CSE 3339 N11

Lab 6

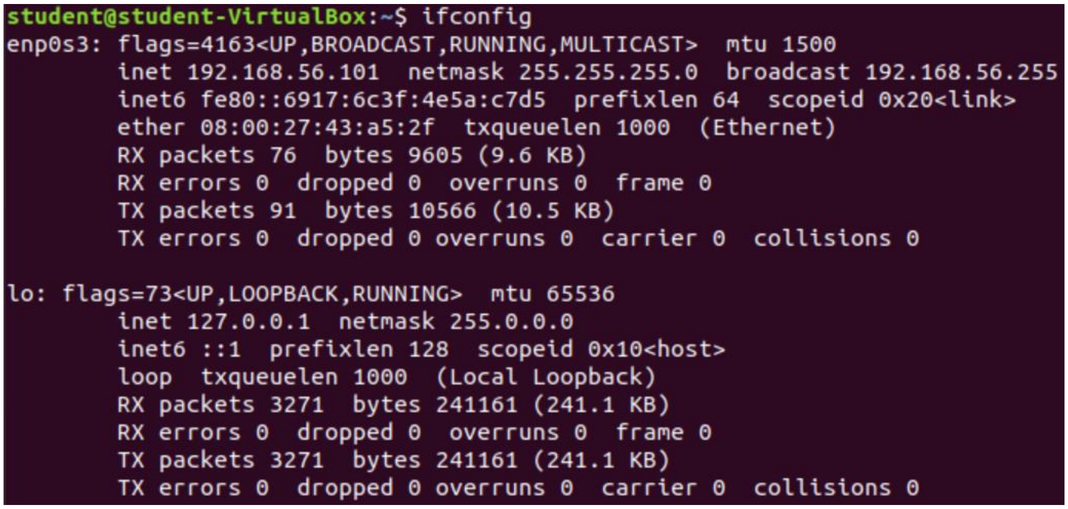
A zero-day attack is an exploit of a previously unknown vulnerability. The exploited system has had zero days to prepare against or mitigate the vulnerability, hence the name.

Snort could catch zero-day network attacks, if the attack uses a port that is typically unused. Snort can easily detect traffic that doesn't resemble typical use and be prompted to block it. On a sematic note, if Snort is catching all network traffic, then by principle it will also catch network attacks, though this greatly harms availability.

Rule:

```
alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
```

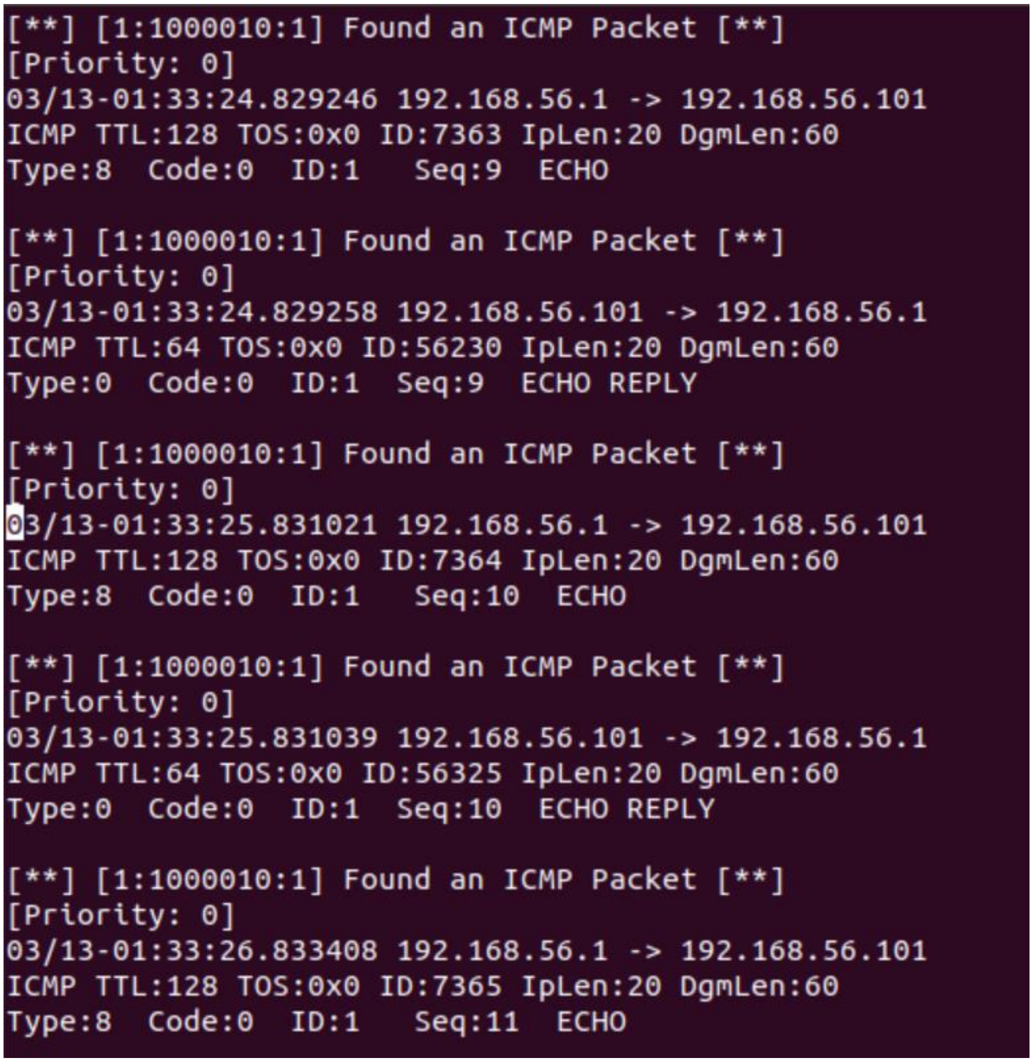
The rule was triggered by sending packets to the virtual machine from any device. This required getting the virtual machine's IP address using ifconfig. From outside of the virtual machine, Windows can send packets to an arbitrary IP with the ping command. Running this command with the virtual machine's IP as the argument sends some packets which trigger the snort rule.



```
student@student-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::6917:6c3f:4e5a:c7d5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:43:a5:2f  txqueuelen 1000  (Ethernet)
        RX packets 76  bytes 9605 (9.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 91  bytes 10566 (10.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3271  bytes 241161 (241.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3271  bytes 241161 (241.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Alert Logs:



```
[**] [1:1000010:1] Found an ICMP Packet [**]
[Priority: 0]
03/13-01:33:24.829246 192.168.56.1 -> 192.168.56.101
ICMP TTL:128 TOS:0x0 ID:7363 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:9  ECHO

[**] [1:1000010:1] Found an ICMP Packet [**]
[Priority: 0]
03/13-01:33:24.829258 192.168.56.101 -> 192.168.56.1
ICMP TTL:64 TOS:0x0 ID:56230 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:9  ECHO REPLY

[**] [1:1000010:1] Found an ICMP Packet [**]
[Priority: 0]
03/13-01:33:25.831021 192.168.56.1 -> 192.168.56.101
ICMP TTL:128 TOS:0x0 ID:7364 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:10  ECHO

[**] [1:1000010:1] Found an ICMP Packet [**]
[Priority: 0]
03/13-01:33:25.831039 192.168.56.101 -> 192.168.56.1
ICMP TTL:64 TOS:0x0 ID:56325 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:10  ECHO REPLY

[**] [1:1000010:1] Found an ICMP Packet [**]
[Priority: 0]
03/13-01:33:26.833408 192.168.56.1 -> 192.168.56.101
ICMP TTL:128 TOS:0x0 ID:7365 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:11  ECHO
```