# PRACTICAL 1: ENCRYPTING AND DECRYPTING DATA USING OPENSSL

1. Type openssl in cmd
2. Create a text file named input.txt and add some text or data in it. Encrypt the file with file command. After encrypting the file, a .enc file will be generated. And decrypt it into another file and name it output.txt.
3. Type the following command :

openssl enc -aes-256-ecb -a -salt -in input.txt -out cipher.enc

1. Enter password
2. Type the following command :

openssl enc -d -aes-256-ecb -a -salt -in cipher.enc -out output.txt

# PRACTICAL 2: DEMONSTRATE THE USE OF SNORT AND FIREWALL RULES

Step-1-> Download snort application from <https://snort.org/downloads> from binaries section [Snort\_2\_9\_20\_Installer.x64.exe](https://snort.org/downloads/snort/Snort_2_9_20_Installer.x64.exe)

**Step-2->** Download rules tar file from the registered section [snortrules-snapshot-29200.tar.gz.](https://snort.org/downloads/registered/snortrules-snapshot-29200.tar.gz) **Step-3->** Install snort.exe file

**Step-4->** Unzip and extract the .tar file

**Step-5->** Copy rules and preproc\_rules folder from the extracted folder and paste it to the Snort folder in C:\Snort thus replacing the existing folder in the same.

**Step-6->** Download and install notepad++ from <https://notepad-plus-plus.org/downloads/> and open the snort.conf file from C:\Snort\etc in the same.

**Step-7->** Search for blacklist from the snort folder in C:\Snort, open in notepad++, do save as and name it to whitelist.rules now you will have files with name blacklist.rules and whitelist.rules in the folder.

**Step-8->** Edit the config file in the following lines (line 45) and line(104)

# Setup the network addresses you

ipvar HOME NET 192.168.0.0/24

# Set up the external network add

ipvar EXTERNAL NET !SHOME NET

var RULE\_PATH C:\Snort\rules

var PREPROC\_RULE\_PATH C:\Snort\prepoc\_rules

var WHITE LIST PATH C:\Snort\rules

var BLACK LIST PATH C:\Snort\rules

config logdir: C:\Snort\log

dynamicpreprocessor directory C:\Snort\lib\snort\_dynamicpreprocessor

# path to base preprocessor engine

dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll

# path to dynamic rules libraries

# dynamicdetection directory /usr/local/lib/snort dynamicrules

**Step-9->** From line no. 546 to 651 replace forward slash to backslash of the path given.

# site specific rules

include $RULE\_PATH\local.rules

include $RULE PATH\app-detect.rules

include $RULE PATH\attack-responses.rules

include $RULE PATH\backdoor. rules

include $RULE PATH\bad-traffic.rules

include $RULE PATH\blacklist.rules

include $RULE PATH\botnet-cnc.rules

include $RULE PATH\browser-chrome.rules

include $RULE PATH\browser-firefox.rules

include $RULE PATH\browser-ie.rules

include $RULE PATH\browser-other.rules

include $RULE PATH\browser-plugins.rules

include $RULE PATH\browser-webkit.rules

include $RULE PATH\chat.rules

include $RULE PATH\content-replace.rules

include $RULE PATH\ddos.rules

include $RULE PATH\dns.rules

include $RULE PATH\dos.rules

include $RULE PATH\experimental.rules

include $RULE\_PATH\exploit-kit.rules

include $RULE PATH\exploit.rules

include $RULE PATH\file-executable.rules

include $RULE PATH\file-flash.rules

include $RULE PATH\file-identify.rules

include $RULE PATH\file-image.rules

include $RULE PATH\file-multimedia.rules

include $RULE PATH\file-office.rules

include $RULE PATH\file-other.rules

# decoder and preprocessor event rules

include $PREPROC RULE PATH/preprocessor. rules

include $PREPROC RULE PATH/decoder.rules

include $PREPROC RULE PATH/sensitive-data.rules

**Step-10->** Open local.rules from C:\Snort\rules in notepad++ and add the following lines of code in it.

alert icmp any any -> any any (msg: "Testing ICMP"; sid:1000001;)

alert udp any any -> any any (msg: "Testing UDP"; sid:1000002;)

alert top any any -> any any (msg: "Testing TCP"; sid:1000003;)

**Step-11->** Open command line in the path C:\Snort\bin and run the command “snort -W”

**Step-12->** Run the command: snort -i 5 -c C:\Snort\etc\snort.conf -A console

# PRACTICAL 3: DEMONSTRATE EXTRACT AN EXECUTABLE FROM A PCAP

**Step-1->** Download packet capture file from : <https://www.cloudshark.org/captures/a9472fbe700a>

**Step-2->** Open the packet capture file in Wireshark by dragging and dropping the capture file into the Wireshark interface.

**Step-3->** Click on File->Export Objects-> HTTP

**Step-4->** Select image/png and click on Save. Select Save Location.

PRACTICAL 4: DEMONSTRATE ANALYSIS OF DNS TRAFFIC

**Step-1->** Open Wireshark, select Wi-Fi and click on Capture to capture the DNS Traffic

Step-2-> Click start

**Step-3->** Following window will open

**Step-4->** Search for dns in the search bar

**Step-5->** Search for some websites and check them on Wireshark, it will give you the following output

**Step-6->** Double click on that and open the DNS arrow and analyse it

PRACTICAL 5: CREATE YOUR OWN SYSLOG SERVER

**Step 1->** Run **sudo apt-get install openssh-server** command to install ssh

**Step 2->** Run **sudo apt-get install net-tools** to install net-tools

**Step 3->** Run **sudo service rsyslog restart** to restart rsyslog service

Step 4-> Edit rsyslog config using **sudo nano /etc/rsyslog.conf** command and uncomment the lines **module(load="imudp") input(type="imudp" port="514") module(load="imtcp") input(type="imtcp" port="514")**

Press **Ctrl+X** & **Enter** to save file

**Step 5->** Restart rsyslog service with **sudo service rsyslog restart** command

**Step 6->** Check status of rsyslog service with **sudo service rsyslog status** command

# PRACTICAL 6: INSTALL AND RUN SPLUNK ON LINUX

**Step-1->** Run “**sudo apt get update” , “sudo apt get upgrade”** primarily. Next run “**sudo apt get install net tools wget openssh server”** . This install necessary tools for this practical.

**Step-2->** Next restart ssh server using “**sudo systemctl restart ssh”** and run “**sudo nano**

**/etc/rsyslog.conf”** to edit rsyslog configuration file.

**Step-3->** Uncomment lines **module(load="imudp") input(type="imudp" port="514")**

**& module(load="imtcp") input(type="imtcp" port="514")** and Press Ctrl+X, then Y, and Enter

**Step-4->** Run **sudo systemctl restart rsyslog** to restart rsyslog service. Run **sudo systemctl rsyslog status** to check status of service. If service is active, you can proceed.

**Step-5->** Add a group using **sudo groupadd <group\_name>** . Add a user to that group using **sudo useradd d /opt/<group\_name> m g splunk splunkdemo**

**Step-6->** Now go to <https://www.splunk.com/> . Register and Click on Free Splunk at top right of page. Click on Free Trials and Downloads page link. On the next screen Click on Get My Free Trial under Splunk Enterprise. Next Choose Linux and click on Download for .tgz. Stop the download and

Click

**Step-7->** Stop the download and click on Dowload via Command Line (wget) and copy the command.

**Step-8->** Now change user using **su - <username>** and paste the command you copied before.

**Step-9->** Now run **tar xvzf splunk-9.0.4.1-419ad9369127-Linux x86\_64.tgz -C**

**/opt** (Note: the splunk version will differ with time. Change version number accordingly.)

**Step-10->** Now access root using su – and **run chown -R splunk: /opt/splunk/** and change directory to **/opt/splunk/bin**

**Step-11->** Start splunk service using **./splunk start** . Hold spacebar to skip through the EULA.

**Step-12->** To accept splunk license run **./splunk start accept license**. You will be prompted to provide a username and password. This will be your login credentials to splunk on your linux system.

**Step-13->** Access the splunk web interface on [http://kali:8000](http://kali:8000/). You will see the following screen if you’ve followed every step to the mark. Now login using the username and password you were asked to provide while accepting license.

# PRACTICAL 7: INSTALL AND CONFIGURE ELK ON LINUX

NOTE: To save a file Press CTRL+X, Y and Press Enter.

**Step-1->** Run **sudo apt-get update** & **sudo apt-get upgrade** in terminal

**Step-2->** Install java JDK using **sudo apt-get install default-jdk default-jre** command

**Step-3->** Check java version using **java -version** command

**Step-4->** Set the java configuration to use using **update-alternatives –config java** command and select the latest version installed.

**Step-5->** to update the system environment configuration enter **sudo nano /etc/environment** command.

**Step-6->** to access remote repositories install APT Transport package using **sudo apt-get install apt-transport-https** command.

**Step-7->** Now run **wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg**

**--dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg** command. This command stores a gpg key fetched from the repository URL and decrypts and store it in keyrings folder.

**Step-8->** run **echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee**

**/etc/apt/sources.list.d/elastic-8.x.list** command. Also run **sudo apt-get update** command

**Step-9->** Now install elasticsearch using **sudo apt-get install elasticsearch** command

**Step-10->** Now we have to restart linux daemon, start and enable elasticsearch service

**Step-11->** edit the elasticsearch.yml file using the **sudo nano**

**/etc/elasticsearch/elasticsearch.yml** command. Uncomment **network.host** and give address **0.0.0.0**. In discovery section add this line in it **discovery.seed\_hosts: []** as it is. Also in same file change the value to false for line **xpack.security.enabled:** to false.

**Step-12->** Now, restart elastic search service using **sudo systemctl restart elasticsearch.service** command

**Step-13->** Now edit jvmoptions for elastic search using **sudo nano /etc/elasticsearch/jvm.options** command. Change line **-Xms4g** and **-Xmx4g** to -**Xms512m** and **-Xmx512m**.

**Step-14->** Now GET the data at localhost:9200 using **curl -X GET "localhost:9200"** command. This command is used to check if elastic search is running on localhost.

**Step-15->** copy the **inet** address of ethernet using **ifconfig** command. Now

**Step-16->** Enter the address into a browser and append port :9200 to the IP address

**Step-17->** to install and enable Logstash use the commands **sudo apt-get install logstash**, **sudo systemctl start logstash**, **sudo systemctl enable logstash**, **sudo systemctl status logstash**.

**Step-18->** install and enable Kibana use the commands **sudo apt-get install kibana**, **sudo systemctl start kibana**, **sudo systemctl enable kibana**, **sudo systemctl status kibana**.

**Step-19->** edit the kibana.yml file using **sudo nano /etc/kibana/kibana.yml** command.

Uncomment these lines: **server.port:5601, server.host: "localhost" to server.host: "0.0.0.0" elasticsearch.hosts: ["http://localhost:9200"]**

**Step-20->** Restart kibana service using **sudo systemctl restart kibana** command

**Step-21->** install filebeat using **sudo apt-get install filebeat** command.

**Step-22->** edit filebeat.yml using **sudo nano /etc/filebeat/filebeat.yml** command. comment this line: **output.elasticsearch: Array of hosts to connect to. hosts: ["localhost:9200"]**. Uncomment this line: **output.logstash hosts: ["0.0.0.0:5044"]**

**Step-23->** Now enable filebeat modules for the system using **sudo filebeat modules enable system** command

**Step-24->** run the curl command **curl -X GET** http: {your\_ip\_address} 9200/\_cat/indices?v**.**

**Step-25->** Now open any browser, type url http: {your\_ip\_address} 9200/\_cat/indices?v

and check if you get the same output.

**Step-26->** Now change the same url to http: {your\_ip\_address} 5601**.**

# PRACTICAL 8: INSTALL AND CONFIGURE GRAYLOG ON LINUX

**Step 1->** Run **sudo apt-get update** & **sudo apt-get upgrade** commands before procceding further

**2->** Install jdk and jre using **sudo apt-get install default-jdk default-jre** command.

**Step 3->** Check if java is installed using **java -version** command.

**Step 4->** Select java version to use with **update-alternatives --config** java command.

**5->** Run **sudo nano /etc/environment** command to edit the environment variables. Append the line **JAVA\_HOME="/usr/lib/jvm/java-17-openjdk-amd64/bin/java"**

**Step 6->** Now save the environment variables using **source /etc/environment** command. Check if **JAVA\_HOME** variable is correctly set using **echo &JAVA\_HOME**.

**Step 7->** Now run **sudo apt-get install apt-transport-https** command.

**8->** Run the command **wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –** .

**Step 9->** Run the command **echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list**.

**Step 10->** Now run **sudo apt-get update** command again.

**Step 11->** Now install elasticsearch using **sudo apt-get install elasticsearch**

**12->** Now run **sudo nano /etc/elasticsearch/elasticsearch.yml** to edit the yml file.

**Step 13->** Add the lines **cluster.name: graylog**, **network.host: your\_linux\_ip\_address**, **discovery.seed\_host: []**. Add **action.auto\_create\_index: false, xpack.security.enabled: false**.

**14->** Run **sudo systemctl daemon-reload, sudo systemctl enable elasticsearch.service, sudo systemctl start elasticsearch.service, sudo systemctl status elasticsearch.service** commands in the given order.

**15->** Run the curl command **curl -X GET "localhost:9200/?pretty"** where localhost is your ip address.

**Step 16->** Now run **sudo apt-get install uuid-runtime pwgen** command.

**17->** Now run **sudo apt-get install gnupg** command.

**Step 18->** Now install gnupg using **sudo apt-get install gnupg** command.

**19->** Now login to root user with **su –** command.

**Step 20->** Now run the command wget -qO - https://www.mongodb.org/static/pgp/server-6.0.asc | sudo apt-key add -

**21->** Next run command **echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/6.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list**. Exit from root access using exit command.

**Step 22->** Run **sudo apt-get update** again

**23->** Now install mongodb using **sudo apt-get install mongodb-org** command

**Step 24->** Enter root user using **su –** again. Run command **wget -qO-**

**'http://keyserver.ubuntu.com/pks/lookup?op=get&search=0xf5679a222c647c87527c2f8cb00a0bd 1e2c63c11' | sudo apt-key add -**.

**Step 25->** Exit root access using **exit** command

**26->** Now run commands **sudo systemctl daemon-reload sudo systemctl enable mongod.service sudo systemctl start mongod.service sudo systemctl --type=service --state=active | grep mongod sudo systemctl status mongod.service**.

**27->** Change directory to Dowloads using **cd Downloads** .Now download graylog Debian package using **sudo wget**

[**https://packages.graylog2.org/repo/packages/graylog-5.0-repository\_latest.deb**](https://packages.graylog2.org/repo/packages/graylog-5.0-repository_latest.deb)command

**Step 28->** Install graylog server using command **sudo dpkg -i graylog-5.0-repository\_latest.deb**.

Change directory once more using **cd** command.

**29->** Run **sudo apt-get update** once more.

**Step 30->** Now install graylog-server using **sudo apt-get install graylog-server** command.

**31->** Run the commands **sudo systemctl enable graylog-server.service sudo systemctl start graylog-server.service sudo systemctl status graylog-server.service**.

**Step 32->** Now edit the server.conf file of graylog server using **sudo nano**

**/etc/graylog/server/server.conf** command.

**33->** Now open another terminal and run **echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1** to generate root password SHA2 hash and **pwgen -N 1 -s 96** to generate password secret. Save both in a text file.

**Step 34->** Now run **sudo nano /etc/graylog/server/server.conf**. Use the keys you generated and paste **sha256** hash after root\_password\_sha2 and password\_secret for **pwgen** key accordingly. Uncomment line **http\_bind\_address** and add **http\_bind\_address** = localhost:9000 (in place of localhost replace with your system ip). Uncomment this line **elasticsearch\_hosts = http://localhost:9200/** (in place of localhost replace with your system ip) comment this line after above line by pressing enter and then type "#" http://user:password@192.168.4.84:19200. Save the file

**Step 35->** Run the commands **sudo systemctl restart graylog-server.service, sudo systemctl**

**--type=service --state=active | grep graylog, sudo systemctl restart graylog-server.service, sudo systemctl status graylog-server.service** commands in same order.

**Step 36->** Now run [**http://localhost:9000/dashboard**](http://localhost:9000/dashboard)and check if graylog gui is shown as below in a browser.