

# **ICMP SMURF ATTACK**

**Name : Akid Abrar**

**Id : 1605100**

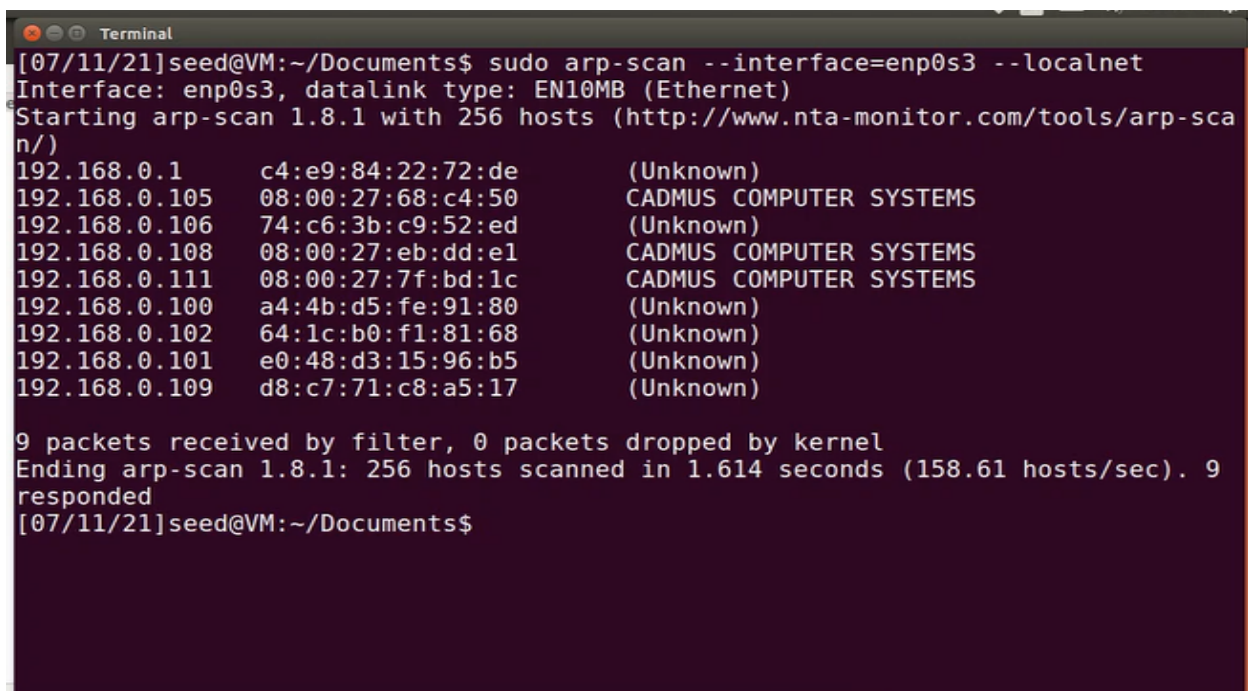
## Steps Of Attack:

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 gets 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 finds 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.

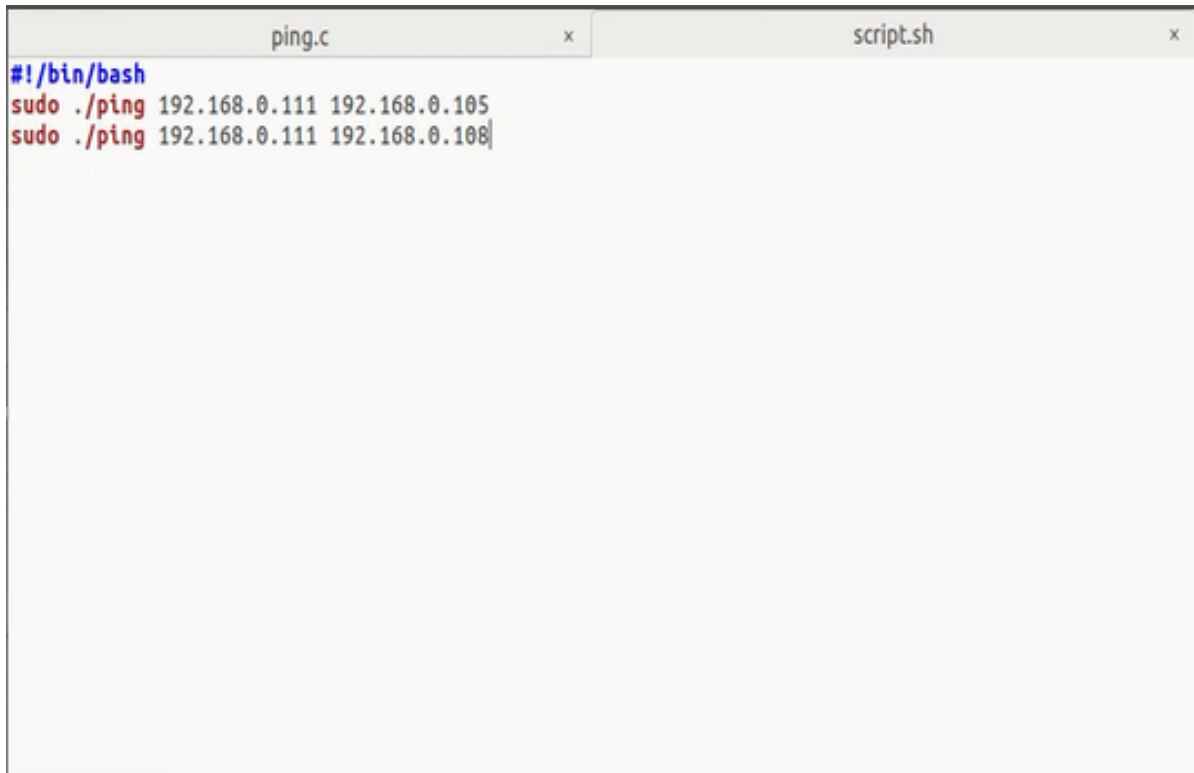


```
[07/11/21]seed@VM:~/Documents$ sudo arp-scan --interface=enp0s3 --localnet
Interface: enp0s3, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.8.1 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.0.1      c4:e9:84:22:72:de      (Unknown)
192.168.0.105   08:00:27:68:c4:50      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.

A screenshot of a terminal window with two tabs: 'ping.c' and 'script.sh'. The 'script.sh' tab is active and shows a bash shell prompt '#!/bin/bash' followed by two lines of code: 'sudo ./ping 192.168.0.111 192.168.0.105' and 'sudo ./ping 192.168.0.111 192.168.0.108'. The cursor is at the end of the second line.

```
#!/bin/bash
sudo ./ping 192.168.0.111 192.168.0.105
sudo ./ping 192.168.0.111 192.168.0.108
```

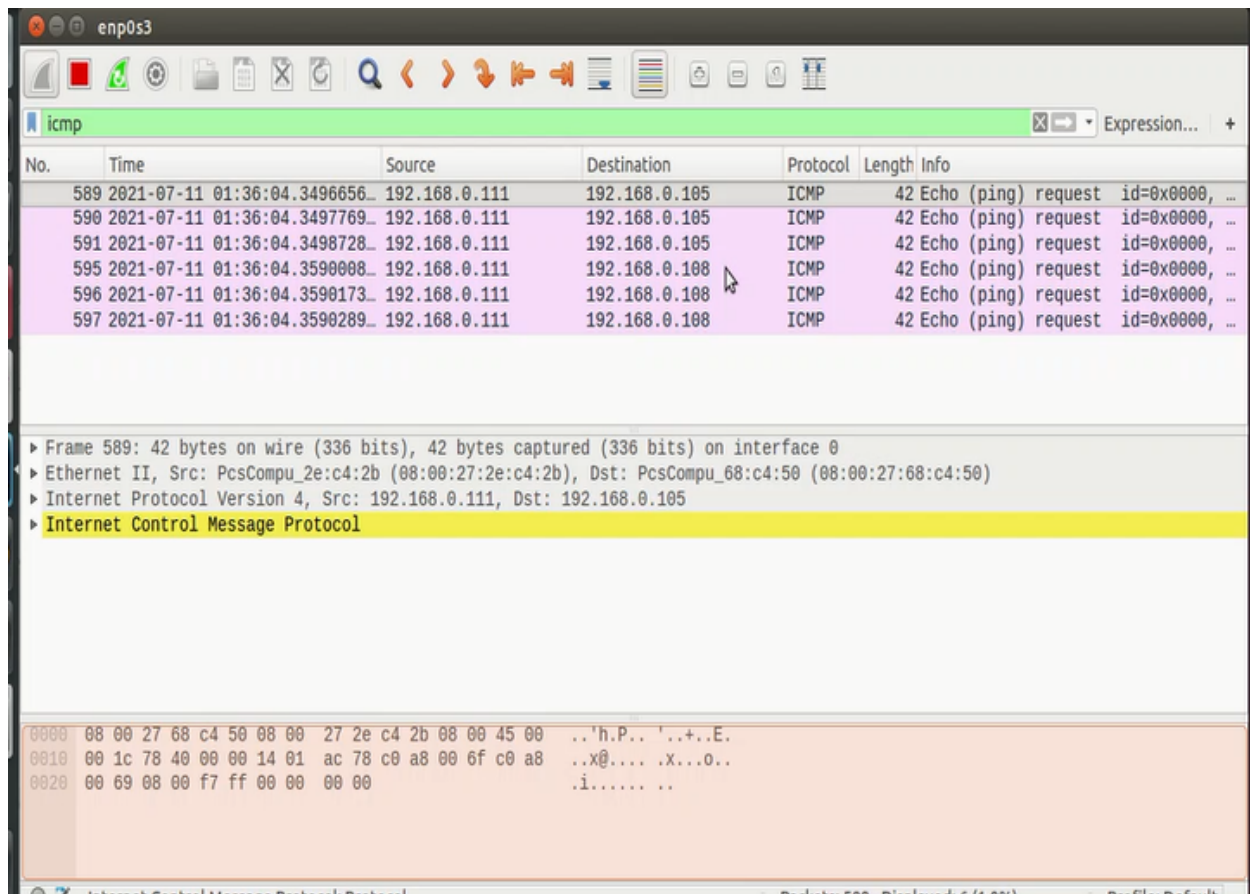
**fig-1.2:**Building the script.sh file with appropriate IP addresses

### **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.

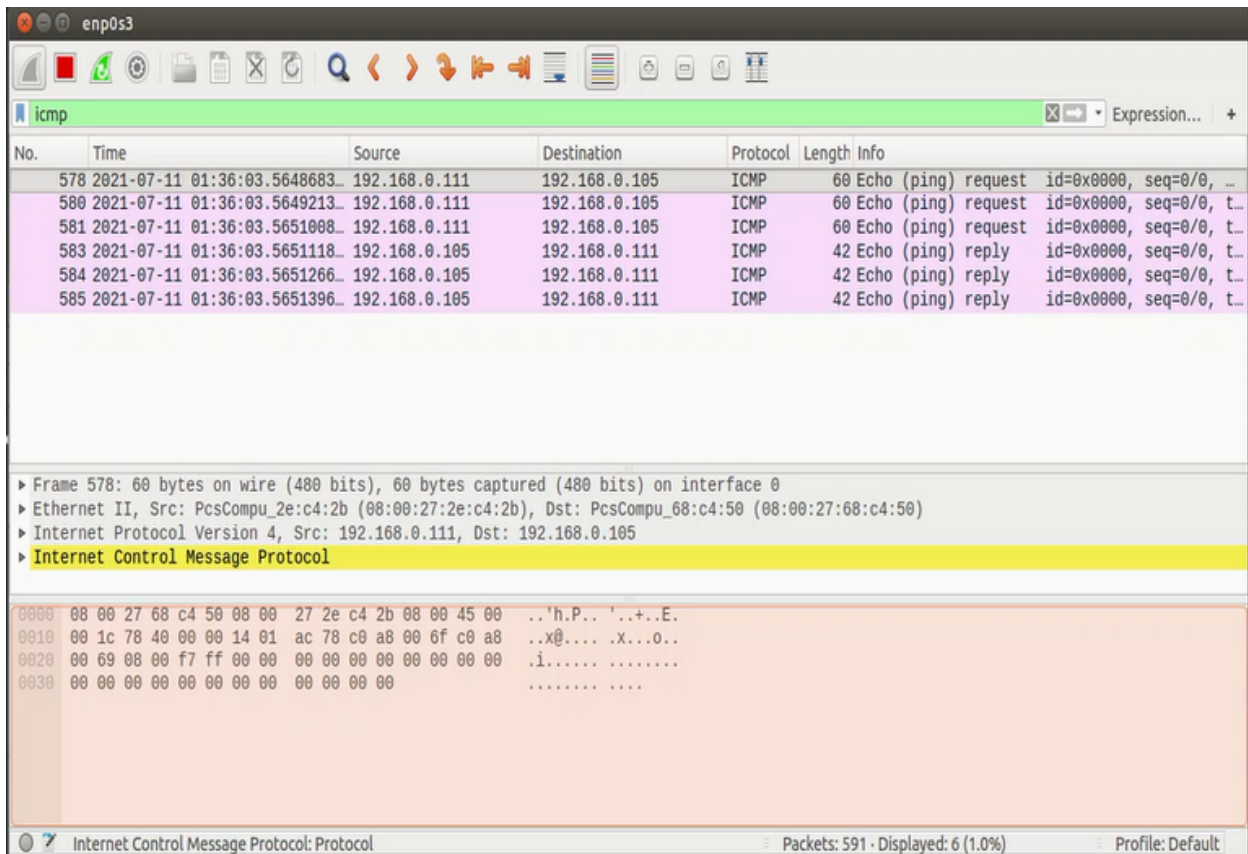
## Observed Outputs:

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.



The image shows a Wireshark packet capture window titled 'enp0s3'. The filter bar is set to 'icmp'. The packet list shows six packets. The first three are Echo (ping) requests from 192.168.0.111 to 192.168.0.105. The next three are Echo (ping) replies from 192.168.0.105 to 192.168.0.111. The packet details pane shows the structure of the selected packet (No. 578), including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
578	2021-07-11 01:36:03.5648683_	192.168.0.111	192.168.0.105	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ...
580	2021-07-11 01:36:03.5649213_	192.168.0.111	192.168.0.105	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, t...
581	2021-07-11 01:36:03.5651008_	192.168.0.111	192.168.0.105	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, t...
583	2021-07-11 01:36:03.5651118_	192.168.0.105	192.168.0.111	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, t...
584	2021-07-11 01:36:03.5651266_	192.168.0.105	192.168.0.111	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, t...
585	2021-07-11 01:36:03.5651396_	192.168.0.105	192.168.0.111	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, t...

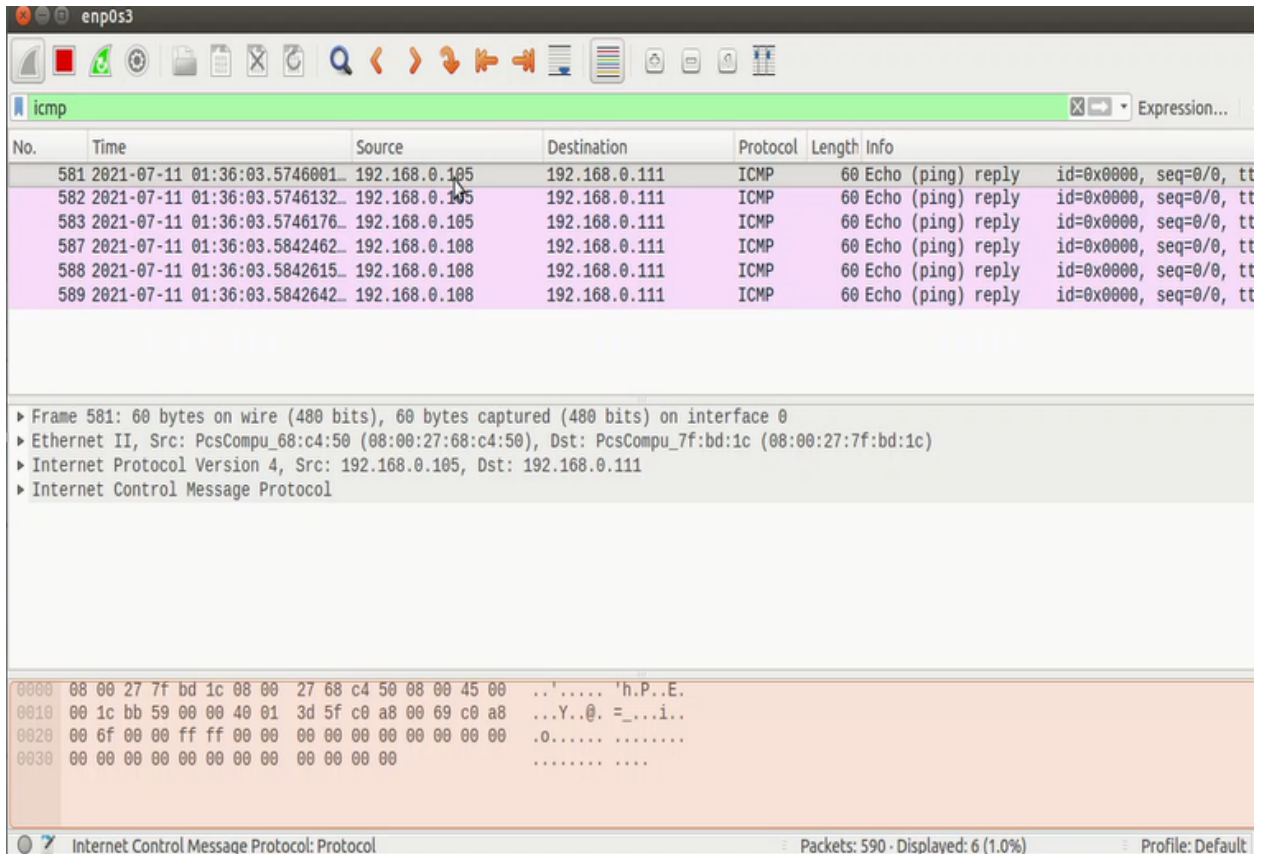
Frame 578: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: PcsCompu\_2e:c4:2b (08:00:27:2e:c4:2b), Dst: PcsCompu\_68:c4:50 (08:00:27:68:c4:50)  
 Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.105  
 Internet Control Message Protocol

0000 08 00 27 68 c4 50 08 00 27 2e c4 2b 08 00 45 00 ..'h.P.. '...E.  
 0010 00 1c 78 40 00 00 14 01 ac 78 c0 a8 00 6f c0 a8 ..x@.... .X...O..  
 0020 00 69 08 00 f7 ff 00 00 00 00 00 00 00 00 00 00 .i.....  
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
 .....

Internet Control Message Protocol: Protocol Packets: 591 · Displayed: 6 (1.0%) Profile: Default

**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**. Though this machine did not send any ICMP ECHO\_REQUEST, ICMP ECHO\_REPLY is sent to this machine due to the attack script executed by the attacker.



The image shows a Wireshark packet capture window titled 'enp0s3'. The filter is set to 'icmp'. The packet list shows six ICMP Echo (ping) reply packets. The first three are from 192.168.0.105 and the next three are from 192.168.0.108, all destined for 192.168.0.111. The packet details pane shows the structure of the first packet (Frame 581): Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
581	2021-07-11 01:36:03.5746001	192.168.0.105	192.168.0.111	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, tt
582	2021-07-11 01:36:03.5746132	192.168.0.105	192.168.0.111	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, tt
583	2021-07-11 01:36:03.5746176	192.168.0.105	192.168.0.111	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, tt
587	2021-07-11 01:36:03.5842462	192.168.0.108	192.168.0.111	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, tt
588	2021-07-11 01:36:03.5842615	192.168.0.108	192.168.0.111	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, tt
589	2021-07-11 01:36:03.5842642	192.168.0.108	192.168.0.111	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, tt

Frame 581: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: PcsCompu\_68:c4:50 (08:00:27:68:c4:50), Dst: PcsCompu\_7f:bd:1c (08:00:27:7f:bd:1c)  
 Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.111  
 Internet Control Message Protocol

0000 08 00 27 7f bd 1c 08 00 27 68 c4 50 08 00 45 00 ..'.... 'h.P..E.  
 0010 00 1c bb 59 00 00 40 01 3d 5f c0 a8 00 69 c0 a8 ...Y..@. =...i..  
 0020 00 6f 00 00 ff ff 00 00 00 00 00 00 00 00 00 .O.....  
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
 0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Internet Control Message Protocol: Protocol Packets: 590 - Displayed: 6 (1.0%) Profile: Default

**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.