ABSTRACT

Network attacks are unauthorised actions on the digital assets within an organisational network . Malicious parties usually execute network attacks to alter ,destroy or steal private data. Since network attacks deal with private data ,prevention of those attacks is more important than storing data securely. Attacking a network can cause problems to the entire network and can possibly harm all the systems . Few such attacks are **ARP Spoofing ,DoS (**Denial of Service **)** and **Fake Ping**.

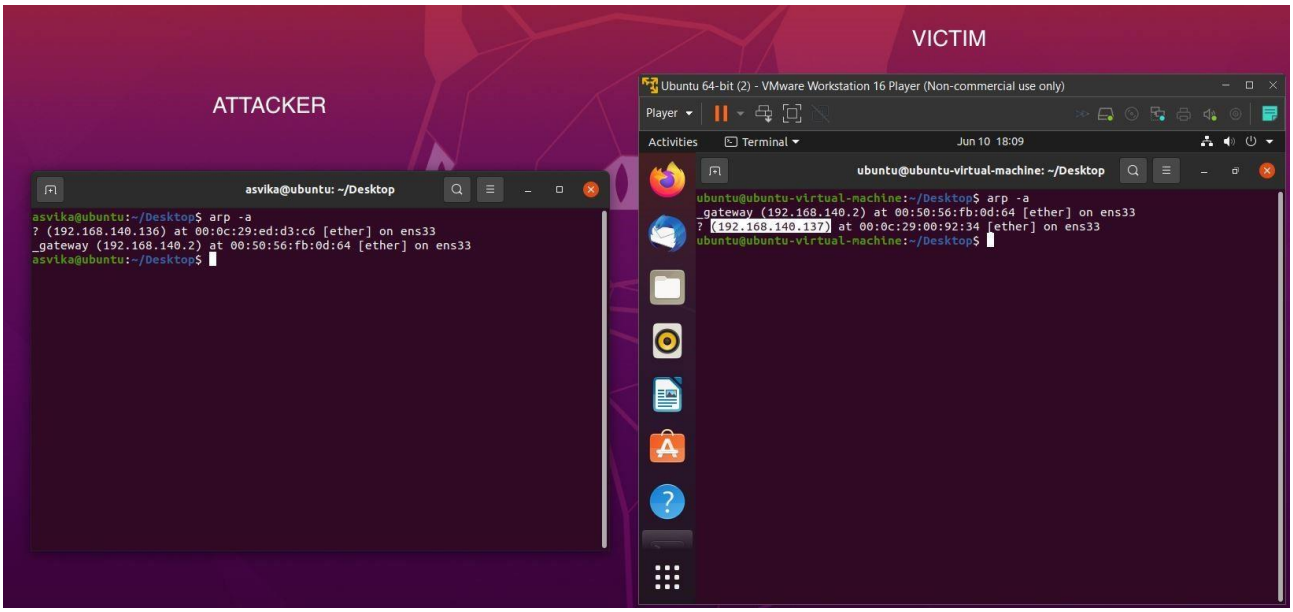
ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Attacker fakes the gateway to tell he is the client machine and the client machine that he is the Gateway . All the traffic now goes through the attacker who forwards it to the desired network. A detector tool for the same which checks the ARP requests and if there are continuous request from the same IP within a period it is informed that there is an attack.

Denial of Service attack is an attack where the attacker sends a lot of request to the server using multi threading . This makes the server throttle and denies the required services even for legitimate users.

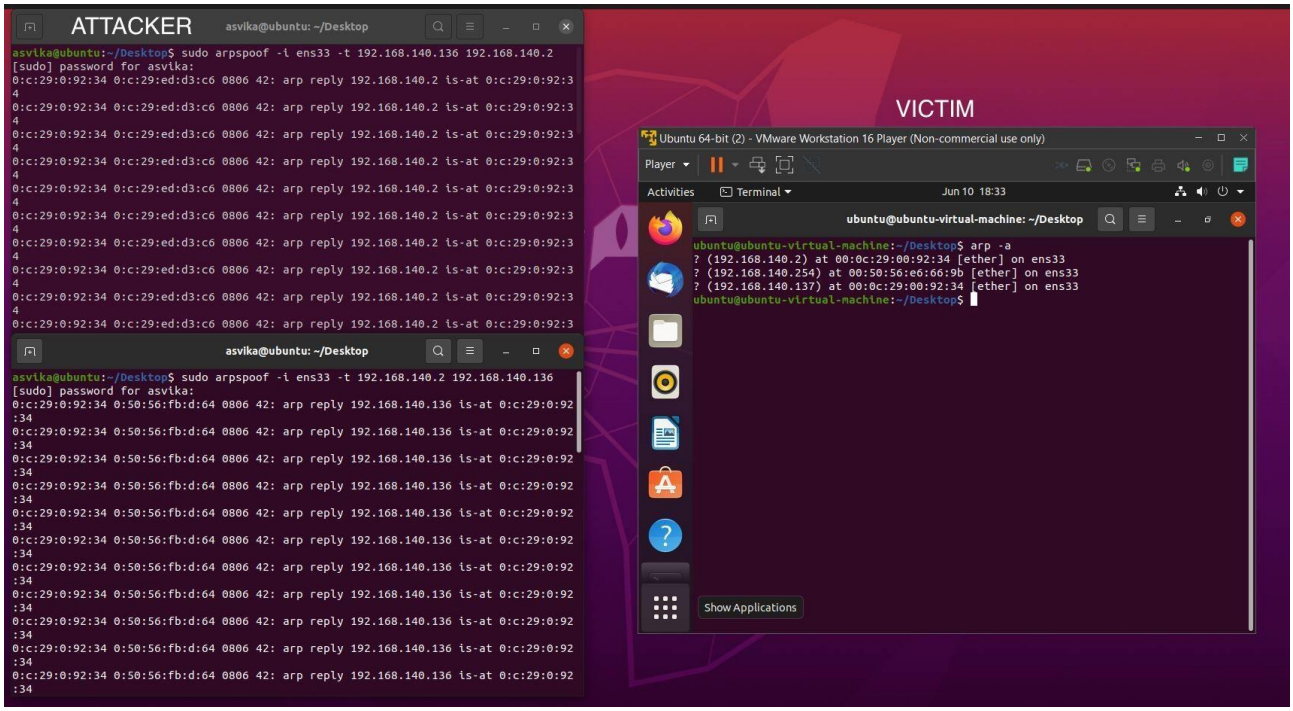
Fake ping attack is where the program sends packet to the user , even when the pinged IP is a non existing one . A dummy packet is created and send to the pinged IP which believes that the IP actually exists. The attacker would fake to be that IP and would receive messages from the user .

ARP SPOOFING WORKING

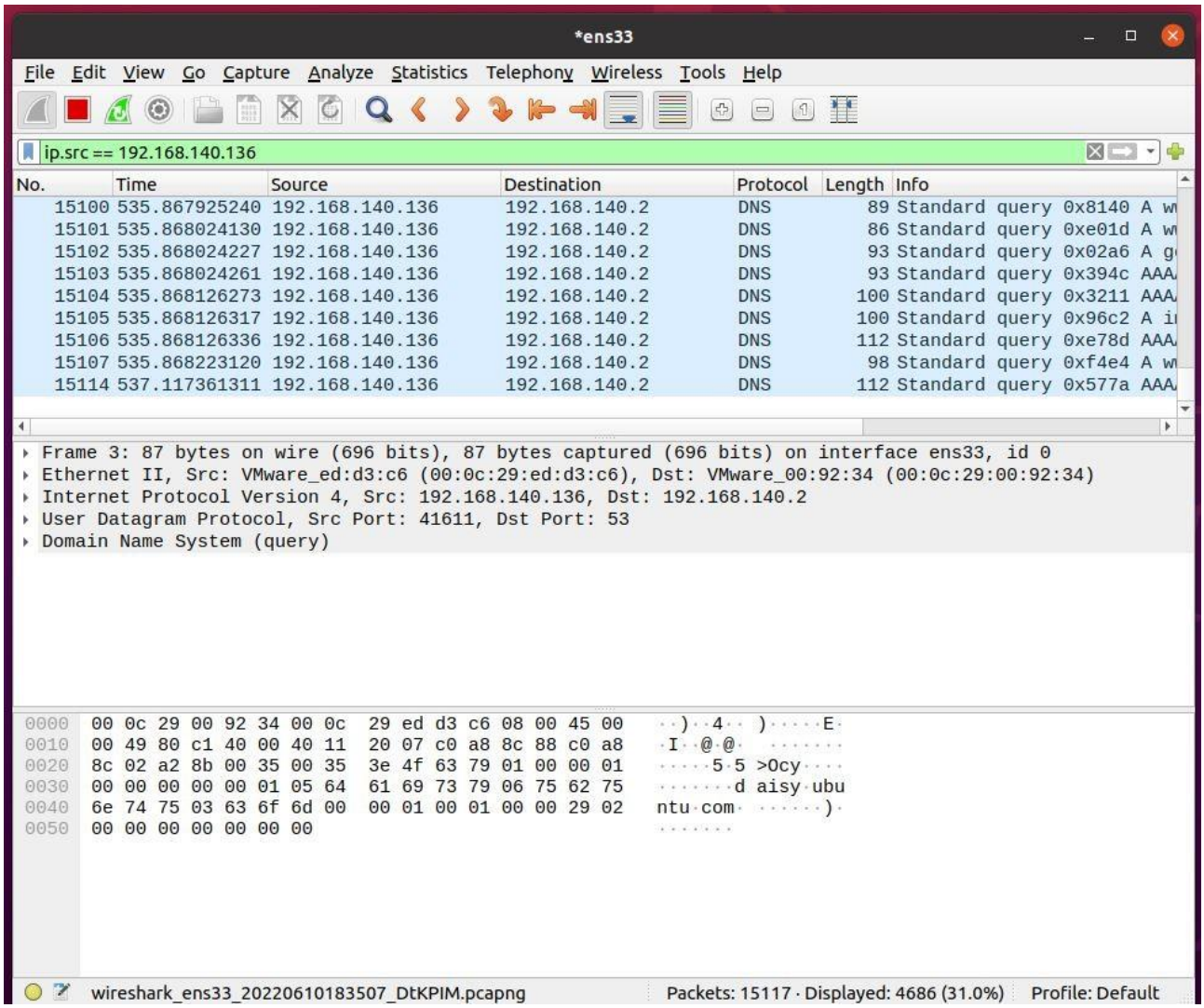
Initially a ping request is send to the victim to add the attacker’s IP and Mac to the ARP table of both attacker and victim .



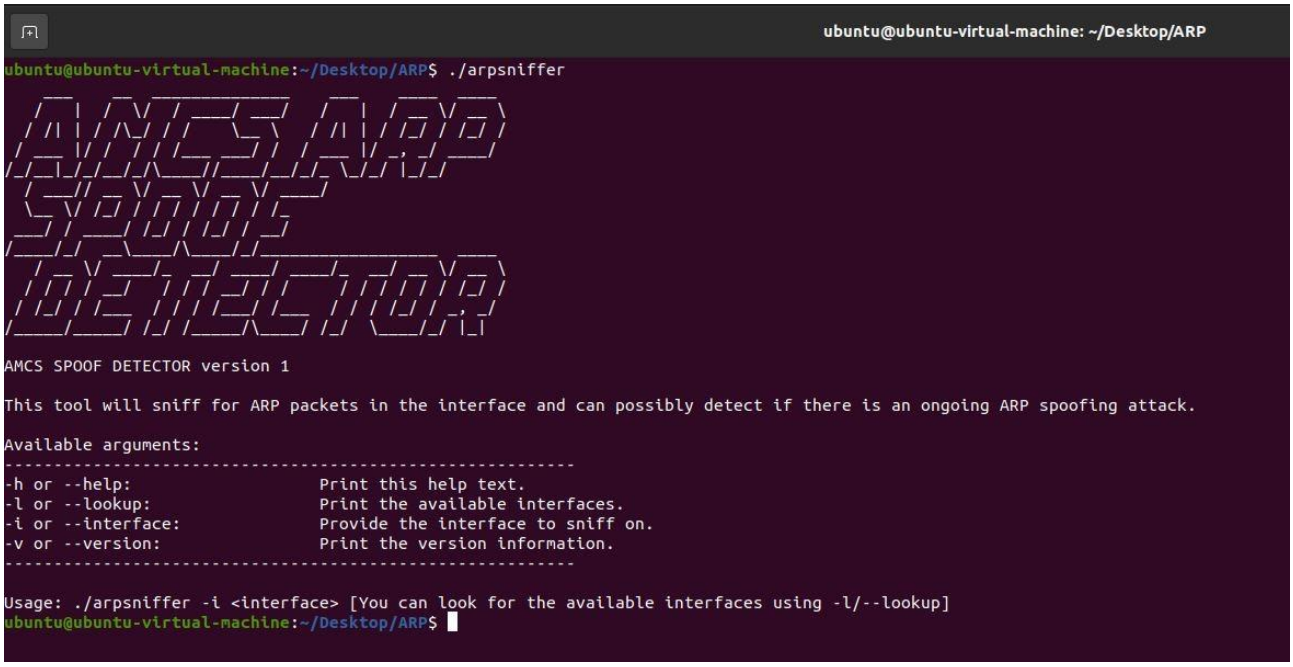
The attacker then spoofs the gateway and the victim which in turn modifies the MAC address of the gateway to be same as that of the attacker .

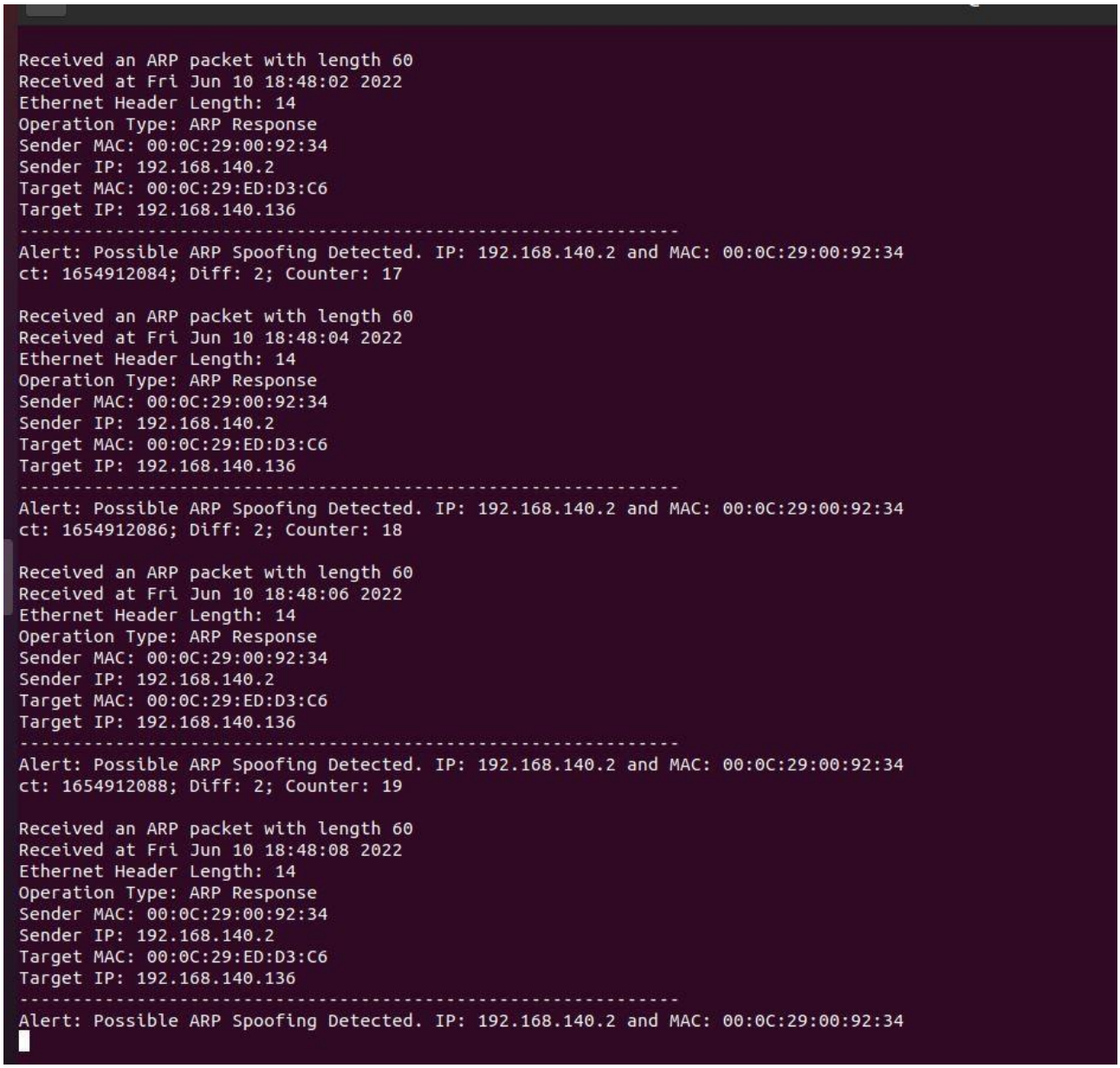


IP forwarding is enabled in the attacker Side which forwards the packets received to the victim. All the traffic between the Gateway and the Victim now goes through the attacker . So attacker is able to capture all the messages.



To detect the ARP Spoofing attack a tool is built.



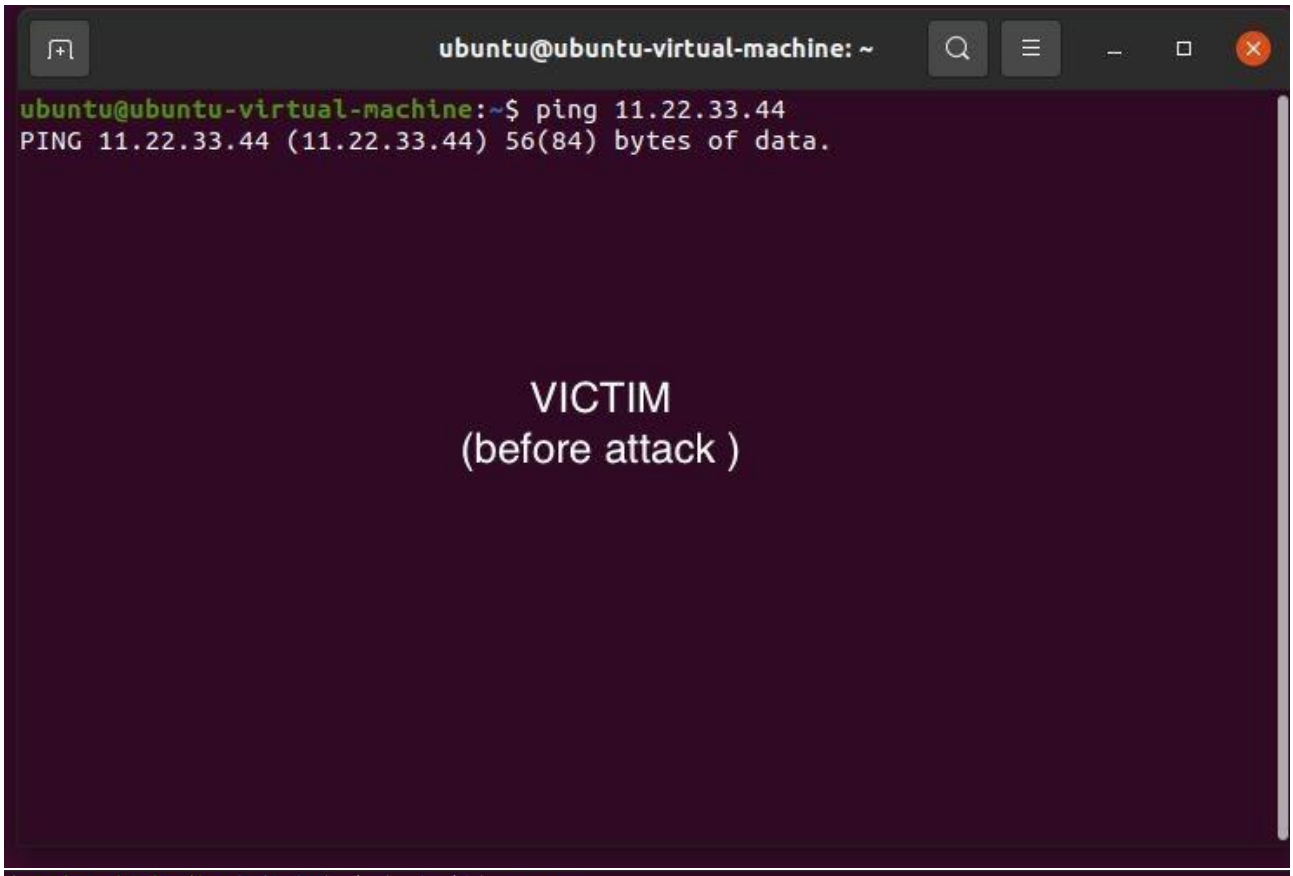


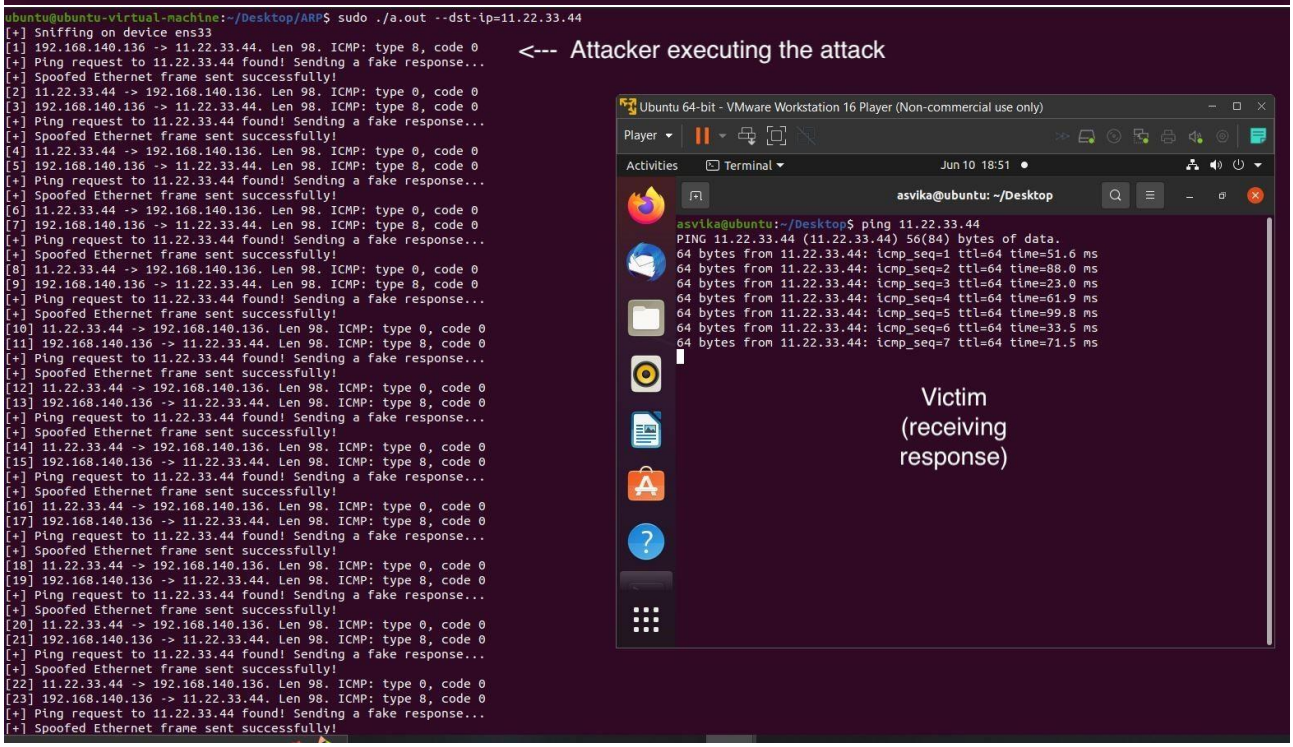
DOS WORKING

A DOS attack is one in which the attacker sends many request to deny the service of the site. When there is an attack from only one computer for heavy websites it only slows down the loading time of the site. When there is Distributed Denial of Service then the site completely goes down.

FAKE PING WORKING

During a fake ping ,when the victim sends a ping request to a non existing IP address the attacker acts as if he is that IP and sends packets to the victim.
When the victim sends data the attacker Is able to capture .


ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ ping 11.22.33.44
PING 11.22.33.44 (11.22.33.44) 56(84) bytes of data.
VICTIM
(before attack)


ubuntu@ubuntu-virtual-machine:~/Desktop/ARP$ sudo ./a.out --dst-ip=11.22.33.44
[+] Sniffing on device ens33
[1] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[2] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[3] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[4] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[5] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[6] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[7] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[8] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[9] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[10] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[11] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[12] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[13] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[14] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[15] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[16] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[17] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[18] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[19] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[20] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[21] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
[22] 11.22.33.44 -> 192.168.140.136. Len 98. ICMP: type 0, code 0
[23] 192.168.140.136 -> 11.22.33.44. Len 98. ICMP: type 8, code 0
[+] Ping request to 11.22.33.44 found! Sending a fake response...
[+] Spoofed Ethernet frame sent successfully!
<--- Attacker executing the attack
Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
Jun 10 18:51
asvika@ubuntu: ~/Desktop
asvika@ubuntu:~/Desktop$ ping 11.22.33.44
PING 11.22.33.44 (11.22.33.44) 56(84) bytes of data.
64 bytes from 11.22.33.44: icmp_seq=1 ttl=64 time=51.6 ms
64 bytes from 11.22.33.44: icmp_seq=2 ttl=64 time=88.0 ms
64 bytes from 11.22.33.44: icmp_seq=3 ttl=64 time=23.0 ms
64 bytes from 11.22.33.44: icmp_seq=4 ttl=64 time=61.9 ms
64 bytes from 11.22.33.44: icmp_seq=5 ttl=64 time=99.8 ms
64 bytes from 11.22.33.44: icmp_seq=6 ttl=64 time=33.5 ms
64 bytes from 11.22.33.44: icmp_seq=7 ttl=64 time=71.5 ms
Victim
(receiving
response)

CONCLUSION

In this package these attacks were executed using Virtual machines . The tools were written using C programming and requires the use of various headers. Detecting the attack early and preventing them is very important for a secure system. When we know how attack is preventing them is easier . So in this package the attacks were performed and then analysed on the prevention measures possible on those attacks .

REFERENCES

- https://www.varonis.com/blog/arp-poisoning
- https://www.imperva.com/learn/application-security/arp-spoofing/
- https://www.comparitech.com/blog/information-security/arp-poisoning-spoofingdetect-prevent/
- Selfmade Ninja Academy
- https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attackdos
- https://www.greycampus.com/opencampus/ethical-hacking/denial-of-serviceattacks-and-its-types