetration testing and security auditing.
    2. Security Assessment of intrusion detection/Prevention System (IDS/IPS)
    3. Security Policy Validation
    4. Firewall and Intrusion Detection
    5. Wireless security evaluation
    6. Quality of service testing