Scenario 1 (Brute Force Attack): J&Y Enterprise is one of the top coffee retails in the world. They are known as tech-coffee shops and serve millions of coffee lover tech geeks and IT specialists every day. They are famous for specific coffee recipes for the IT community and unique names for these products. Their top five recipe names are; WannaWhite, ZeroSleep, MacDown, BerryKeep and CryptoY. J&Y's latest recipe, "Shot4J", attracted great attention at the global coffee festival. J&Y officials promised that the product will hit the stores in the coming months. The super-secret of this recipe is hidden in a digital safe. Attackers are after this recipe, and J&Y enterprises are having difficulties protecting their digital assets. Last week, they received multiple attacks and decided to work with you to help them improve their security level and protect their recipe secrets.

+==========+

1. First, we start the snort in log mode and capture some traffic using the command “sudo snort –dev –l .” Then stop it after some time.

```
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:         3048 ( 22.544%)
     Other:            0 (  0.000%)
Bad Chk Sum:         2416 ( 17.870%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:        13520
===============================================================================
Snort exiting
ubuntu@ip-10-10-131-93:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  snort.log.1668753619
ubuntu@ip-10-10-131-93:~$
```

2. By analyzing it we can see two of the well-known ports in the traffic. Port 22 and 80.

```
TCP Options (3) => NOP NOP TS: 2211333589 540832450
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-06:40:56.959516 10.100.2.28:58224 -> 10.10.131.93:80
TCP TTL:64 TOS:0x0 ID:65374 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x88D2BCE8  Ack: 0xA5A5D460  Win: 0x1E10  TcpLen: 32
TCP Options (3) => NOP NOP TS: 540832451 2211333588
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/18-06:40:56.981870 10.10.140.29:22 -> 10.10.245.36:46462
TCP TTL:64 TOS:0x0 ID:60259 IpLen:20 DgmLen:332 DF
***AP*** Seq: 0xDFC2ABFA  Ack: 0x63925BF0  Win: 0x1E3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4119651925 1884544473
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-06:40:56.994992 10.10.245.36:46462 -> 10.10.140.29:22
TCP TTL:64 TOS:0x0 ID:9419 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0x63925BF0  Ack: 0xDFC2AD12  Win: 0x1E1  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1884544491 4119651925
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-06:40:57.013866 10.10.245.36:46462 -> 10.10.140.29:22
TCP TTL:64 TOS:0x0 ID:9420 IpLen:20 DgmLen:104 DF
***AP*** Seq: 0x63925C00  Ack: 0xDFC2AD12  Win: 0x1E1  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1884544491 4119651925
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/18-06:40:57.024424 10.10.140.29:22 -> 10.10.245.36:46462
TCP TTL:64 TOS:0x0 ID:60260 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xDFC2AD12  Ack: 0x63925C00  Win: 0x1E3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4119651925 1884544491
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/18-06:40:57.034980 10.10.140.29:22 -> 10.10.245.36:46462
TCP TTL:64 TOS:0x0 ID:60261 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xDFC2AD12  Ack: 0x63925C34  Win: 0x1E3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4119651925 1884544491
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-06:40:57.040476 10.100.2.28:58224 -> 10.10.131.93:80
TCP TTL:64 TOS:0x0 ID:65375 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0x88D2BCE8  Ack: 0xA5A5D460  Win: 0x1E10  TcpLen: 32
TCP Options (3) => NOP NOP TS: 540832532 2211333588
```

3. Let's filter the traffic with port 22. 1490 packets were capture for it

```
     S5 G 2:            0 (  0.000%)
      Total:         1490
===============================================================================
Snort exiting
ubuntu@ip-10-10-131-93:~$
```

4. Let's filter traffic with port 80. 12026 packets were capture for it

```
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:        12026
===============================================================================
Snort exiting
ubuntu@ip-10-10-131-93:~$
```

5. From investigating the flow of traffic for both port 22 and port 80 we can say that port 22 is the brute force which is ssh. The reason is that for port 22, there is a pattern of the attacker sending packets to port 22 and port 22 send packets to attacker's port and vice versa, whereas it’s the same for port 80.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
11/18-12:22:44.295077 10.100.1.33:45840 -> 10.10.233.91:80
TCP TTL:64 TOS:0x0 ID:59440 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xA6BBB45B  Ack: 0x125295CE  Win: 0xC7F  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2845384662 171301364
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-12:22:44.391666 10.100.1.33:45840 -> 10.10.233.91:80
TCP TTL:64 TOS:0x0 ID:59441 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0xA6BBB45B  Ack: 0x125295CE  Win: 0xC8F  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2845384754 171301364
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-12:22:44.391666 10.100.1.33:45840 -> 10.10.233.91:80
TCP TTL:64 TOS:0x0 ID:59442 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0xA6BBB46B  Ack: 0x125295CE  Win: 0xC8F  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2845384755 171301364
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-12:22:44.391666 10.100.1.33:45840 -> 10.10.233.91:80
TCP TTL:64 TOS:0x0 ID:59443 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0xA6BBB47B  Ack: 0x125295CE  Win: 0xC8F  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2845384756 171301364
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/18-12:22:44.391666 10.100.1.33:45840 -> 10.10.233.91:80
TCP TTL:64 TOS:0x0 ID:59444 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0xA6BBB48B  Ack: 0x125295CE  Win: 0xC8F  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2845384757 171301364
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/18-12:22:44.391889 10.10.233.91:80 -> 10.100.1.33:45840
TCP TTL:64 TOS:0x0 ID:9978 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x125295CE  Ack: 0xA6BBB49B  Win: 0x1C6  TcpLen: 32
TCP Options (3) => NOP NOP TS: 171301461 2845384754
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

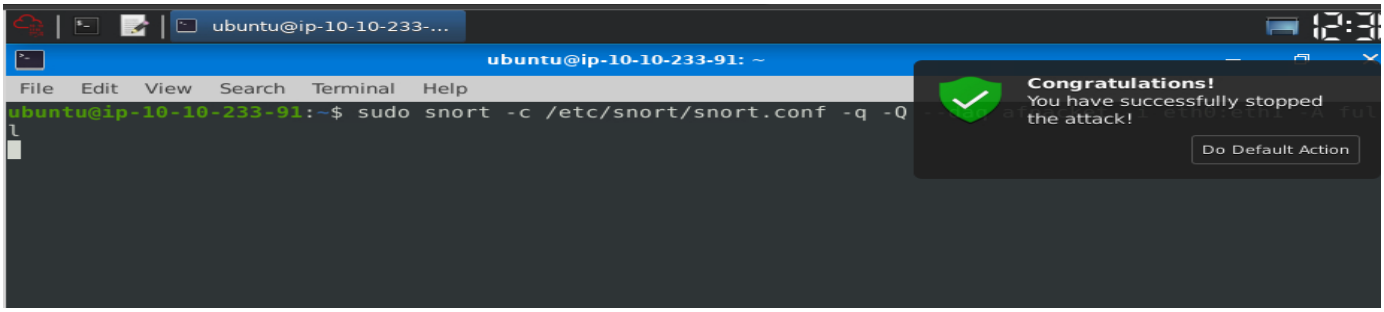
6. Therefore, we need to put some rules for port 22 or SSH, by editing the local rules file in /etc/snort/rules/local.rules.

```
ubuntu@ip-10-10-233-91: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 4.8                 /etc/snort/rules/local.rules                 Modified
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

drop tcp any 22 <- any any (msg: "SSH Brute Forc"; sid: 100001; rev:1;)
```

7. By running this command, we will apply the rule and stop the attack

```
File  Edit  View  Search  Terminal  Help
ubuntu@ip-10-10-233-91:~$ sudo snort -c /etc/snort/snort.conf -q -Q --daq afpacket -i eth0:eth1 -A ful
l
```


ubuntu@ip-10-10-233-...
ubuntu@ip-10-10-233-91: ~
File Edit View Search Terminal Help
ubuntu@ip-10-10-233-91:~$ sudo snort -c /etc/snort/snort.conf -q -Q
l
Congratulations!
You have successfully stopped the attack!
Do Default Action