

[illegible]

3: Catch ICMP alert.

```
[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:34.629380 192.168.0.105 → 192.168.0.184
ICMP TTL:128 TOS:0x0 ID:25596 Iplen:20 Dgmlen:60
Type:8 Code:0 ID:1 Seq:12 ECHO

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:34.629400 192.168.0.184 → 192.168.0.105
ICMP TTL:64 TOS:0x0 ID:37820 Iplen:20 Dgmlen:60
Type:0 Code:0 ID:1 Seq:12 ECHO REPLY

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:41.005633 fe80::103a:5843:ee49:fcea → ff02::16
IPv6-ICMP TTL:1 TOS:0x0 ID:84017152 Iplen:40 Dgmlen:76

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:50:43.011306 fe80::103a:5843:ee49:fcea → ff02::16
IPv6-ICMP TTL:1 TOS:0x0 ID:84017152 Iplen:40 Dgmlen:76

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:12.272649 fe80::103a:5843:ee49:fcea → ff02::16
IPv6-ICMP TTL:1 TOS:0x0 ID:84017152 Iplen:40 Dgmlen:76

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:18.784507 fe80::a00:27ff:fe32:31bc → ff02::2
IPv6-ICMP TTL:255 TOS:0x0 ID:0 Iplen:40 Dgmlen:48

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:20.995849 192.168.0.184 → 192.168.0.1
ICMP TTL:64 TOS:0xC0 ID:3648 Iplen:20 Dgmlen:106
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.1:56130 → 192.168.0.184:137
UDP TTL:64 TOS:0x0 ID:0 Iplen:20 Dgmlen:78 DF
Len: 50 Csum: 5081
(50 more bytes of original packet)
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
03/28-18:51:21.006034 192.168.0.184 → 192.168.0.1
ICMP TTL:64 TOS:0xC0 ID:3649 Iplen:20 Dgmlen:106
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.0.1:35236 → 192.168.0.184:137
UDP TTL:64 TOS:0x0 ID:0 Iplen:20 Dgmlen:78 DF
Len: 50 Csum: 25974
(50 more bytes of original packet)
** END OF DUMP
```

4: What is a zero-day attack?

Zero-day attack is a type of attack which the hacker exploits the vulnerability before software developers can find a fix. It's called zero-day because the hacker exploits the vulnerability usually in the same day that the vulnerability is exposed and the updated patch is published.

5: Can Snort catch zero-day network attacks? If not, why not? If yes, how?

Snort itself may be hard to find the zero-day network attacks if the security staff does not know the vulnerability; if the staff does not know where the vulnerability is, it would be hard to set a trigger and can catch the attack. However, to mitigate the issue at the beginning, the security staff can use ML or other artificial intelligence technique to predict the vulnerability attack and monitor the protocol packet transfer wisely.

6: Add a new rule.

- 1) alert tcp any any -> any any (msg:"TCP Packet found";sid:1000002; rev:1;)
- 2) Instead of catching the ICMP packet, I've changed the rule to let it capture the TCP packet transfer. Then, I test the rule by accessing www.facebook.com, www.twitter.com and several websites.
- 3) The log data becomes:

```
[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.355391 192.168.0.184:59788 -> 104.244.42.194:443
TCP TTL:64 TOS:0x0 ID:0 Iplen:20 Dgmlen:40 DF
*****R** Seq: 0xDDF7D785 Ack: 0x0 Win: 0x0 TcpLen: 20

[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.406834 34.212.188.196:443 -> 192.168.0.184:43458
TCP TTL:226 TOS:0x0 ID:1721 Iplen:20 Dgmlen:64 DF
**A**** Seq: 0x61D90F0D Ack: 0x7F46D3DB Win: 0x76 TcpLen: 44
TCP Options (6) => NOP NOP TS: 1653759613 2695438558 NOP NOP Sack: 32582@54234

[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.411994 34.212.188.196:443 -> 192.168.0.184:43458
TCP TTL:226 TOS:0x0 ID:1722 Iplen:20 Dgmlen:52 DF
**A**** Seq: 0x61D90F0D Ack: 0x7F46D3DB Win: 0x76 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1653759618 2695438694

[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.420156 34.212.188.196:443 -> 192.168.0.184:43458
TCP TTL:226 TOS:0x0 ID:1723 Iplen:20 Dgmlen:83 DF
**AP*** Seq: 0x61D90F0D Ack: 0x7F46D3DB Win: 0x76 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1653759627 2695438694

[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.420176 192.168.0.184:43458 -> 34.212.188.196:443
TCP TTL:64 TOS:0x0 ID:0 Iplen:20 Dgmlen:40 DF
*****R** Seq: 0x7F46D3DB Ack: 0x0 Win: 0x0 TcpLen: 20

[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.420313 34.212.188.196:443 -> 192.168.0.184:43458
TCP TTL:226 TOS:0x0 ID:1724 Iplen:20 Dgmlen:83 DF
**AP*** Seq: 0x61D90F2C Ack: 0x7F46D3DB Win: 0x76 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1653759627 2695438694

[**] [1:1000002:1] TCP Packet found [**]
[Priority: 0]
03/28-19:52:55.420318 192.168.0.184:43458 -> 34.212.188.196:443
TCP TTL:64 TOS:0x0 ID:0 Iplen:20 Dgmlen:40 DF
*****R** Seq: 0x7F46D3DB Ack: 0x0 Win: 0x0 TcpLen: 20
```