Snort challenge – the basics

Task-1 Http

**Navigate to the task folder.**

Use the given pcap file.

Write rules to detect "**all TCP port 80 traffic**" packets in the given pcap file.

1) What is the number of detected packets?

Sol: Local Rules

alert tcp any any < > any 80 (msg:"Found";sid:100001;rev:1;)

alert tcp any 80 < > any any (msg:"Found";sid:100002;rev:2;)

Run file

Sudo snort -c local.rules -r mx-3.pcap

2) Investigate the log file. What is the destination address of packet 63?

Sol: create a log file:

sudo snort -c local.rules -dev -l . -r mx-3.pcap

sudo snort -d -r snort.log.168802944 -n 63

3) Investigate the log file. What is the ACK number of packet 64?

Sol: sudo snort -r snort.log.168802944 -n 64

Task -2 FTP

File transfer protocol (FTP) is a way to download, upload, and transfer files from one location to another on the Internet and between computer systems.

Let's create IDS Rules for FTP traffic!

Use the given pcap file.

Write rules to detect "**all TCP port 21**"  traffic in the given pcap.

Q-1) What is the number of detected packets?

Sol: alert tcp any any <> any 21 (msg:"FTP packet Found"; sid: 100001;rev:1;)

alert tcp any 21 <> any any (msg:"FTP packet Found"; sid: 100002;rev:2;)

sudo snort -c local.rules -dev -l . -r <filename>

Investigate the log file.

What is the FTP service name?

Sol: sudo snort -d -r snort.log.1711199531

sudo snort -r snort.log.1711199531 -d "tcp and port 21" -n 10

**Clear the previous log and alarm files.**

Deactivate/comment on the old rules.

Write a rule to detect failed FTP login attempts in the given pcap.

What is the number of detected packets?

Sol:

Sudo rm alert snort.log.1711199531\*

Local.rules files:

alert tcp any any <> any any (msg:”Failed ftp login”;content: “530 User”;sid:100001;rev:1)

sudo snort -c local.rules -r <filename>

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

Write a rule to detect successful FTP logins in the given pcap.

What is the number of detected packets?

Sol:

Alert tcp any any <> any any (msg: “FTP login”;content:”230 User”;sid: 100001; rev:1;)

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

Write a rule to detect failed FTP login attempts with a valid username but a bad password or no password.

What is the number of detected packets?

Sol: Alert tcp any any <> any any (msg: “FTP Failed login Found”;content:”331 Password”;sid: 100001; rev:1;)

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

Write a rule to detect failed FTP login attempts with "Administrator" username but a bad password or no password.

What is the number of detected packets?

Sol: Alert tcp any any <> any any (msg: “Failed login”;content:”311 Password”; content: “Administrator”;sid: 100001; rev:1;)

Task -3 PNG

**Navigate to the task folder.**

Use the given pcap file.

Write a rule to detect the PNG file in the given pcap.

Investigate the logs and identify the software name embedded in the packet.

Sol:

Here content have file signature of png

Alert tcp any any <> any any (msg: “PNG FOUND”;content:”|89 50 4E 47 0D 0A 1A 0A|”;sid: 100001; rev:1;)

Sudo snort -c local.rules -dev -l . -r ftp-png-gif.pcap

**Clear the previous log and alarm files.**

Deactivate/comment on the old rule.

Write a rule to detect the GIF file in the given pcap.

Investigate the logs and identify the image format embedded in the packet.

Sol: Alert tcp any any <> any any (msg: “GIF FOUND”;content:”GIF89a”;sid: 100001; rev:1;)

Task – 4 MetaFile / torrent file

Let's create IDS Rules for torrent metafiles in the traffic!

Use the given pcap file.

Write a rule to detect the torrent metafile in the given pcap.

 What is the number of detected packets?

Sol: alert tcp any any <> any any (msg: “Torrent file”;content: “torrent”; sid:100001;rev:1;)

Sudo snort -c local.rules -dev -l . -r torrent.pcap

Investigate the log/alarm files.

What is the name of the torrent application?

Sol: sudo snort -d -r snort.log.16…………………

Investigate the log/alarm files.

What is the MIME (Multipurpose Internet Mail Extensions) type of the torrent metafile?

Sol: sudo snort -d -r snort.log.16…………………

Use **local-1.rules** empty file to write a new rule to detect packet payloads **between 770 and 855 bytes**.

What is the number of detected packets?

Sol: alert tcp any any <> any any (msg:”Abnormal packet size”;dsize: 770<>855; sid:100001; rev:1;)