SNORT – LIVE ATTACKS TEST (REVERSE SHELL)

+] You
Thanks team. J.A.V.A. can you do a quick scan for me? We haven't investigated the outbound traffic yet.

[+] J.A.V.A.
Yes, sir. Outbound traffic investigation has begun.

[+] THE NARRATOR
The outbound traffic? Why?

[+] YOU
We have stopped some inbound access attempts, so we didn't let the bad guys get in. How about the bad guys who are already inside? Also, no need to mention the insider risks, huh? The dwell time is still around 1-3 months, and I am quite new here, so it is worth checking the outgoing traffic as well.

[+] J.A.V.A.
Sir, persistent outbound traffic is detected. Possibly a reverse shell...

[+] YOU
You got it!

[+] J.A.V.A.
Sir, you need to observe the traffic with Snort and identify the anomaly first. Then you can create a rule to stop the reverse shell. GOOD LUCK!

Answer the questions below

First of all, start Snort in sniffer mode and try to figure out the attack source, service and port.
Then, write an IPS rule and run Snort in IPS mode to stop the brute-force attack. Once you stop the attack properly, you will have the flag on the desktop!

Here are a few points to remember:

- Create the rule and test it with "-A console" mode.
- Use "-A full" mode and the default log path to stop the attack.
- Write the correct rule and run the Snort in IPS "-A full" mode.
- Block the traffic at least for a minute and then the flag file will appear on your desktop.

1.Stop the attack and get the flag (which will appear on your Desktop)

2.What is the used protocol/port in the attack?

3.Which tool is highly associated with this specific port number?

My first task is to use SNORT in sniffer mode and then to log the packets.
-v = verbose, displays the TCP/IP in the console
-l = to log the packets and save it in the current directory.

```
Snort exiting
ubuntu@ip-10-10-86-41:~$ sudo snort -v -l .
```

I used the command above to achieve this.

```
        IPX:              0 (  0.000%)
   Eth Loop:              0 (  0.000%)
   Eth Disc:              0 (  0.000%)
   IP4 Disc:           1292 ( 19.292%)
   IP6 Disc:              0 (  0.000%)
   TCP Disc:              0 (  0.000%)
   UDP Disc:              0 (  0.000%)
  ICMP Disc:              0 (  0.000%)
All Discard:           1292 ( 19.292%)
      Other:              0 (  0.000%)
Bad Chk Sum:           1467 ( 21.905%)
    Bad TTL:              0 (  0.000%)
     S5 G 1:              0 (  0.000%)
     S5 G 2:              0 (  0.000%)
      Total:           6697
```

I let it run for 15 seconds and then stopped snort which provided me with 6697 alerts.

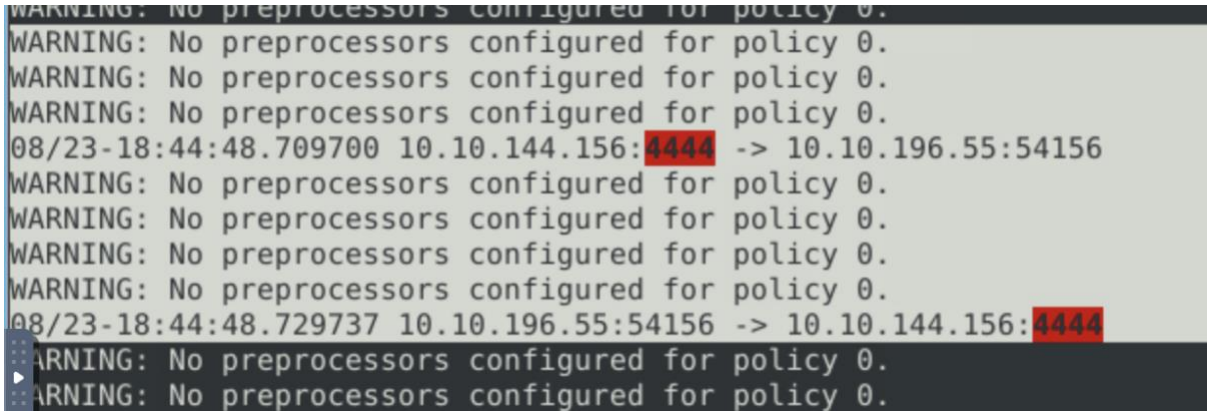
Automatically snort created a log within the same directory so I used the following command "sudo snort -r snort.log.1672697486 -X" to analyse the log. I used "-X" to provide a more in depth analysis on the data packets.

```
Snort exiting
ubuntu@ip-10-10-86-41:~$ sudo snort -r snort.log.16928162
```

Whilst scanning the log I noticed the port number ":4444" appear frequently. ":4444" is commonly used by hackers in reverse shell connections so it was immediately suspicious.

```
WARNING: No preprocessors configured for policy 0.
08/23-18:44:48.613538 10.10.144.156:4444 -> 10.10.196.55:54156
TCP TTL:64 TOS:0x0 ID:9999 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x50ED9601  Ack: 0xBCF7ADED  Win: 0x1E9  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1981027452 2358859753
0x0000: 02 7C 9A 93 DF DD 02 15 8B 5C 4F EF 08 00 45 00  .|.......\O...E.
0x0010: 00 34 27 0F 40 00 40 06 AA CD 0A 0A 90 9C 0A 0A  .4'.@.@.........
0x0020: C4 37 11 5C D3 8C 50 ED 96 01 BC F7 AD ED 80 10  .7.\..P.........
0x0030: 01 E9 66 1C 00 00 01 01 08 0A 76 14 14 7C 8C 99  ..f.......v..|..
0x0040: 57 E9                                            W.
```

The IP attached to the port (10.10.144.156) was also most likely an internal IP. I then decided to use “sudo snort -r snort.log.1672697486 -X | grep ":4444" to further investigate.



Once my suspicions were confirmed I decided to try and answer question 2 and 3. Question 3 I decided to go online and find out which tool was associated with the port number “4444”. As you can see below a tool called “Metasploit” is popular amount hackers and security professionals

2.What is the used protocol/port in the attack?

Answer: tcp/4444

3.Which tool is highly associated with this specific port number?

Answer: Metasploit

what tool is associated with port number 4444

Port number 4444 is commonly associated with the tool Metasploit's reverse TCP payloads. Metasploit is a popular penetration testing framework used by security professionals to assess the security of systems and networks. Port 4444 is often used as the default port for establishing a reverse TCP connection between an attacker's system and a compromised target.

Now that I had answered both questions 2 and 3 I was able to start creating the rule to stop the attack and capture the flag
I used the following to start building my rule
sudo nano /etc/snort/rules/local.rules

```
ubuntu@ip-10-10-86-41:~$ sudo nano etc/snort/rules/local.files
ubuntu@ip-10-10-86-41:~$ sudo nano /etc/snort/rules/local.files
```

I have used 'drop' instead of "alert" as we actually want to stop/block the attack from happening.
tcp protocol and 4444 as this is the number of the port we need to stop.

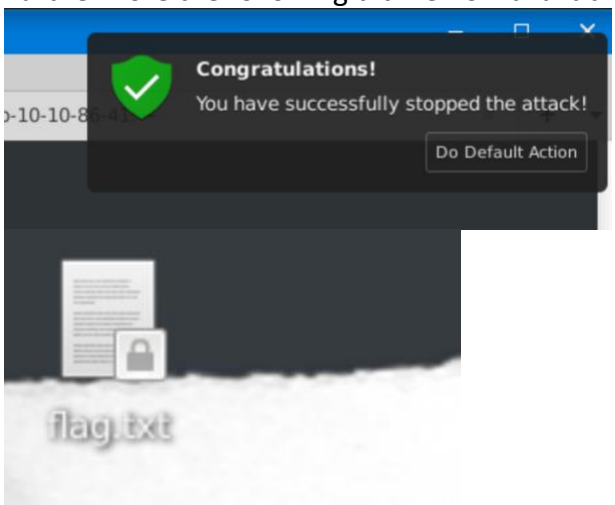
```
  GNU nano 4.8                                          /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
drop tcp any 4444 <> any any (msg: "Reverse Shell Found"; sid: 10001; rev:1;)
```

Once the rule is saved, I was able to use the following code below which was used in previous snort sessions to run against the live traffic

sudo snort -c /ect/snort/snort.conf -q -Q --daq afpacket -i eth0:eth1 -A full

```
08/23-18:44:49.389106 10.10.196.55:54172 -> 10.10.144.156:4444
ubuntu@ip-10-10-86-41:~$ sudo snort -c /etc/snort/snort.conf -q -Q --daq afpacket -i eth0:eth1 -A full
```

After a couple of minutes this notification popped up proving the rule was a success.
Furthermore the following txt file now available on desktop



Once opened the flag appeared.

All questions and answers below

1.Stop the attack and get the flag (which will appear on your Desktop)

Answer : THM{0ead8c494861079b1b74ec2380d2cd24}

2.What is the used protocol/port in the attack?

Answer: tcp/4444

3.Which tool is highly associated with this specific port number?

Answer: Metasploit