ICMP SMURF ATTACK

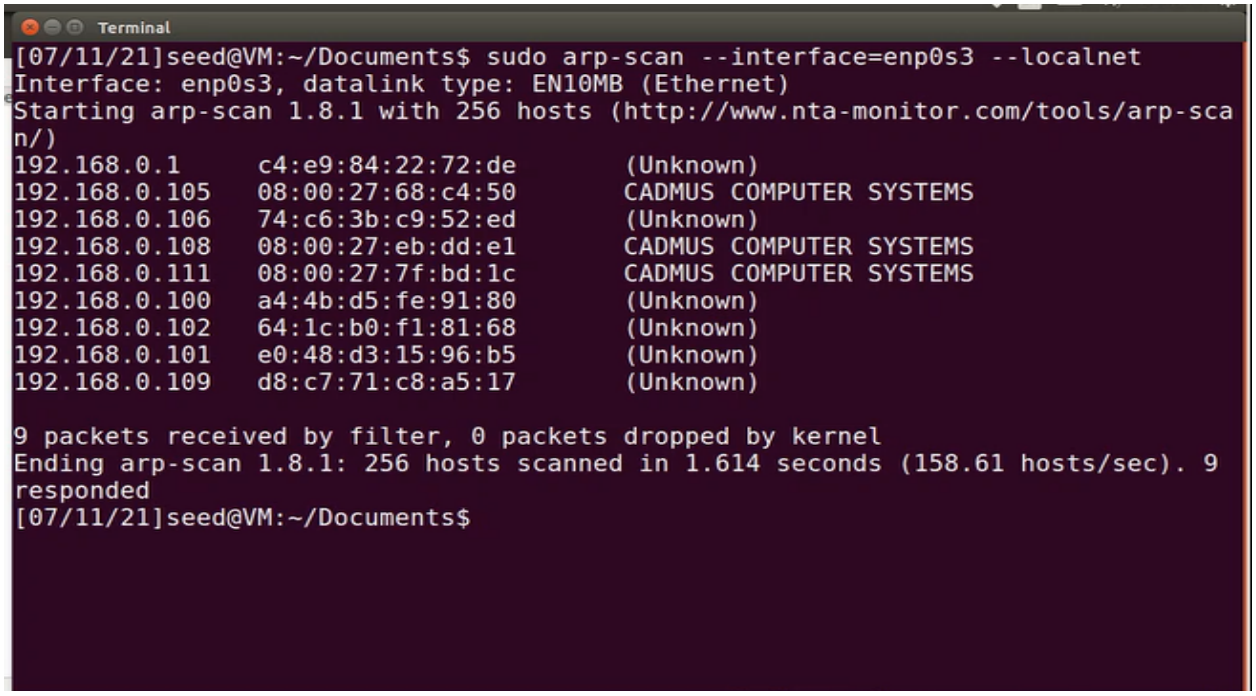
Name : Akid Abrar
Id : 1605100

Steps Of Attack:

Here are the steps how the attack was proceeded:

- One virtual machine is used as attacker,one as victim and two others as normal LAN components.The attacker get the IP addresses of all the victims using **sudo arp-scan --interface=enp0s3 --localnet** command.This shows all the device's IP addresses within the LAN.From the result of this command the attacker find the IP address to be spoofed.
- The **ping.c_** program sends the ICMP ECHO_REQUEST from a specific IP address to a specific IP address.The source and destination IP addresses are given as command line arguments.This program sends 3 ICMP ECHO_REQUESTS from source to destination IP.
- In the program **ping.c ,** two structures are used,one for IP header and another for ICMP header,The source IP and destination IP is assigned in the IP Header field.
- A **script** is used to run the **ping.c** program by the attacker.In the **script**,the victim's IP is used as the source IP.The IP address of the another device in the LAN is used as the destination IP.In the **script**,the **ping.c** program is executed several times with different destination IP addresses.

Here are the snapshots of the attack:
First,the IP addresses of all the devices in the LAN are found.The IP address with **192.168.0.111** is chosen as the victim.The other 2 devices with IP address **192.168.0.105** and **192.168.0.108** was chosen to demonstrate the attack.



```
Terminal
[07/11/21]seed@VM:~/Documents$ sudo arp-scan --interface=enp0s3 --localnet
Interface: enp0s3, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.8.1 with 256 hosts (http://www.nta-monitor.com/tools/arp-sca
n/)
192.168.0.1     c4:e9:84:22:72:de       (Unknown)
192.168.0.105   08:00:27:68:c4:50       CADMUS COMPUTER SYSTEMS
192.168.0.106   74:c6:3b:c9:52:ed       (Unknown)
192.168.0.108   08:00:27:eb:dd:e1       CADMUS COMPUTER SYSTEMS
192.168.0.111   08:00:27:7f:bd:1c       CADMUS COMPUTER SYSTEMS
192.168.0.100   a4:4b:d5:fe:91:80       (Unknown)
192.168.0.102   64:1c:b0:f1:81:68       (Unknown)
192.168.0.101   e0:48:d3:15:96:b5       (Unknown)
192.168.0.109   d8:c7:71:c8:a5:17       (Unknown)

9 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.8.1: 256 hosts scanned in 1.614 seconds (158.61 hosts/sec). 9
responded
[07/11/21]seed@VM:~/Documents$
```

fig-1.1:Finding the iP addresses in the LAN

Then the **script.sh** file is constructed where the **ping.c** program is executed 2 times using the victim's IP,which is **192.168.0.111 ,** as the source IP in both times and **192.168.0.105** as destination IP in one execution,**192.168.0.108** in the other.

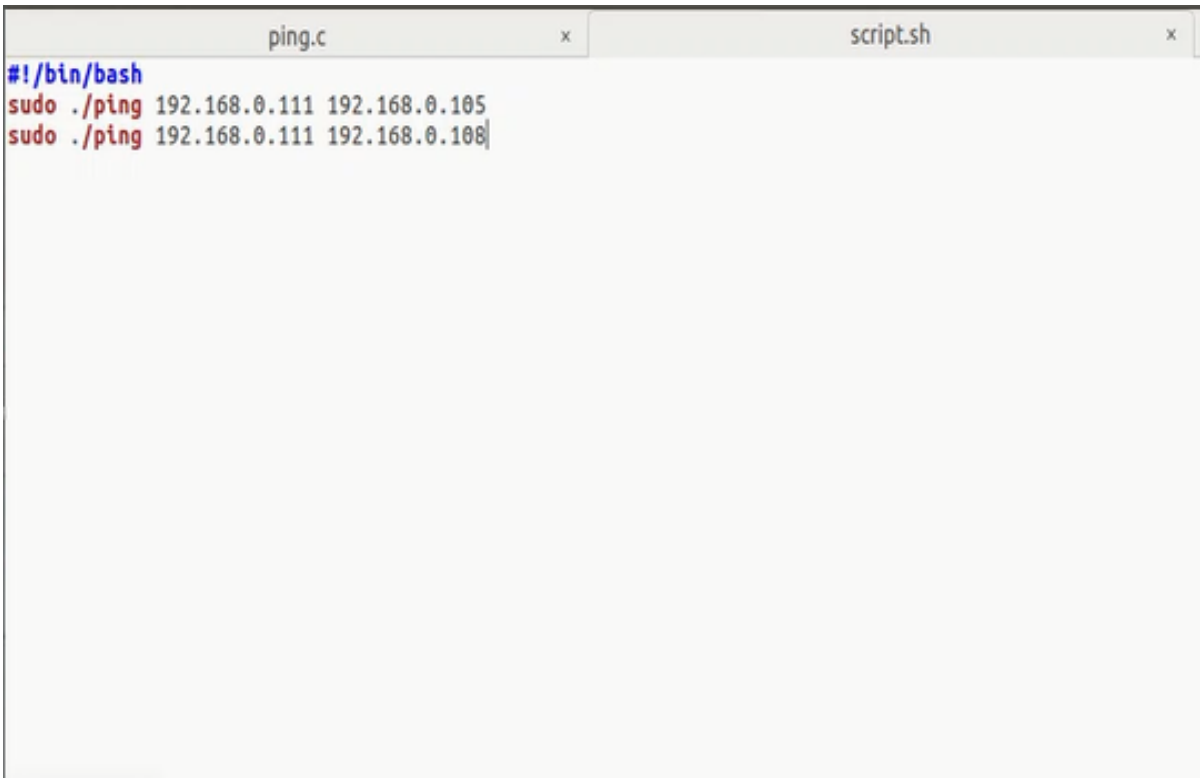


fig-1.2:Building the script.sh file with appropriate IP addresses

If The Attack Is Successful Or Not:

I think the attack is successful as per my design report.I needed to send ICMP ECHO_REPLY packets to the victim's machine from other machines connected to the LAN without sending ICMP ECHO_REQUEST packets from the victim and it was done by the attack script.

Observed Outputs:

After the script is run.,we filter the ICMP packets in the WIRESHARK.It was found from the attacker's PC that 3 ICMP ECHO_REQUEST is sent with source IP as **192.168.0.111** and destination as **192.168.0.105.**Then other 3 ICMP ECHO_REQUEST is sent with source IP as **192.168.0.111** and destination as **192.168.0.108.**

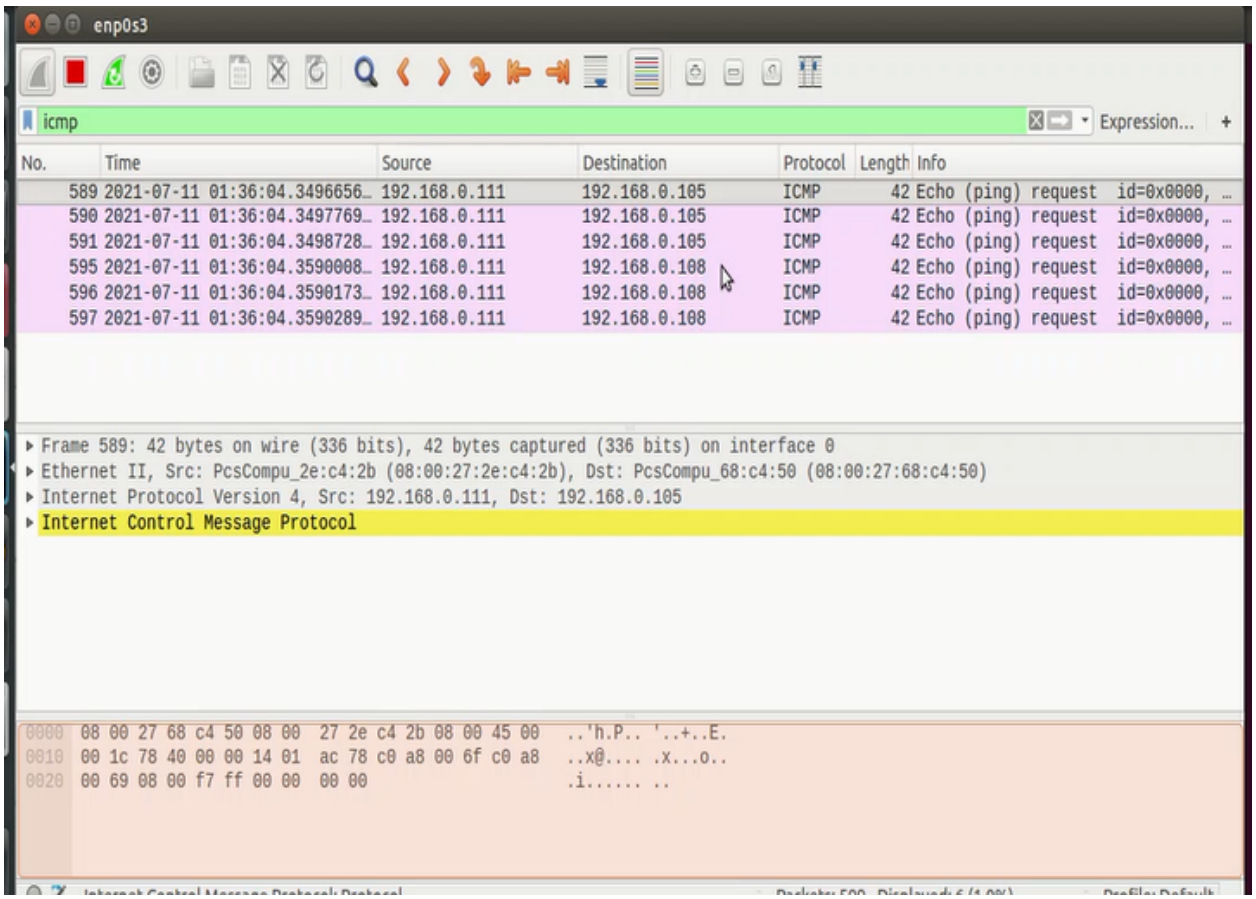


fig-1.3:Inspecting ICMP packets from attacker's machine

If we observe ICMP packets from one of the machines with IP **192.168.0.105** we can see that 3 ICMP ECHO_REQUEST is send to this machine from the machine with IP **192.168.0.111.**We can also see that this machine sends 3 ICMP ECHO_REPLY to the machine **192.168.0.111,**which was exactly the attacker wanted.

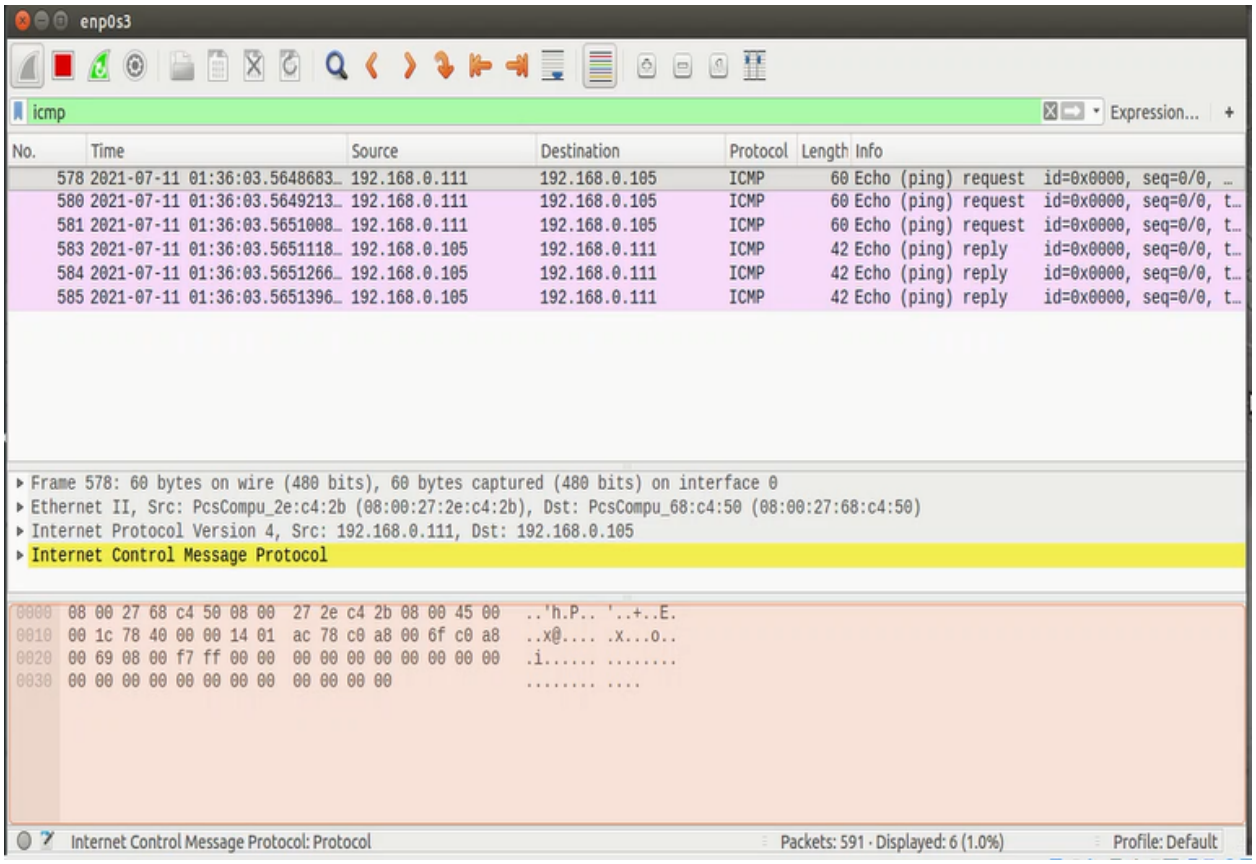


fig-1.4:Inspecting ICMP packets from on of the machines in the LAN which is involved in the attack

If we observe iCMP packets from the victim's machine,we can see that 6 ICMP ECHO_REPLY is sent to the machine.3 is from the machine **192.168.0.105** and 3 is from **192.168.0.108.**Tough this machine did not sent any ICMP ECHO_REQUEST,ICMP ECHO_REPLY is sent to this machine due to the attack script executed by the attacker.

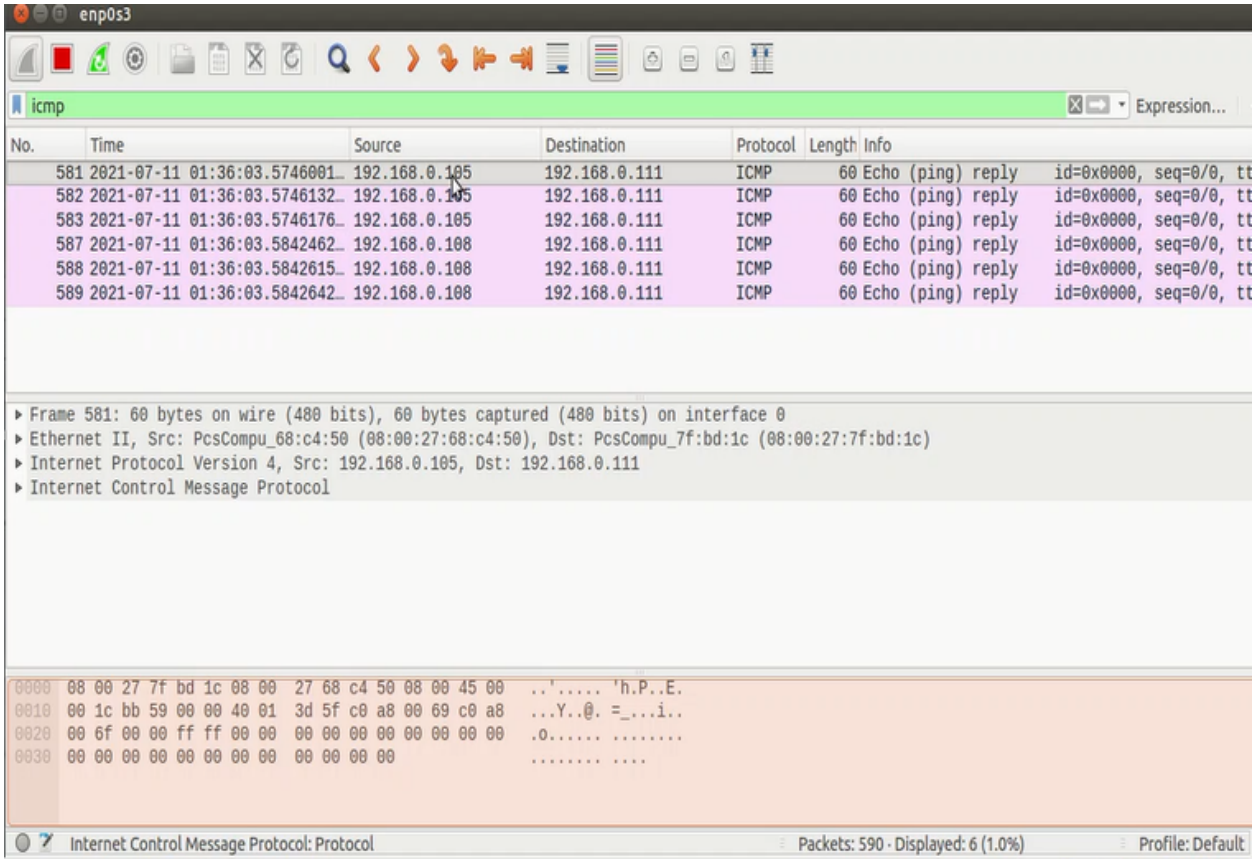


fig-1.5:Inspecting ICMP packets from victim's machine

Here,I tried to demonstrate the attack with a few ICMP packets.If the attacker sends a lot of ICMP ECHO_REQUESTS to the other machines in the LAN,the victim will receive plenty of ICMP ECHO_REPLY packets from the other machines,which will certainly be considered as a DOS attack.

Countermeasure Of The Attack:

I didn't design any countermeasure for the attack.But it can be prevented in two ways:

1. If any IP address send too many ICMP ECHO_REQUEST packets,block the incoming packets from that IP.
2. Block any packets that come from Router's broadcast address.