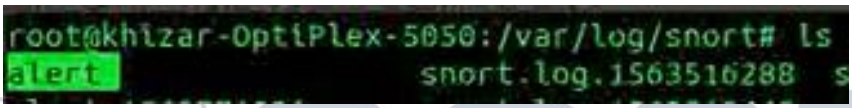
Snort working Proof of Concept (PoC) (Part-2):

After launching the DoS attack on the target snort machine, In the live feed you will see a whole lot of traffic coming in from the attacker machine (The one with LOIC deployed).

This attack will be documented in the form of an alert in the alert file present in the var/log/snort directory.

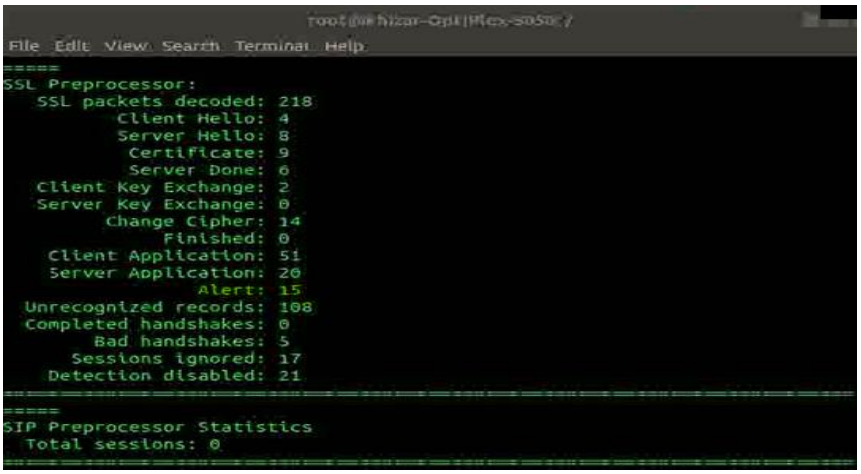


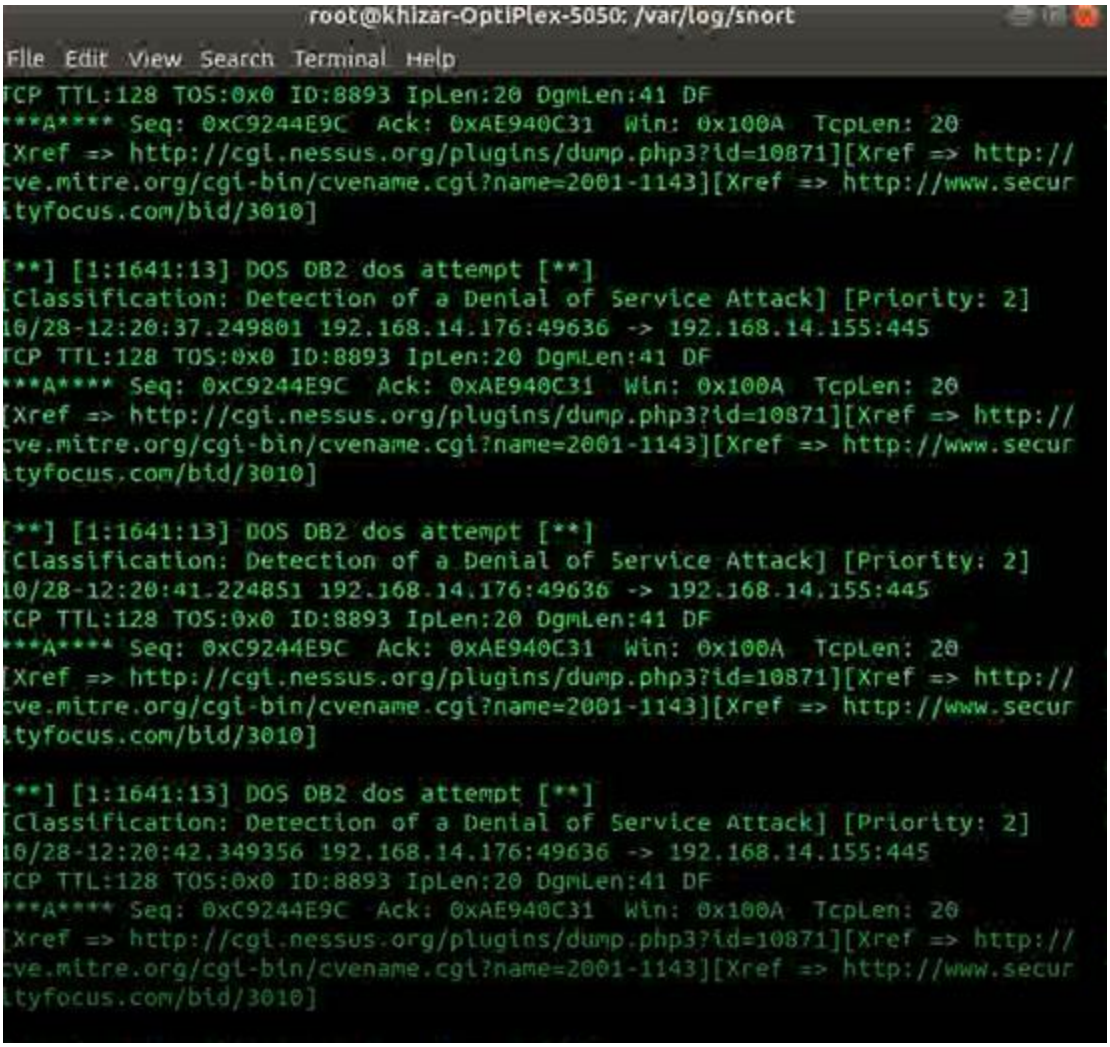
These alerts are generated based on the rules that are present in the etc/snort/rules folder.

You can define your own custom rules as well.

If you define your own custom rules file for example custom.rules in the above folder make sure to include the path to your custom rules in the etc/snort/snort.conf file like shown below:

When you open up the alert file after the DoS attack, you should be able to see alerts that were generated as shown below:




root@khizar-OptiPlex-5050: /var/log/snort
File Edit View Search Terminal Help
TCP TTL:128 TOS:0x0 ID:8893 IpLen:20 DgmLen:41 DF
A* Seq: 0xC9244E9C Ack: 0xAE940C31 Win: 0x100A TcpLen: 20
[Xref => http://cgi.nessus.org/plugins/dump.php3?id=10871][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2001-1143][Xref => http://www.secur
ityfocus.com/bid/3010]
[**] [1:1641:13] DOS DB2 dos attempt [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
10/28-12:20:37.249801 192.168.14.176:49636 -> 192.168.14.155:445
TCP TTL:128 TOS:0x0 ID:8893 IpLen:20 DgmLen:41 DF
A* Seq: 0xC9244E9C Ack: 0xAE940C31 Win: 0x100A TcpLen: 20
[Xref => http://cgi.nessus.org/plugins/dump.php3?id=10871][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2001-1143][Xref => http://www.secur
ityfocus.com/bid/3010]
[**] [1:1641:13] DOS DB2 dos attempt [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
10/28-12:20:41.224851 192.168.14.176:49636 -> 192.168.14.155:445
TCP TTL:128 TOS:0x0 ID:8893 IpLen:20 DgmLen:41 DF
A* Seq: 0xC9244E9C Ack: 0xAE940C31 Win: 0x100A TcpLen: 20
[Xref => http://cgi.nessus.org/plugins/dump.php3?id=10871][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2001-1143][Xref => http://www.secur
ityfocus.com/bid/3010]
[**] [1:1641:13] DOS DB2 dos attempt [**]
[Classification: Detection of a Denial of Service Attack] [Priority: 2]
10/28-12:20:42.349356 192.168.14.176:49636 -> 192.168.14.155:445
TCP TTL:128 TOS:0x0 ID:8893 IpLen:20 DgmLen:41 DF
A* Seq: 0xC9244E9C Ack: 0xAE940C31 Win: 0x100A TcpLen: 20
[Xref => http://cgi.nessus.org/plugins/dump.php3?id=10871][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2001-1143][Xref => http://www.secur
ityfocus.com/bid/3010]