ICMP Redirect Attack

The objective of this lab is for students to gain the first-hand experience on various attacks at the IP layer. Some of the attacks may not work anymore, but their underlying techniques are quite generic, and it is important for students to learn these attacking techniques, so when they design or analyze network protocols, they are aware of what attackers can do to protocols.

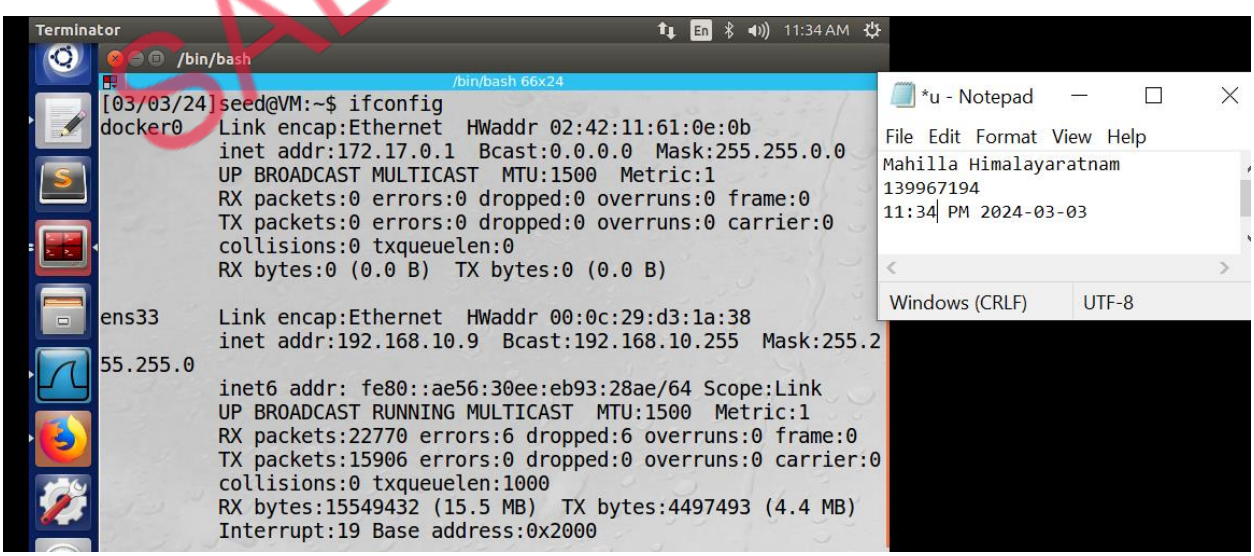
Moreover, due to the complexity of IP fragmentation, spoofing fragmented IP packets is non-trivial. Constructing spoofed IP fragments is a good practice for students to hone their packet spoofing skills, which are essential in network security. We will use Scapy to conduct packet spoofing.

This lab covers the following topics:

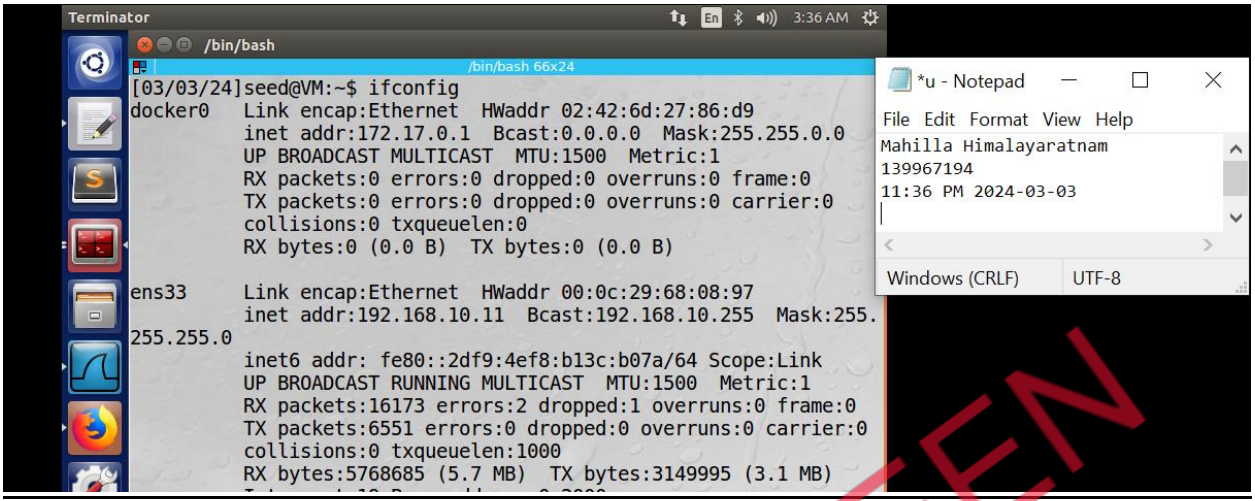
- The IP and ICMP protocols
- IP Fragmentation and the related attacks
- ICMP redirect attack
- Routing

FINDING IP'S

Machine A (10.9)



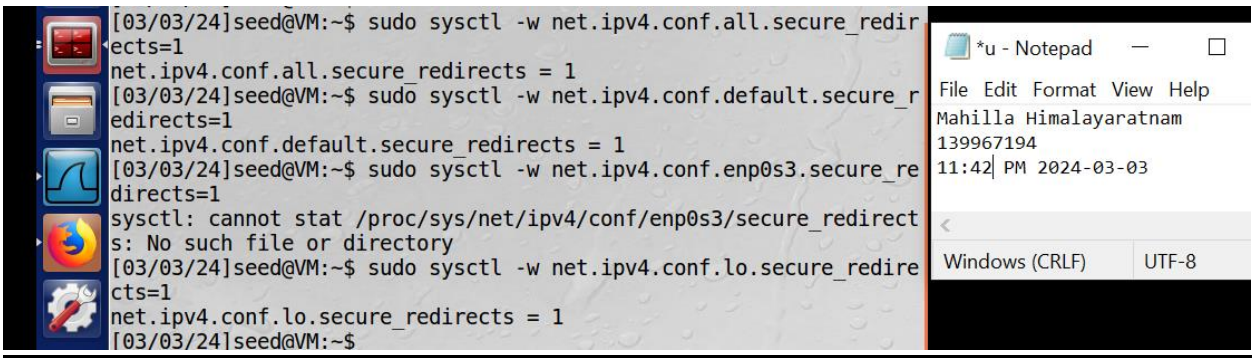
Machine B (10.11)



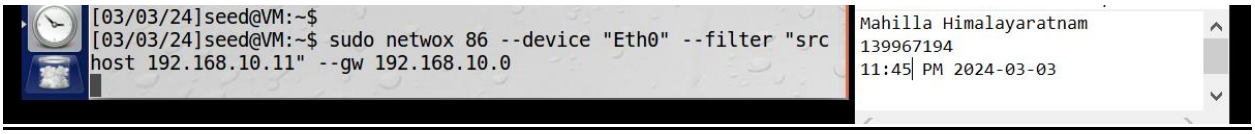
OFF secure Redirects

Machine A COMMANDS

MACHINE B COMMANDS

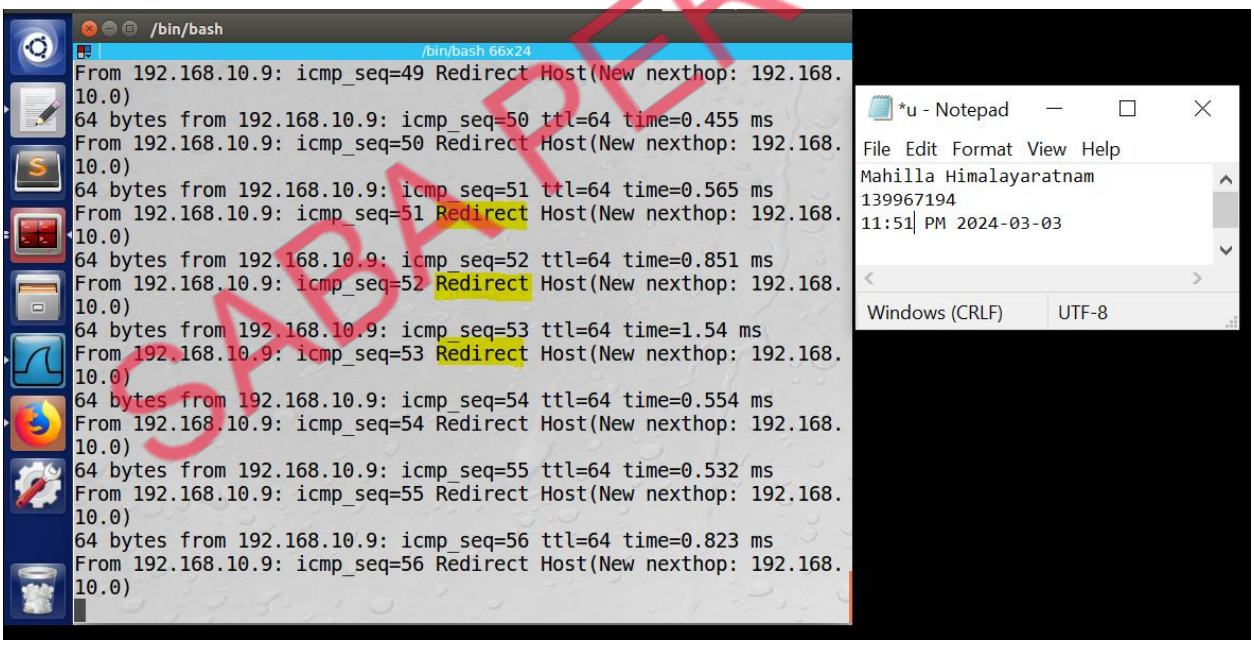


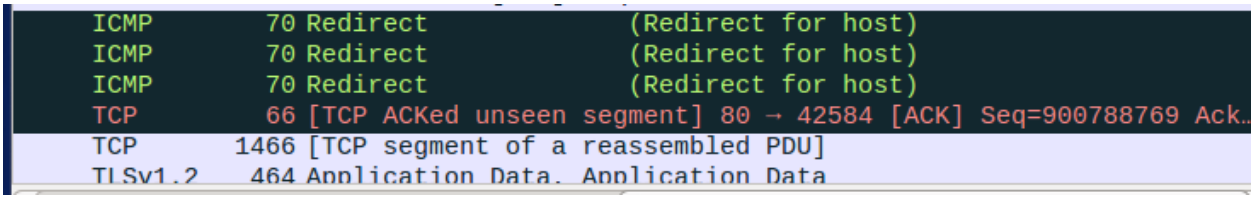
ON MACHINE A

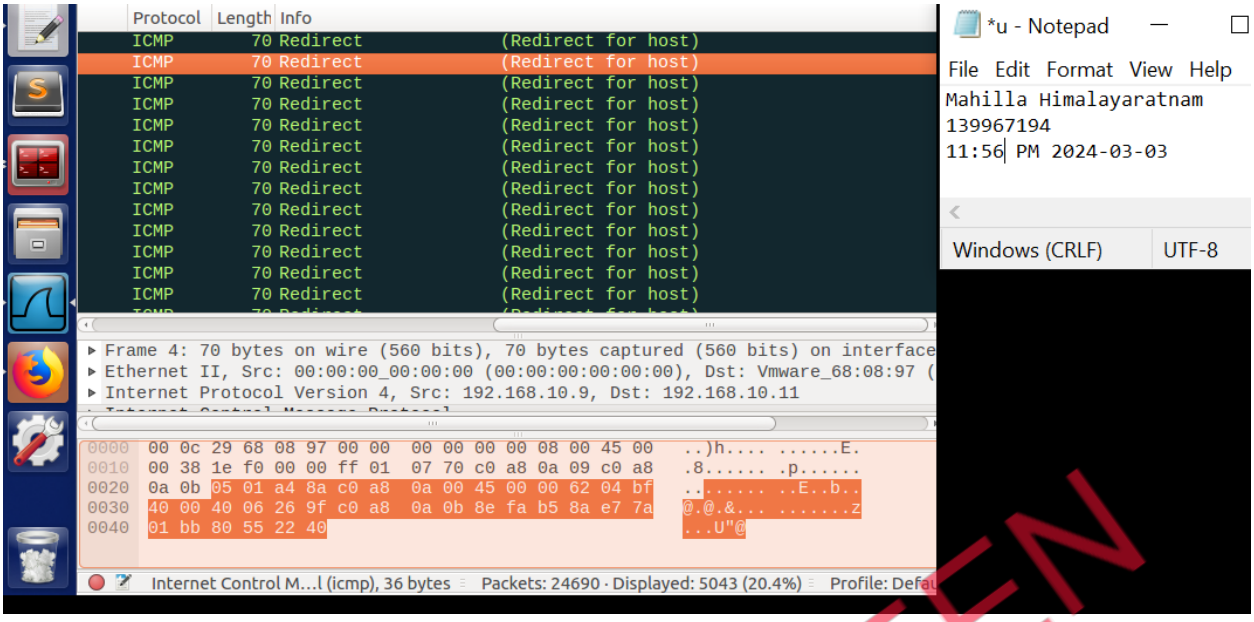


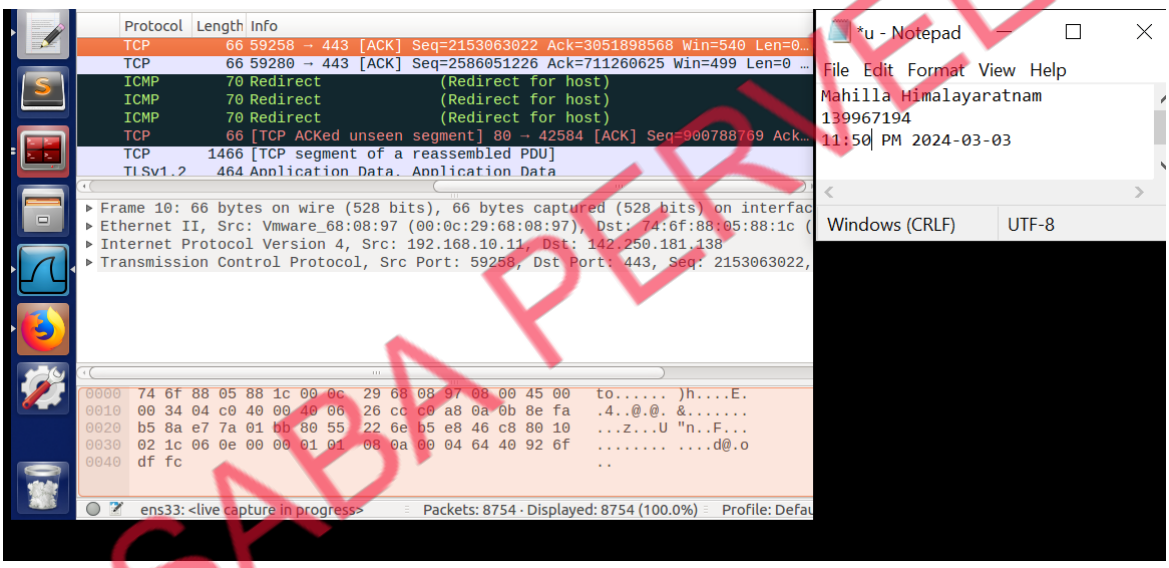
ON MACHINE B

An ICMP redirect is an error message sent by a router to the sender of an IP packet. Redirects are used when a router believes a packet is being routed incorrectly, and it would like to inform the sender that it should use a different router for the subsequent packets sent to that same destination. ICMP redirect can be used by attackers to change a victim's routing.









We observed that the malicious router sends only one packet at a time typed on the victim side along with the length of the message typed with the attack. To conclude, we can use the A's MAC address instead of IP address as it does not create unnecessary flooding where continuous TCP retransmission occurs