

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.

```
root@khizar-OptiPlex-5050:/var/log/snort# ls
alert snort.log.1563516288 s
```

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

```
:/etc/snort/rules# ls
sponses.rules      community-web-dos.rules  policy.rules
rules              community-web-iis.rules  pop2.rules
ic.rules           community-web-misc.rules  pop3.rules
s                 community-web-php.rules  porn.rules
-bot.rules         ddos.rules              rpc.rules
-deleted.rules     deleted.rules           rservices.rules
-dos.rules         dns.rules               scan.rules
-exploit.rules     dos.rules               shellcode.rules
-ftp.rules         experimental.rules     smtp.rules
-game.rules        exploit.rules           snmp.rules
-icmp.rules        finger.rules            sql.rules
-imap.rules        ftp.rules               telnet.rules
-inappropriate.rules  icmp-info.rules       tftp.rules
-mail-client.rules  icmp.rules              virus.rules
-misc.rules         imap.rules              web-attacks.rules
-nntp.rules         info.rules               web-cgi.rules
-oracle.rules       local.rules              web-client.rules
-policy.rules       misc.rules               web-coldfusion.rules
-sip.rules          multimedia.rules         web-frontpage.rules
-smtp.rules         mysql.rules              web-iis.rules
-sql-injection.rules  netbios.rules           web-misc.rules
-virus.rules        nntp.rules               web-php.rules
-web-attacks.rules  oracle.rules             x11.rules
-web-cgi.rules      other-ids.rules
-web-client.rules   p2p.rules
```

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:

```
GNU nano 2.9.8 snort.conf

# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

include $RULE_PATH/custom.rules
```

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@kali:~/Hacker-Op1/HTex-SD50k/
File Edit View Search Terminal Help
=====
SSL Preprocessor:
  SSL packets decoded: 218
    Client Hello: 4
    Server Hello: 8
    Certificate: 9
    Server Done: 6
  Client Key Exchange: 2
  Server Key Exchange: 0
    Change Cipher: 14
    Finished: 0
  Client Application: 51
  Server Application: 20
    Alert: 15
  Unrecognized records: 108
  Completed handshakes: 0
    Bad handshakes: 5
  Sessions ignored: 17
  Detection disabled: 21
=====
SIP Preprocessor Statistics
  Total sessions: 0
=====
```

```
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://cgl.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://cgl.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://cgl.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://cgl.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]
```