Security Operations & Incident Management

Lab: Host infection intrusion analysis

1. Setting up the Environment

As part of this workshop, you will get to analyse malware traffic, as generated by an infected host.

Power on **Ubuntu 26** image, using the following roles and user credentials:

username: student
password: student

2. Run snort to generate alerts using community rules

Go to "/home/Desktop/data/2-running-snort/spam-traffic"

Create spamlogs folder

mkdir spamlogs

Run snort

snort -c snort.lua -r spamsnapshot -l spamlogs -A alert_full --lua "alert_full={file=true}"

```
snort -c snort.lua -r spamsnapshot -l spamlogs -A alert_full --lua "alert_full={file=true}"
```

Check output

```
student@student:~/Desktop/data/2-running-snort/spam-traffic$ ls spamlogs
alert_full.txt
```

3. Host Infection: Mass Mailing Malware

Now, let's analyse a dataset containing a mass mailing malware. This dataset was captured in 2009 when a user complained about slow performance on their system. The reason became clear pretty soon!!!

The characteristic of mass mailing malware is that they propagate by sending illegitimate emails en masse. They usually connect to command and control servers to send and receive updates and commands. More sophisticated malware use their own Dynamic DNS infrastructure, also known as fast-flux. Such a volume of attacking activity is also likely to generate error messages from external hosts/routers that deny and block the offending traffic.

Mass Mailing Dataset File	
Image	**Location**
Ubuntu 26	`Desktop/data/2-running-snort/spam-traffic/`**`spamsnapshot`**

Analyse the dataset above with Snort and find out what happened.
Tips: After you generate the alerts, you might want to enter VMware into 'Full Screen Mode'.

You might want to consider the following stages of Intrusion Analysis. Use the spaces below to write any commands, notes, filters that you use in this process:

1. Is this an attack? If yes, how do you know? Which IDS alerts suggest this is the case? (Hint: do the IDS alerts capture the offending traffic or the responses to it?)
2. Which hosts are affected? It is essential to determine the target. How do you do that?
3. Immediate step to take infected host offline. (No action needed for you)

1. How does the malware work and propagate? (Hint: You might want to open the dataset with Wireshark. You might want to use features, such as ‘Statistics -> Protocol Hierarchy’).
2. What is the extent of the damage? Are there any other hosts affected? How would you find out? (Hint: You might want to use BPF tcpdump filters)

6. ***Cleaning up the image***

Please make sure that you delete all the alerts you created, to avoid interfering with other students’ work.