

Lab 2 – Sniffing, Spoofing and ARP Poisoning (Total: 4 Marks)

Part A - Netlab (1.5 Marks Total)

Sign in into the NETLAB (<https://netlab.ecs.vuw.ac.nz/>) with the provided credentials and complete the following labs:

- Lab: Investigating ARP poisoning
- Lab: Capturing Network Traffic

1. Explain the utility of the following settings/commands used in these labs. Provide clear, concise answers with one example scenario highlighting their significance (0.25 Mark each).

a. Promiscuous mode

Captures all traffic on a network segment (even those not addressed to specific network interface controllers(NIC)), useful for monitoring network traffic and detecting attacks. For example, if an attacker is using a different MAC address to communicate on the network, promiscuous mode will allow the NIC to capture that traffic and help detect the attack.

b. IP forward field

Determines if a device forwards packets between its interfaces, useful for connecting multiple networks.

For example if there are two subnets, subnet A and subnet B, and a server on subnet A needs to communicate with a device on subnet B. Enabling IP forwarding on a router that connects both subnets would allow packets to be forwarded between the two subnets, allowing the server and device to communicate with each other.

c. Arpwatch

Monitors network activity and detects ARP spoofing attacks. Tracks of MAC and IP addresses on a network, and alerts network administrators of any changes in the mappings. For example, if an attacker is attempting to spoof the MAC address of a legitimate device on the network, arpwatch will detect the change and alert the administrator.

d. Urlsnarf

Monitors web traffic on a network and captures HTTP requests and responses.

This can be useful for detecting potential security breaches or inappropriate network usage. For example, this can be useful for detecting potential security breaches or inappropriate network usage e.g users visiting phishing websites, or inappropriate network usage, such as employees spending excessive amounts of time on social media sites during work hours.

e. Tcpdump

Captures and displays network traffic for troubleshooting and security investigations.

For example, if a user reports a problem with accessing a particular website, tcpdump can be used to capture and examine the network traffic between the user's device and the website's server. The administrator can then analyse the captured packets to determine the source of the problem, such as a misconfigured firewall or network congestion.

f. Netstat

Displays active network connections and statistics, useful for monitoring network activity and identifying security risks.

For example, an administrator can use netstat to view all open ports on a device, which can be useful for identifying unauthorised access attempts or malware infections. If an open port is discovered that should not be open, the administrator can investigate and take appropriate actions to block the port or remove the malware. Netstat can also be used to view active network connections and their status, such as established, listening, or closed.

Part B - Netlab (2.5 Marks Total)

Sign in into the NETLAB (<https://netlab.ecs.vuw.ac.nz/>) with the provided credentials and complete the following lab:

- Lab: Packet Crafting with Scapy

1. Explain the utility of the following settings/commands used in this lab (0.25 Mark each).

a. TTL

TTL (Time To Live) indicates how many hops a packet can take before it is discarded (used to prevent packets from circulating indefinitely). It is useful for network troubleshooting and monitoring (can help identify excessive latency or network congestion).

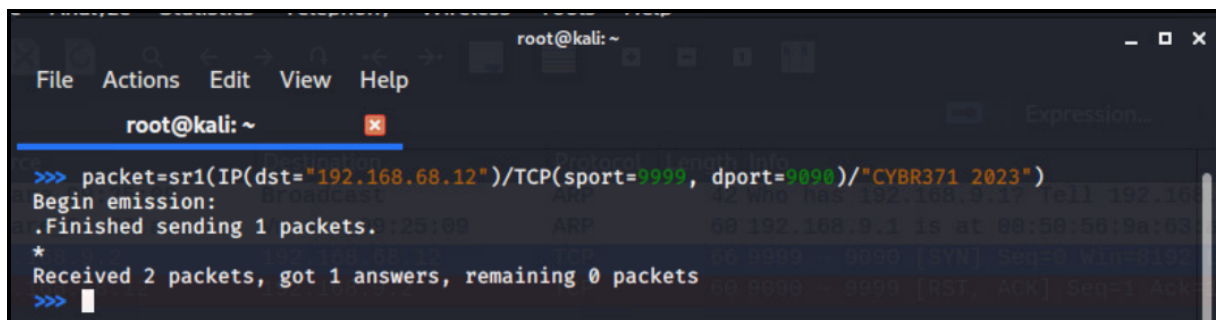
b. / Operator (Provide an example)

/ is used to stack layers in scapy. This means that the lower layer and its default fields are overloaded by the upper layer.

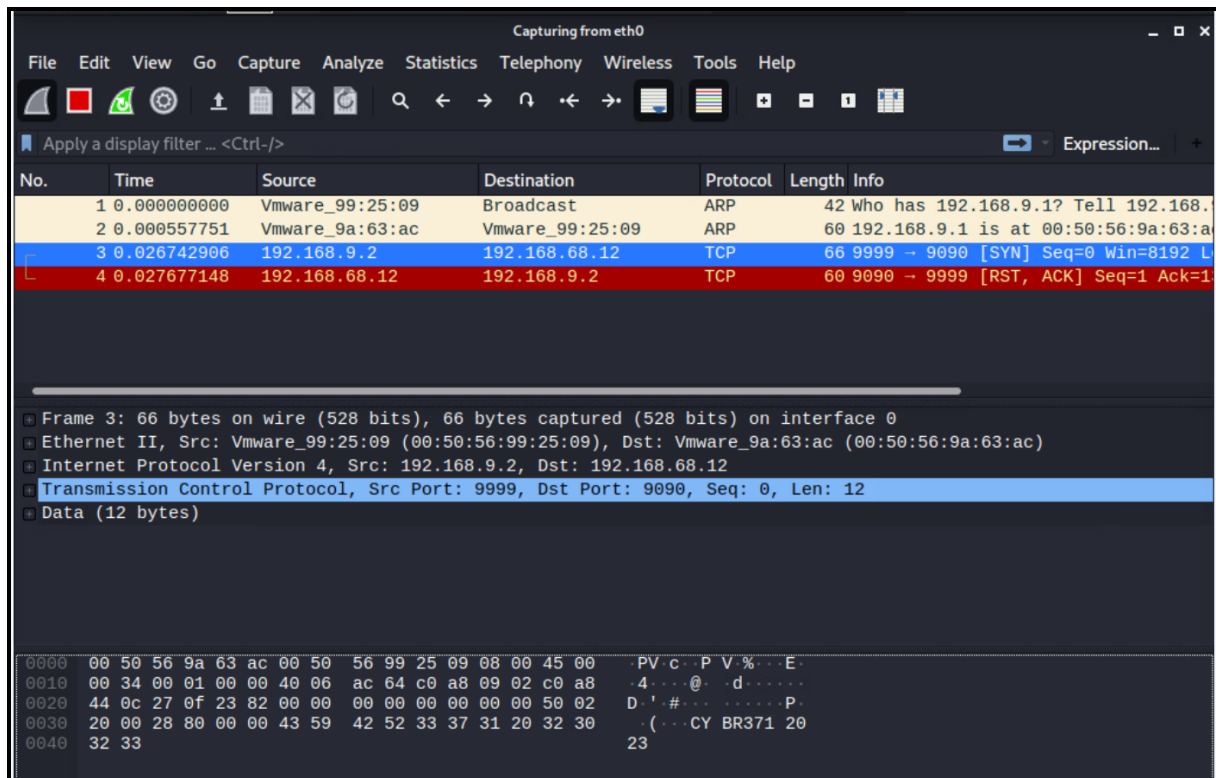
For example, to send a tcp over an ip packet in a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

2. Write the commands in Scapy for the following. Please make sure your Scapy code matches the requirements in each task. Partially correct answers are not accepted. (0.5 Mark each):

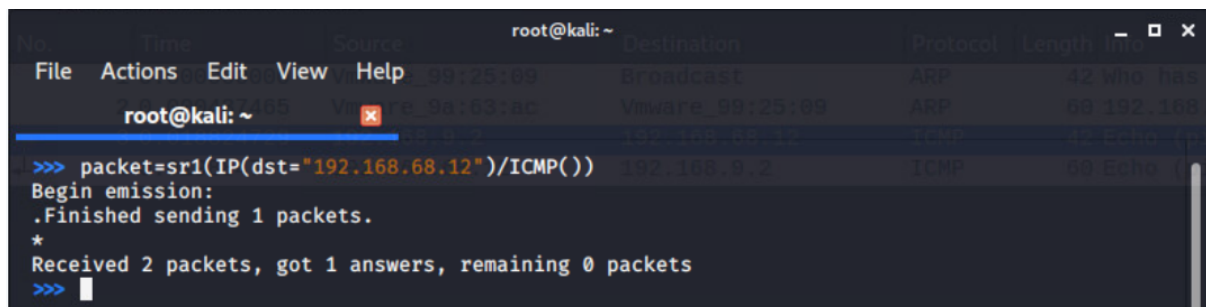
- a) Create and send a TCP packet with the payload "CYBR371 2023" with source port of 9999 from the Kali host, and to OWASP BWA host on destination port of 9090. Take a screenshot of the tcpdump capture on the destination, confirming your packet was delivered.**

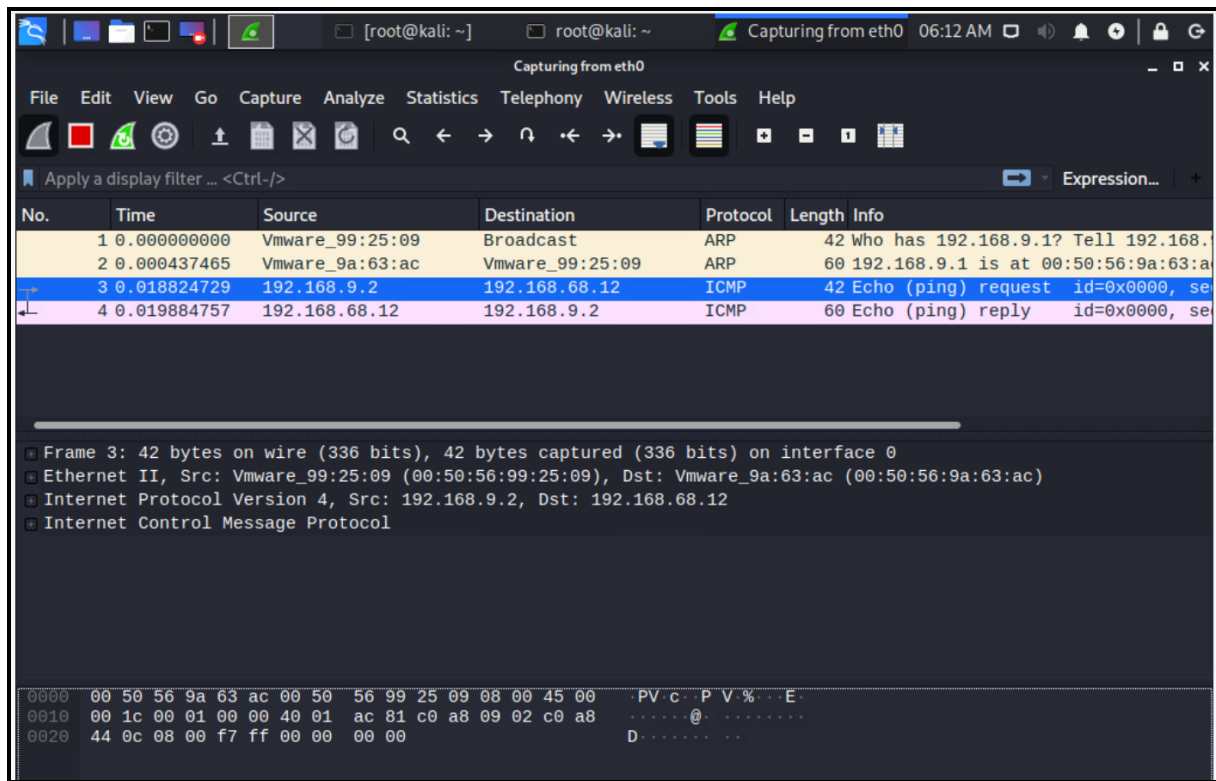


```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
>>> packet=sr1(IP(dst="192.168.68.12")/TCP(sport=9999, dport=9090)/"CYBR371 2023")  
Begin emission:  
.Finished sending 1 packets.  
*  
Received 2 packets, got 1 answers, remaining 0 packets  
>>>
```



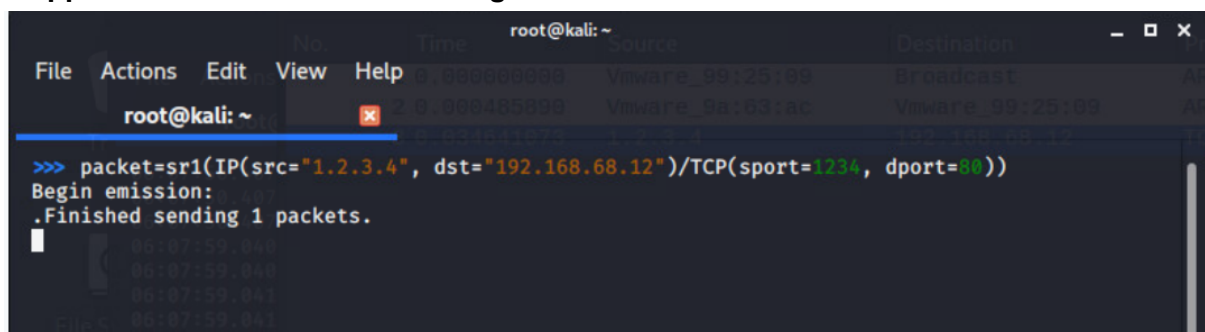
b) Create and send an ICMP packet from the host (Kali) to the destination OWASP BWA. Take a screenshot of the tcpdump capture on the destination confirming your ICMP packet was delivered.

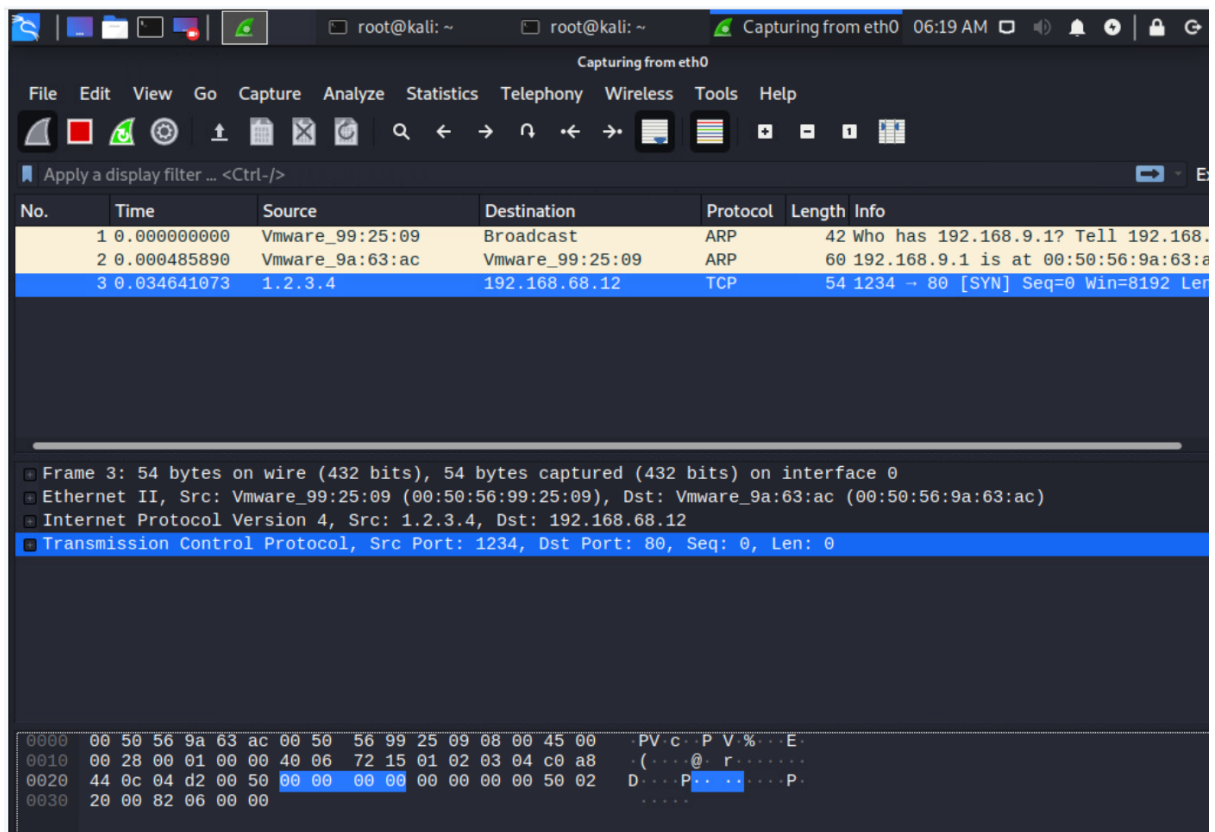




c) Sniff (i.e. capture) TCP traffic on all the interfaces on the host machine (i.e. Kali) sniff(filter="tcp", iface=None)

d) Create and send a spoofed TCP/IP packet (with forged source IP address) from the host (Kali) to the destination machine, OWASP BWA with forged source IP address of 1.2.3.4. Take a screenshot of the tcpdump capture on the destination proving your message was delivered. Briefly explain why the message was not dropped in transmission even though the source IP address does not exist.





When the packet is sent from Kali it is accepted by the router/switches as source IP is not checked for correctness therefore it is allowed to be sent to its destination. When the packet reaches the destination machine a reply is sent by OWASP to the forged IP address (1.2.3.4) - as the IP address does not exist, the reply packet is discarded and the reply is not received by the attacker.

Source:

<https://www.techtarget.com/searchsecurity/definition/promiscuous-mode#:~:text=In%20computer%20networking%2C%20promiscuous%20mode,each%20network%20packet%20that%20arrives.>

<https://tools.ietf.org/html/rfc2096>

<https://linux.die.net/man/8/arpwatch>

<https://linux.die.net/man/8/urllib3>

<https://www.tcpdump.org/>

<https://www.ibm.com/docs/hr/aix/7.2?topic=command-using-netstat#:~:text=The%20netstat%20command%20displays%20the,netstat%20%2Di%20%2DZ%20command>