Task-1 Brute-ForceUseM to finish this task.

**[+] THE NARRATOR**

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.

This is your assistant **J.A.V.A. (Just Another Virtual Assistant).** She is an AI-driven virtual assistant and will help you notice possible anomalies. Hey, wait, something is happening...

**[+] J.A.V.A.**

Welcome, sir. I am sorry for the interruption. It is an emergency. Somebody is knocking on the door!

**[+] YOU**

Knocking on the door? What do you mean by "knocking on the door"?

**[+] J.A.V.A.**

We have a brute-force attack, sir.

**[+] THE NARRATOR**

This is not a comic book! Would you mind going and checking what's going on! Please... 

**[+] 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 brute-force attack. 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.

Ans: There are Two mode 1st is sniffer and another one is logger mode sniff packet and log them

For this we use logger mode

1) “sudo snort -dev -l .” to get a traffic and create a log file

2) “sudo snort -r snort.log.1675….” to read a log file

Qus: What is the name of the service under attack?

Ans: ssh because after ip address it show port 22 which is ssh

3) now we can filter the traffic according to port number because we observer

sudo snort -r snort.log.1675…. ‘port 22’

as you can see there are traffic who continusly talk to our ip which mean multiple time login attempt

Qus: What is the used protocol/port in the attack?

tcp/22

Qus: Stop the attack and get the flag (which will appear on your Desktop)

Ans: sudo nano /etc/snort/rules/local.rules

So in task we want to find drop packets and block them

Local.rules “drop tcp any 22 <> any any (msg:”Drop packets”;sid:100001;rev:1;)”

Sudo snort -c /etc/snort/snort.conf -q -Q –daq afpacket -i eth0:eth1 -A full

Task-2 Reverse-Shell

**[+] THE NARRATOR**

Good Job! Glad to have you in the team!

**[+] J.A.V.A.**

Congratulations sir. It is inspiring watching you work.

**[+] 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. Sudo snort -dev -l .
2. You can see most of the traffic is generate using port 4444 and it mostly used by metaspolit

What is the used protocol/port in the attack?

Tcp/4444

Which tool is highly associated with this specific port number?

Metasploit

1. Stop the attack and get the flag (which will appear on your Desktop)
2. sudo nano /etc/snort/rules/local.rules
3. “drop tcp any 4444 -> any any (msg:”Drop packets”;sid:100001;rev:1;)”
4. Sudo snort -c /etc/snort/snort.conf -q -Q –daq afpacket -i eth0:eth1 -A full