

SECURITY OPERATION CENTER

INDEX

SR.NO	PRACTICAL NAME	DATE	SIGN
01	ENCRYPTING AND DECRYPTING DATA USING OPENSSL		
02	DEMONSTRATE THE USE OF SNORT AND FIREWALL RULES		
03	DEMONSTRATE EXTRACT AN EXECUTABLE FROM A PCAP		
04	DEMONSTRATE ANALYSIS OF DNS TRAFFIC		
05	CREATE YOUR OWN SYSLOG SERVER		
06	CONFIGURE YOUR LINUX SYSTEM TO SEND SYSLOG MESSAGES TO A SYSLOG SERVER AND READ THEM		
07	INSTALL AND RUN SPLUNK ON LINUX		
08	INSTALL AND CONFIGURE ELK ON LINUX		
09	INSTALL AND CONFIGURE GRAYLOG ON LINUX		
10	DEMONSTRATE CONVERSION OF DATA INTO A UNIVERSAL FORMAT		

PRACTICAL NO.01: ENCRYPTING AND DECRYPTING DATA USING OPENSSL.

Part 1: Encrypting Messages with OpenSSL

Part 2: Decrypting Messages with OpenSSL

Part 1: Encrypting Messages with OpenSSL

Before Start the installation you need to follow these instruction from CyberOps Workstation from this link:

<https://contenthub.netacad.com/legacy/CyberOps/1.1/en/course/files/1.1.1.4%20Lab%20-%20Installing%20the%20CyberOps%20Workstation%20Virtual%20Machine.pdf>

OpenSSL can be used as a standalone tool for encryption. While many encryption algorithms can be used, this lab focuses on AES. To use AES to encrypt a text file directly from the command line using OpenSSL,

1. Start the Security Workstation VM and log in with username

2. Open a terminal window.

3. Because the text file to be encrypted is in the /home/sec_admin/lab.support.files/directory, change to that directory:

Command:

```
[analyst@secOps ~]$ cd lab.support.files/
```

```
[analyst@secOps lab.support.files]$ ls
```

```
apache_in_epoch.log      cyops.mn          letter_to_grandma.txt  openssl_lab
sample.img_SHA256.sig
applicationX_in_epoch.log  elk_services    logstash-tutorial.log pcaps      scripts
attack_scripts           h2_dropbear.banner malware        pox       SQL_Lab.pcap
confidential.txt         instructor      mininet_services   sample.img
```

```
[analyst@secOps lab.support.files]$ cat letter_to_grandma.txt
```

Hi Grandma,

I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious!

I wish you all the best. Love,
Your cookie-eater grandchild.

```
[analyst@secOps lab.support.files]$ openssl aes-256-cbc -in letter_to_grandma.txt -out message.enc
```

enter aes-256-cbc encryption password:

Verifying - enter aes-256-cbc encryption password:

[analyst@secOps lab.support.files]\$ cat message.enc

```
[analyst@secOps lab.support.files]$ openssl aes-256-cbc -a -in letter_to_grandma.txt -out message.enc  
enter aes-256-cbc encryption password:  
Verifying - enter aes-256-cbc encryption password:
```

```
[analyst@secOps lab.support.files]$ cat message.enc
```

```
[analyst@secOps lab.support.files]$ openssl aes-256-cbc -a -in letter_to_grandma.txt -out message.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
[analyst@secOps lab.support.files]$ cat message.enc
U2FsdGVkX1+UR4fxmVLuitbgb0Dskdb9Dz12fEz+6ESyQWaSYobATbJ0xUbLZXo
tzHnuZzR0DZp44WstfqC7eg2aXEHTV0YCBvr6jzhJJuxFxBsFDpGmVKch4fr2
FZ+pam+xMFT8/5uZoq1QdeBd36VoQYJK5EpCIO4WA9pXpI/40uAKLwCMcJKR
alwauWeCtQTHVXPtzX6o4uEeduQRT/430pP5y69i1K751Hm3iVndhRnONuD0aL
/0LmeJm1+UW1aqtlVh/2o6laxUKmNYNcHKX9CrXpExSfdrcwezD7sR9S9ng5Lz/6
TVMdUwU562tXjkwiobUeYXdOrKjkktMhjff7a7AYd6c=
```

Part 2: Decrypting Messages with OpenSSL

```
[analyst@secOps lab.support.files]$ openssl aes-256-cbc -a -d -in message.enc -out decrypted_letter.txt  
enter aes-256-cbc decryption password:
```

When OpenSSL finishes decrypting the message.enc file, it saves the decrypted message in a text file called decrypted_letter.txt. Use the cat command to display the contents of decrypted_letter.txt

```
[analyst@secOps lab.support.files]$ cat decrypted_letter.txt
```

```
Terminal - analyst@secOps:~/lab.support.files
File Edit View Terminal Tabs Help
[analyst@secOps lab.support.files]$ cat decrypted_letter.txt
Hi Grandma,
I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have
already eaten half of the box! They are absolutely delicious!
I wish you all the best. Love,
Your cookie-eater grandchild.
```

PRACTICAL NO.02: SNORT AND FIREWALL RULES

Part 1: Preparing the Virtual Environment

Part 2: Firewall and IDS Logs

Part 1: Preparing the Virtual Environment

Launch Oracle VirtualBox and change the CyberOps Workstation for Bridged mode.
Launch the CyberOps Workstation VM, open a terminal and configure its network by executing the configure_as_dhcp.sh script.

Command:

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/configure_as_dhcp.sh  
[sudo] password for analyst:  
Configuring the NIC to request IP info via DHCP...  
Requesting IP information...  
IP Configuration successful.
```

Part 2: Firewall and IDS Logs

1. Real-Time IDS Log Monitoring

From the CyberOps Workstation VM, run the script to start mininet.

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/cyberops_extended_topo_no_fw.py  
*** Adding controller  
*** Add switches  
*** Add hosts  
*** Add links  
*** Starting network  
*** Configuring hosts  
R1 R4 H1 H2 H3 H4 H5 H6 H7 H8 H9 H10 H11  
*** Starting controllers  
*** Starting switches  
*** Add routes  
*** Post configure switches and hosts  
*** Starting CLI:  
mininet>
```

From R1's shell, start the Linux-based IDS, Snort.

Note: You will not see a prompt as Snort is now running in this window. If for any reason, Snort stops running and the [root@secOps analysts]# prompt is displayed, rerun the script to launch Snort. Snort must be running to capture alerts later in the lab.

From the CyberOps Workstation VM mininet prompt, open shells for hosts H5 and H10.

```
mininet> xterm H5  
mininet> xterm H10
```

H10 will simulate a server on the Internet that is hosting malware. On H10, run the mal_server_start.sh script to start the server.

```
"Node: H10"
[root@secOps analyst]# ./lab.support.files/scripts/mal_server_start.sh
[root@secOps analyst]# netstat -tunpa
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
PID/Program name
tcp      0      0 0.0.0.0:6666              0.0.0.0:*              LISTEN
1237/nginx: master
```

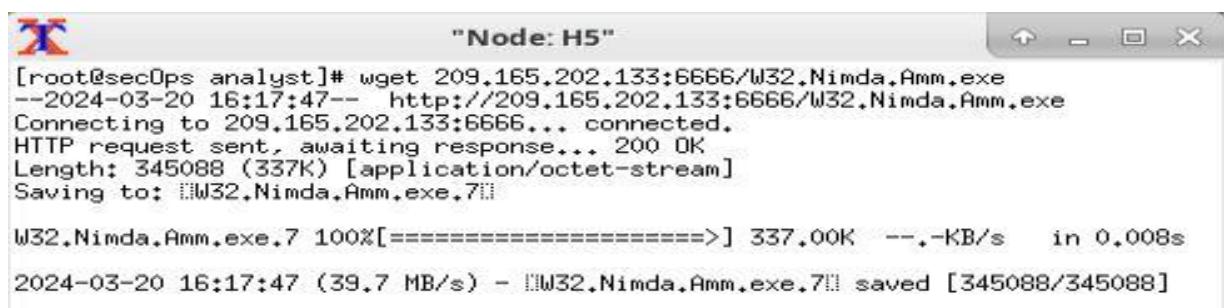
The lightweight webserver *nginx* is running and listening to connections on port *TCP 6666*.

In the new R1 terminal tab, run the tail command with the - f option to monitor the /var/log/snort/alert file in real - time. This file is where snort is con figured to record alerts.

```
[root@secOps analyst]# tail -f /var/log/snort/alert
03/20-06:45:07.515524 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0] {TCP} 209.165.200.235:58632 -> 209.165.202.133:6666
03/20-06:47:55.406393 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0] {TCP} 209.165.200.235:58636 -> 209.165.202.133:6666
03/20-06:54:47.173486 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0] {TCP} 209.165.200.235:58646 -> 209.165.202.133:6666
03/20-07:00:52.692618 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0] {TCP} 209.165.200.235:58652 -> 209.165.202.133:6666
03/20-07:02:03.430895 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0] {TCP} 209.165.200.235:58654 -> 209.165.202.133:6666
03/20-07:04:16.737714 [**] [1:1000003:0] Malicious Server Hit! [**] [Priority: 0] {TCP} 209.165.200.235:58660 -> 209.165.202.133:6666
```

In above image, snort is running with the help of these command tail -f /var/log/snort/alert It shows alert entries shown with timestamp, IP address, pointer and port number.

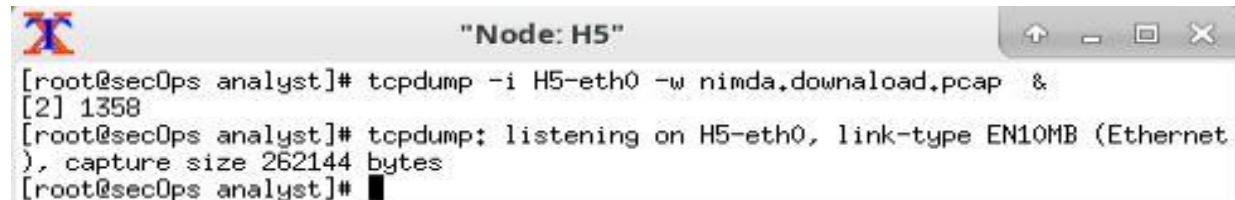
From H5, use the wget command to download a file named W32.Nimda.Amm.exe. Designed to download content via HTTP, wget is a great tool for downloading files from web servers directly from the command line.



```
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2024-03-20 16:17:47-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... connected.
HTTP request sent, awaiting response... 200 OK
Length: 345088 (337K) [application/octet-stream]
Saving to: W32.Nimda.Amm.exe.7

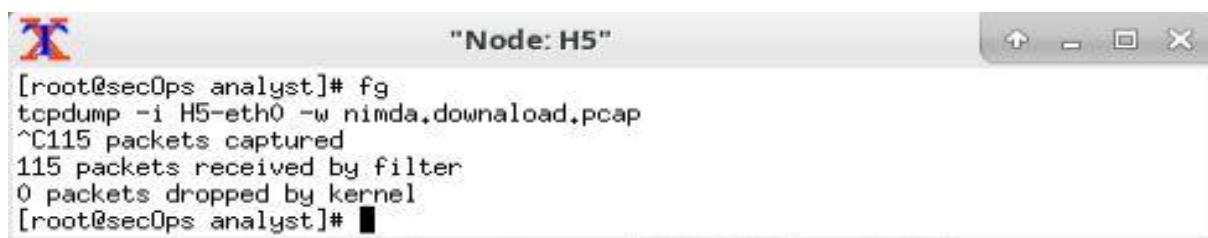
W32.Nimda.Amm.exe.7 100%[=====] 337.00K --.-KB/s in 0.008s
2024-03-20 16:17:47 (39.7 MB/s) - W32.Nimda.Amm.exe.7 saved [345088/345088]
```

On H5, use the tcpdump command to capture the event and download the malware file again so you can capture the transaction. Issue the following command below start the packet capture:



```
[root@secOps analyst]# tcpdump -i H5-eth0 -w nimda.download.pcap &
[2] 1358
[root@secOps analyst]# tcpdump: listening on H5-eth0, link-type EN10MB (Ethernet)
, capture size 262144 bytes
[root@secOps analyst]#
```

Stop the capture by bringing tcpdump to foreground with the fg command. Because tcpdump was the only process sent to background, there is no need to specify the PID . Stop the tcpdump process with Ctrl+C . The tcpdump process stops and displays a summary of the capture. The number of packets may be different for your capture.



```
[root@secOps analyst]# fg
tcpdump -i H5-eth0 -w nimda.download.pcap
^C115 packets captured
115 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

On H5, Use the ls command to verify the pcap file was in fact saved to disk and has size greater than zero:



"Node: H5"

```
[root@secOps analyst]# ls -l
total 1048
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 20 06:16 Downloads
drwxr-xr-x 9 analyst analyst 4096 Mar 20 15:20 lab.support.files
-rw-r--r-- 1 root root 703280 Mar 20 16:33 nimda.download.pca
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.1
-rw-r--r-- 1 root root 345088 Mar 23 2018 W32.Nimda.Amm.exe.2
-rw-r--r-- 1 root root 301 Mar 20 07:08 wget-log
[root@secOps analyst]#
```

2. Tuning Firewall Rules Based on IDS Alerts

mininet> xterm R1

In the new R1 terminal window, use the iptables command to list the chains and their rules currently in use:



"Node: R1"

```
[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
[root@secOps analyst]#
```

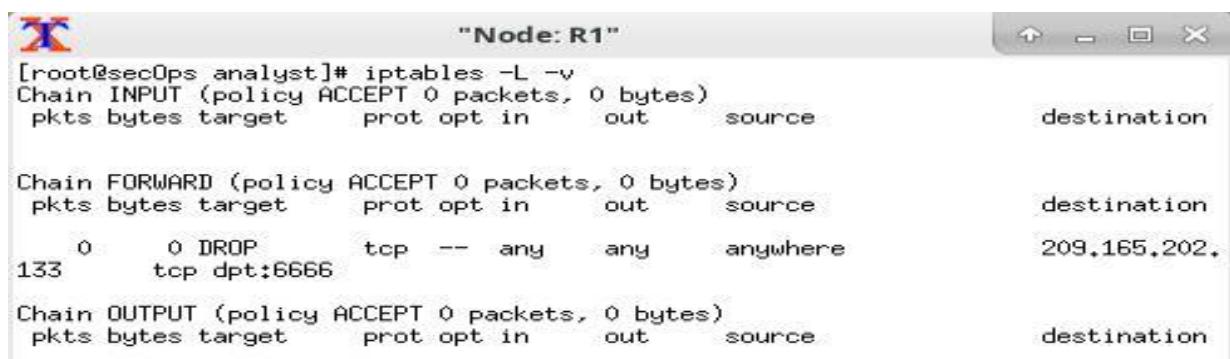
Connections to the malicious server generate packets that must transverse the iptables firewall on R1. Packets traversing the firewall are handled by the FORWARD rule and therefore, that is the chain that will receive the blocking rule. To keep user computers from connecting to the malicious server identified in Step 1, add the following rule to the FORWARD chain on R1:



"Node: R1"

```
[root@secOps analyst]# iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 66 -j DROP
```

Use the iptables command again to ensure the rule was added to the FORWARD chain. The CyberOps Workstation VM may take a few seconds to generate the output:



```
"Node: R1"
[root@secOps analyst]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
  0     0 DROP       tcp   --  any    any    anywhere           209.165.202.
133
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source               destination
```

On H5, try to download the file again:



```
"Node: H5"
[root@secOps analyst]# wget 209.165.202.133:6666/W32.Nimda.Amm.exe
--2024-03-20 16:53:44-- http://209.165.202.133:6666/W32.Nimda.Amm.exe
Connecting to 209.165.202.133:6666... ■
```

PRACTICAL NO.03: DEMONSTRATE EXTRACT AN EXECUTABLE FROM A PCAP

Part 1: Analyze Pre-Captured Logs and Traffic Captures

Part 2: Extract Downloaded Files from PCAP

Part 1: Analyze Pre-Captured Logs and Traffic Captures.

Change directory to the support.files/pcaps folder, and get a listing of files using the ls -l command.

Command:

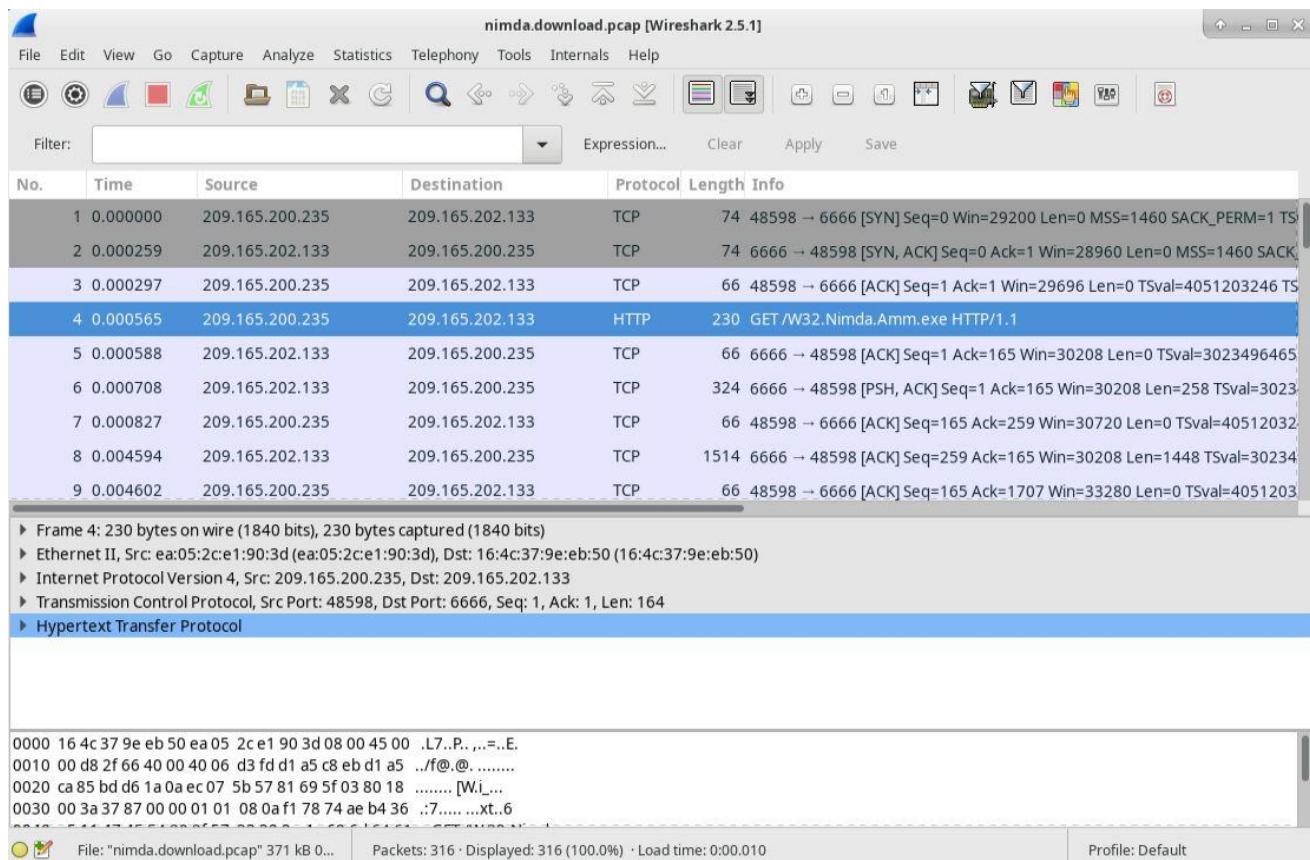
```
[analyst@secOps ~]$ cd lab.support.files/pcaps/
```

```
[analyst@secOps pcaps]$ ls -l
```

```
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
```

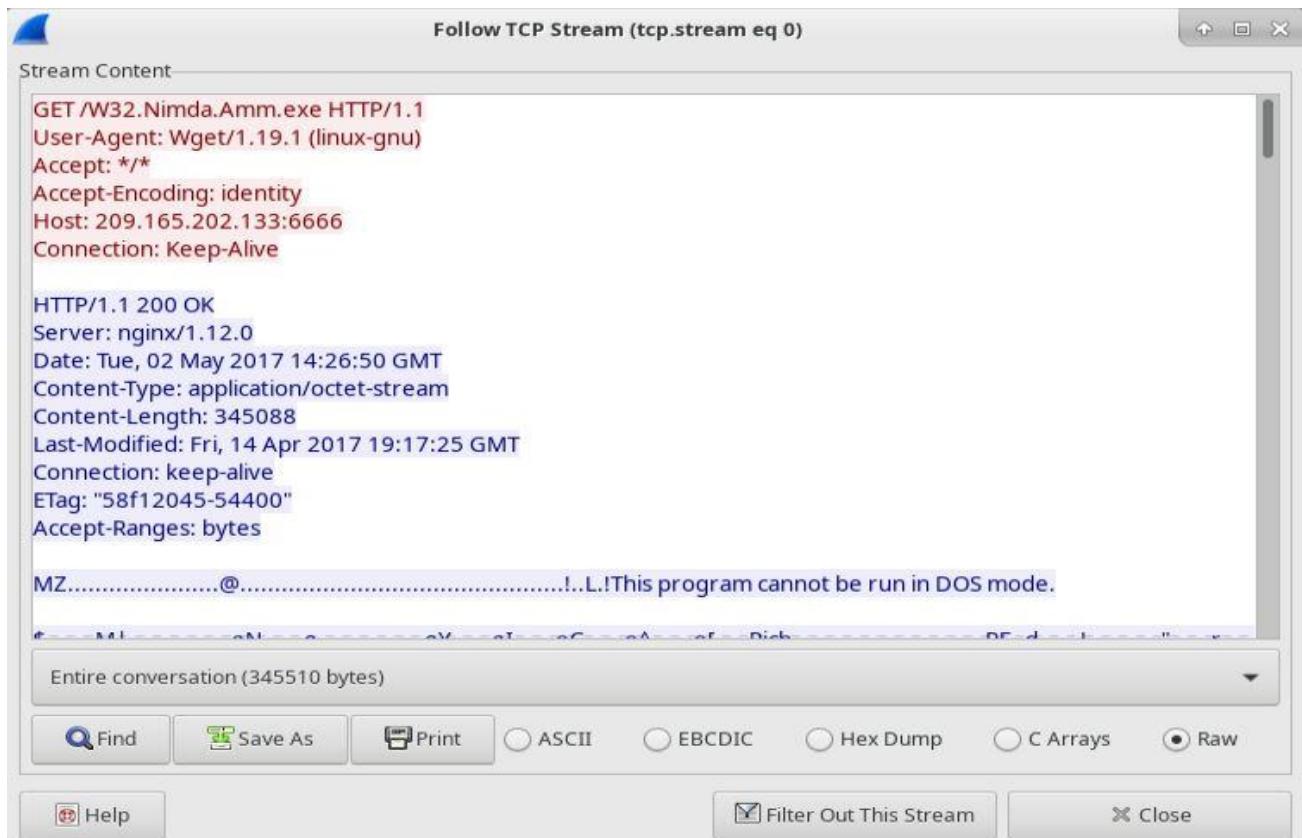
Issue the command below to open the download.pcap file in Wireshark.

```
[analyst@secOps pcaps]$ wireshark-gtk nimda.download.pcap
```



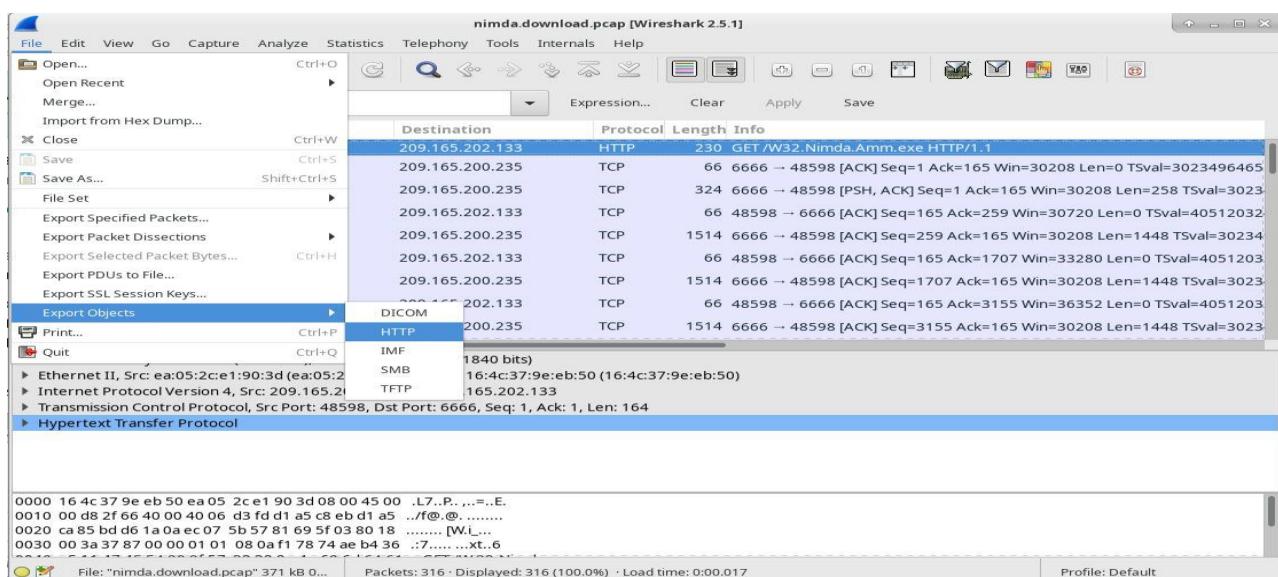
Select the fourth packet in the capture and expand the Hypertext Transfer Protocol to display as shown below.

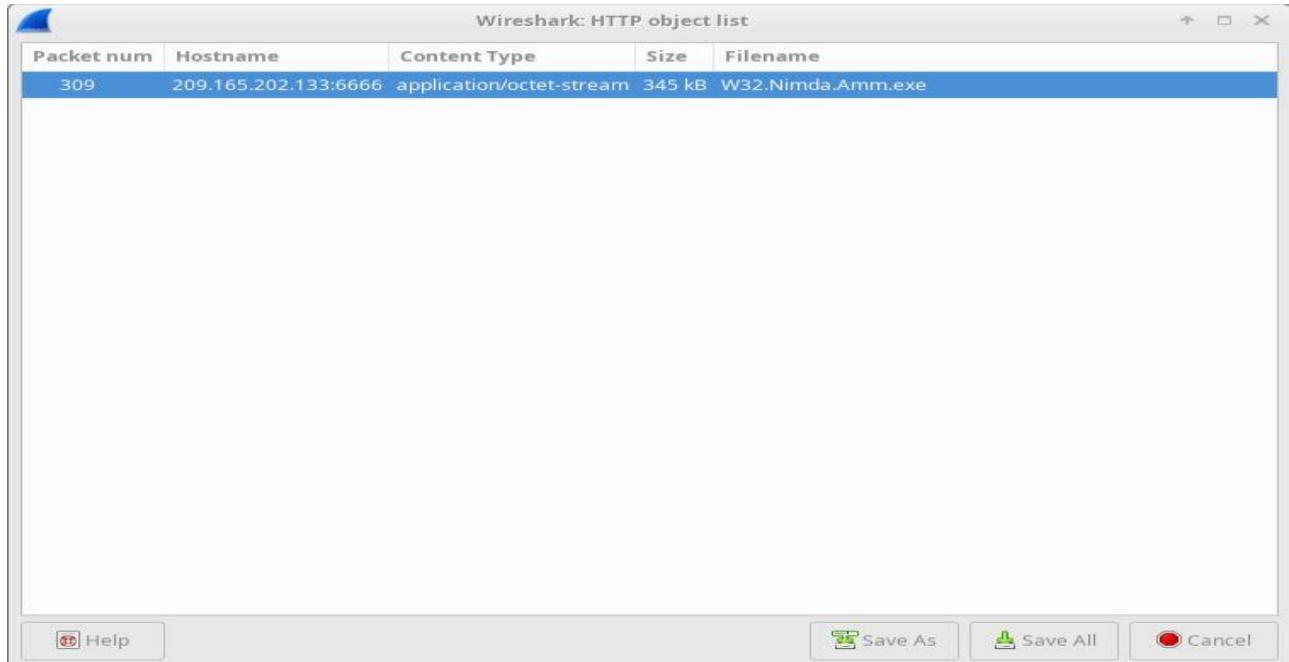
Because HTTP runs over TCP, it is possible to use Wireshark's Follow TCP Stream feature to rebuild the TCP transaction. Select the first TCP packet in the capture, a SYN packet. Right-click it and choose TCP Stream.



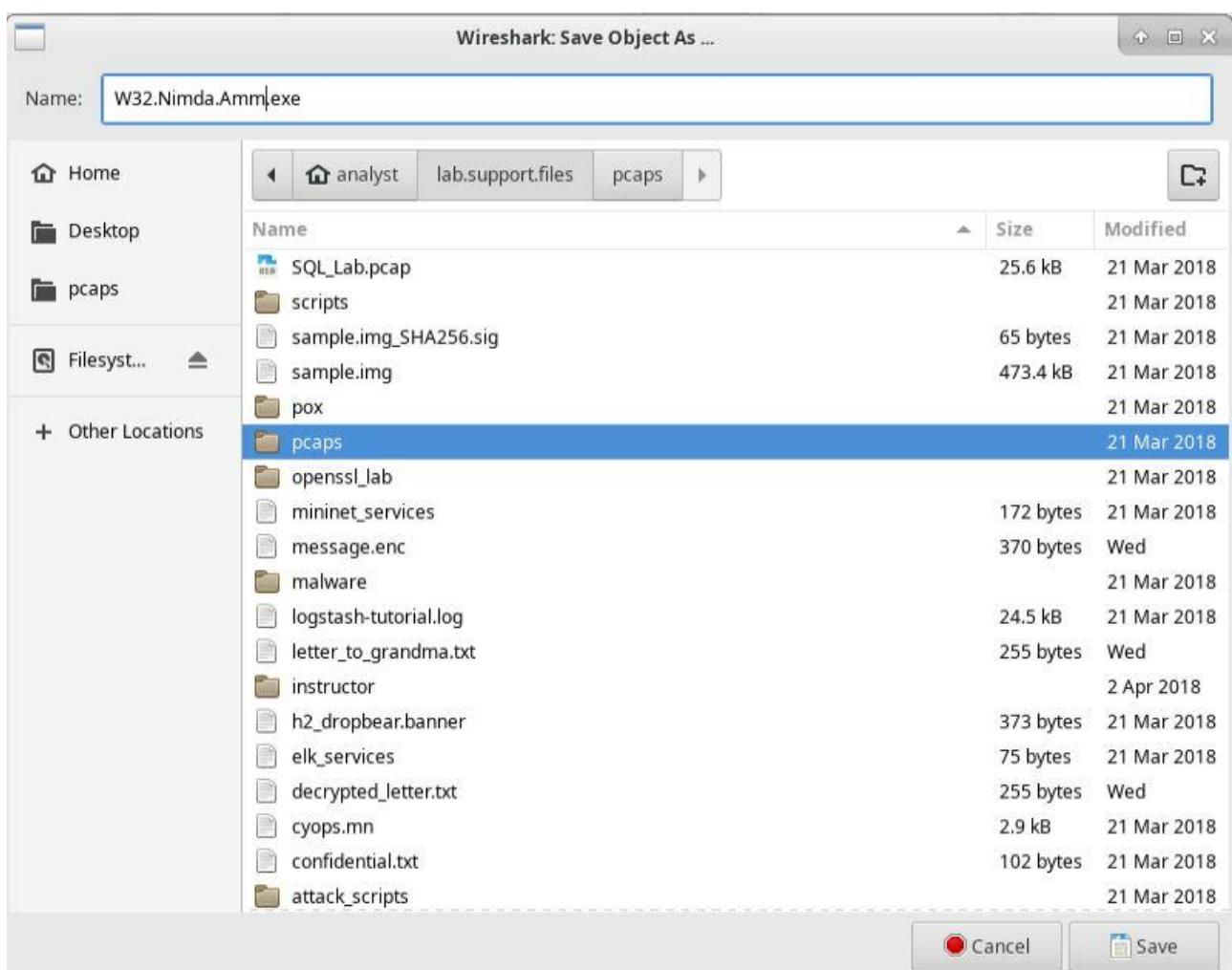
Part 2: Extract Downloaded Files from PCAP

In that fourth packet in the download.pcap file, notice that the HTTP GET request was generated from 209.165.200.235 to 209.165.202.133. The Info column also shows this is in fact the GET request for the file.

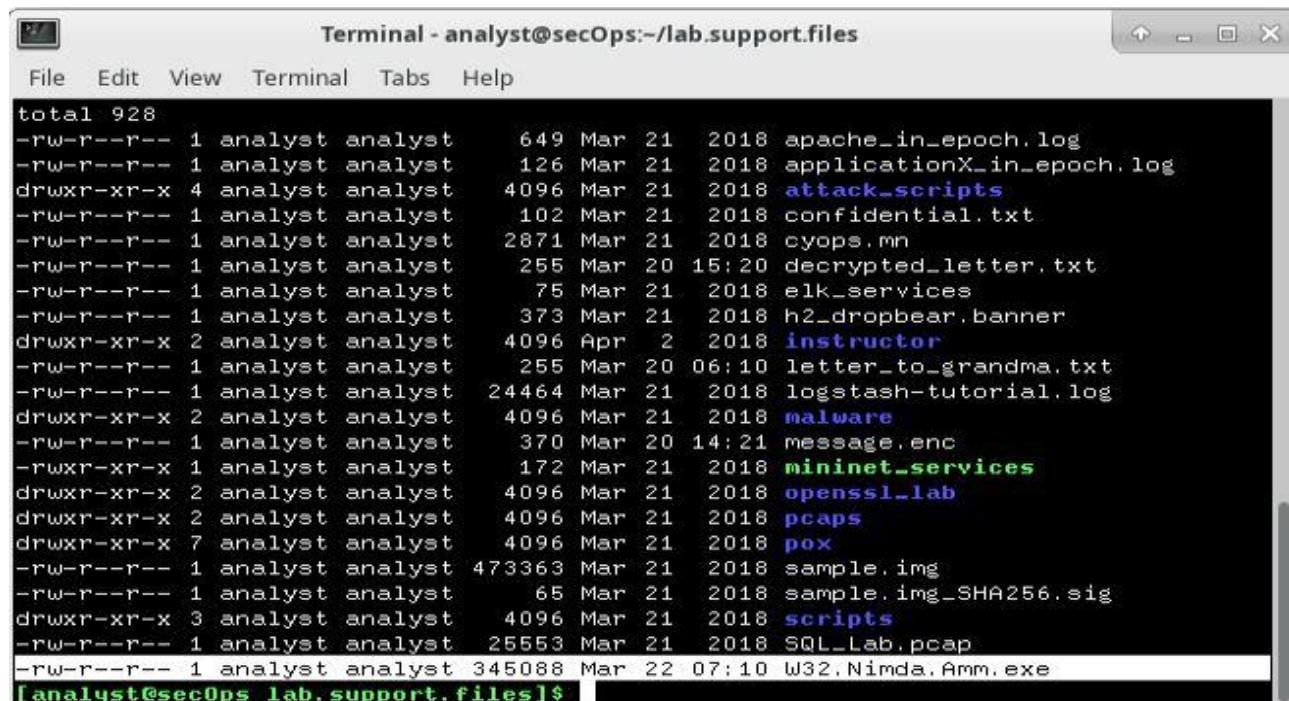




In the **HTTP object list** window, select the **Nimda.Amm.exe** file and click **Save As** at the bottom of the screen.



Return to your terminal window and ensure the file was saved. Change directory to the /home/analyst folder and list the files in the folder using the ls -l.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/lab.support.files". The window contains the output of the "ls -l" command, listing various files and their details. The files include logs (apache_in_epoch.log, applicationX_in_epoch.log), scripts (attack_scripts, scripts), configuration files (confidential.txt, cyops.mn), encrypted files (decrypted_letter.txt), logstash files (logstash-tutorial.log), malware samples (malware), network configuration files (elk_services, h2_dropbear.banner), instructor files (instructor), and various system and utility files (letter_to_grandma.txt, message.enc, mininet_services, openssl_lab, pcaps, pox, sample.img, sample.img_SHA256.sig, SQL_Lab.pcap, W32.Nimda.Amm.exe). The file "attack_scripts" is highlighted in blue, and "scripts" is also highlighted in blue. The terminal prompt "[analyst@secOps lab.support.files]\$" is visible at the bottom.

```
total 928
-rw-r--r-- 1 analyst analyst      649 Mar 21  2018 apache_in_epoch.log
-rw-r--r-- 1 analyst analyst     126 Mar 21  2018 applicationX_in_epoch.log
drwxr-xr-x  4 analyst analyst   4096 Mar 21  2018 attack_scripts
-rw-r--r--  1 analyst analyst     102 Mar 21  2018 confidential.txt
-rw-r--r--  1 analyst analyst    2871 Mar 21  2018 cyops.mn
-rw-r--r--  1 analyst analyst     255 Mar 20 15:20 decrypted_letter.txt
-rw-r--r--  1 analyst analyst      75 Mar 21  2018 elk_services
-rw-r--r--  1 analyst analyst     373 Mar 21  2018 h2_dropbear.banner
drwxr-xr-x  2 analyst analyst   4096 Apr  2  2018 instructor
-rw-r--r--  1 analyst analyst     255 Mar 20 06:10 letter_to_grandma.txt
-rw-r--r--  1 analyst analyst  24464 Mar 21  2018 logstash-tutorial.log
drwxr-xr-x  2 analyst analyst   4096 Mar 21  2018 malware
-rw-r--r--  1 analyst analyst     370 Mar 20 14:21 message.enc
-rwxr-xr-x  1 analyst analyst     172 Mar 21  2018 mininet_services
drwxr-xr-x  2 analyst analyst   4096 Mar 21  2018 openssl_lab
drwxr-xr-x  2 analyst analyst   4096 Mar 21  2018 pcaps
drwxr-xr-x  7 analyst analyst   4096 Mar 21  2018 pox
-rw-r--r--  1 analyst analyst 473363 Mar 21  2018 sample.img
-rw-r--r--  1 analyst analyst      65 Mar 21  2018 sample.img_SHA256.sig
drwxr-xr-x  3 analyst analyst   4096 Mar 21  2018 scripts
-rw-r--r--  1 analyst analyst  25553 Mar 21  2018 SQL_Lab.pcap
-rw-r--r--  1 analyst analyst 345088 Mar 22 07:10 W32.Nimda.Amm.exe
[analyst@secOps lab.support.files]$
```

PRACTICAL NO.04: DEMONSTRATE ANALYSIS OF DNS TRAFFIC

Part 1: Capture DNS Traffic

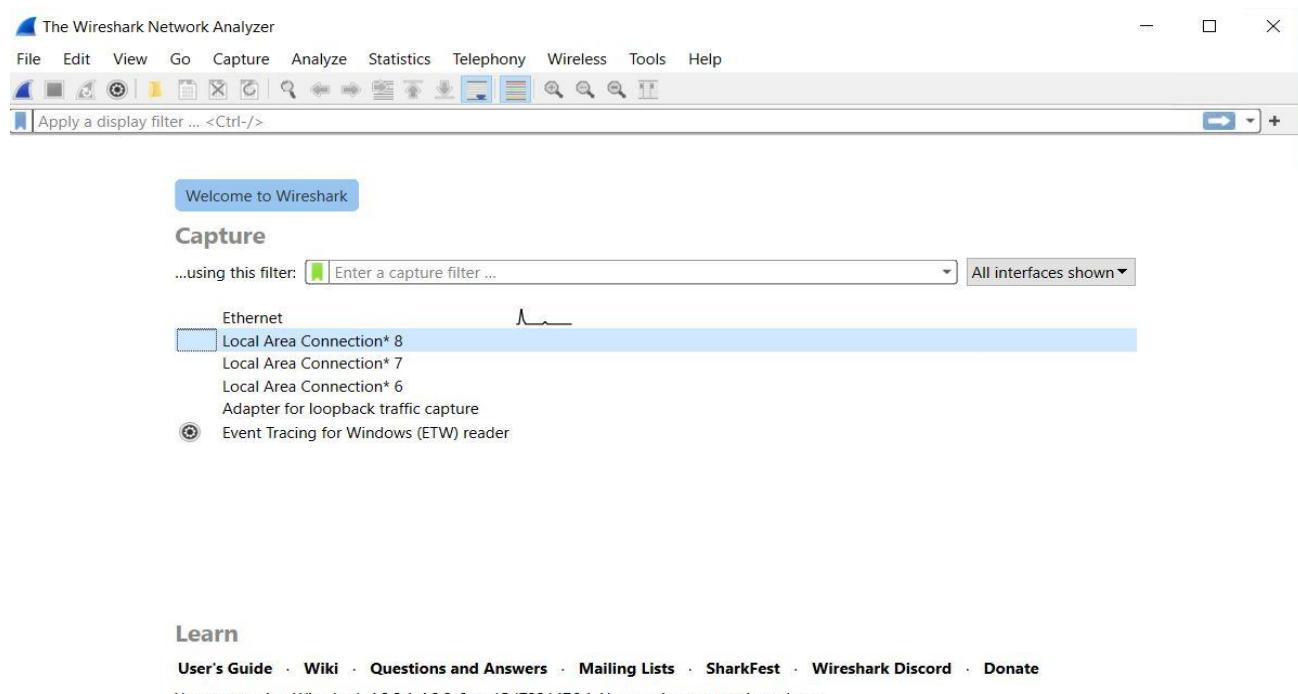
Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

Step 2: Capture DNS traffic.



Start Wireshark. Select an active interface with traffic for packet capture. In Windows, enter ipconfig /flushdns in Command Prompt.

Command:

```
C:\Users\WDAGUtilityAccount>ipconfig/flushdns
```

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

At a command prompt or terminal, type nslookup enter the interactive mode, the domain name is www.cisco.com type exit when finished. Close the command prompt.

```
C:\Users\WDAGUtilityAccount>nslookup www.cisco.com
```

Server: Home-Laptop.mshome.net

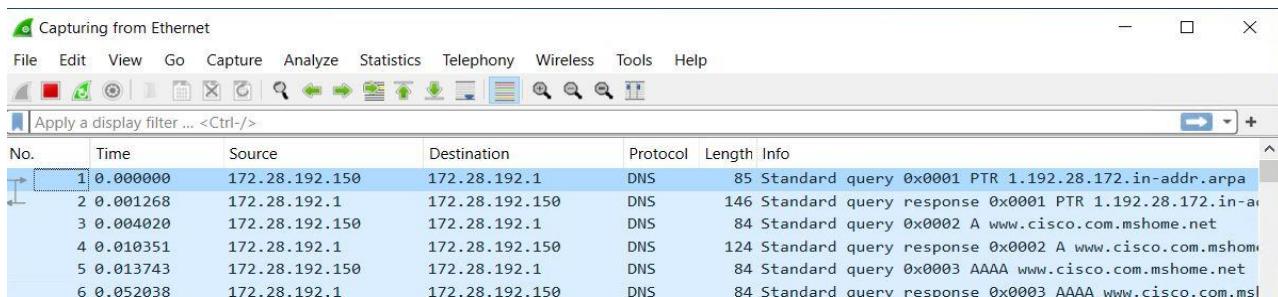
Address: 172.28.192.1

Non-authoritative answer:

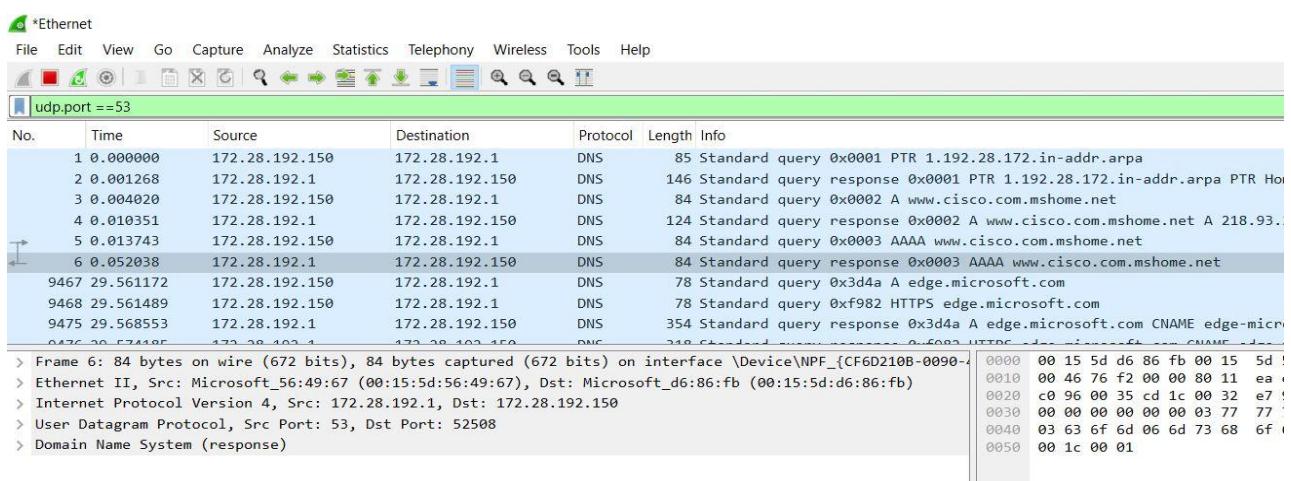
Name: www.cisco.com.mshome.net
Address: 218.93.250.18

Part 2: Explore DNS Query Traffic

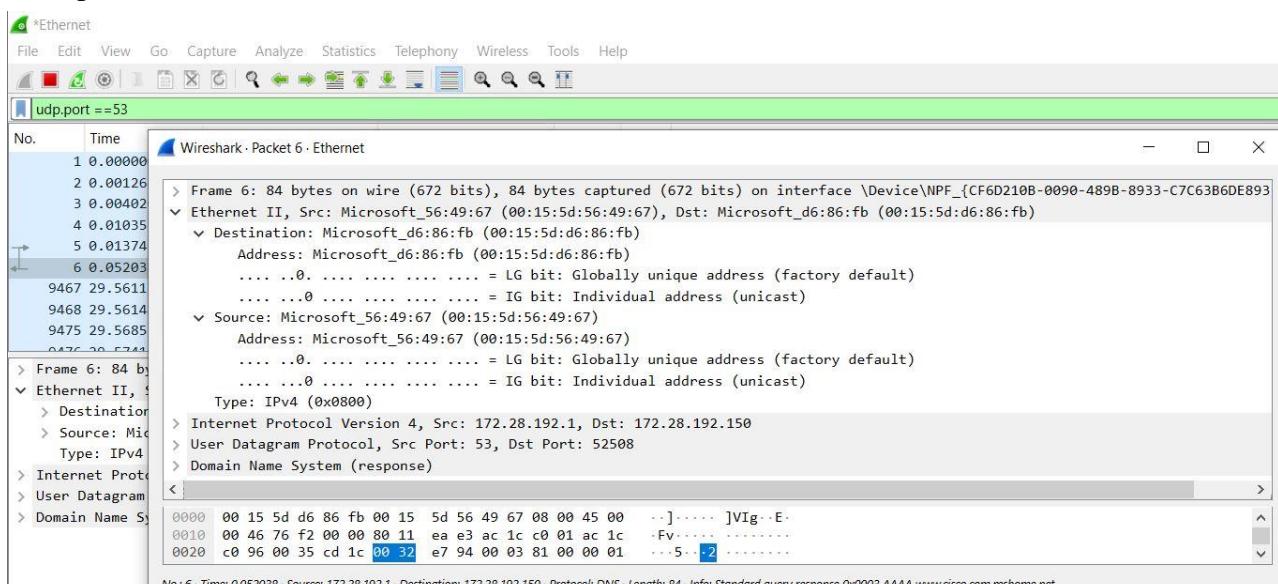
Observe the traffic captured in the Wireshark Packet List pane. Enter udp.port == 53 in the filter box and click the arrow (or press enter) to display only DNS packets.



Select the DNS packet contains Standard query and A www.cisco.com in the Info column.



Expand Ethernet II to view the details



Expand Internet Protocol Version 4.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port ==53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.28.192.150	172.28.192.1	DNS	85	Standard query 0x0001 PTR 1.192.28.172.in-addr.arpa
2	0.001268	172.28.192.1	172.28.192.150	DNS	146	Standard query response 0x0001 PTR 1.192.28.172.in-addr.arpa P
3	0.004020	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0002 A www.cisco.com.mshome.net
4	0.010351	172.28.192.1	172.28.192.150	DNS	124	Standard query response 0x0002 A www.cisco.com.mshome.net A 21
5	0.013743	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0003 AAAA www.cisco.com.mshome.net
6	0.052038	172.28.192.1	172.28.192.150	DNS	84	Standard query response 0x0003 AAAA www.cisco.com.mshome.net
9467	29.561172	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x3d4a A edge.microsoft.com
9468	29.561489	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xf982 HTTPS edge.microsoft.com
9475	29.568553	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0x3d4a A edge.microsoft.com CNAME edge
9476	29.574185	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0xf982 HTTPS edge.microsoft.com CNAME
9639	96.212878	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xfe28 A edge.microsoft.com
9640	96.213192	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x1f72 HTTPS edge.microsoft.com
9647	96.220437	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0xe28 A edge.microsoft.com CNAME edge
9648	96.227994	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0x1f72 HTTPS edge.microsoft.com CNAME
9991	166.997464	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x9c8e A edge.microsoft.com
9992	166.997654	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x2519 HTTPS edge.microsoft.com

```
> Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{CF6D210B-0090-489B-8933-C7C63B6DE893}, id 0
> Ethernet II, Src: Microsoft_56:49:67 (00:15:5d:56:49:67), Dst: Microsoft_d6:86:fb (00:15:5d:d6:86:fb)
< Internet Protocol Version 4, Src: 172.28.192.1, Dst: 172.28.192.150
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 70
        Identification: 0x76f2 (30450)
    > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: UDP (17)
        Header Checksum: 0xaeae3 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 172.28.192.1
        Destination Address: 172.28.192.150
```

Expand the User Datagram Protocol.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port ==53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.28.192.150	172.28.192.1	DNS	85	Standard query 0x0001 PTR 1.192.28.172.in-addr.arpa
2	0.001268	172.28.192.1	172.28.192.150	DNS	146	Standard query response 0x0001 PTR 1.192.28.172.in-addr.arpa P
3	0.004020	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0002 A www.cisco.com.mshome.net
4	0.010351	172.28.192.1	172.28.192.150	DNS	124	Standard query response 0x0002 A www.cisco.com.mshome.net A 21
5	0.013743	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0003 AAAA www.cisco.com.mshome.net
6	0.052038	172.28.192.1	172.28.192.150	DNS	84	Standard query response 0x0003 AAAA www.cisco.com.mshome.net
9467	29.561172	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x3d4a A edge.microsoft.com
9468	29.561489	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xf982 HTTPS edge.microsoft.com
9475	29.568553	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0x3d4a A edge.microsoft.com CNAME edge
9476	29.574185	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0xf982 HTTPS edge.microsoft.com CNAME
9639	96.212878	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xfe28 A edge.microsoft.com
9640	96.213192	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x1f72 HTTPS edge.microsoft.com
9647	96.220437	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0xe28 A edge.microsoft.com CNAME edge
9648	96.227994	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0x1f72 HTTPS edge.microsoft.com CNAME
9991	166.997464	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x9c8e A edge.microsoft.com
9992	166.997654	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x2519 HTTPS edge.microsoft.com

```
> Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{CF6D210B-0090-489B-8933-C7C63B6DE893}, id 0
> Ethernet II, Src: Microsoft_56:49:67 (00:15:5d:56:49:67), Dst: Microsoft_d6:86:fb (00:15:5d:d6:86:fb)
< Internet Protocol Version 4, Src: 172.28.192.1, Dst: 172.28.192.150
< User Datagram Protocol, Src Port: 53, Dst Port: 52508
    Source Port: 53
    Destination Port: 52508
    Length: 50
    Checksum: 0xe794 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    > [Timestamps]
        [No payload (12 bytes)]
```

Expand Domain Name System (query) in the Packet Details pane.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port ==53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.28.192.150	172.28.192.1	DNS	85	Standard query 0x0001 PTR 1.192.28.172.in-addr.arpa
2	0.001268	172.28.192.1	172.28.192.150	DNS	146	Standard query response 0x0001 PTR 1.192.28.172.in-addr.arpa P
3	0.004020	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0002 A www.cisco.com.mshome.net
4	0.010351	172.28.192.1	172.28.192.150	DNS	124	Standard query response 0x0002 A www.cisco.com.mshome.net A 218
5	0.013743	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0003 AAAA www.cisco.com.mshome.net
6	0.052038	172.28.192.1	172.28.192.150	DNS	84	Standard query response 0x0003 AAAA www.cisco.com.mshome.net
9467	29.561172	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x3d4a A edge.microsoft.com
9468	29.561489	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xf982 HTTPS edge.microsoft.com
9475	29.568553	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0x3d4a A edge.microsoft.com CNAME edge
9476	29.574185	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0xf982 HTTPS edge.microsoft.com CNAME e
9639	96.212878	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xfe28 A edge.microsoft.com
9640	96.213192	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x1f72 HTTPS edge.microsoft.com
9647	96.220437	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0xe28 A edge.microsoft.com CNAME edge
9648	96.227994	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0x1f72 HTTPS edge.microsoft.com CNAME e
9991	166.997464	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x9c8e A edge.microsoft.com
9992	166.997654	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x2519 HTTPS edge.microsoft.com

```
> Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{CF6D210B-0090-489B-8933-C7C63B6DE893}, id 0
> Ethernet II, Src: Microsoft_56:49:67 (00:15:5d:56:49:67), Dst: Microsoft_d6:86:fb (00:15:5d:d6:86:fb)
> Internet Protocol Version 4, Src: 172.28.192.1, Dst: 172.28.192.150
> User Datagram Protocol, Src Port: 53, Dst Port: 52508
  Domain Name System (response)
    Transaction ID: 0x0003
    Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      [Request In: 5]
      [Time: 0.038295000 seconds]
```

Part 3: Explore DNS Response Traffic

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port ==53

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.28.192.150	172.28.192.1	DNS	85	Standard query 0x0001 PTR 1.192.28.172.in-addr.arpa
2	0.001268	172.28.192.1	172.28.192.150	DNS	146	Standard query response 0x0001 PTR 1.192.28.172.in-addr.arpa P
3	0.004020	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0002 A www.cisco.com.mshome.net
4	0.010351	172.28.192.1	172.28.192.150	DNS	124	Standard query response 0x0002 A www.cisco.com.mshome.net A 218
5	0.013743	172.28.192.150	172.28.192.1	DNS	84	Standard query 0x0003 AAAA www.cisco.com.mshome.net
6	0.052038	172.28.192.1	172.28.192.150	DNS	84	Standard query response 0x0003 AAAA www.cisco.com.mshome.net
9467	29.561172	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x3d4a A edge.microsoft.com
9468	29.561489	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xf982 HTTPS edge.microsoft.com
9475	29.568553	172.28.192.1	172.28.192.150	DNS	354	Standard query response 0x3d4a A edge.microsoft.com CNAME edge
9476	29.574185	172.28.192.1	172.28.192.150	DNS	318	Standard query response 0xf982 HTTPS edge.microsoft.com CNAME e
9639	96.212878	172.28.192.150	172.28.192.1	DNS	78	Standard query 0xfe28 A edge.microsoft.com
9640	96.213192	172.28.192.150	172.28.192.1	DNS	78	Standard query 0x1f72 HTTPS edge.microsoft.com

```
> Frame 6: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{CF6D210B-0090-489B-8933-C7C63B6DE893}, id 0
> Ethernet II, Src: Microsoft_56:49:67 (00:15:5d:56:49:67), Dst: Microsoft_d6:86:fb (00:15:5d:d6:86:fb)
> Internet Protocol Version 4, Src: 172.28.192.1, Dst: 172.28.192.150
> User Datagram Protocol, Src Port: 53, Dst Port: 52508
  Domain Name System (response)
    Transaction ID: 0x0003
    Flags: 0x8100 Standard query response, No error
      Flags: 0x8100 Standard query response, No error
        1... .... .... = Response: Message is a response
        .000 0.... .... = OPCODE: Standard query (0)
        .... 0.... .... = Authoritative: Server is not an authority for domain
        .... 0.... .... = Truncated: Message is not truncated
        .... 1.... .... = Recursion desired: Do query recursively
        .... 0.... .... = Recursion available: Server can't do recursive queries
        .... 0.... .... = Z: reserved (0)
        .... 0.... .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... 0.... .... = Non-authenticated data: Unacceptable
        .... 0.... .... = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
      > www.cisco.com.mshome.net: type AAAA, class IN
      [Request In: 5]
      [Time: 0.038295000 seconds]
```

PRACTICAL NO.05: CREATE YOUR OWN SYSLOG SERVER

How to configure a Syslog Server:

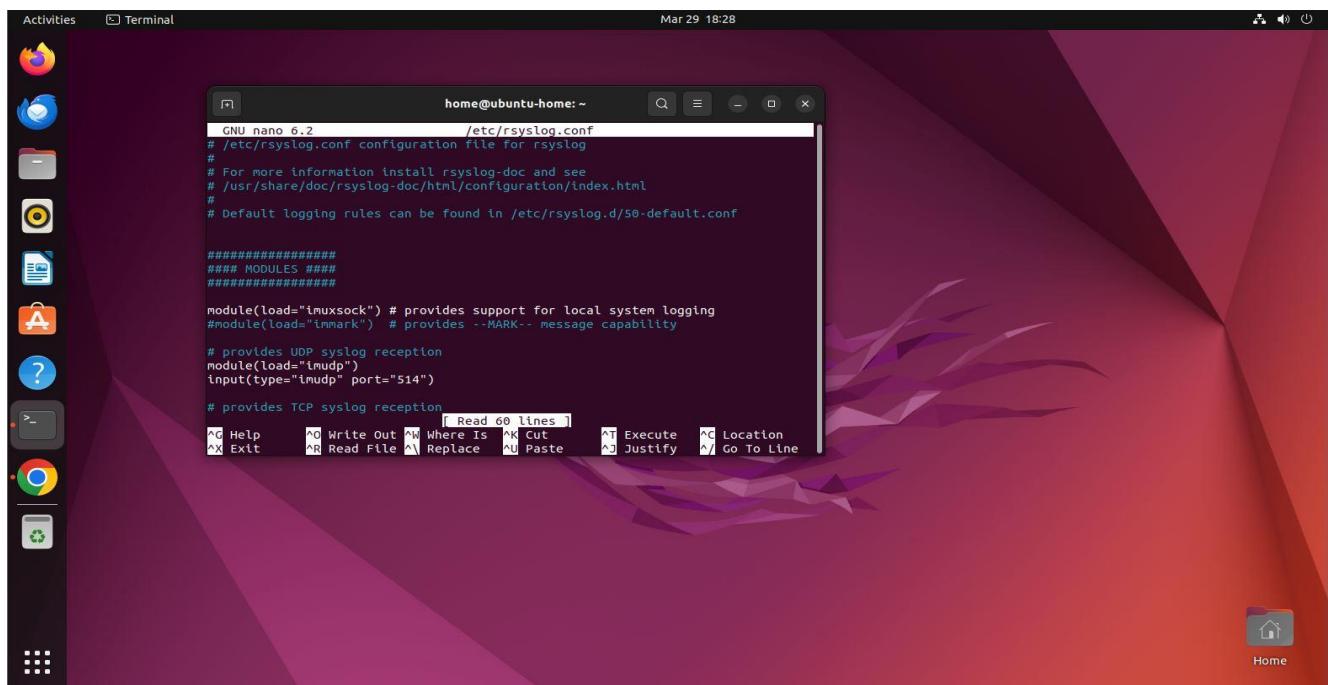
The first step to creating this logging solution is to login to the Linux host you would like to be the Syslog Server. This is where the log files will be stored.

As always, we will open a terminal and update our system.

```
home@ubuntu-home:~$ sudo apt-get update && sudo apt-get update
```

Once your machine is finished updating, we need to edit the rsyslog.conf file. This can be done by entering the command:

```
home@ubuntu-home:~$ sudo nano /etc/rsyslog.conf
```



Once we have made these changes, go ahead and exit and save the file by pressing. Next, we need to start the rsyslog service, so it is aware of our new configuration. We will do this by entering the following command:

```
home@ubuntu-home:~$ sudo service rsyslog restart
```

What we have just done there is, allowed our Linux host to listen on UDP port 514. You can change the port number if you would like, but I will stick with the default Syslog port. The final step we need to take on the server side, is to confirm that our server is in fact listening on port 514.

```
home@ubuntu-home:~$ sudo netstat -lunp
```

```

Activities Terminal Mar 29 18:32
home@ubuntu-home:~ W: Target CNF (main/cnf/Commands-amd64) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target CNF (main/cnf/Commands-all) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: GPG error: https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 Release: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 65640BE390CFB1F5
E: The repository 'https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 Release' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: Target Packages (main/binary-amd64/Packages) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Packages (main/binary-i386/Packages) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Packages (main/binary-all/Packages) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Translations (main/i18n/Translation-en_IN) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Translations (main/i18n/Translation-en) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11 (main/dep11/Components-amd64.yml) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11 (main/dep11/Components-all.yml) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11-Icons-small (main/dep11/icons-48x48.tar) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11-Icons (main/dep11/icons-64x64.tar) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11-Icons-hdpi (main/dep11/icons-64x64@2.tar) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target CNF (main/cnf/Commands-amd64) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target CNF (main/cnf/Commands-all) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
home@ubuntu-home:~ $ sudo nano /etc/rsyslog.conf
home@ubuntu-home:~ $ sudo service rsyslog restart
home@ubuntu-home:~ $ sudo netstat -lunp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
udp        0      0 0.0.0.0:514              0.0.0.0:*               5833/rsyslog
udp        0      0 0.0.0.0:1816             0.0.0.0:*               755/avahi-daemon: r
udp        0      0 0.0.0.0:631              0.0.0.0:*               987/cups-browsed
udp        0    1792 0.0.0.0:38860            0.0.0.0:*               5833/rsyslog
udp        0      0 127.0.0.53:53             0.0.0.0:*               540/systemd-resolve
udp        0      0 224.0.0.251:5353            0.0.0.0:*               4348/chrome
udp        0      0 0.0.0.0:5353             0.0.0.0:*               755/avahi-daemon: r
udp6       0      0 ::1:514                ::*:*                  5833/rsyslog
udp6       0      0 ::1:5353               ::*:*                  755/avahi-daemon: r
udp6       0      0 ::1:54568              ::*:*                  755/avahi-daemon: r
home@ubuntu-home:~ $

```

We can see that we are listening on port 514.

We can check the log whether it is creating the log message.

home@ubuntu-home:~\$ logger Welcome to our own Syslog Server

We can check our logs on the Syslog Server with the command:

home@ubuntu-home:~\$ sudo tail /var/log/syslog

```

Activities Terminal Mar 29 18:47
home@ubuntu-home:~ W: Target CNF (main/cnf/Commands-amd64) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target CNF (main/cnf/Commands-all) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: GPG error: https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 Release: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 65640BE390CFB1F5
E: The repository 'https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 Release' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: Target Packages (main/binary-amd64/Packages) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Packages (main/binary-i386/Packages) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Packages (main/binary-all/Packages) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Translations (main/i18n/Translation-en_IN) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target Translations (main/i18n/Translation-en) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11 (main/dep11/Components-amd64.yml) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11 (main/dep11/Components-all.yml) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11-Icons-small (main/dep11/icons-48x48.tar) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11-Icons (main/dep11/icons-64x64.tar) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target DEP-11-Icons-hdpi (main/dep11/icons-64x64@2.tar) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target CNF (main/cnf/Commands-amd64) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
W: Target CNF (main/cnf/Commands-all) is configured multiple times in /etc/apt/sources.list.d/elastic-6.x.list:1 and /etc/apt/sources.list.d/elastic-6.x.list:2
home@ubuntu-home:~ $ sudo nano /etc/rsyslog.conf
home@ubuntu-home:~ $ sudo service rsyslog restart
home@ubuntu-home:~ $ logger Welcome to our own Syslog Server
home@ubuntu-home:~ $ sudo tail /var/log/syslog
Mar 29 18:47:28 ubuntu-home systemd[1]: Started System Logging Service.
Mar 29 18:47:28 ubuntu-home systemd[1]: rsyslog.service: Consumed 1min 14.547s CPU time.
Mar 29 18:47:28 ubuntu-home systemd[1]: Starting System Logging Service...
Mar 29 18:47:28 ubuntu-home rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2112.0]
Mar 29 18:47:28 ubuntu-home systemd[1]: Started System Logging Service.
Mar 29 18:47:28 ubuntu-home rsyslogd: rsyslogd's groupid changed to 111
Mar 29 18:47:28 ubuntu-home rsyslogd: rsyslogd's userid changed to 104
Mar 29 18:47:28 ubuntu-home rsyslogd: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="5391" x-info="https://www.rsyslog.com"] start
Mar 29 18:47:32 ubuntu-home logger: Welcome to our own Syslog Server
Mar 29 18:47:32 ubuntu-home systemd[1]: Stopping System Logging Service...
home@ubuntu-home:~ $

```

PRACTICAL NO.06: CONFIGURE YOUR LINUX SYSTEM TO SEND SYSLOG MESSAGES TO A SYSLOG SERVER AND READ THEM

Prerequisites:

- 1.A Linux host (Ubuntu Server)
- 2.Another Linux Host (Syslog Client)

We will perform these two processes

- 1.How to configure a Syslog Server.
- 2.How to configure a Linux Host to forward logs to the Syslog Server.

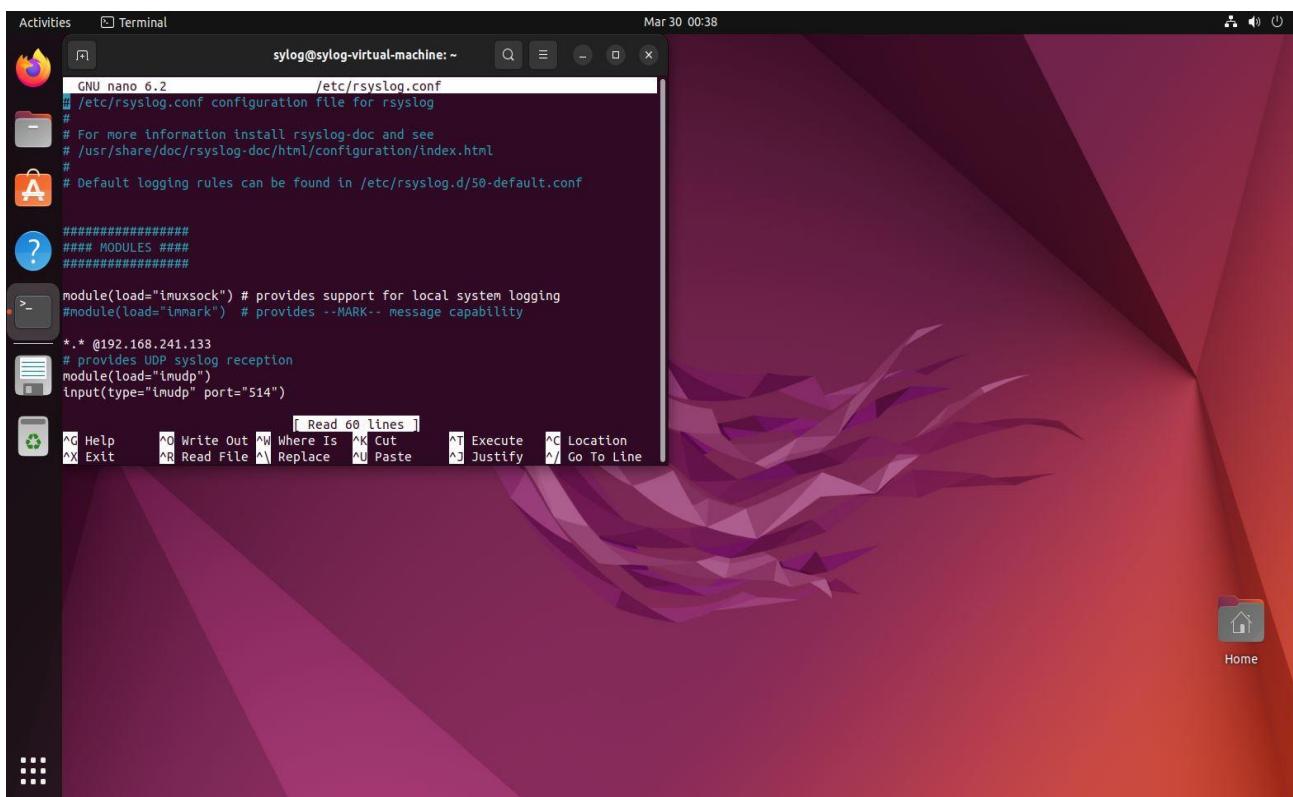
1st step we are skipped because above practical we had been configuring a Syslog Server (Ubuntu), so now that we need to configure a Syslog Client that can forwards its logs to Syslog Server (Ubuntu).

Go ahead and login to your Syslog client machine, and open up the terminal. Next run your update commands:

Command:

```
sylog@sylog-virtual-machine:~$ sudo apt-get upgrade && apt-get update
```

Once the machine is up to date, we need to edit the same configuration file from earlier, but on this machine now.



If you would like to send all of your client machine logs to your Syslog server, Next, we will save and exit the file using.

Now all we need to do is check to make sure the logs are actually being sent to our server. We can do this quickly with the logger command, restart the rsyslog server.

```
sylog@sylog-virtual-machine:~$ sudo service rsyslog restart
```

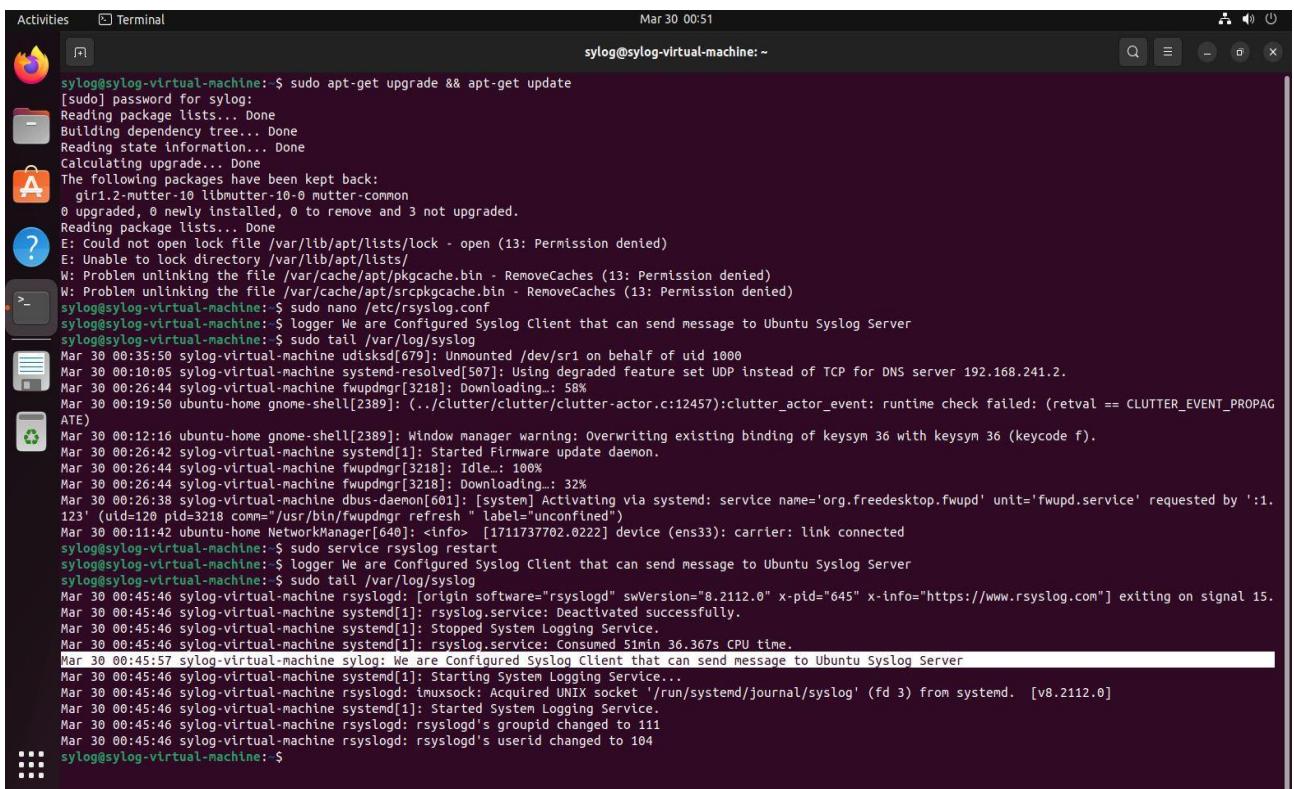
The logger command will allow us to write to our logs directly.

```
sylog@sylog-virtual-machine:~$ logger We are Configured Syslog Client that can send message to Ubuntu Syslog Server
```

We can check our logs on the client machine with the command:

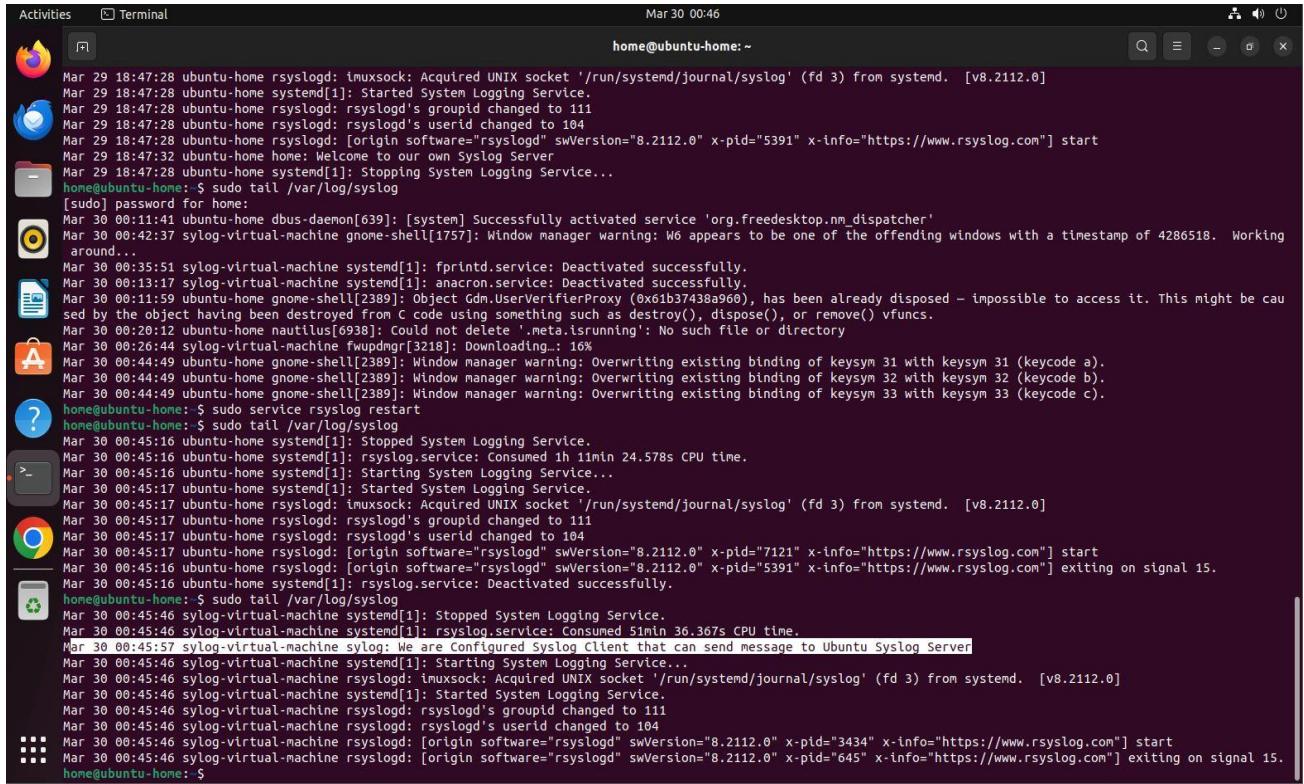
```
sylog@sylog-virtual-machine:~$ sudo tail /var/log/syslog
```

We should be able to see our logger log.



```
Activities Terminal Mar 30 00:51
sylog@sylog-virtual-machine: ~
sylog@sylog-virtual-machine: $ sudo apt-get upgrade && apt-get update
[sudo] password for sylog:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  gtr1.2-mutter-10 libmutter-10-0 mutter-common
  0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Reading package lists... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgscache.bin - RemoveCaches (13: Permission denied)
W: Problem unlinking the file /var/cache/apt/srcpkgscache.bin - RemoveCaches (13: Permission denied)
sylog@sylog-virtual-machine: $ sudo nano /etc/rsyslog.conf
sylog@sylog-virtual-machine: $ logger We are Configured Syslog Client that can send message to Ubuntu Syslog Server
sylog@sylog-virtual-machine: $ sudo tail /var/log/syslog
Mar 30 00:35:50 sylog-virtual-machine udisksd[679]: Unmounted /dev/sr1 on behalf of uid 1000
Mar 30 00:10:05 sylog-virtual-machine systemd-resolved[507]: Using degraded feature set UDP instead of TCP for DNS server 192.168.241.2.
Mar 30 00:26:44 sylog-virtual-machine fwupdngr[3218]: Downloading...: 58%
Mar 30 00:19:50 ubuntu-home gnome-shell[2389]: ./clutter/clutter/clutter-actor.c:12457):clutter_actor_event: runtime check failed: (retval == CLUTTER_EVENT_PROPAGATE)
ATE)
Mar 30 00:12:16 ubuntu-home gnome-shell[2389]: Window manager warning: Overwriting existing binding of keysym 36 with keysym 36 (keycode f).
Mar 30 00:26:42 sylog-virtual-machine systemd[1]: Started Firmware update daemon.
Mar 30 00:26:44 sylog-virtual-machine fwupdngr[3218]: Idle.: 100%
Mar 30 00:26:44 sylog-virtual-machine fwupdngr[3218]: Downloading...: 32%
Mar 30 00:26:38 sylog-virtual-machine dbus-daemon[601]: [system] Activating via systemd: service name='org.freedesktop/fwupd' unit='fwupd.service' requested by ':1.123' (uid=120 pid=3218 comm="/usr/bin/fwupdngr refresh" label="unconfined")
Mar 30 00:11:42 ubuntu-home NetworkManager[640]: <info> [1711737702.022] device (ens3): carrier: link connected
sylog@sylog-virtual-machine: $ sudo service rsyslog restart
sylog@sylog-virtual-machine: $ logger We are Configured Syslog Client that can send message to Ubuntu Syslog Server
sylog@sylog-virtual-machine: $ sudo tail /var/log/syslog
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="645" x-info="https://www.rsyslog.com"] exiting on signal 15.
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: rsyslog.service: Deactivated successfully.
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: Stopped System Logging Service.
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: rsyslog.service: Consumed 5min 36.367s CPU time.
Mar 30 00:45:57 sylog-virtual-machine syslog: We are Configured Syslog Client that can send message to Ubuntu Syslog Server
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: Starting System Logging Service...
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2112.0]
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: Started System Logging Service.
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: rsyslogd's groupid changed to 111
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: rsyslogd's userid changed to 104
sylog@sylog-virtual-machine: $
```

Now, we run the exact same command on our server. As you can see, we can see our test log entry on both our server and client.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and the user is "home@ubuntu-home:~". The terminal displays a log of messages from the "rsyslogd" service. The log entries include:

```
Mar 29 18:47:28 ubuntu-home rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2112.0]
Mar 29 18:47:28 ubuntu-home systemd[1]: Started System Logging Service.
Mar 29 18:47:28 ubuntu-home rsyslogd: rsyslogd's groupid changed to 111
Mar 29 18:47:28 ubuntu-home rsyslogd: rsyslogd's userid changed to 104
Mar 29 18:47:28 ubuntu-home rsyslogd: [origin software="rsyslog" swVersion="8.2112.0" x-pid="5391" x-info="https://www.rsyslog.com"] start
Mar 29 18:47:32 ubuntu-home home: Welcome to our own Syslog Server
Mar 29 18:47:28 ubuntu-home systemd[1]: Stopping System Logging Service...
home@ubuntu-home: $ sudo tail /var/log/syslog
[sudo] password for home:
Mar 30 00:11:41 ubuntu-home dbus-daemon[639]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Mar 30 00:13:17 sylog-virtual-machine gnome-shell[1757]: Window manager warning: W6 appears to be one of the offending windows with a timestamp of 4286518. Working around...
Mar 30 00:35:51 sylog-virtual-machine systemd[1]: fprintd.service: Deactivated successfully.
Mar 30 00:44:49 sylog-virtual-machine systemd[1]: anacron.service: Deactivated successfully.
Mar 30 00:44:49 ubuntu-home gnome-shell[2389]: Object Gdm.UserVerifierProxy (0x61b37438a960), has been already disposed - impossible to access it. This might be caused by the object having been destroyed from C code using something such as destroy(), dispose(), or remove() vfuncs.
Mar 30 00:20:12 ubuntu-home nautilus[6938]: Could not delete '.meta.isrunning': No such file or directory
Mar 30 00:26:44 sylog-virtual-machine fwupdmgr[3218]: Downloading... 168
Mar 30 00:44:49 ubuntu-home gnome-shell[2389]: Window manager warning: Overwriting existing binding of keysym 31 with keysym 31 (keycode a).
Mar 30 00:44:49 ubuntu-home gnome-shell[2389]: Window manager warning: Overwriting existing binding of keysym 32 with keysym 32 (keycode b).
Mar 30 00:44:49 ubuntu-home gnome-shell[2389]: Window manager warning: Overwriting existing binding of keysym 33 with keysym 33 (keycode c).
home@ubuntu-home: $ sudo service rsyslog restart
home@ubuntu-home: $ sudo tail /var/log/syslog
Mar 30 00:45:16 ubuntu-home systemd[1]: Stopped System Logging Service.
Mar 30 00:45:16 ubuntu-home systemd[1]: rsyslog.service: Consumed 1min 24.578s CPU time.
Mar 30 00:45:16 ubuntu-home systemd[1]: Starting System Logging Service...
Mar 30 00:45:17 ubuntu-home systemd[1]: Started System Logging Service.
Mar 30 00:45:17 ubuntu-home rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2112.0]
Mar 30 00:45:17 ubuntu-home rsyslogd: rsyslogd's groupid changed to 111
Mar 30 00:45:17 ubuntu-home rsyslogd: rsyslogd's userid changed to 104
Mar 30 00:45:17 ubuntu-home rsyslogd: [origin software="rsyslog" swVersion="8.2112.0" x-pid="7121" x-info="https://www.rsyslog.com"] start
Mar 30 00:45:16 ubuntu-home rsyslogd: [origin software="rsyslog" swVersion="8.2112.0" x-pid="5391" x-info="https://www.rsyslog.com"] exiting on signal 15.
home@ubuntu-home: $ sudo tail /var/log/syslog
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: Stopped System Logging Service.
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: rsyslog.service: Consumed 51min 36.367s CPU time.
Mar 30 00:45:46 sylog-virtual-machine rsyslog: We are Configured Syslog Client that can send message to Ubuntu Syslog Server
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: Starting System Logging Service...
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2112.0]
Mar 30 00:45:46 sylog-virtual-machine systemd[1]: Started System Logging Service.
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: rsyslogd's groupid changed to 111
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: rsyslogd's userid changed to 104
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: [origin software="rsyslog" swVersion="8.2112.0" x-pid="3434" x-info="https://www.rsyslog.com"] start
Mar 30 00:45:46 sylog-virtual-machine rsyslogd: [origin software="rsyslog" swVersion="8.2112.0" x-pid="645" x-info="https://www.rsyslog.com"] exiting on signal 15.
home@ubuntu-home: $
```

PRACTICAL NO.07: INSTALL AND RUN SPLUNK ON LINUX

Before using Splunk we need to install and configure Splunk within the kali Linux operating system, we have to follow these steps.

1.Go to Splunk Official website → create account select → Splunk Enterprise Choose the installation package splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb

```
wget -O splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb  
"https://download.splunk.com/products/splunk/releases/9.2.0.1/linux/splunk-9.2.0.1-  
d8ae995bf219-linux-2.6-amd64.deb"
```

2.Install the Splunk on Kali Linux.

Command:

```
└──(yusuf㉿kali)-[~/home/yusuf]  
└─PS> wget -O splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb  
"https://download.splunk.com/products/splunk/releases/9.2.0.1/linux/splunk-9.2.0.1-  
d8ae995bf219-linux-2.6-amd64.deb"  
--2024-03-25 00:47:45--  
https://download.splunk.com/products/splunk/releases/9.2.0.1/linux/splunk-9.2.0.1-  
d8ae995bf219-linux-2.6-amd64.deb
```

Unpacked the Package and retrieving we need to use the command dpkg -i

```
└──(yusuf㉿kali)-[~/home/yusuf/Desktop/Security Operation Center]  
└─PS> sudo dpkg -i ./splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb  
[sudo] password for yusuf:  
Selecting previously unselected package splunk.  
(Reading database ... 437967 files and directories currently installed.)  
Preparing to unpack .../splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb ...  
Unpacking splunk (9.2.0.1+d8ae995bf219) ...  
Setting up splunk (9.2.0.1+d8ae995bf219) ...  
Complete
```

3.Configure the Splunk using sudo /opt/splunk/bin/splunk start.

```
└──(yusuf㉿kali)-[~/home/yusuf/Desktop/Security Operation Center]  
└─PS> sudo /opt/splunk/bin/splunk start
```

Its show all terms and condition which we need to accepted through Y keyword and press enter key.

Splunk software must create an administrator account during startup, Create administrator username.

Please enter an administrator username: Yusuf

Please enter a new password: ****

Please confirm new password: ****

After Some few seconds it will loads and configure the web interface, it will provide port number:8000

The Splunk web interface is at <http://kali:8000>

Check your network address using ifconfig command

```
└──(yusuf㉿kali)-[/home/yusuf/Desktop/Security Operation Center]
```

```
└─PS> ifconfig
```

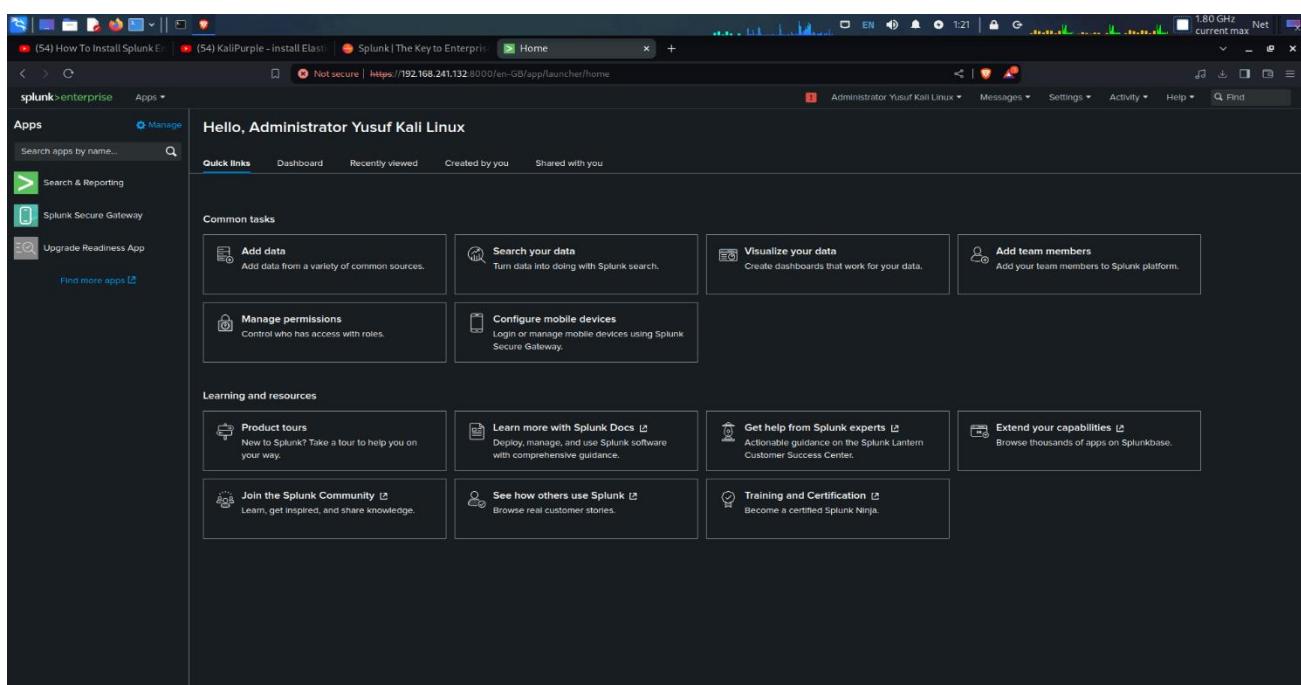
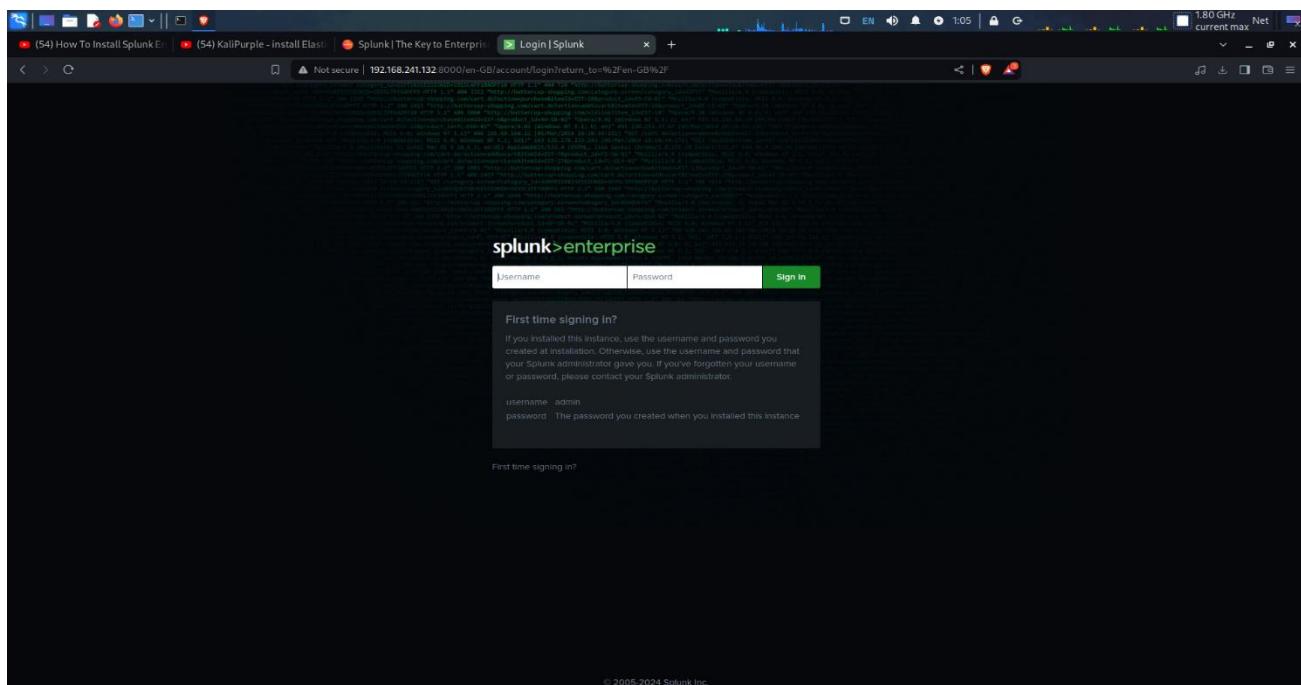
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.241.132 netmask 255.255.255.0 broadcast 192.168.241.255
      inet6 fe80::20c:29ff:fea:be7c prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:aa:be:7c txqueuelen 1000 (Ethernet)
          RX packets 864228 bytes 1259317972 (1.1 GiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 214422 bytes 15379301 (14.6 MiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

```
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 2030 bytes 465743 (454.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 2030 bytes 465743 (454.8 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. Open the Browser type in URL

<https://192.168.241.132:8000/en-GB/app/launcher/home>



PRACTICAL NO.08: INSTALL AND CONFIGURE ELK ON LINUX

Step 1: Install Dependencies

Command:

```
home@ubuntu-home:~$ sudo apt-get install openjdk-8-jdk
```

Step 2: Install Nginx

Nginx works as a web server and proxy server. It's used to configure password-controlled access to the Kibana dashboard.

```
home@ubuntu-home:~$ sudo apt-get install nginx
```

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

nginx is already the newest version (1.18.0-6ubuntu14.4).

0 upgraded, 0 newly installed, 0 to remove and 347 not upgraded.

Step 3: Add Elastic Repository

Elastic repositories enable access to all the open-source software in the ELK stack. To add them, start by importing the GPG key.

```
home@ubuntu-home:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).

OK

Next, install the apt-transport-https package:

```
home@ubuntu-home:~$ sudo apt-get install apt-transport-https
```

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

apt-transport-https is already the newest version (2.4.11).

0 upgraded, 0 newly installed, 0 to remove and 347 not upgraded.

Add the Elastic repository to your system's repository list:

```
home@ubuntu-home:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

```
deb https://artifacts.elastic.co/packages/7.x/apt stable main
```

Step 4: Install Elasticsearch

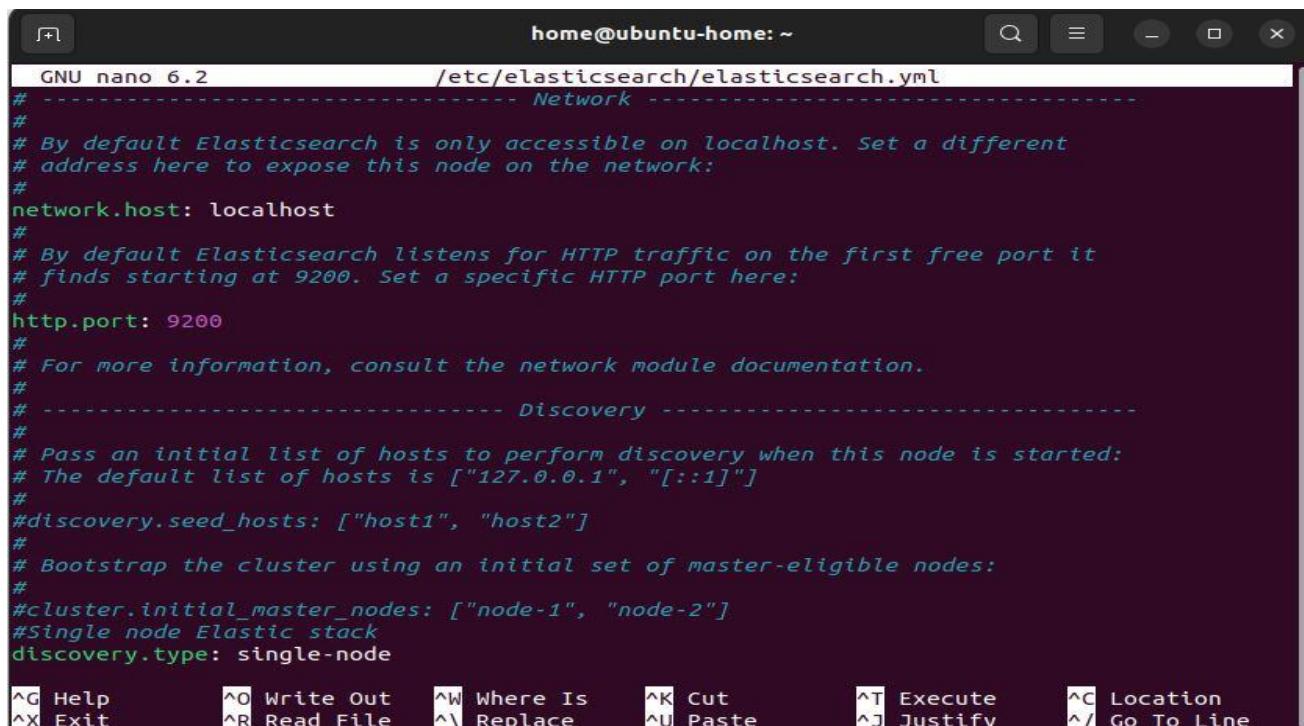
```
home@ubuntu-home:~$ sudo apt-get update
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:4 https://dl.google.com/linux/chrome/deb stable InRelease
Get:5 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:6 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Fetched 229 kB in 6s (38.0 kB/s)
Reading package lists... Done
```

Install Elasticsearch with the following command:

```
home@ubuntu-home:~$ sudo apt-get install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
elasticsearch is already the newest version (7.17.18).
0 upgraded, 0 newly installed, 0 to remove and 347 not upgraded.
```

Configure Elasticsearch

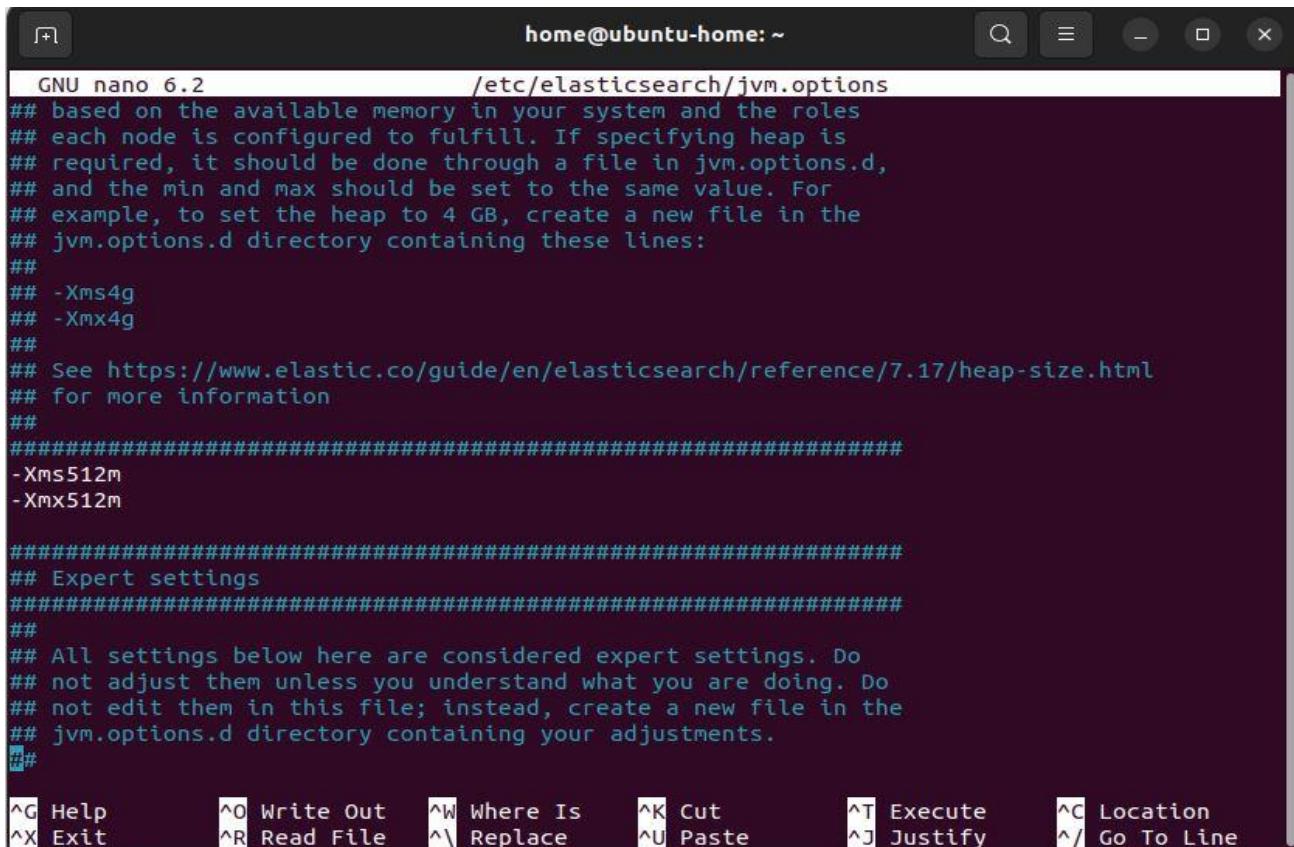
1. Elasticsearch uses a configuration file to control how it behaves. Open the configuration file for editing in a text editor of your choice. We will be using nano:



The screenshot shows a terminal window titled "home@ubuntu-home: ~". The window contains the contents of the /etc/elasticsearch/elasticsearch.yml file. The file is a YAML configuration for Elasticsearch, specifically for the network and discovery modules. It includes comments explaining the default settings and how to change them for accessibility and discovery. The nano text editor interface is visible at the bottom, with various keyboard shortcuts like ^G Help, ^O Write Out, and ^C Location.

```
GNU nano 6.2          /etc/elasticsearch/elasticsearch.yml
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: localhost
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#Single node Elastic stack
discovery.type: single-node
```

By default, JVM heap size is set at 1GB. We recommend setting it to no more than half the size of your total memory. Open the following file for editing:



The screenshot shows a terminal window titled "home@ubuntu-home: ~". The file being edited is "/etc/elasticsearch/jvm.options". The content of the file is as follows:

```
GNU nano 6.2          /etc/elasticsearch/jvm.options
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
## -Xms4g
## -Xmx4g
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
## for more information
##
#####
-Xms512m
-Xmx512m

#####
## Expert settings
#####
## All settings below here are considered expert settings. Do
## not adjust them unless you understand what you are doing. Do
## not edit them in this file; instead, create a new file in the
## jvm.options.d directory containing your adjustments.
##
```

At the bottom of the terminal window, there is a menu bar with the following options: Help (Alt+G), Write Out (Alt+O), Where Is (Alt+W), Cut (Alt+K), Execute (Alt+T), Location (Alt+C), Exit (Alt+X), Read File (Alt+R), Replace (Alt+\), Paste (Alt+U), Justify (Alt+J), and Go To Line (Alt+/).

Start Elasticsearch

Start the Elasticsearch service by running a systemctl command:

```
home@ubuntu-home:~$ sudo systemctl start elasticsearch.service
```

Enable Elasticsearch to start on boot:

```
home@ubuntu-home:~$ sudo systemctl enable elasticsearch.service
```

Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.

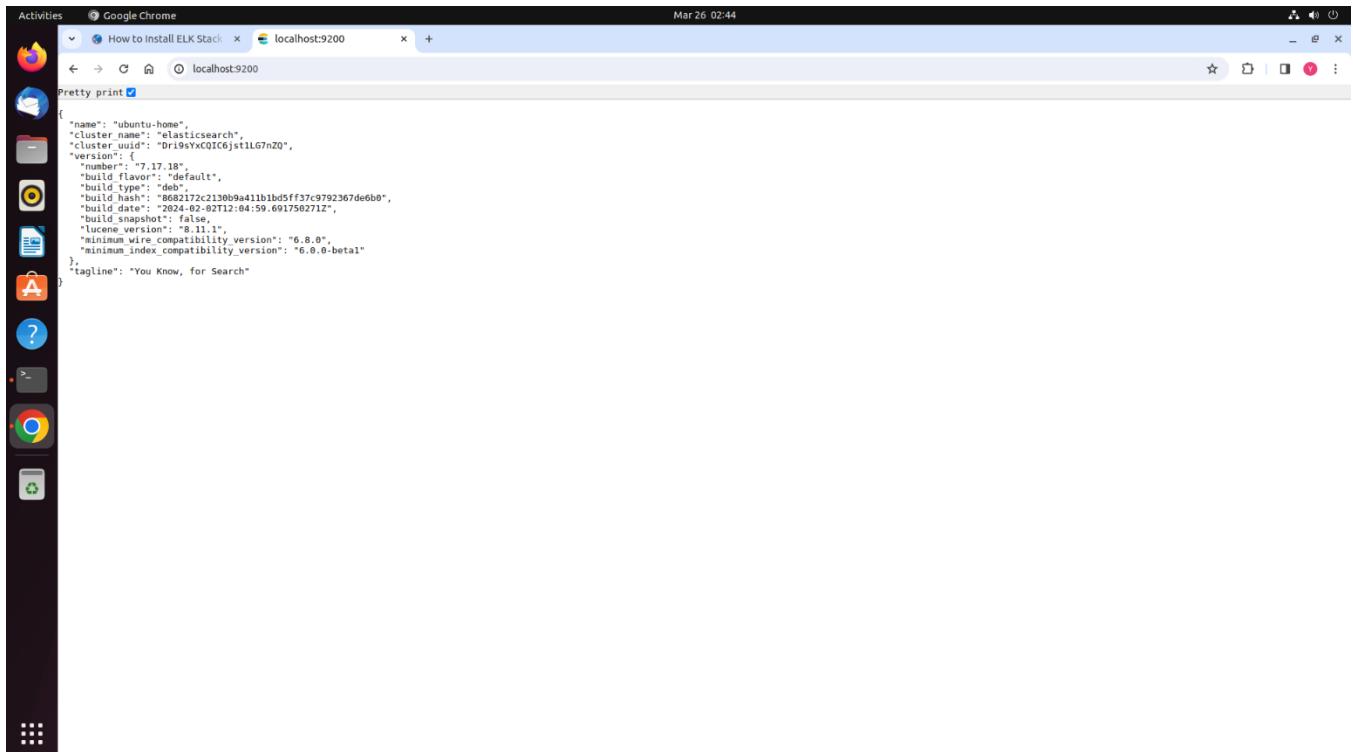
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch

Test Elasticsearch

Use the curl command to test your configuration. Enter the following:

```
home@ubuntu-home:~$ curl -X GET "localhost:9200"
```

```
{  
  "name" : "ubuntu-home",  
  "cluster_name" : "elasticsearch",  
  "cluster_uuid" : "Dri9sYxCQIC6jst1LG7nZQ",  
  "version" : {  
    "number" : "7.17.18",  
    "build_flavor" : "default",  
    "build_type" : "deb",  
    "build_hash" : "8682172c2130b9a411b1bd5ff37c9792367de6b0",  
    "build_date" : "2024-02-02T12:04:59.691750271Z",  
    "build_snapshot" : false,  
    "lucene_version" : "8.11.1",  
    "minimum_wire_compatibility_version" : "6.8.0",  
    "minimum_index_compatibility_version" : "6.0.0-beta1"  
  },  
  "tagline" : "You Know, for Search"  
}
```



PRACTICAL NO.09: INSTALL AND CONFIGURE GRAYLOG ON LINUX

Graylog is an open-source, web-based log management and aggregation system used to analyze large amounts of data. It stores and analyzes logs collected from the server and sends alerts. It uses Elasticsearch for indexing logs data with MongoDB for storing meta information.

Before using installing graylog you need to install some pre-requisite packages, you need to follow these commands.

Command:

1. Install OpenJDK

Install OpenJDK required by Elasticsearch and other dependencies.

```
sylog@sylog-virtual-machine:~$ sudo apt -y install bash-completion apt-transport-https uuid-runtime pwgen openjdk-11-jre-headless
```

[sudo] password for sylog:

```
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
bash-completion is already the newest version (1:2.11-5ubuntu1).  
bash-completion set to manually installed.  
uuid-runtime is already the newest version (2.37.2-4ubuntu3).  
uuid-runtime set to manually installed.
```

Suggested packages:

```
default-jre fonts-dejavu-extra fonts-ipafont-gothic fonts-ipafont-mincho  
fonts-wqy-microhei | fonts-wqy-zenhei
```

The following NEW packages will be installed:

```
apt-transport-https ca-certificates-java java-common openjdk-11-jre-headless  
pwgen
```

0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.

2. Install Elasticsearch

Import the Elasticsearch PGP signing key.

```
sylog@sylog-virtual-machine:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-  
elasticsearch | sudo apt-key add -
```

Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).

OK

Add the Elasticsearch repository.

```
sylog@sylog-virtual-machine:~$ echo "deb https://artifacts.elastic.co/packages/oss-6.x/apt  
stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list
```

```
deb https://artifacts.elastic.co/packages/oss-6.x/apt stable main
```

Update the system.

```
sylog@sylog-virtual-machine:~$ sudo apt update
```

Install Elasticsearch.

```
sylog@sylog-virtual-machine:~$ sudo apt -y install elasticsearch-oss
```

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

The following NEW packages will be installed:

elasticsearch-oss

0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.

Need to get 68.5 MB of archives.

After this operation, 108 MB of additional disk space will be used.

```
Get:1 https://artifacts.elastic.co/packages/oss-6.x/apt stable/main amd64 elasticsearch-oss all 6.8.23 [68.5 MB]
```

Fetched 68.5 MB in 22s (3,179 kB/s)

Selecting previously unselected package elasticsearch-oss.

(Reading database ... 178673 files and directories currently installed.)

Preparing to unpack .../elasticsearch-oss_6.8.23_all.deb ...

Creating elasticsearch group... OK

Creating elasticsearch user... OK

Unpacking elasticsearch-oss (6.8.23) ...

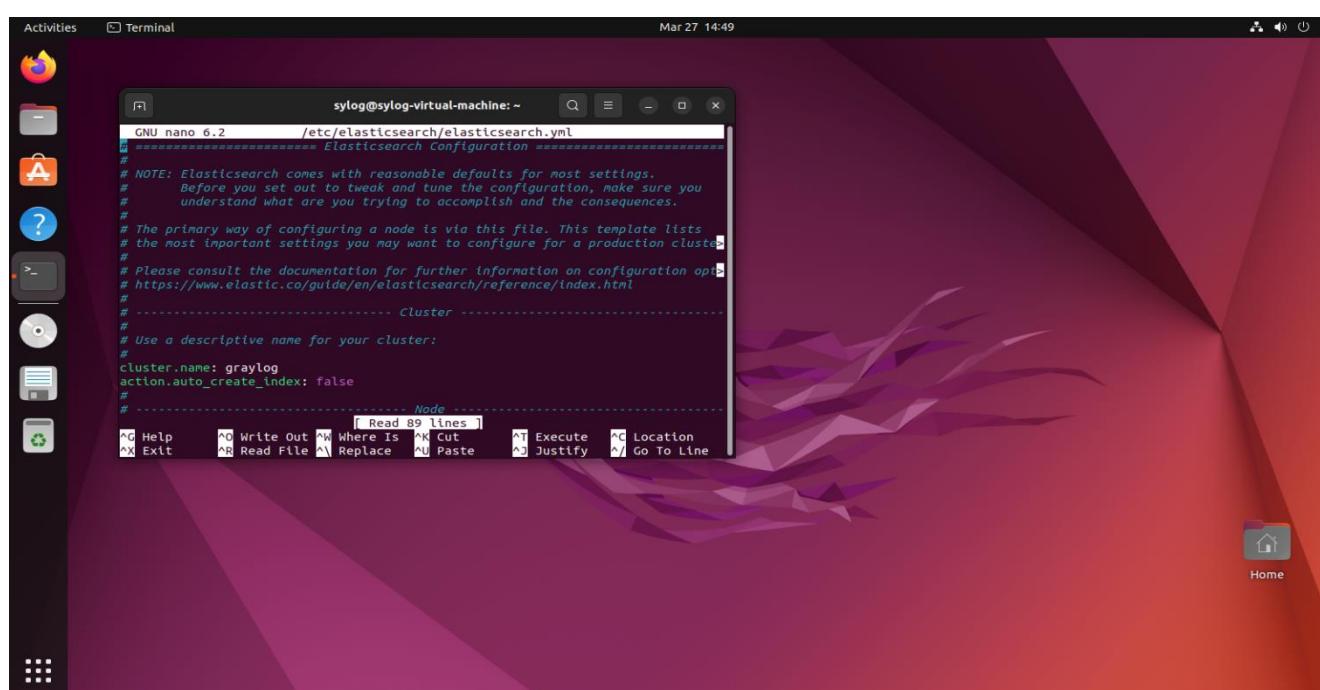
Setting up elasticsearch-oss (6.8.23) ...

Created elasticsearch keystore in /etc/elasticsearch

Edit the Elasticsearch configuration file.

```
sylog@sylog-virtual-machine:~$ sudo nano /etc/elasticsearch/elasticsearch.yml
```

Add these two lines to the end of the file.



Save and exit the file & reload the system daemon.

Restart Elasticsearch service.

```
sylog@sylog-virtual-machine:~$ sudo systemctl daemon-reload
```

```
sylog@sylog-virtual-machine:~$ sudo systemctl restart elasticsearch
```

Enable Elasticsearch to run on system startup.

```
sylog@sylog-virtual-machine:~$ sudo systemctl enable elasticsearch
```

```
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
```

```
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service →  
/lib/systemd/system/elasticsearch.service.
```

3. Install MongoDB

Start the MongoDB service.

```
sylog@sylog-virtual-machine:~$ sudo apt-get install gnupg
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
gnupg is already the newest version (2.2.27-3ubuntu2.1).
```

```
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

```
sylog@sylog-virtual-machine:~$ wget -qO - https://www.mongodb.org/static/pgp/server-6.0.asc | sudo apt-key add -
```

```
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
```

```
OK
```

```
sylog@sylog-virtual-machine:~$ 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
```

```
deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/6.0 multiverse
```

Start the MongoDB service.

```
sylog@sylog-virtual-machine:~$ sudo service mongod start
```

Enable MongoDB service to start at system startup.

```
sylog@sylog-virtual-machine:~$ sudo systemctl enable mongod
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/mongod.service →  
/lib/systemd/system/mongod.service.
```

4. Install Graylog

Add the Graylog repository.

```
sylog@sylog-virtual-machine:~$ wget https://packages.graylog2.org/repo/packages/graylog-4.1-repository\_latest.deb
```

```
--2024-03-27 15:13:32-- https://packages.graylog2.org/repo/packages/graylog-4.1-repository_latest.deb
```

```
Resolving packages.graylog2.org (packages.graylog2.org)... 172.67.153.95, 104.21.88.209, 2606:4700:3035::ac43:995f, ...
```

```
Connecting to packages.graylog2.org (packages.graylog2.org)|172.67.153.95|:443... connected.
```

```
HTTP request sent, awaiting response... 302 Found
```

```
Location: https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-4.1-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20240327T094333Z&X-Amz-SignedHeaders=host&X-Amz-Expires=600&X-Amz-Credential=AKIAIJSI6MCSPXFVDPIA%2F20240327%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signature=c1e744cd4c12cb014592e342f2bcb104f46e56f7f53d13c8c91cfed67f6fa587 [following]
```

```
--2024-03-27 15:13:33-- https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-4.1-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20240327T094333Z&X-Amz-SignedHeaders=host&X-Amz-Expires=600&X-Amz-Credential=AKIAIJSI6MCSPXFVDPIA%2F20240327%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signature=c1e744cd4c12cb014592e342f2bcb104f46e56f7f53d13c8c91cfed67f6fa587
```

```
Resolving graylog-package-repository.s3.eu-west-1.amazonaws.com (graylog-package-repository.s3.eu-west-1.amazonaws.com)... 3.5.69.106, 3.5.66.218, 52.218.56.64, ...
```

```
Connecting to graylog-package-repository.s3.eu-west-1.amazonaws.com (graylog-package-repository.s3.eu-west-1.amazonaws.com)|3.5.69.106|:443... connected.
```

```
HTTP request sent, awaiting response... 200 OK
```

```
Length: 2084 (2.0K) [application/x-debian-package]
```

```
Saving to: 'graylog-4.1-repository_latest.deb'
```

```
graylog-4.1-repository 100%[=====] 2.04K --.KB/s in 0s
```

```
2024-03-27 15:13:34 (44.8 MB/s) - 'graylog-4.1-repository_latest.deb' saved [2084/2084]
```

Install the Graylog server package.

```
sylog@sylog-virtual-machine:~$ sudo dpkg -i graylog-4.1-repository_latest.deb
```

```
Selecting previously unselected package graylog-4.1-repository.
```

```
(Reading database ... 178903 files and directories currently installed.)
```

```
Preparing to unpack graylog-4.1-repository_latest.deb ...
```

```
Unpacking graylog-4.1-repository (1-3) ...
```

```
Setting up graylog-4.1-repository (1-3) ...
```

Update the system.

```
sylog@sylog-virtual-machine:~$ sudo apt update
```

Install Graylog.

```
sylog@sylog-virtual-machine:~$ sudo apt -y install graylog-server
```

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

The following NEW packages will be installed:

graylog-server

0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.

Need to get 197 MB of archives.

After this operation, 218 MB of additional disk space will be used.

```
Get:1 https://packages.graylog2.org/repo/debian_stable/4.1 amd64 graylog-server all 4.1.14-1 [197 MB]
```

Fetched 197 MB in 1min 42s (1,927 kB/s)

Selecting previously unselected package graylog-server.

(Reading database ... 178907 files and directories currently installed.)

Preparing to unpack .../graylog-server_4.1.14-1_all.deb ...

Unpacking graylog-server (4.1.14-1) ...

Setting up graylog-server (4.1.14-1) ...

```
#####
# Graylog does NOT start automatically!
```

Please run the following commands if you want to start Graylog automatically on system boot:

```
sudo systemctl enable graylog-server.service
```

```
sudo systemctl start graylog-server.service
```

```
#####
#
```

Generate a 96-character random string for Graylog and save a copy to use in the Graylog server configuration file.

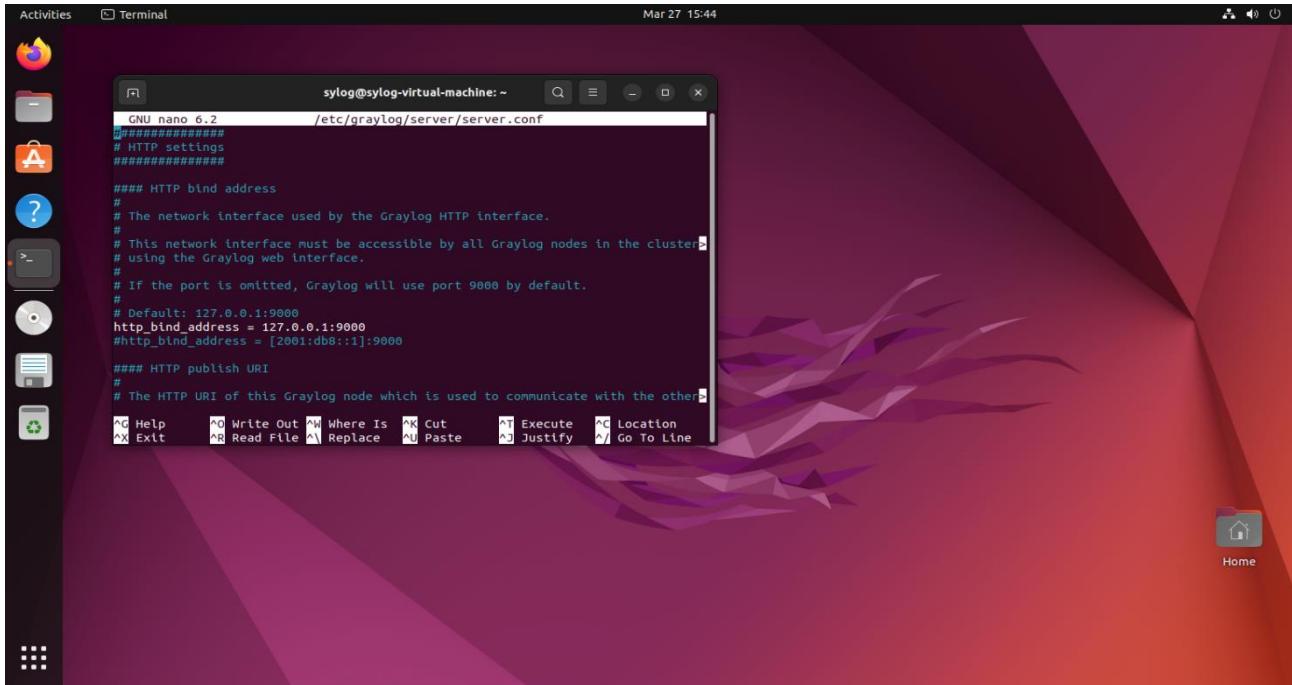
```
yZi6xi10Ww8UkbLi7yBCnbpi54QqqCcYXtGTcLIOercyAgflffd9hmoVjQV2yYzHABe5rT  
YTUBZOz3wAiny7VQMehkWRs7Wg
```

Choose a strong password for your admin account and generate a 64-character hash. For example, if you choose StrongPassword:

```
05a181f00c157f70413d33701778a6ee7d2747ac18b9c0fbb8bd71a62dd7a223 -
```

Edit the Graylog configuration file.

```
sylog@sylog-virtual-machine:~$ sudo nano /etc/graylog/server/server.conf
```



Update http_bind_address as shown:

```
http_bind_address = 127.0.0.1:9000
```

Save and close the file & restart the system daemon.

```
sylog@sylog-virtual-machine:~$ sudo systemctl daemon-reload
```

Restart the Graylog service.

```
sylog@sylog-virtual-machine:~$ sudo systemctl restart graylog-server
```

Enable the Graylog service to run on system startup.

Synchronizing state of graylog-server.service with SysV service script with /lib/systemd/systemd-sysv-install.

Executing: /lib/systemd/systemd-sysv-install enable graylog-server

Created symlink /etc/systemd/system/multi-user.target.wants/graylog-server.service →
/lib/systemd/system/graylog-server.service.

Verify the status of the Graylog server.

```
sylog@sylog-virtual-machine:~$ sudo systemctl status graylog-server
```

- graylog-server.service - Graylog server

```
Loaded: loaded (/lib/systemd/system/graylog-server.service; enabled; vendor>
```

```
Active: active (running) since Wed 2024-03-27 15:47:50 IST; 1min 4s ago
```

Docs: <http://docs.graylog.org/>

Main PID: 10605 (graylog-server)

Tasks: 108 (limit: 2217)

Memory: 729.1M

CPU: 41.739s

CGroup: /system.slice/graylog-server.service

```
|─10605 /bin/sh /usr/share/graylog-server/bin/graylog-server
└─10642 /usr/bin/java -Xms1g -Xmx1g -XX:NewRatio=1 -server -XX:+Re>
```

Mar 27 15:47:50 sylog-virtual-machine systemd[1]: Started Graylog server.

Mar 27 15:47:50 sylog-virtual-machine graylog-server[10642]: OpenJDK 64-Bit Ser>

Mar 27 15:47:51 sylog-virtual-machine graylog-server[10642]: WARNING: sun.refle>

Mar 27 15:48:01 sylog-virtual-machine graylog-server[10642]: WARNING: An illega>

Mar 27 15:48:01 sylog-virtual-machine graylog-server[10642]: WARNING: Illegal r>

Mar 27 15:48:01 sylog-virtual-machine graylog-server[10642]: WARNING: Please co>

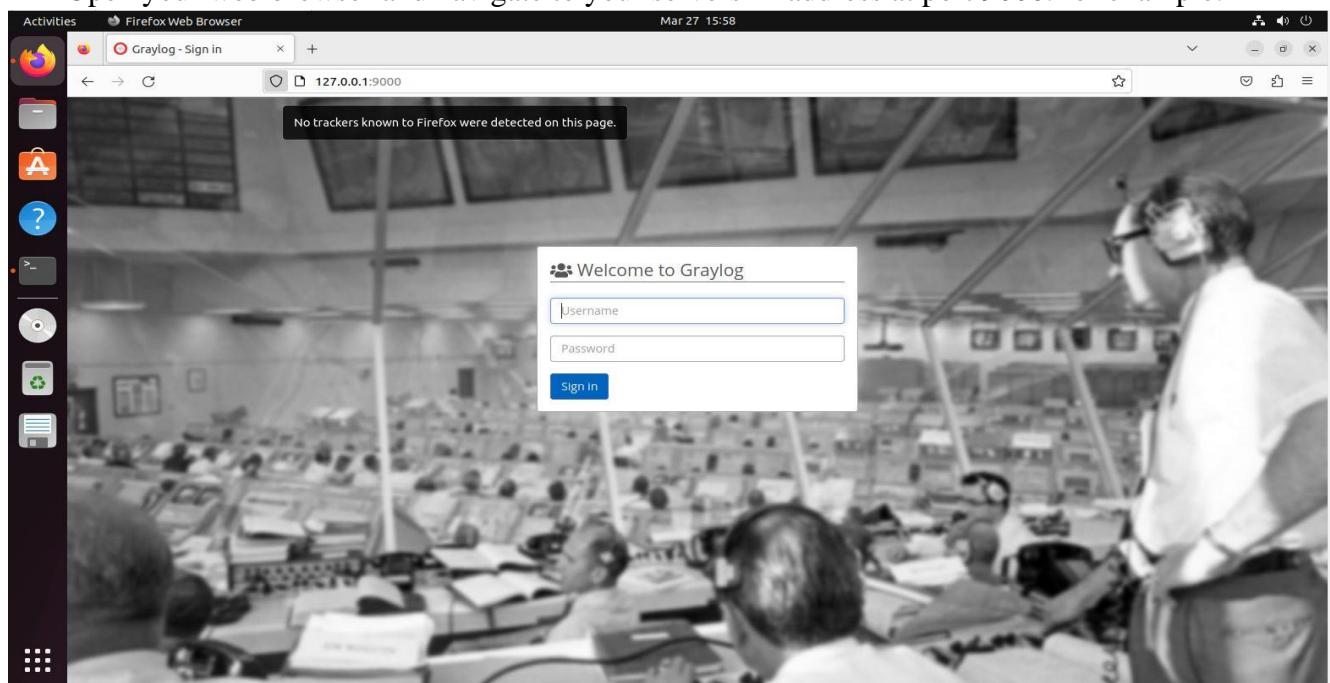
Mar 27 15:48:01 sylog-virtual-machine graylog-server[10642]: WARNING: Use --ill>

Mar 27 15:48:01 sylog-virtual-machine graylog-server[10642]: WARNING: All illeg>

lines 1-20/20 (END)

5. Access Graylog Web UI

Open your web browser and navigate to your servers IP address at port 9000. for example:



PRACTICAL NO.10: DEMONSTRATE CONVERSION OF DATA INTO A UNIVERSAL FORMAT

Part 1: Normalize Timestamps in a Log File

Part 2: Normalize Timestamps in an Apache Log File

Part 1: Normalize Timestamps in a Log File

Timestamps are used in log entries to specify when the recorded event took place. While it is best practice to record timestamps in UTC, the format of the timestamp varies from log source to log source. There are two common timestamp formats, known as Unix Epoch and Human Readable.

Converting Epoch to Human Readable Timestamps with AWK

Command:

Use the cd command to change to the /home/analyst/lab.support.files/ directory. A copy of the file shown above is stored there.

```
[analyst@secOps ~]$ cd ./lab.support.files/  
[analyst@secOps lab.support.files]$ ls -l  
total 932  
-rw-r--r-- 1 analyst analyst 649 Mar 21 2018 apache_in_epoch.log  
-rw-r--r-- 1 analyst analyst 126 Mar 25 06:31 applicationX_in_epoch.log  
-rw-r--r-- 1 analyst analyst 285 Mar 25 06:33 applicationX_in_human.log  
drwxr-xr-x 4 analyst analyst 4096 Mar 21 2018 attack_scripts  
-rw-r--r-- 1 analyst analyst 102 Mar 21 2018 confidential.txt  
-rw-r--r-- 1 analyst analyst 2871 Mar 21 2018 cyops.mn  
-rw-r--r-- 1 analyst analyst 255 Mar 20 15:20 decrypted_letter.txt  
-rw-r--r-- 1 analyst analyst 75 Mar 21 2018 elk_services  
-rw-r--r-- 1 analyst analyst 373 Mar 21 2018 h2_dropbear.banner  
drwxr-xr-x 2 analyst analyst 4096 Apr 2 2018 instructor  
-rw-r--r-- 1 analyst analyst 255 Mar 20 06:10 letter_to_grandma.txt  
-rw-r--r-- 1 analyst analyst 24464 Mar 21 2018 logstash-tutorial.log  
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 malware  
-rw-r--r-- 1 analyst analyst 370 Mar 20 14:21 message.enc  
-rwxr-xr-x 1 analyst analyst 172 Mar 21 2018 mininet_services  
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 openssl_lab  
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 pcaps  
drwxr-xr-x 7 analyst analyst 4096 Mar 21 2018 pox  
-rw-r--r-- 1 analyst analyst 473363 Mar 21 2018 sample.img  
-rw-r--r-- 1 analyst analyst 65 Mar 21 2018 sample.img_SHA256.sig  
drwxr-xr-x 3 analyst analyst 4096 Mar 21 2018 scripts  
-rw-r--r-- 1 analyst analyst 25553 Mar 21 2018 SQL_Lab.pcap  
-rw-r--r-- 1 analyst analyst 345088 Mar 22 07:10 W32.Nimda.Amm.exe
```

Issue the following AWK command to convert and print the result on the terminal:

```
[analyst@secOps lab.support.files]$
```

```
[analyst@secOps lab.support.files]$ awk &apos;BEGIN {FS=OFS="|"}  
{$3=strftime("%c",$3)} {print}&apos; applicationX_in_epoch.log  
2|Z|Mon 18 Aug 2008 11:00:00 AM EDT|AF|0  
3|N|Tue 19 Aug 2008 11:00:00 AM EDT|AF|89  
4|N|Sun 07 Sep 2008 11:00:00 AM EDT|AS|12  
1|Z|Mon 08 Sep 2008 11:00:00 AM EDT|AS|67  
5|N|Tue 09 Sep 2008 11:00:00 AM EDT|EU|23  
6|R|Wed 10 Sep 2008 11:00:00 AM EDT|OC|89  
||Wed 31 Dec 1969 07:00:00 PM EST
```

Use nano (or your favorite text editor) to remove the extra empty line at the end of the file and run the AWK script again.

```
[analyst@secOps lab.support.files]$ nano applicationX_in_epoch.log
```

While printing the result on the screen is useful for troubleshooting the script, analysts will likely need to save the output in a text file. Redirect the output of the script above to a file named applicationX_in_human.log to save it to a file:

```
[analyst@secOps lab.support.files]$ awk &apos;BEGIN {FS=OFS="|"}  
{$3=strftime("%c",$3)} {print}&apos;  
applicationX_in_epoch.log>applicationX_in_human.log
```

Use cat to view the applicationX_in_human.log.

```
[analyst@secOps lab.support.files]$ cat applicationX_in_human.log  
2|Z|Mon 18 Aug 2008 11:00:00 AM EDT|AF|0  
3|N|Tue 19 Aug 2008 11:00:00 AM EDT|AF|89  
4|N|Sun 07 Sep 2008 11:00:00 AM EDT|AS|12  
1|Z|Mon 08 Sep 2008 11:00:00 AM EDT|AS|67  
5|N|Tue 09 Sep 2008 11:00:00 AM EDT|EU|23  
6|R|Wed 10 Sep 2008 11:00:00 AM EDT|OC|89  
||Wed 31 Dec 1969 07:00:00 PM EST
```

Part 2: Normalize Timestamps in an Apache Log File

convert Unix Epoch to Human Readable timestamps.

```
[analyst@secOps lab.support.files]$ cat apache_in_epoch.log
```

```
198.51.100.213 - - [1219071600] "GET  
/twiki/bin/edit/Main/Double_bounce_sender?topicparent>Main.ConfigurationVariables HTTP/1.1" 401 12846  
  
198.51.100.213 - - [1219158000] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2  
HTTP/1.1" 200 4523  
  
198.51.100.213 - - [1220799600] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291  
  
198.51.100.213 - - [1220886000] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352  
  
198.51.100.213 - - [1220972400] "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253  
  
198.51.100.213 - - [1221058800] "GET  
/twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382
```

Use an awk script to convert the timestamp field to a human readable format. Notice that the command contains the same script used previously, but with a few adjustments for the timestamp field and file name.

```
[analyst@secOps lab.support.files]$ awk &apos;BEGIN {FS=OFS=""}  
"{$4=strftime("%c",$4)} {print}&apos;  
/home/analyst/lab.support.files/apache_in_epoch.log
```

```
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST "GET  
/twiki/bin/edit/Main/Double_bounce_sender?topicparent>Main.ConfigurationVariables HTTP/1.1" 401 12846  
  
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST "GET  
/twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523  
  
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291  
  
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352  
  
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST "GET /twiki/bin/view/Main/DCCAndPostFix  
HTTP/1.1" 200 5253  
  
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST "GET /twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382
```

To fix the problem, the square brackets must be removed from the timestamp field before the conversion takes place. Adjust the script by adding two actions before the conversion, as shown below:

```
[analyst@secOps lab.support.files]$ awk &apos;BEGIN {FS=OFS=""}  
"{$4=gsub(/\[\]/,"",$4)}{print} {$4=strftime("%c",$4)}{print}&apos; apache_in_epoch.log  
  
198.51.100.213 - - 1219071600 "GET  
/twiki/bin/edit/Main/Double_bounce_sender?topicparent>Main.ConfigurationVariables HTTP/1.1" 401 12846
```

198.51.100.213 - - Mon 18 Aug 2008 11:00:00 AM EDT "GET
/twiki/bin/edit/Main/Double_bounce_sender?topicparent>Main.ConfigurationVariables HTTP/1.1" 401 12846

198.51.100.213 - - 1219158000 "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2
HTTP/1.1" 200 4523

*198.51.100.213 - - Tue 19 Aug 2008 11:00:00 AM EDT "GET
/twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523*

198.51.100.213 - - 1220799600 "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291

198.51.100.213 - - Sun 07 Sep 2008 11:00:00 AM EDT "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291

198.51.100.213 - - 1220886000 "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352

198.51.100.213 - - Mon 08 Sep 2008 11:00:00 AM EDT "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352

198.51.100.213 - - 1220972400 "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 200 5253

*198.51.100.213 - - Tue 09 Sep 2008 11:00:00 AM EDT "GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1"
200 5253*

198.51.100.213 - - 1221058800 "GET
/twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382

*198.51.100.213 - - Wed 10 Sep 2008 11:00:00 AM EDT "GET
/twiki/bin/oops/TWiki/AppendixFileSystem?template=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382*