Snort — IPS & IDS Working PoC

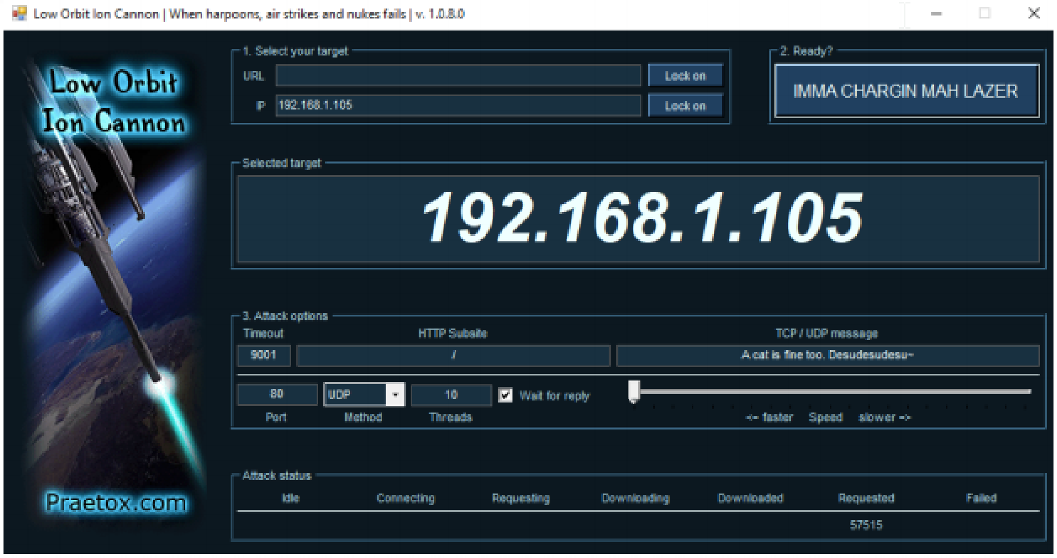
To demonstrate the working of Snort IPS/IDS, we will simulate a Denial of Service attack.

For this purpose the Lower Orbit Ion Canon (LOIC) tool is used to launch a Denial of Service (DoS) attack on the target machine where the snort is deployed.

To download the LOIC tool use the link given below: https://sourceforge.net/projects/loic/files/latest/download

Note: Before downloading make sure to turn off any antivirus on your machine.

After the download is complete, you can extract the file, and it will give you an executable file named LOIC.exe. Double click the executable file and you will be shown the following screen.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
URL:
IP: 192.168.1.105

Selected target: 192.168.1.105

3. Attack options
Timeout: 9001
HTTP Subsite: /
TCP / UDP message: A cat is fine too. Desudesudesu~
Port: 80
Method: UDP
Threads: 10
☑ Wait for reply

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					57515	

Figure 1: LOIC's interface

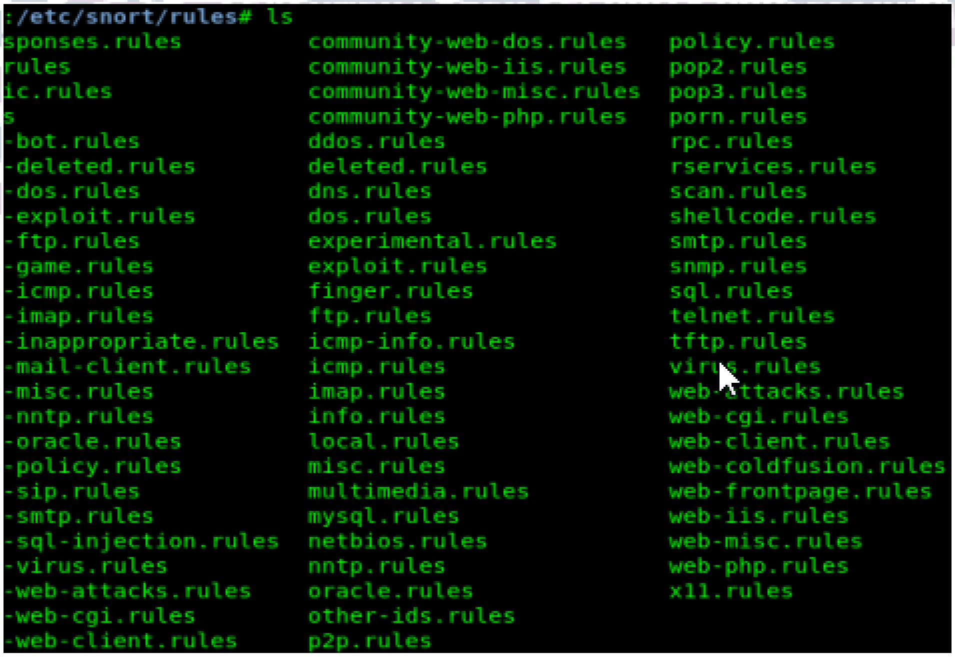
In the IP dialogue box, enter the IP address of your target machine (on which snort is installed) and select any one of the three methods of attack, you can leave the port to default 80 or change it in accordance with your own scenario.

Next Click ***IMMA CHARGIN MAH LAZER*** button to start the attack.

After launching the DoS attack on the target machine having Snort already installed, you will see an immense amount of traffic coming in from the attacker machine (i.e. the system with LOIC deployed).

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

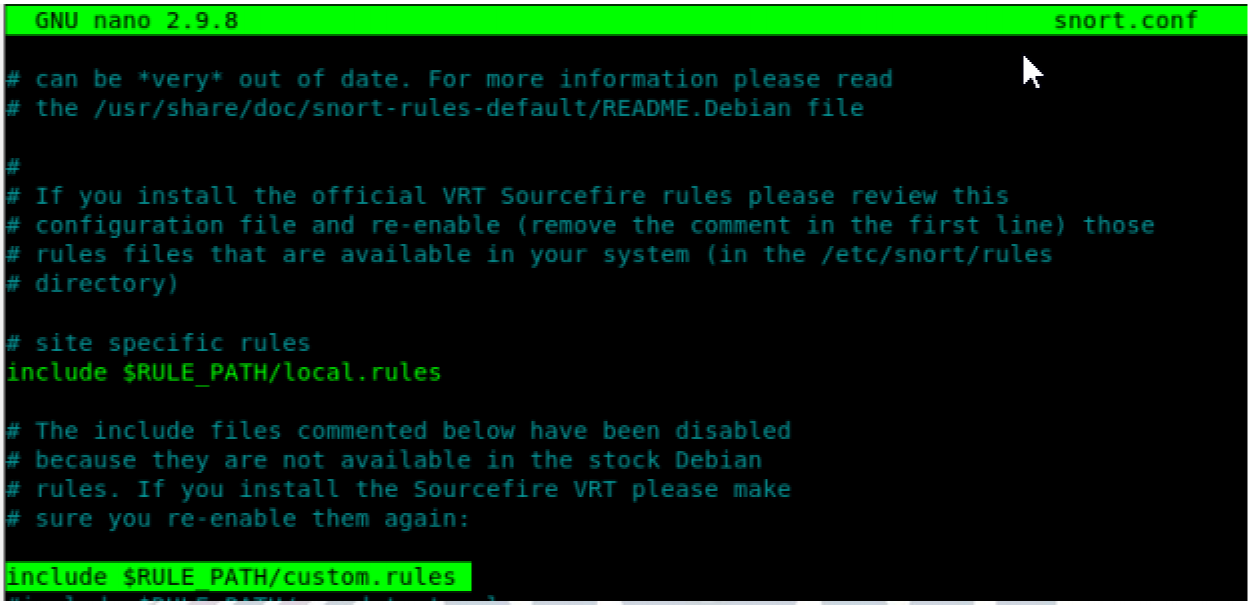
These alerts are generated based on the rules that are present in the ***etc/snort/rules*** folder.



```
:/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
```

Figure 2: Snort Rules

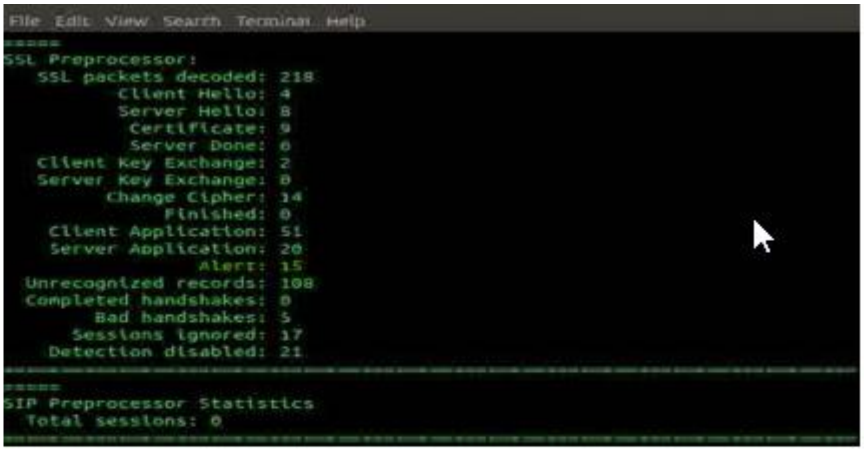
You can also define your own custom rules as well. If you do so, for example you create your own rule set called custom.rules in the above folder, make sure to include the path of your custom rules in the ***etc/snort/snort.conf*** file, as shown below:



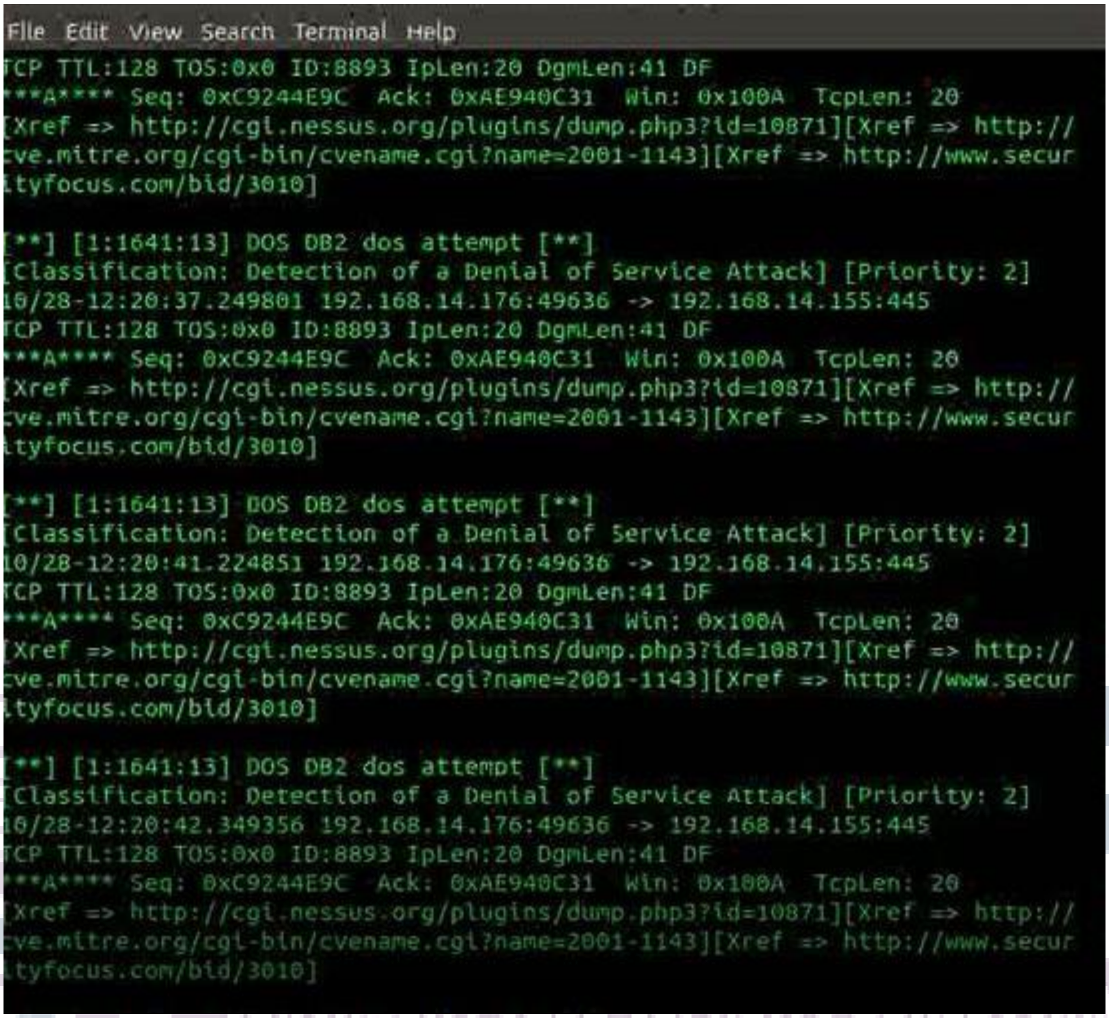
```
  GNU nano 2.9.8                                                             snort.conf

# 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
```

Figure 3: snort.config

Now going back to the original example of the DoS attack, when you open up the alert file after the DoS attack, you should be able to see alerts that were generated as shown below:



```
=====
SSL Preprocessor:
   SSL packets decoded: 218
          Client Hello: 4
          Server Hello: 8
           Certificate: 9
           Server Done: 0
   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
===============================================================================
```



```
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]
```

Figure 4: Snort alert file

As shown above, you can see Snort documented that a DoS attack took place, the attackers IP address and the port number.

You can configure Snort as per your requirement and environment to handle such alerts accordingly.