Practical no: 1

A. Encrypting and Decrypting Data Using a Hacker Tool.

Step 1: Create a Directory and Navigate into It

1. Open your terminal.
2. Create a directory named first: mkdir first
3. Navigate into the first directory:
   cd first

Step 2: Create Sample Text Files

1. Create three sample text files (sample1.txt, sample2.txt, sample3.txt) with some content:
2. echo "this is my first practicle1" > sample1.txt
3. echo "this is my first practicle2" > sample2.txt echo "this is my first practicle3" > sample3.txt

Step 3: Encrypt the Files into a ZIP Archive

1. Create an encrypted ZIP file (file1.zip) with the sample files:
   zip -e file1.zip sample ○ When prompted, set
   the password as g.
2. Create another encrypted ZIP file (file2.zip) with the same sample files:
   zip -e file2.zip sample ○ When prompted, set the
   password as w1.

Step 4: Unzip the Encrypted Archive

1. Unzip file1.zip to verify the encryption:
   unzip file1.zip ○ Enter the password g when
   prompted.

Step 5: Use fcrackzip to Crack the ZIP Passwords

1. Check the help menu of fcrackzip to understand its usage:
   fcrackzip --help
2. Attempt to crack the password for file1.zip:
   fcrackzip -vul 1-2 file1.zip ○ -v: Verbose
   mode. ○ -u: Try to unzip the file after
   cracking.
   ○ -l 1-2: Password length between 1 and 2 characters.
3. Attempt to crack the password for file2.zip:
   fcrackzip -vul 1-2 file2.zip

Expected Results

- file1.zip should be cracked with the password g.
- file2.zip should be cracked with the password w1.

```
CyberOps Workstation 64 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Applications   Terminal - analyst@secOps:...
Terminal - analyst@secOps:~/f
File  Edit  View  Terminal  Tabs  Help
analyst@secOps ~]$ cd first
analyst@secOps first]$ echo "this is my first practicle1" > sample1.txt
analyst@secOps first]$ echo "this is my first practicle2" > sample2.txt
analyst@secOps first]$ echo "this is my first practicle3" > sample3.txt
analyst@secOps first]$ zip -e file1.zip sample*
nter password:
erify password:

ip error: Invalid command arguments (password verification failed)
analyst@secOps first]$ zip -e file1.zip sample*
nter password:
erify password:
 adding: sample1.txt (stored 0%)
 adding: sample2.txt (stored 0%)
 adding: sample3.txt (stored 0%)
analyst@secOps first]$ zip -e file2.zip sample*
nter password:
erify password:
 adding: sample1.txt (stored 0%)
 adding: sample2.txt (stored 0%)
 adding: sample3.txt (stored 0%)
analyst@secOps first]$ unzip file1.zip
rchive:  file1.zip
file1.zip] sample1.txt password:
eplace sample1.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
eplace sample2.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
eplace sample3.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
analyst@secOps first]$ fcrackzip -vul 1-2 file1.zip
ound file 'sample1.txt', (size cp/uc     40/    28, flags 9, chk b3c7)
ound file 'sample2.txt', (size cp/uc     40/    28, flags 9, chk b3d2)
ound file 'sample3.txt', (size cp/uc     40/    28, flags 9, chk b3d9)


ASSWORD FOUND!!!!: pw == g
```

```
[analyst@secOps first]$ fcrackzip -vul 1-2 file1.zip
found file 'sample1.txt', (size cp/uc     40/    28, flags 9, chk b3c7)
found file 'sample2.txt', (size cp/uc     40/    28, flags 9, chk b3d2)
found file 'sample3.txt', (size cp/uc     40/    28, flags 9, chk b3d9)


PASSWORD FOUND!!!!: pw == g
[analyst@secOps first]$ fcrackzip -vul 1-2 file2.zip
found file 'sample1.txt', (size cp/uc     40/    28, flags 9, chk b3c7)
found file 'sample2.txt', (size cp/uc     40/    28, flags 9, chk b3d2)
found file 'sample3.txt', (size cp/uc     40/    28, flags 9, chk b3d9)


PASSWORD FOUND!!!!: pw == w1
[analyst@secOps first]$
```

B. Encrypting and Decrypting Data Using OpenSSL.

Step 1: Create a Sample Text File

1. Open your terminal.
2. Create a text file named text1.txt with the content "hello world":
   echo "hello world" > text1.txt

Step 2: Encrypt the File Using OpenSSL

1. Encrypt text1.txt using AES-256-CBC encryption and save the output to text2.txt:
   openssl aes-256-cbc -a -in text1.txt -out text2.txt ○ You will be prompted to enter and confirm a password. Remember this password for decryption.
2. View the encrypted content of text2.txt:
   cat text2.txt

Step 3: Decrypt the File Using OpenSSL

1. Decrypt text2.txt and save the output to text3.txt:
   openssl aes-256-cbc -a -d -in text2.txt -out text3.txt ○
   Enter the password you used during encryption.
2. View the decrypted content of text3.txt:
   cat text3.txt
   Alternatively, you can decrypt and display the content directly without saving to a file:
   openssl aes-256-cbc -a -d -in text2.txt

Step 4: Create and Encrypt a Custom Text File

1. Create a custom text file named letter_to_grandma.txt:
   nano letter_to_grandma.txt
   - Add the following content to the file:

   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.
   Save and exit the editor (Ctrl + O and enter, then Ctrl + X).
2. Encrypt letter_to_grandma.txt and save the output to msg.enc:
   openssl aes-256-cbc -a -in letter_to_grandma.txt -out msg.enc
   ○ Set a password when prompted.

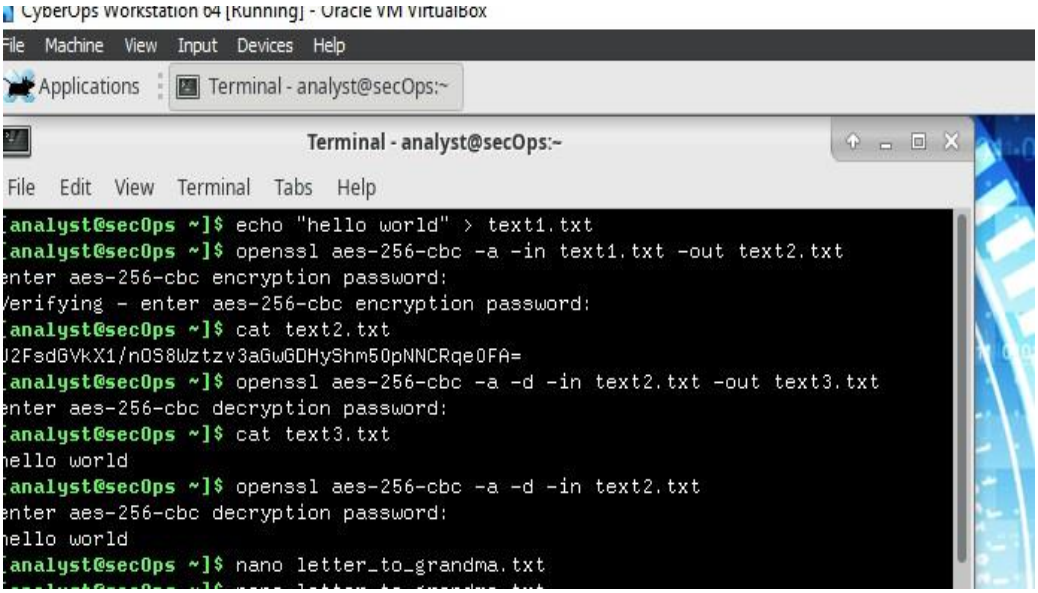
Step 5: Decrypt the Custom Encrypted File

1. Decrypt msg.enc and save the output to text4.txt:
   openssl aes-256-cbc -a -d -in msg.enc -out text4.txt ○
   Enter the password you used during encryption.
2. View the decrypted content of text4.txt:

   cat text4.txt

Expected Results

- The content of text1.txt and text3.txt should match after encryption and decryption.
- The content of letter_to_grandma.txt and text4.txt should match after encryption and decryption.



c. Hashing Files Using OpenSSL.

Step 1: Create a Custom Text File

1. Open your terminal.
2. Create a custom text file named letter_to_grandma.txt:
   nano letter_to_grandma.txt

3.Add the following content to the file:

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.

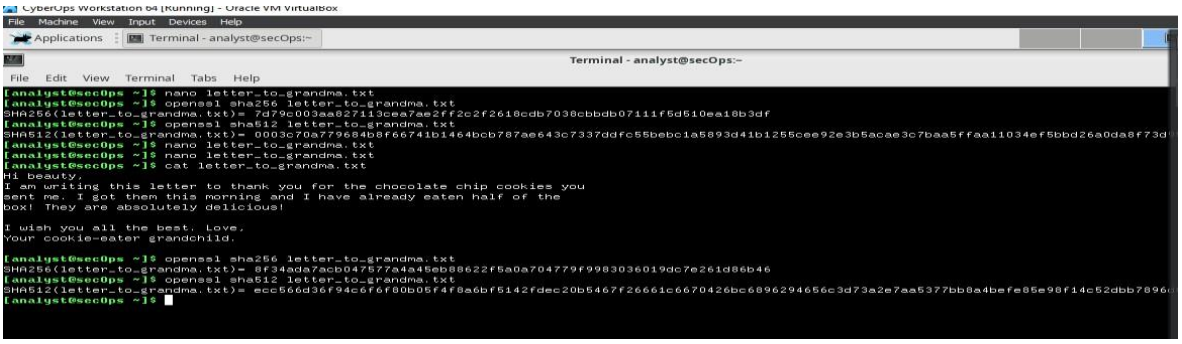
Save and exit the editor (Ctrl + O, and enter then Ctrl + X).

Step 2: Generate SHA-256 and SHA-512 Hashes

1. Generate the SHA-256 hash of letter_to_grandma.txt:
   openssl sha256 letter_to_grandma.txt ○
   Copy the hash value for future reference.
2. Generate the SHA-512 hash of letter_to_grandma.txt:
   openssl sha512 letter_to_grandma.txt ○
   Copy the hash value for future reference.

Step 3: Modify the File and Recalculate Hashes

1. Open the letter_to_grandma.txt file and make a small change (e.g., add or remove a word):
   nano letter_to_grandma.txt
   1. For example, change "delicious" to "amazing".
   2. Save and exit the editor (Ctrl + O and enter then Ctrl + X).
2. View the updated content of the file:
   cat letter_to_grandma.txt
3. Recalculate the SHA-256 hash of the modified file:
   openssl sha256 letter_to_grandma.txt
   1. Compare this hash with the original SHA-256 hash. They should be different.
4. Recalculate the SHA-512 hash of the modified file:
   openssl sha512 letter_to_grandma.txt
   1.Compare this hash with the original SHA-512 hash. They should be different.



Practical No : 2

A. Examining Telnet and SSH in Wireshark.

Step 1: Capture data.

a. Start the CyberOps Workstation VM and log in with username **analyst** and password **cyberops.**

b. Open a terminal window and start Wireshark. Press **OK** to continue after reading the warning message.

c. Start a **Wireshark** capture on the **Loopback: lo** interface.

d. Open another terminal window. Start a Telnet session to the localhost. Enter username **analyst** and password **cyberops** when prompted. Note that it may take several minutes for the "connected to localhost" and login prompt to appear.

e. Stop the Wireshark capture after you have provided the user credentials.

Step 2: Examine the Telnet session.

a. Apply a filter that only displays Telnet-related traffic. Enter **Telnet** in the filter field and click **Apply.**

b. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow TCP Stream**.

c. The Follow TCP Stream window displays the data for your Telnet session with the CyberOps Workstation VM. The entire session is displayed in plaintext, including your password. Notice that the username that you entered is displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.

d. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**

e. Type **exit** at the terminal to exit the **Telnet** session.

Part 2: Examine an SSH Session with Wireshark

In Part 2, you will establish an SSH session with the localhost. Wireshark will be used to capture and view the data of this SSH session.

a. Start another Wireshark capture.

b. You will establish an SSH session with the localhost. At the terminal prompt, enter **ssh localhost**. Enter **yes** to continue connecting. Enter the **cyberops** when prompted. c.

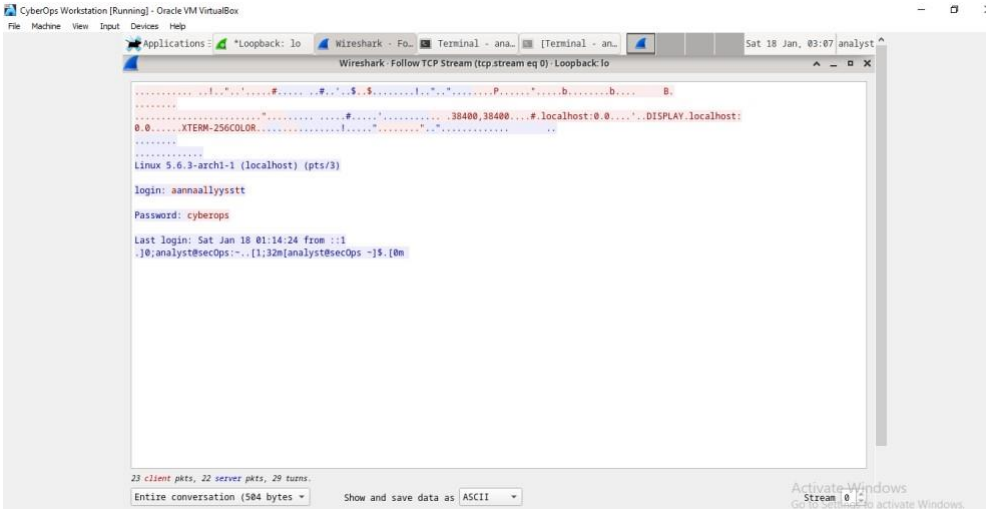
Stop the Wireshark capture.

d. Apply an **SSH** filter on the Wireshark capture data. Enter ssh in the filter field and click **Apply.**

e. Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow TCP Stream** option.

f. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session. g. After examining your SSH session, click **Close.**

h. Close Wireshark.


CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Loopback: lo
Linux 5.6.3-arch1-1 (localhost) (pts/3)
login: aannaallyysstt
Password: cyberops
Last login: Sat Jan 18 01:14:24 from ::1
23 client pkts, 22 server pkts, 29 turns.
Entire conversation (504 bytes
Show and save data as ASCII
Stream 0

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Loopback: lo
SSH-2.0-OpenSSH_8.2
SSH-2.0-OpenSSH_8.2

B. Investigating an Attack on a Windows Host

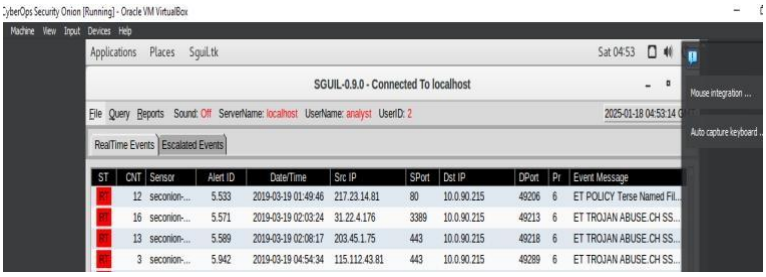
Step 1: Open Sguil and locate the alerts on 3-19-2019.

a. Login to Security Onion VM with the **analyst** username and **cyberops**

b. Launch Sguil from the desktop. Login with username **analyst** and password **cyberops**. Click **Select All** and **Start Sguil** to view all the alerts generated by the network sensors. c. Locate the group of alerts from 19 March 2019.

According to Sguil, what are the timestamps for the first and last of the alerts that occurred on 3-192019?

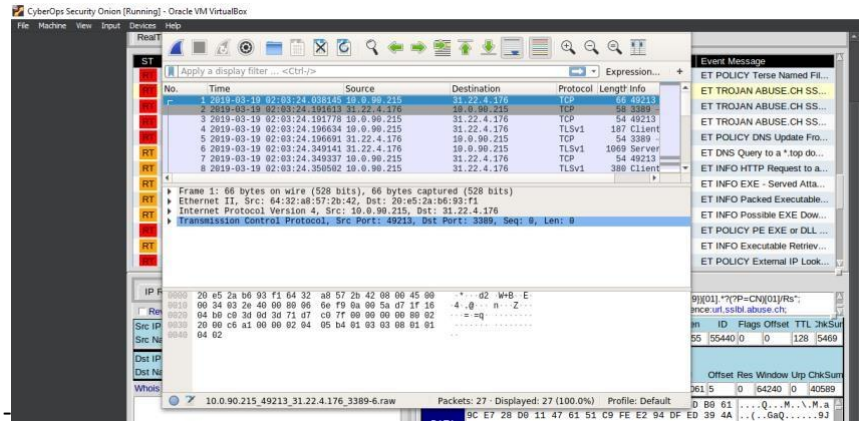
What is interesting about the timestamps of all the alerts on 3-19-2019?

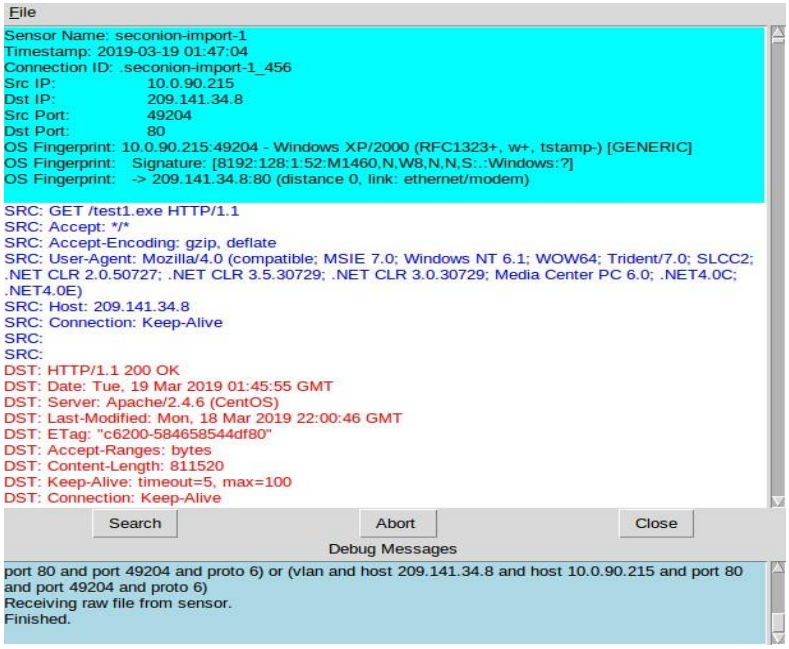


Step 2: Review the alerts in detail.

a. In Sguil, click the first of the alerts on 3-19-2019 (Alert ID 5.439). Make sure to check the **Show Packet Data** and **Show Rule** checkboxes to examine the packet header information and the IDS signature rule related to the alert. Right on the **Alert ID** and pivot to Wireshark. Based on the information derived from this initial alert answer the following questions:

b. In Sguil, select the second of the alerts on 3-19-2019. Right click the Alert ID 5.440 and select **Transcript**.





c. Close the transcript. Use Wireshark to export the executable file for malware analysis (**File > Export Objects > HTTP…**). Save the file to the analyst's home folder.

d. Open a terminal in Security Onion VM and create a SHA256 hash from the exported file. Use the following command:

e. Copy the file hash and submit it to the Cisco Talos file reputation center at https://talosintelligence.com/talos_file_reputation.

f. In Sguil select the alert with **Alert ID 5.480** and the **Event Message** Remcos RAT Checkin 23. Notice that the IDS signature has detected the Remcos RAT based on the binary hex codes at the beginning of communication.

g. Right click the Alert ID and select Transcript.

h. Using Sguil and the remaining alerts from 3-19-2019, locate the second executable file that was downloaded and check to see if it is known malware.

i. Examine the remaining three alerts from 3-19-2019 by looking at the header information in Show Packet Data, the IDS signature in Show Rule, and the Alert ID Transcripts.

j. Even though you have examined all the alerts in Sguil related to an attack on a Windows host on 3-19-2019, there may be additional related information available in Kibana. Close Sguil and launch Kibana from the desktop.

Part 2: Use Kibana to Investigate Alerts

Step 1: Open Kibana and narrow the timeframe.

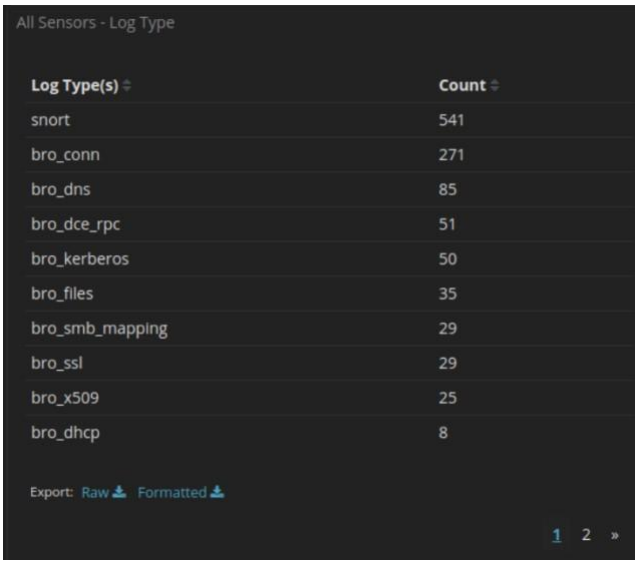
a. Login to Kibana with the **analyst** username and **cyberops**

b. Open Kibana (username **analyst** and password **cyberops**), click **Last 24 Hours** and the **Absolute** time range tab to change the time range to March 1, 2019 to March 31, 2019.

c. The **Total Log Count Over Time** timeline will show an event on March 19. Click that event to narrow the focus to the specific time range of the attack.

Step 2: Review the alerts in the narrowed timeframe.

a. In the Kibana dashboard scroll down to the **All Sensors – Log Type** visualization. Review both pages and note the variety of log types related to this attack.



All Sensors - Log Type

Log Type(s)	Count
snort	541
bro_conn	271
bro_dns	85
bro_dce_rpc	51
bro_kerberos	50
bro_files	35
bro_smb_mapping	29
bro_ssl	29
bro_x509	25
bro_dhcp	8

Export: Raw Formatted

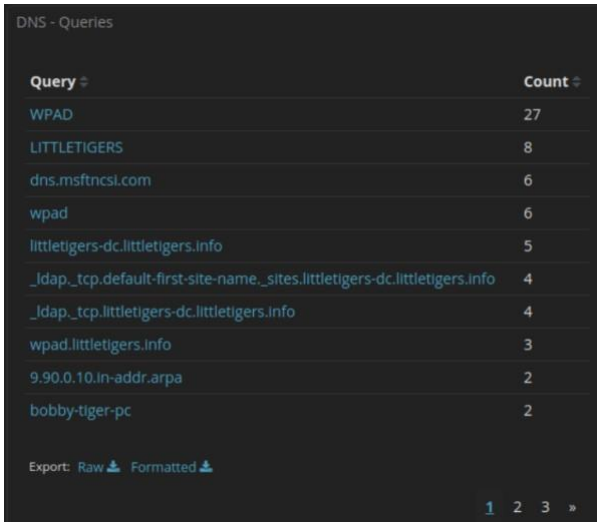
1 2 »

b. Scroll down and notice that the NIDS Alert Summary in Kibana has many of the same IDS alerts as listed in Sguil. Click the magnifier to filter on the second alert ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) from Source IP Address 31.22.4.176.

c. Scroll down to All Logs and click the arrow to expand the first log in the list with source IP address 31.22.4.176.

d. Scroll back to the top of the page and click the Home link under Navigation.

e. Earlier we noted log types like bro_http listed in the Home dashboard. You can filter for the various log type but the built-in dashboards will probably have more information. Scroll back to the top of the page and click **HTTP** in dashboard link under Zeek Hunting in Navigation.
f. Scroll through the HTTP dashboard taking notice of the information presented
g. Match the **HTTP – URIs** to the **HTTP – Sites** on the dashboard.
h. Scroll back to the top of the web page and under Navigation – Zeek Hunting click **DNS**. Scroll to the DNS Queries visualization. Notice page 1 and page 3 of the DNS queries.


DNS - Queries

Query	Count
WPAD	27
LITTLETIGERS	8
dns.msftncsi.com	6
wpad	6
littletigers-dc.littletigers.info	5
_ldap._tcp.default-first-site-name._sites.littletigers-dc.littletigers.info	4
_ldap._tcp.littletigers-dc.littletigers.info	4
wpad.littletigers.info	3
9.90.0.10.in-addr.arpa	2
bobby-tiger-pc	2

Export: Raw Formatted

1 2 3 »

i. For further investigation and curiosity, try examining the following Zeek Hunting dashboards:

C. Investigating a Malware Exploit.

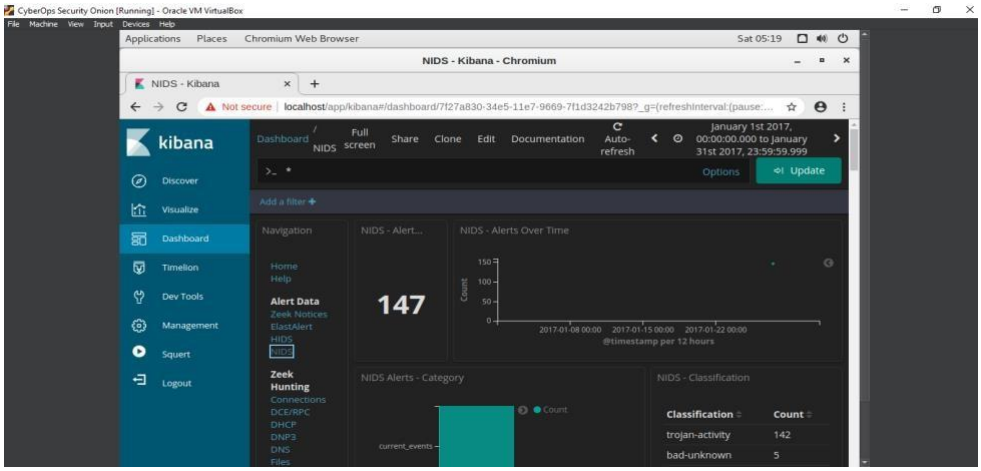
Step 1: Narrow the timeframe.

a. Login to Security Onion with the analyst username and cyberops

b. Open Kibana (username analyst and password cyberops) and set an Absolute time range to narrow the focus to log data from January 2017.

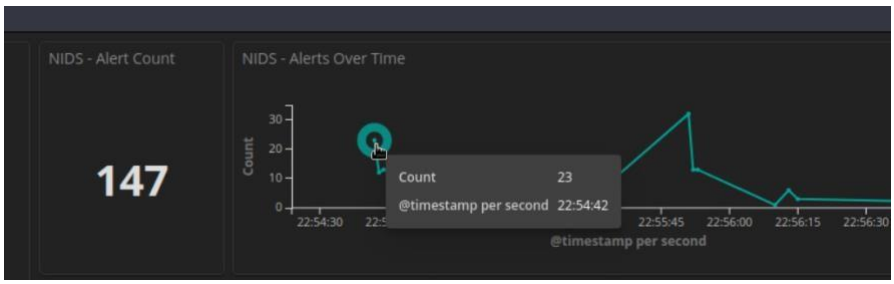
Step 2: Locate the Event in Kibana

a. After narrowing the time range in the main Kibana dashboard, go to the **NIDS** Alert Data dashboard by clicking NIDS.



b. Zoom in on the event by clicking and dragging in the NIDS – Alerts Over Time visualization further focus in on the event timeframe. Since the event happened over a very short period of time, select just the graph plot line. Zoom in until your display resembles the one below.

c. Click the first point on the timeline to filter for only that first event.



d. Now view details for the events that occurred at that time. Scroll all the way to the bottom of the dashboard until you see the **NIDS Alerts** section of the page. The alerts are arranged by time. Expand the first event in the list by clicking the pointer arrow that is to the left of the timestamp.

e. In a web browser on a computer that can connect to the internet, go to the link that is provided in the signature_info field of the alert. This will take you to the Emerging Threats Snort alert rule for the exploit. There are a series of rules shown. This is because signatures can change over time, or new and more accurate rules are developed. The newest rule is at the top of the page.

Step 3: View the Transcript capME!

a. Click the **alert _id** value, you can pivot to CapME to inspect the transcript of the event.

b. Close the CapME! browser tab.

c. From the top of the NIDS Alert Dashboard click the **HTTP** entry located under **Zeek Hunting**

d. In the HTTP dashboard, verify that your absolute time range includes **2017-01-27 22:54:30.000** to **2017-01-27 22:56:00.000**.

Scroll down to the HTTP – Sites section of the dashboard.

Part 2: Investigate the Exploit with Sguil

Step 1: Open Sguil and locate the alerts.

a. Launch Sguil from the desktop. Login with username **analyst** and password **cyberops**.

Enable all sensors and click **Start**.

b. Locate the group of alerts from January 27th2017 **Step 2: Investigate the alerts in Sguil.**

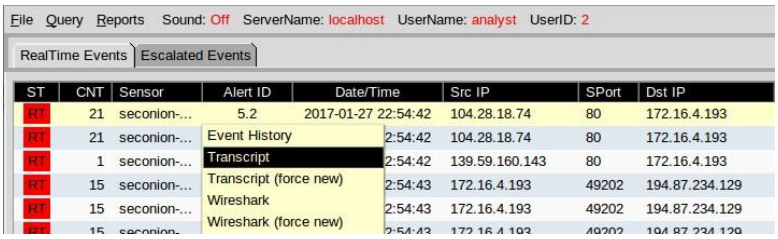
a. Click the **Show Packet Data** and **Show Rule** checkboxes to see the packet header field information and the IDS signature rule related to the alert.

b. Select the alert ID 5.2 (Event message **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**).

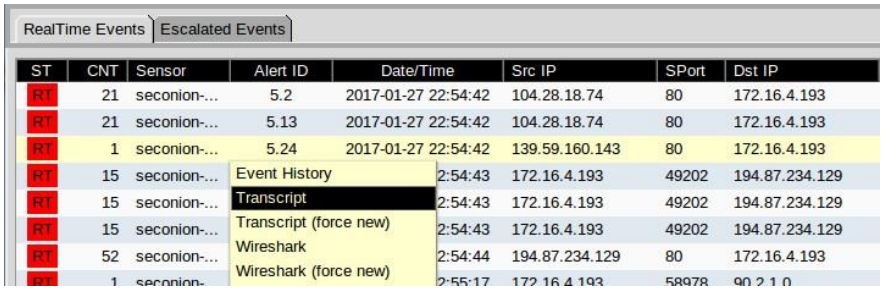
c. Maximize the Sguil window and size the Event Message column so that you can see the text of the entire message. Look at the Event Messages for each of the alert IDs related to this attack.

Step 3: View Transcripts of Events

a. Right-click the associated alert ID 5.2 (Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016**).



b. Right-click the alert ID 5.24 (source IP address of **59.160.143** and Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017)** and choose **Transcript** to open a transcript of the conversation.



d. Close the current transcript window. In the Sguil window, right-click the alert ID 5.25 (Event Message **ET CURRENT_EVENTS Rig EK URI Struct Mar 13 2017 M2**) and open the transcript.

e. Close the transcript window.

f. Right-click the same ID again and choose Network Miner. Click the **Files** tab.

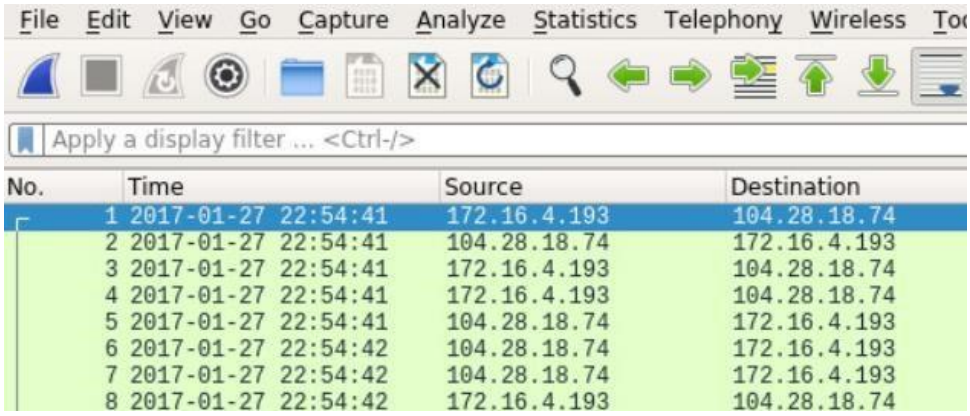
Part 3: Use Wireshark to Investigate an Attack

Step 1: Pivot to Wireshark and Change Settings.

a. In Sguil, right-click the alert ID 5.2 (Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016**) and pivot to select Wireshark from the menu. The pcap that is associated with this alert will open in Wireshark.

b. The default Wireshark setting uses a relative time per-packet which is not very helpful for isolating the exact time an event occurred. To fix this, select to **View > Time Display Format >**

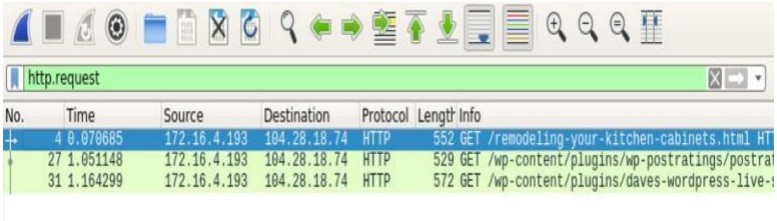
Date and Time of Day and then repeat a second time, **View > Time Display Format > Seconds**. Now your Wireshark Time column has the date and timestamps. Resize the columns to make the display clearer if necessary.



No.	Time	Source	Destination
1	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
2	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
3	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
4	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
5	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
6	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
7	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
8	2017-01-27 22:54:42	172.16.4.193	104.28.18.74

Step 2: Investigate HTTP Traffic.

a. In Wireshark, use the **http.request** display filter to filter for web requests only.



No.	Time	Source	Destination	Protocol	Length	Info
4	0.070685	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HT
27	1.051148	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postra
31	1.164299	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-

b. Select the first packet. In the packet details area, expand the Hypertext Transfer Protocol application layer data. **Step 3: View HTTP Objects.**

a. In Wireshark, choose **File > Export Objects > HTTP**.

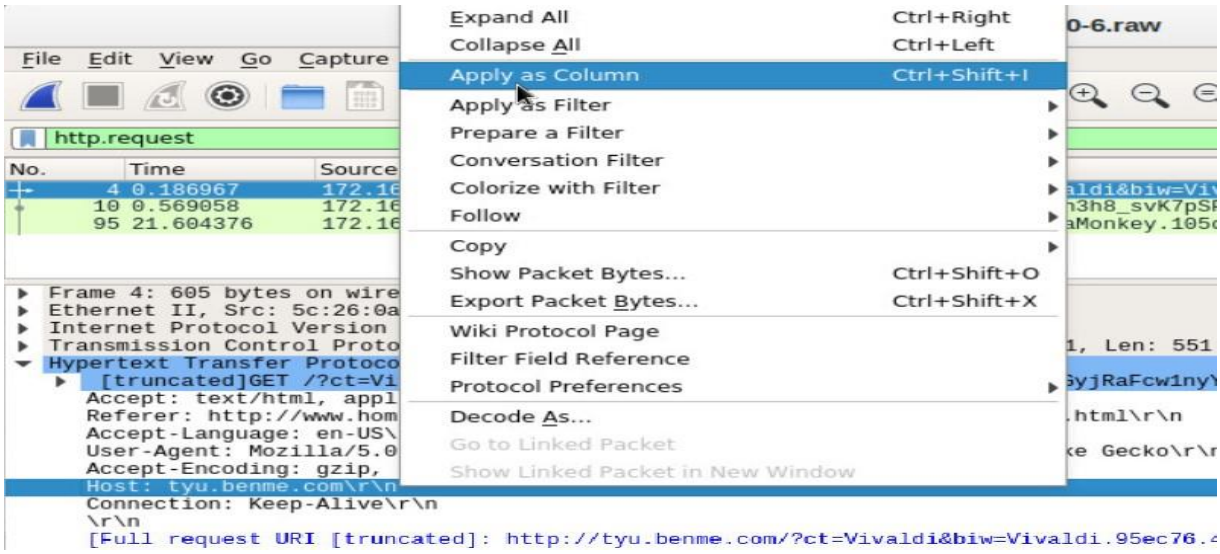
b. In the Export HTTP objects list window, select the remodeling-your-kitchen-cabinets.html packet and save it to your home folder.

c. Close Wireshark. In Sguil, right-click the alert ID 5.24 (source IP address **59.160.143** and Event Message **ET CURRRENT_EVENTS Evil Redirector Leading to EK March 15 2017**) and choose **Wireshark** to pivot to Wireshark. Apply an **http.request** display filter

d. In Wireshark, go to **File > Export Objects > HTTP** and save the JavaScript file to your home folder.

e. Close Wireshark. In Sguil, right-click the alert ID 5.25 (Event Message **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) and choose **Wireshark** to pivot to Wireshark. Apply an **request** display filter

f. With the first packet selected, in the packet details area, expand the Hypertext Transfer Protocol application layer data. Right-click the **Host information** and choose **Apply as Column** to add the Host information to the packet list columns, as shown in the figure.



g. To make room for the Host column right-click the Length column header and uncheck it. This will remove the Length column from the display.

h. The names of the servers are now clearly visible in the Host column of the packet list.

Step 4: Create a Hash for an Exported Malware File.

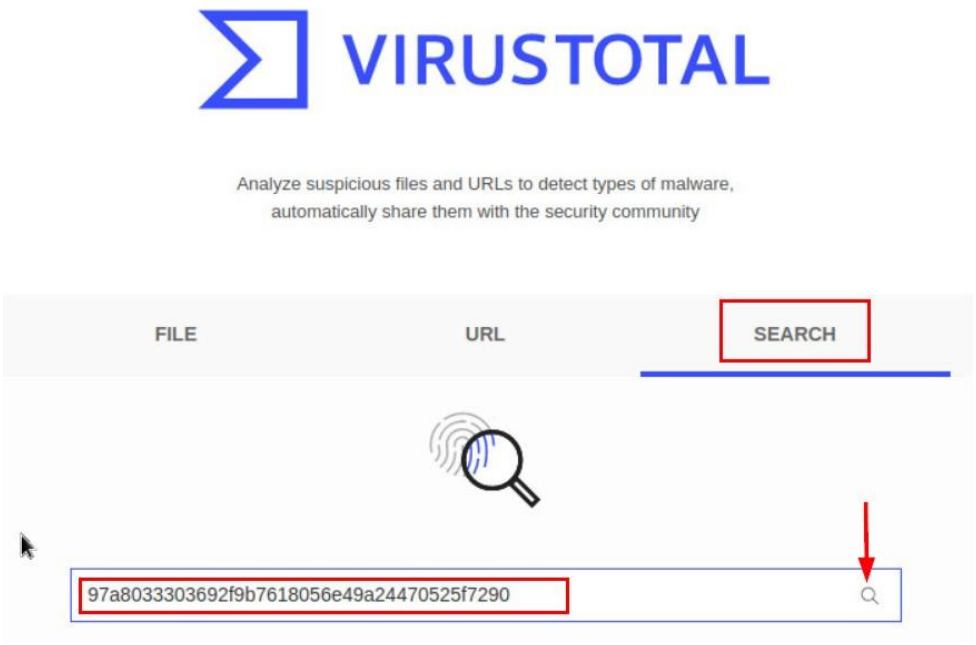
a. In Wireshark, go to **File > Export Objects > HTTP** and save the two text/html files and the application/x-shockwave-flash file to your home directory.

b. Now that you have saved the three files to your home folder, test to see if one of the files matches a known hash value for malware at **com**. Issue a ls -l command to look at the files saved in your home directory. The flash file has the word SeaMonkey near the beginning of the long filename. The filename begins with **%3fbiw=SeaMonkey**. Use the ls -l command with **grep** to filter out the filename with the pattern **seamonkey**. The option **-i** ignores the case distinction.

c. Generate a SHA-1 hash for the SeaMonkey flash file with the command **sha1sum** followed by the filename. Type the first 4 letters %3fb of the filename and then press the **tab** key to auto fill the rest of the filename. Press enter and sha1sum will compute a 40 digit long fixed length hash value.

d. You can also generate a hash value by using NetworkMiner. Navigate to Sguil and rightclick the alert ID 5.25 (Event Message **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) and select **NetworkMinor** to pivot to NetworkMinor. Select the **Files** In this example, right-click the file with swf extension and select **Calculate MD5 / SHA1 / SHA256 hash**. Compare the SHA1 hash value with the one from the previous step. The SHA1 hash values should be the same.

e. Open a web browser and go to **com**. Click the **Search** tab and enter the hash value to search for a match in the database of known malware hashes. VirusTotal will return a list of the virus detection engines that have a rule that matches this hash.



f. Investigate the Detection and Details tabs. Review the information that is provided on this hash value.

g. Close the browser and Wireshark. In Sguil, use alert ID 5.37 (Event Message **ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2**) to pivot to Wireshark and examine the HTTP requests.

h. Create a SHA-1 hash of the SWF file as you did previously.

i. In Sguil, the last 4 alerts in this series are related, and they also seem to be post-infection.

j. Go to virustotal.com and do a URL search for the .top domain used in the attack.

k. Examine the last alert in the series in Wireshark. If it has any objects worth saving, export and save them to your home folder.

Part 4: Examine Exploit Artifacts

a. In Security Onion, open **the remodeling-your-kitchen-cabinets.html** file using your choice of text editor. This webpage initiated the attack.

b. Open the dle_js.js file in choice of text editor and examine it.

c. In a text editor, open the text/html file that was saved to your home folder with Vivaldi as part of the filename.

practical No: 3

A.Demonstrate the use of Snort and Firewall Rules

Step 1: Preparing the Virtual Environment

a. Launch Oracle VirtualBox and change the CyberOps Workstation for Bridged mode, if necessary. Select Machine > Settings > Network. Under Attached To, select Bridged Adapter (or if you are using WiFi with a proxy, you may need NAT adapter) and click OK.

b. Launch the CyberOps Workstation VM, open a terminal and configure its network by executing the sh script.

Because the script requires super-user privileges, provide the password for the user analyst.

[analyst@secOps ~]$ sudo ./lab.support.files/scripts/configure_as_dhcp.sh [sudo]
password for analyst:
[analyst@secOps ~]$

c. Use the ifconfig command to verify CyberOps Workstation VM now has an IP address on your local network. You can also test connectivity to a public webserver by pinging www.cisco.com. Use Ctrl+C to stop the pings.

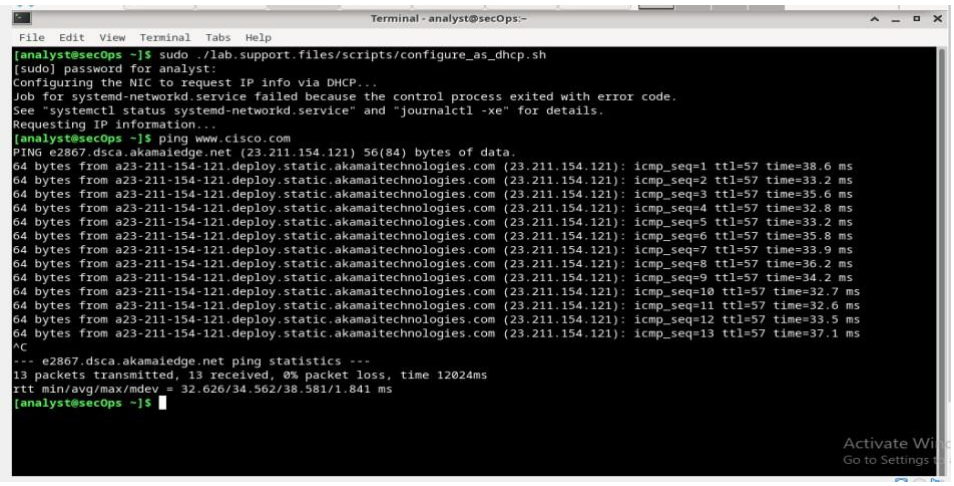
[analyst@secOps ~]$ ping www.cisco.com
PING e2867.dsca.akamaiedge.net (23.204.15.199) 56(84) bytes of data.
64 bytes from a23-204-15-199.deploy.static.akamaitechnologies.com (23.204.15.199): icmp_seq=1 ttl=54 time=28.4 ms
64 bytes from a23-204-15-199.deploy.static.akamaitechnologies.com (23.204.15.199): icmp_seq=2 ttl=54 time=35.5 ms
^C
e2867.dsca.akamaiedge.net ping statistics
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 28.446/32.020/35.595/3.578 ms

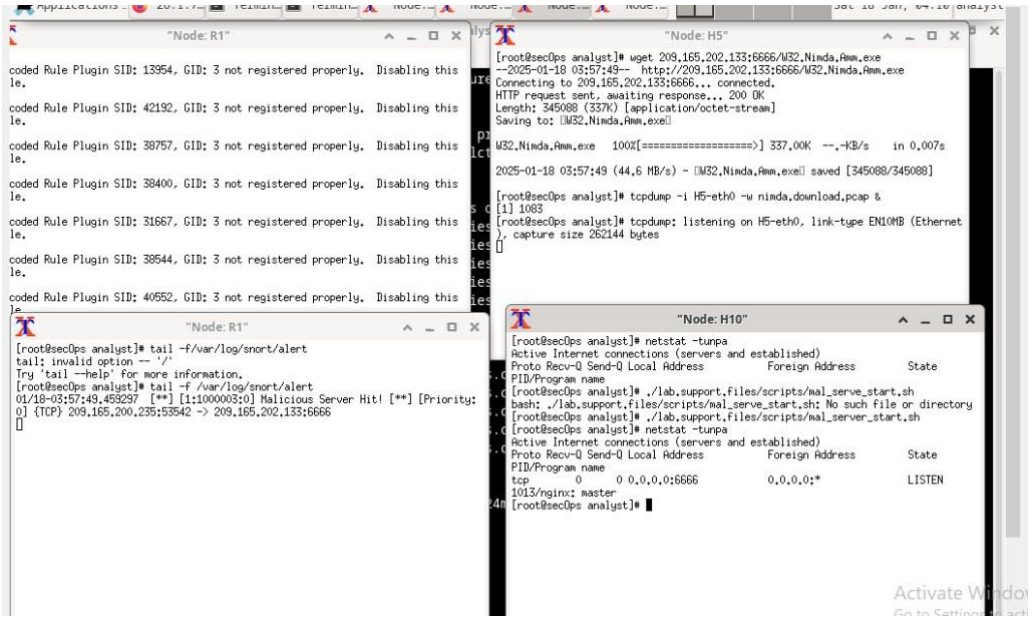
Step 1: Real-Time IDS Log Monitoring

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

[analyst@secOps ~]$ sudo ./lab.support.files/scripts/cyberops_extended_topo_no_fw.py [sudo]
password for analyst:
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>
The mininet prompt should be displayed, indicating mininet is ready for commands. b.
From the mininet prompt, open a shell on R1 using the command below:
mininet> xterm R1 mininet>





B. Demonstrate Extract an Executable from a PCAP

Part 1: Analyze Pre-Captured Logs and Traffic Captures

In Part 2, you will work with the nimda.download.pcap file. Captured in a previous lab, nimda.download.pcap contains the packets related to the download of the Nimda malware. Your version of the file, if you created it in the previous lab and did not reimport your CyberOps Workstation VM, is stored in the /home/analyst directory. However, a copy of that file is also stored in the CyberOps Workstation VM, under the /home/analyst/lab.support.files/pcaps directory so that you can complete this lab. For consistency of output, the lab will use the stored version in the pcaps directory.

While tcpdump can be used to analyze captured files, Wireshark's graphical interface makes the task much easier. It is also important to note that tcpdump and Wireshark share the same file format for packet captures; therefore, PCAP files created by one tool can be opened by the other.

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

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

[analyst@secOps pcaps]$ ls -l total

7460

-rw-r--r-- 1 analyst analyst 3510551 Aug 7 15:25 lab_prep.pcap

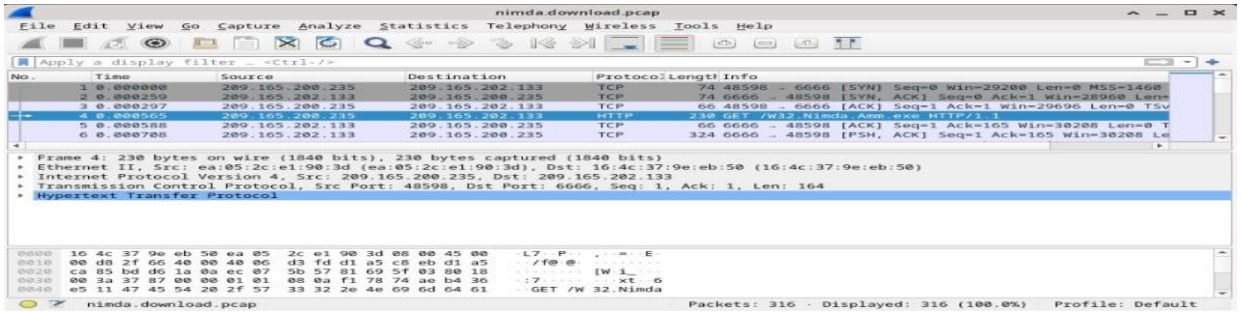
-rw-r--r-- 1 analyst analyst 371462 Jun 22 10:47 nimda.download.pcap

-rw-r--r-- 1 analyst analyst 3750153 May 25 11:10 wannacry_download_pcap.pcap

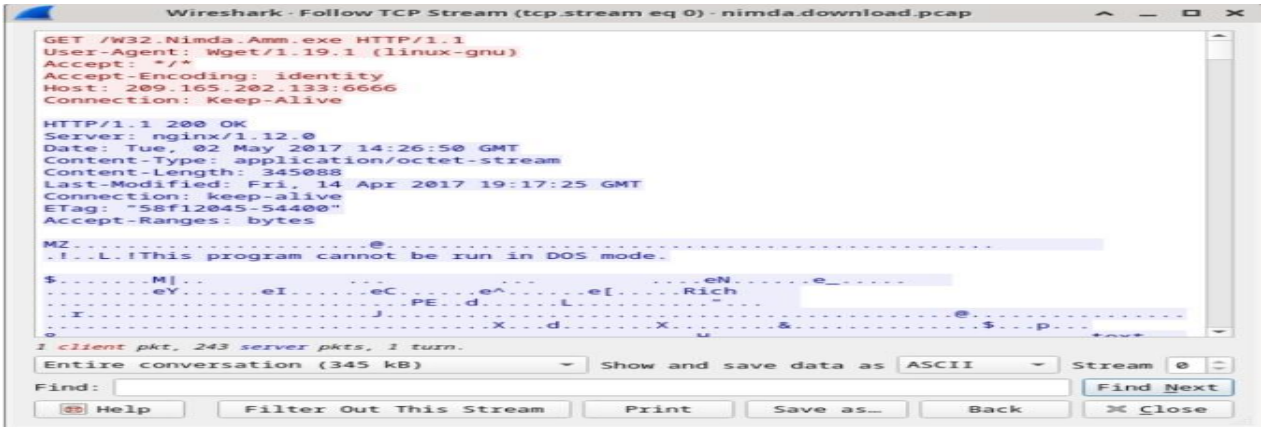
[analyst@secOps pcaps]$

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

[analyst@secOps pcaps]$ wireshark nimda.download.pcap &



c. The download.pcap file contains the packet capture related to the malware download performed in a previous lab. The pcap contains all the packets sent and received while tcpdump was running. Select the fourth packet in the capture and expand the Hypertext Transfer Protocol to display as shown below.



d. 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 Follow > TCP Stream.

Part 2: Extract Downloaded Files from PCAP

Follow the steps below to use **Wireshark** to retrieve the Nimda malware.

a. 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.

b. With the GET request packet selected, navigate to **File > Export Objects > HTTP**, from **Wireshark**'s menu.

c. Wireshark will display all HTTP objects present in the TCP flow that contains the GET request. In this case, only the **Nimda.Amm.exe** file is present in the capture. It will take a few seconds before the file is displayed

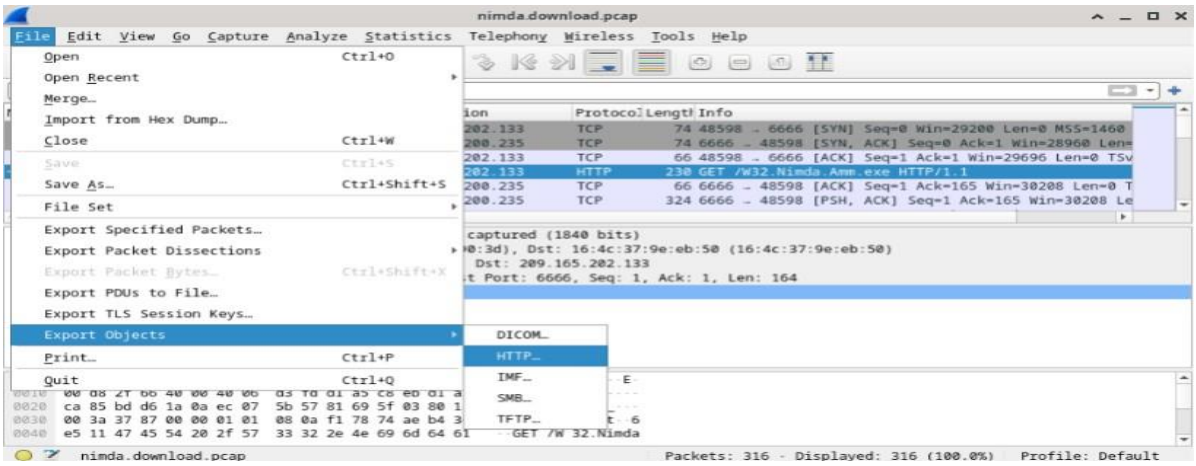
d. In the **HTTP object list** window, select the **Nimda.Amm.exe** file and click **Save As** at the bottom of the screen.

e. Click the left arrow until you see the **Home** Click Home and then click the **analyst** folder (not the analyst tab). Save the file there.

f. 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 [analyst@secOps pcaps]$ cd /home/analyst**

[analyst@secOps ~]$ ls –l total 364 drwxr-xr-x 2 analyst analyst
4096 Sep 26 2014 Desktop drwx 3 analyst analyst 4096 May
25 11:16 Downloads drwxr-xr-x 2 analyst analyst 4096 May 22
08:39 extra drwxr-xr-x 8 analyst analyst 4096 Jun 22 11:38
lab.support.files drwxr-xr-x 2 analyst analyst 4096 Mar 3
15:56 second_drive
-rw-r--r-- 1 analyst analyst 345088 Jun 22 15:12 W32.Nimda.Amm.exe
[analyst@secOps ~]$
[analyst@secOps ~]$ **file W32.Nimda.Amm.exe**
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$

As seen above, **W32.Nimda.Amm.exe** is indeed a Windows executable file.



c. Demonstrate a practical for Exploring DNS Traffic

Part 1: Capture DNS Traffic

Step 1: Download and install Wireshark.

a. Download the latest stable version of Wireshark from www.wireshark.org. Choose the software version you need based on your PC's architecture and operating system.

Step 2: Capture DNS traffic.

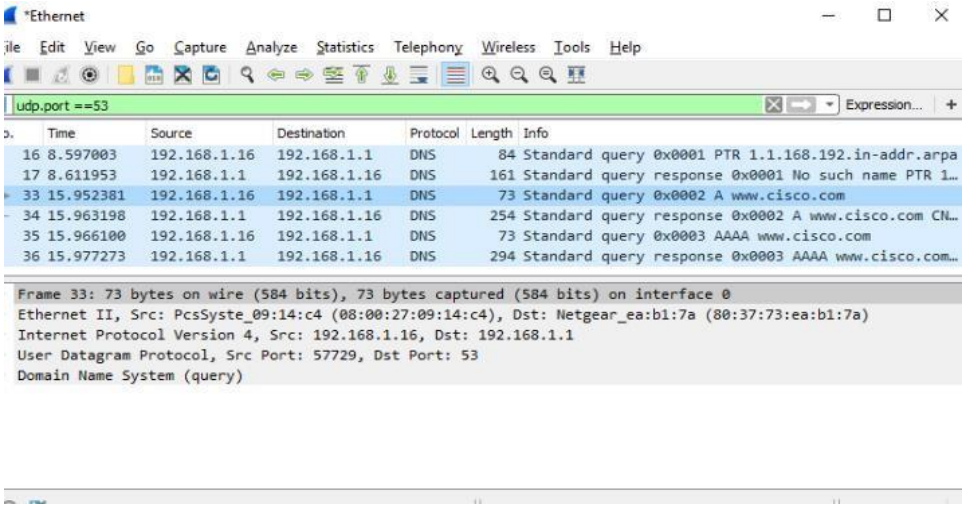
a.Start Wireshark. Select an active interface with traffic for packet capture.

b. Clear the DNS cache.

c.In Windows, enter **ipconfig /flushdns** in Command Prompt.

d.Type **exit** when finished. Close the command prompt.

e.Click **Stop capturing packets** to stop the Wireshark capture.



Part 2: Explore DNS Query Traffic

A.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.

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

c. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

d. Expand **Ethernet II** to view the details. Observe the source and destination fields.

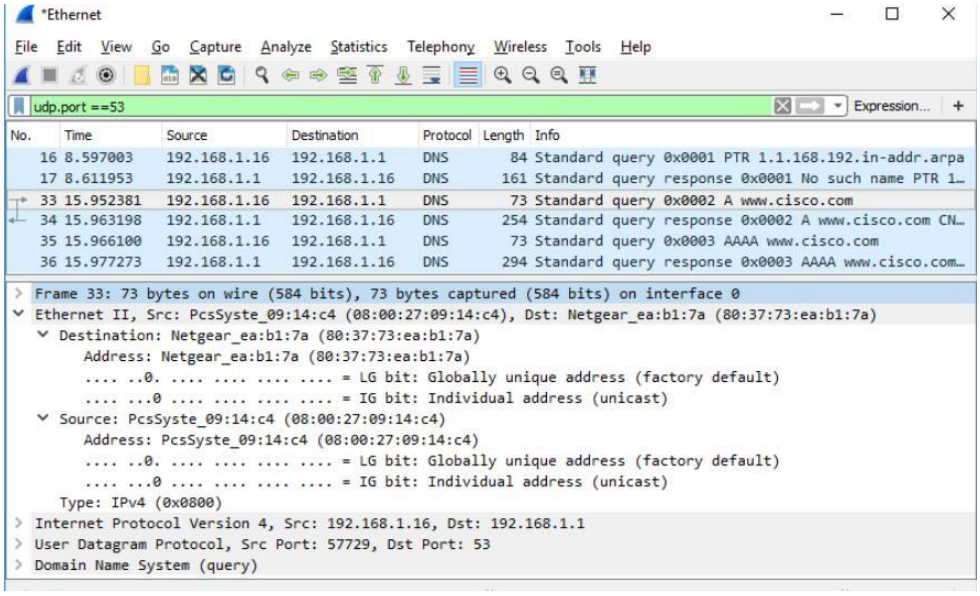
e. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.

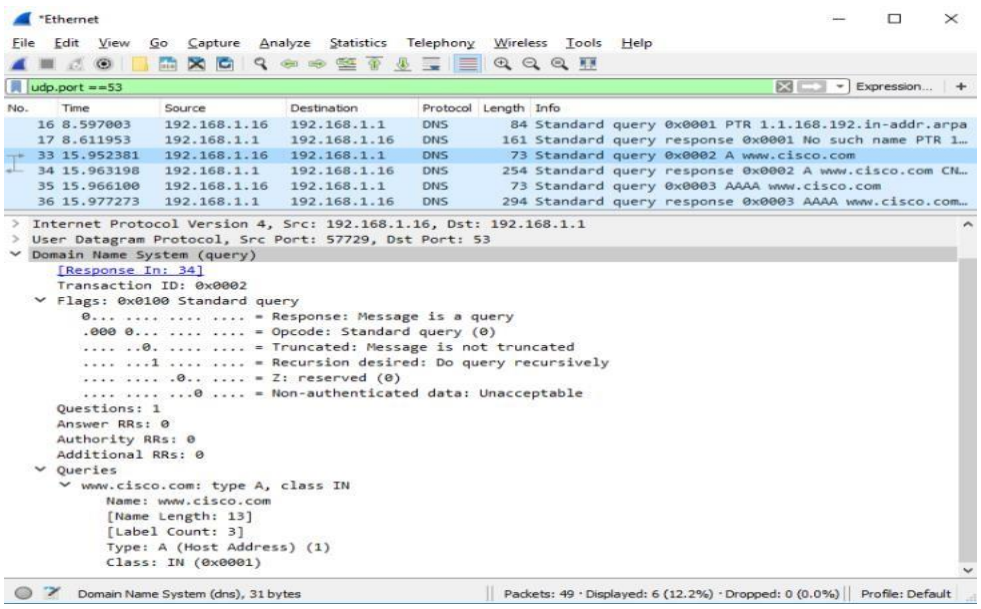
f. Expand the **User Datagram Protocol**. Observe the source and destination ports.

g. Determine the IP and MAC address of the PC.

   1. In a Windows command prompt, enter **arp –a** and **ipconfig /all** to record the MAC and IP addresses of the PC.
   2. For Linux and macOS PC, enter **ifconfig** or **ip address** in a terminal.

h. Expand **Domain Name System (query)** in the Packet Details pane. Then expand the **Flags** and **Queries**.



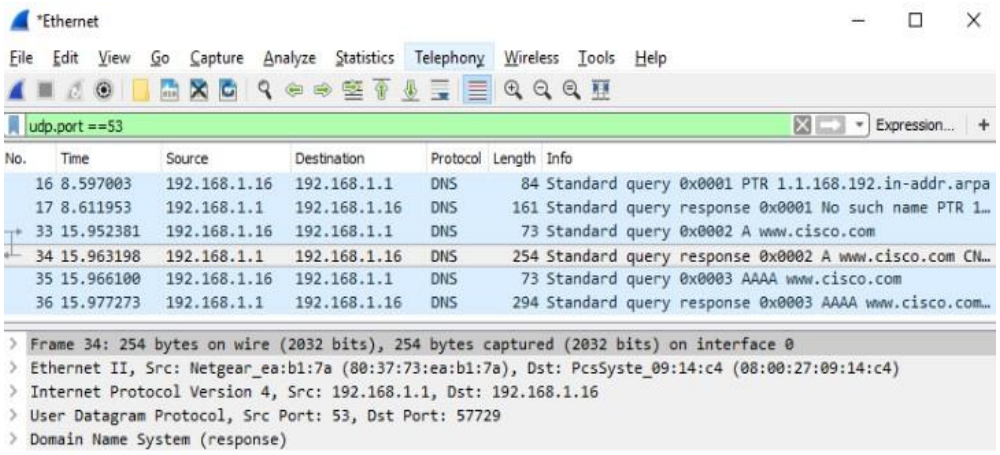


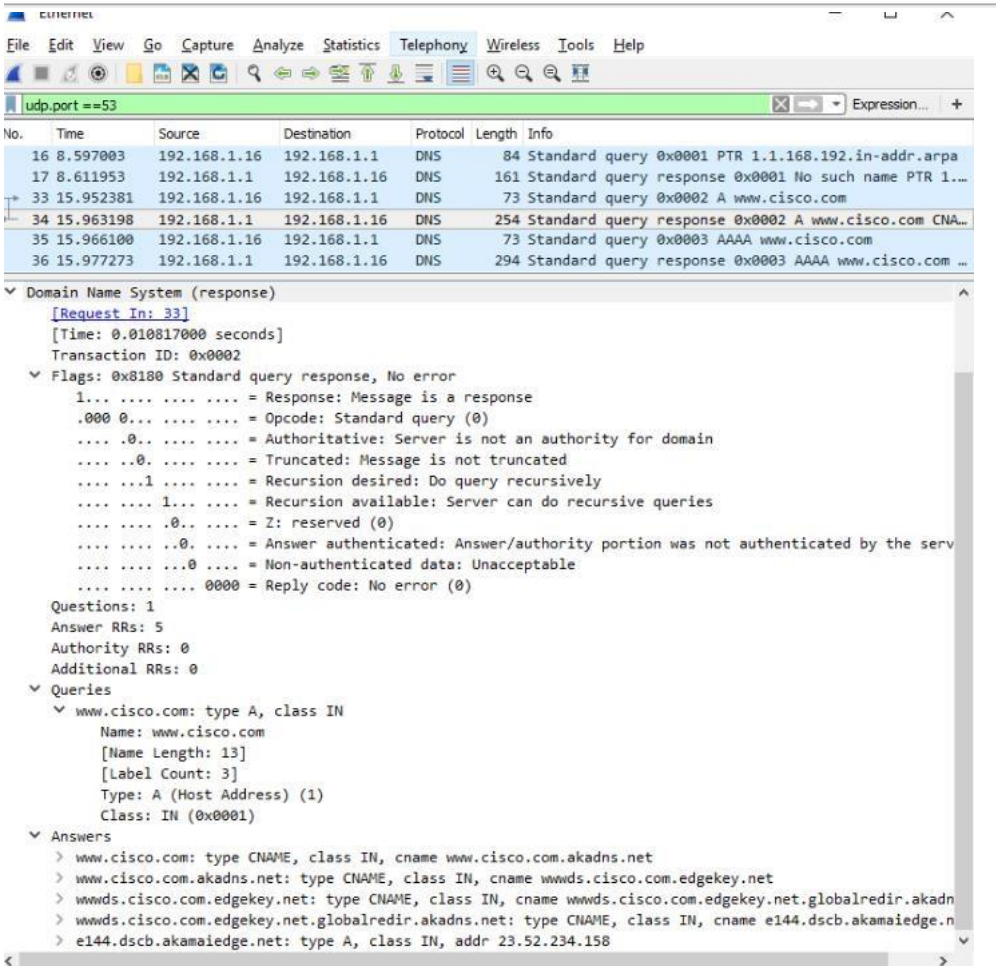
Part 3: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.

b. Expand **Domain Name System (response)**. Then expand the **Flags, Queries,** and **Answers.** c. Observe the results.

d. Observe the CNAME and A records in the Answers details.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port ==53
Expression...
No. Time Source Destination Protocol Length Info
16 8.597003 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17 8.611953 192.168.1.1 192.168.1.16 DNS 161 Standard query response 0x0001 No such name PTR 1…
33 15.952381 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0002 A www.cisco.com
34 15.963198 192.168.1.1 192.168.1.16 DNS 254 Standard query response 0x0002 A www.cisco.com CN…
35 15.966100 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0003 AAAA www.cisco.com
36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com…
Frame 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
User Datagram Protocol, Src Port: 53, Dst Port: 57729
Domain Name System (response)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port ==53
Expression...
No. Time Source Destination Protocol Length Info
16 8.597003 192.168.1.16 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17 8.611953 192.168.1.1 192.168.1.16 DNS 161 Standard query response 0x0001 No such name PTR 1.…
33 15.952381 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0002 A www.cisco.com
34 15.963198 192.168.1.1 192.168.1.16 DNS 254 Standard query response 0x0002 A www.cisco.com CNA…
35 15.966100 192.168.1.16 192.168.1.1 DNS 73 Standard query 0x0003 AAAA www.cisco.com
36 15.977273 192.168.1.1 192.168.1.16 DNS 294 Standard query response 0x0003 AAAA www.cisco.com …
Domain Name System (response)
[Request In: 33]
[Time: 0.010817000 seconds]
Transaction ID: 0x0002
Flags: 0x8180 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
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the serv
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 5
Authority RRs: 0
Additional RRs: 0
Queries
www.cisco.com: type A, class IN
Name: www.cisco.com
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadn
wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e144.dscb.akamaiedge.n
e144.dscb.akamaiedge.net: type A, class IN, addr 23.52.234.158

Practical No.4

A. Using Wireshark to Examine HTTP and HTTPS Traffic

Part 1: Capture and View HTTP Traffic

Step 1: Start the virtual machine and log in.

Start the CyberOps Workstation VM. Use the following user credentials:

Username: analyst

Password: cyberops

Step 2: Open a terminal and start tcpdump.

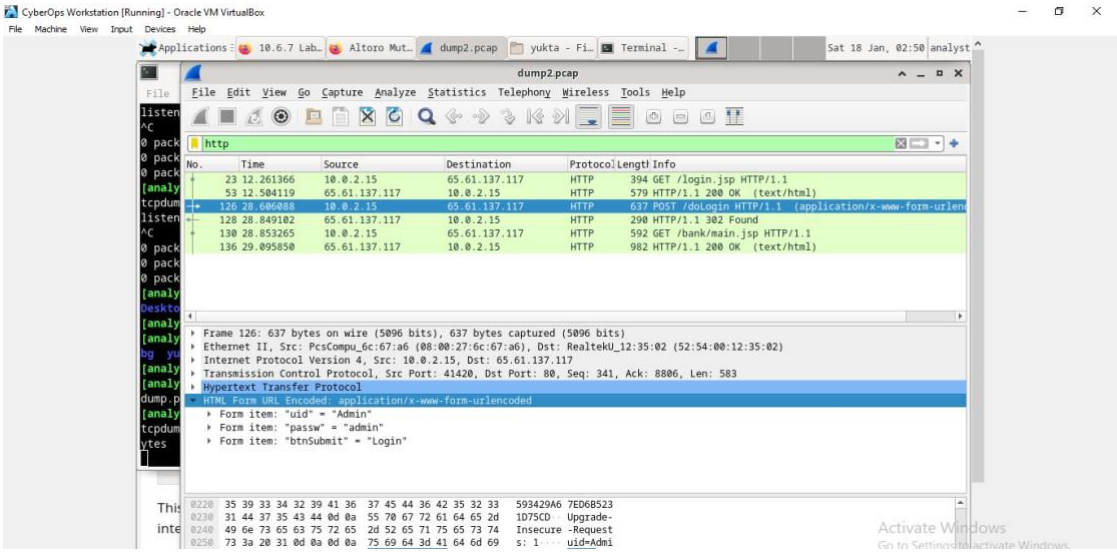
a. Open a terminal application and enter the command ip address.

[analyst@secOps ~]$ ip address

b. List the interfaces and their IP addresses displayed in the ip address output.

c. While in the terminal application, enter the command sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap. Enter the password cyberops for the user analyst when prompted.

[analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap [sudo] password for analyst:



d. Open a web browser from the launch bar within the CyberOps Workstation VM. Navigate t http://www.altoromutual.com/login.jsp

Because this website uses HTTP, the traffic is not encrypted. Click the Password field to see the warning pop up.

e. Enter a username of Admin with a password of Admin and click Login.

f. Close the web browser.

g. Return to the terminal window where tcpdump is running. Enter CTRL+C to stop the packet capture.

Step 3: View the HTTP capture.

a. Click the File Manager icon on the desktop and browse to the home folder for the user analyst. Double-click the httpdump.pcap file, in the Open With dialog box scroll down to Wireshark and then click Open.

b. In the Wireshark application, filter for http and click Apply.

c. Browse through the different HTTP messages and select the POST message.

d. In the lower window, the message is displayed. Expand the HTML Form URL Encoded: application/x-www-form-urlencoded section.

e. Close the Wireshark application.

Part 2: Capture and View HTTPS Traffic Step

1: Start tcpdump within a terminal.

a. While in the terminal application, enter the command sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap. Enter the password cyberops for the user analyst when prompted.
[analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap [sudo] password for analyst: tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

This command will start tcpdump and record network traffic on the enp0s3 interface of the Linux workstation. If your interface is different than enp0s3, please modify it when using the above command.

All recorded traffic will be printed to the file httpsdump.pcap in the home directory of the user analyst.

b. Open a web browser from the launch bar within the CyberOps Workstation VM. Navigate to www.netacad.com.

[analyst@secOps ~]$ sudo date -s "12 MAY 2020 21:38:20

c. Click Log in.

e. Close the web browser in the VM.

f. Return to the terminal window where tcpdump is running. Enter CTRL+C to stop the packet capture.

Step 2: View the HTTPS capture.

The tcpdump executed in Step 1 printed the output to a file named httpsdump.pcap. This file is located in the home directory for the user analyst.

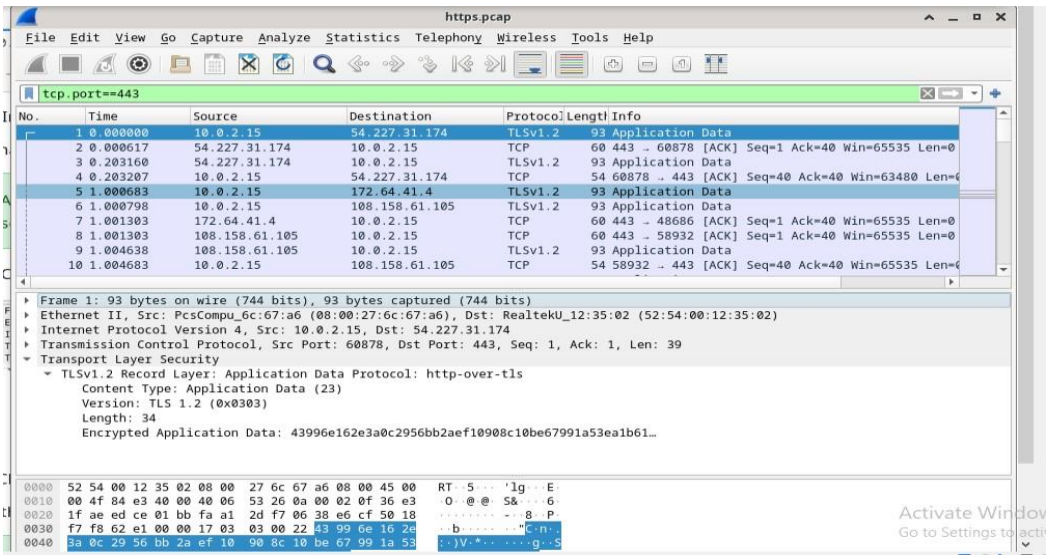
a. Click the Filesystem icon on the desktop and browse to the home folder for the user analyst. Open the httpsdump.pcap file.

b. In the Wireshark application, expand the capture window vertically and then filter by HTTPS traffic via port 443.

Enter tcp.port==443 as a filter, and click Apply.

f. Click the Encrypted Application Data.

g. Close all windows and shut down the virtual machine.



B. Exploring Processes, Threads, Handles, and Windows Registry

Part 1: Exploring Processes

Step 1: Download Windows SysInternals Suite.

a. Navigate to the following link to download Windows SysInternals Suite:
https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

b. After the download is completed, extract the files from the folder.

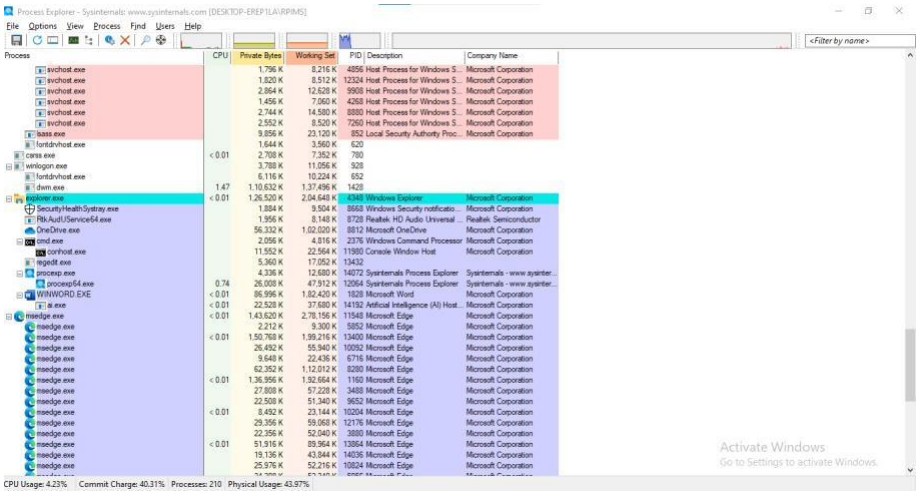
c. Leave the web browser open for the following steps. **Step 2: Explore an active process.**

a. Navigate to the SysinternalsSuite folder with all the extracted files.

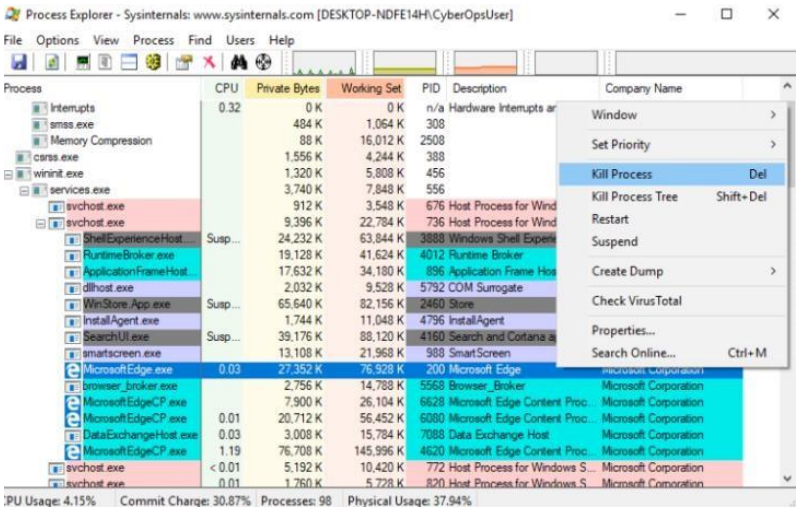
b. Open **procexp.exe**. Accept the Process Explorer License Agreement when prompted.

c. The Process Explorer displays a list of currently active processes.

d. To locate the web browser process, drag the Find Window's Process icon into the opened web browser window. Microsoft Edge was used in this example.



e. The Microsoft Edge process can be terminated in the Process Explorer. Right-click the selected process and select Kill Process. Click OK to continue.



Step 3: Start another process.

a. Open a Command Prompt. (**Start** > search **Command Prompt** > select **Command Prompt**)

b. Drag the **Find Window's Process** icon into the Command Prompt window and locate the highlighted Command Prompt process in Process Explorer.

c. The process for the Command Prompt is cmd.exe. Its parent process is explorer.exe process. The cmd.exe has a child process, conhost.exe.

d. Navigate to the Command Prompt window. Start a ping at the prompt and observe the changes under the cmd.exe process.

Part 2: Exploring Threads and Handles Step

1: Explore threads.

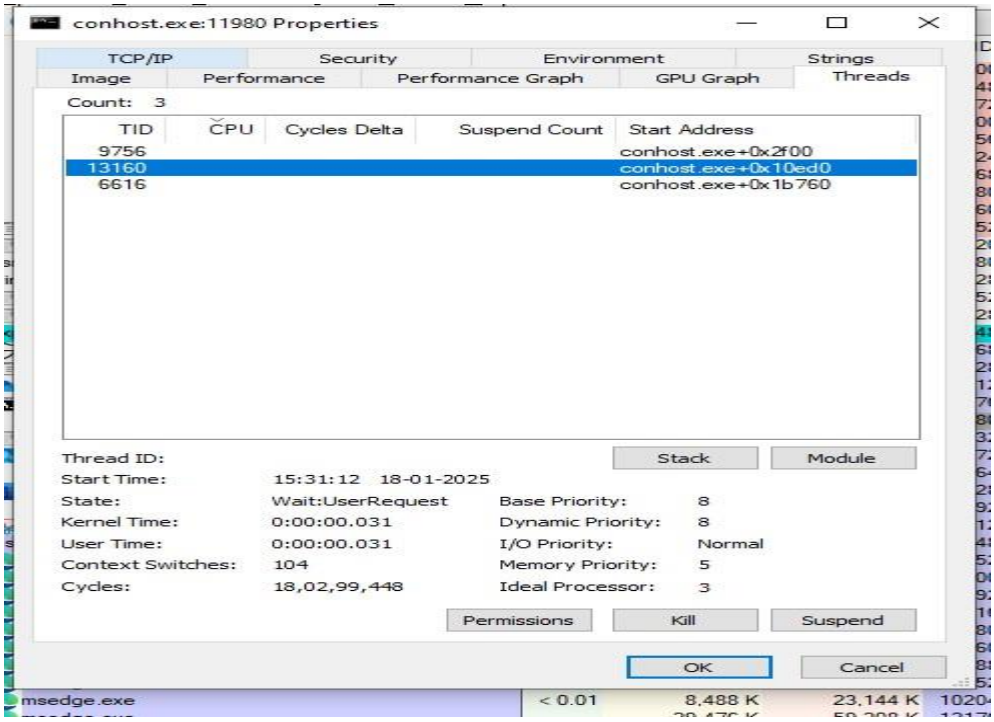
a. Open a command prompt.

b. In Process Explorer window, right-click conhost.exe and Select **Properties…..** Click the **Threads** tab to view the active threads for the conhost.exe process. Click **OK** to continue if prompted by a warning dialog box.

c. Examine the details of the thread

Step 2: Explore handles.

a. In the Process Explorer, click **View** > select **Lower Pane View** > **Handles** to view the handles associated with the conhost.exe process.



Part 3: Exploring Windows Registry

a. To access the Windows Registry, click **Start** > Search for **regedit** and select **Registry Editor**. Click **Yes** when asked to allow this app to make changes.

The Registry Editor has five hives. These hives are at the top level of the registry.

- HKEY_CLASSES_ROOT is actually the Classes subkey of HKEY_LOCAL_MACHINE\Software\. It stores information used by registered applications like file extension association, as well as a programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data.
- HKEY_CURRENT_USER contains the settings and configurations for the users who are currently logged in.
- HKEY_LOCAL_MACHINE stores configuration information specific to the local computer.
- HKEY_USERS contains the settings and configurations for all the users on the local computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS.

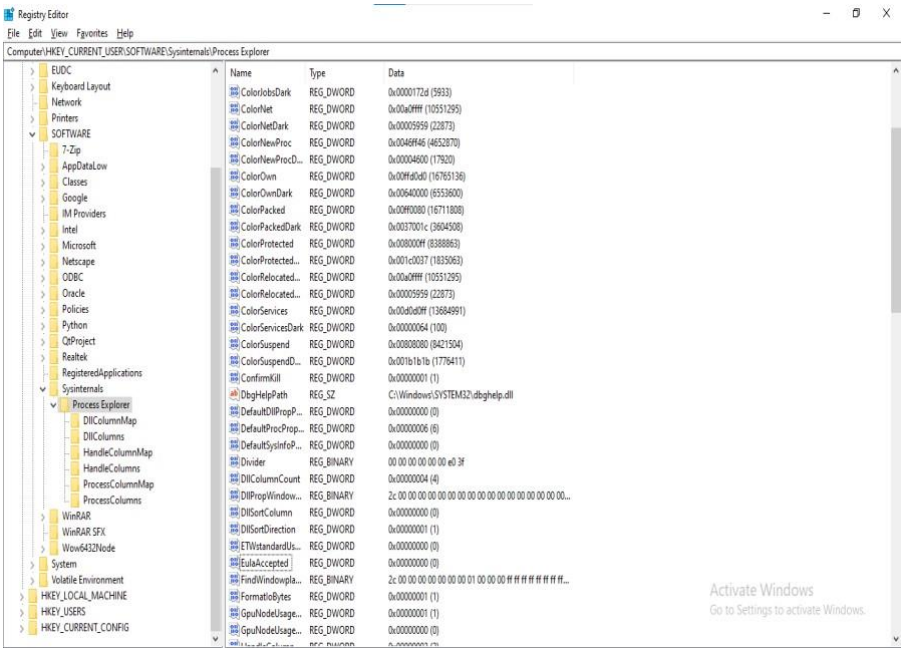
- HKEY_CURRENT_CONFIG stores the hardware information that is used at bootup by the local computer.

b. In a previous step, you had accepted the EULA for Process Explorer. Navigate to the EulaAccepted registry key for Process Explorer.

Click to select Process Explorer in **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer**. Scroll down to locate the key **EulaAccepted**. Currently, the value for the registry key EulaAccepted is 0x00000001(1).

c. Double-click **EulaAccepted** registry key. Currently the value data is set to 1. The value of 1 indicates that the EULA has been accepted by the user.

d. Change the **1** to **0** for Value data. The value of 0 indicates that the EULA was not accepted. Click **OK** to continue.



e. Open the **Process Explorer**. Navigate to the folder where you have downloaded SysInternals. Open the folder **SysInternalsSuite** > Open **procexp.exe.**

Practical No: 5

Perform a practical to Attack on a mySQL Database by using PCAP file.

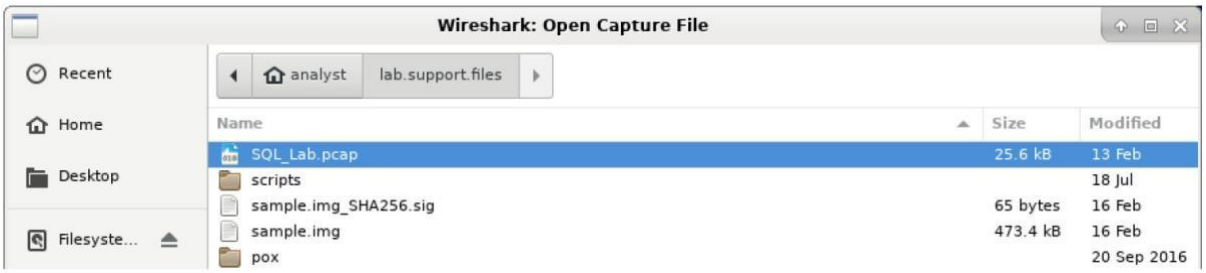
Step 1: Open Wireshark and load the PCAP file.

The Wireshark application can be opened using a variety of methods on a Linux workstation. a. Start the CyberOps Workstation VM

b. Click on Applications > CyberOPS >Wireshark on the desktop and browse to the Wireshark application

c. In the Wireshark application, click Open in the middle of the application under Files.

d. Browse through the /home/analyst/ directory and search for lab.support.files. In the lab.support.files directory and open the SQL_Lab.pcap file.

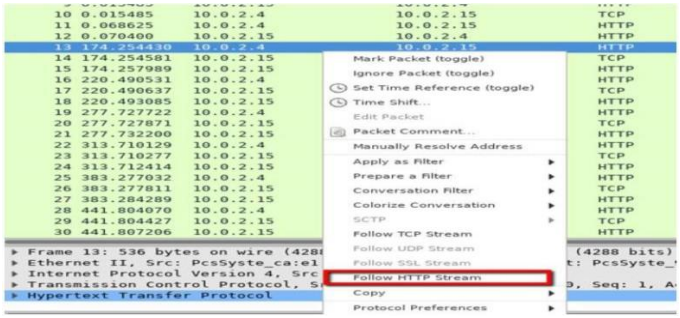


e. The PCAP file opens within Wireshark and displays the captured network traffic. This capture file extends over an 8-minute (441 second) period, the duration of this SQL injection attack.

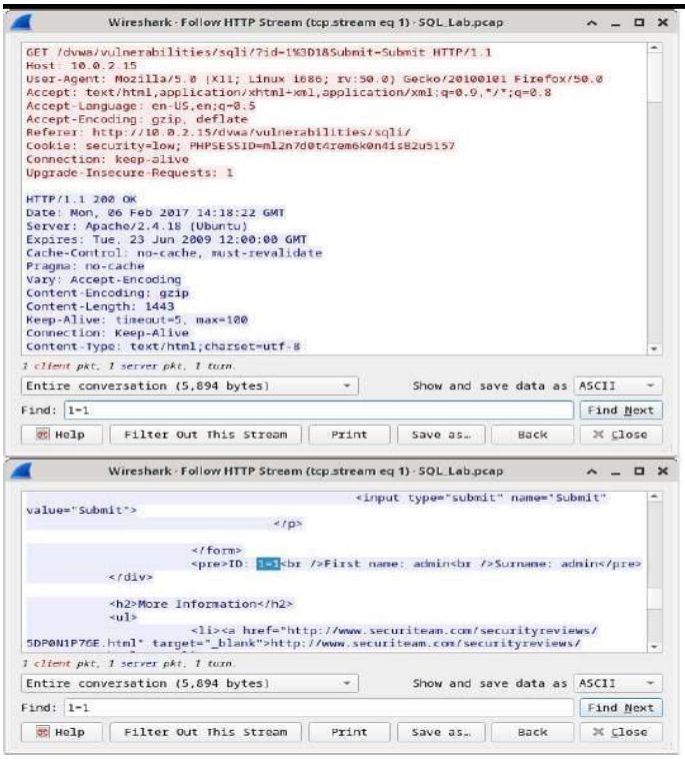
Step 2: View the SQL Injection Attack.

In this step, you will be viewing the beginning of an attack.

a. Within the Wireshark capture, right-click line 13 and select Follow HTTP Stream. Line 13 was chosen because it is a GET HTTP request. This will be very helpful in following the data stream as the application layers sees it and leads up to the query testing for the SQL injection.



The source traffic is shown in red. The source has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.



b. Click Find and enter 1=1. Search for this entry. When the text is located, click Cancel in the Find text search box. The string 1=1

c. The attacker has entered a query (1=1) into a UserID search box on the target 10.0.2.15 to see if the application is vulnerable to SQL injection. Instead of the application responding with a login failure message, it responded with a record from a database. The attacker has verified they can input an SQL command and the database will respond. The search string 1=1 creates an SQL statement that will be always true. In the example, it does not matter what is entered into the field, it will always be true. d. Close the Follow HTTP Stream window.

e. Click Clear to display the entire Wireshark conversation.

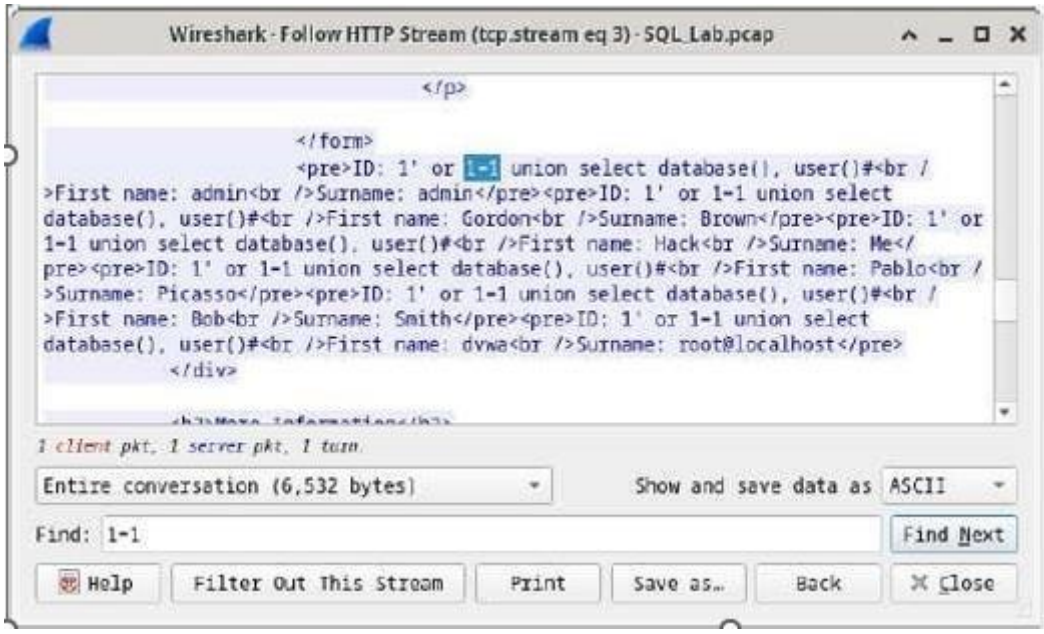
Step 3: The SQL Injection Attack continues…

In this step, you will be viewing the continuation of an attack.

a. Within the Wireshark capture, right-click line 19, and select Follow HTTP Stream.

b. Click Find and enter 1=1. Search for this entry. When the text is located, click Cancel in the Find text search box.

c. The attacker has entered a query (1' or 1=1 union select database(), user()) into a UserID search box on the target 10.0.2.15. Instead of the application responding with a login failure message, it responded with the following information:



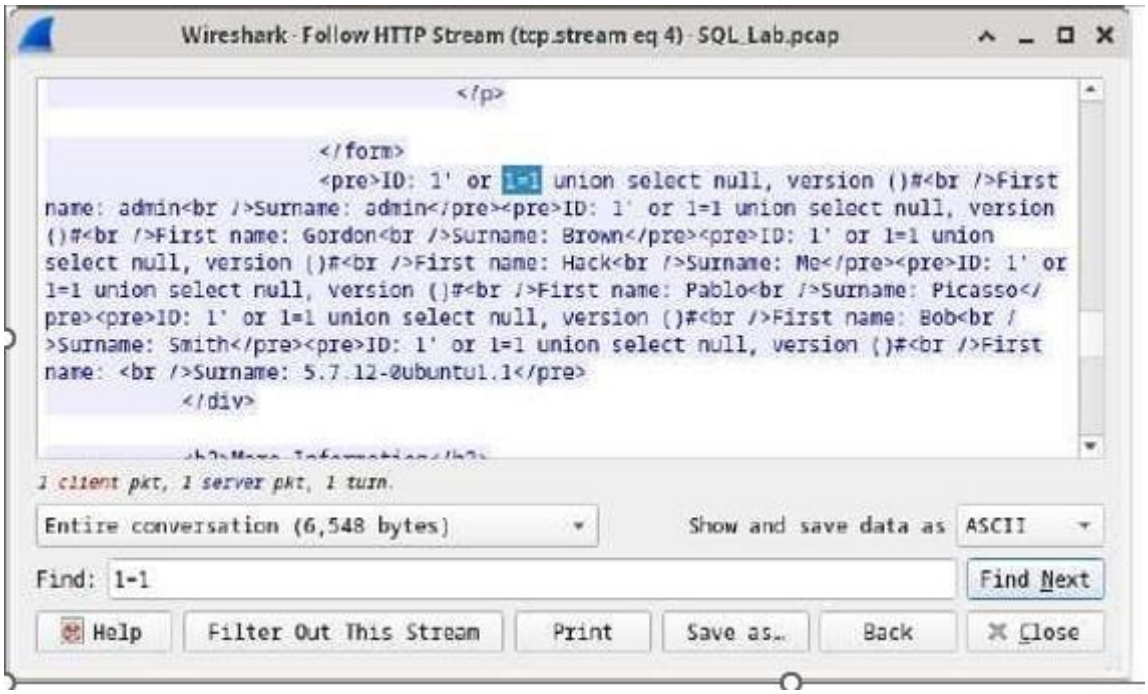
The database name is dvwa and the database user is dvwa@localhost. There are also multiple user accounts being displayed.

d. Close the Follow HTTP Stream window.

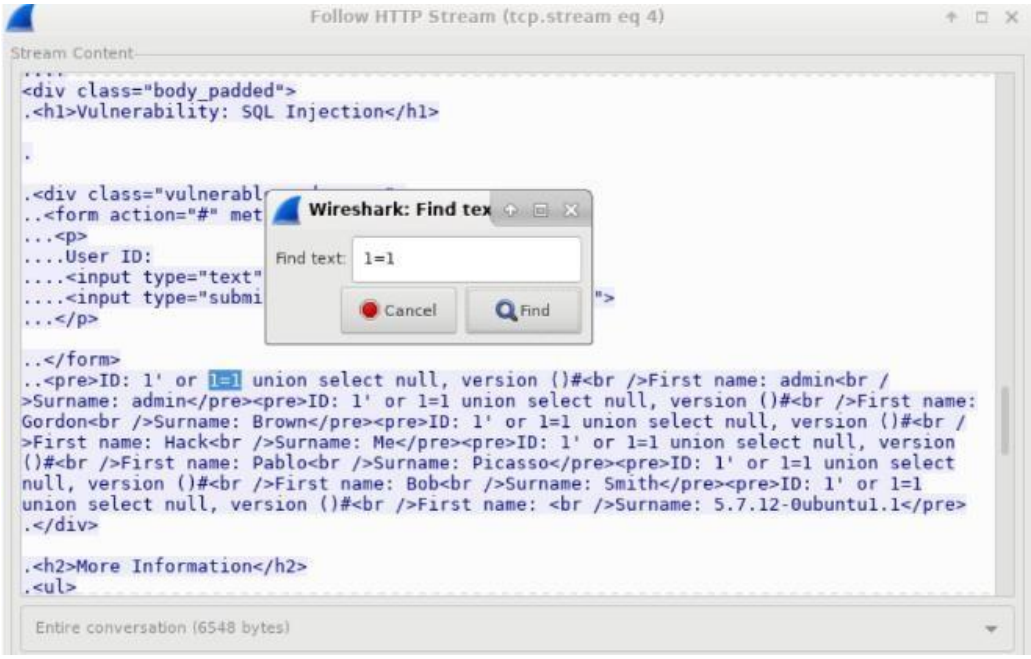
e. Click "Clear" to display the entire Wireshark conversation.

Step 4: The SQL Injection Attack provides system information. The attacker continues and starts targeting more specific information.

a. Within the Wireshark capture, right-click line 22 and select Follow HTTP Stream. In red, the source traffic is shown and is sending the GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.



b. Click Find and type in 1=1. Search for this entry. When the text is located, click Cancel in the Find text search box.



c. The attacker has entered a query (1' or 1=1 union select null, version ()) into a UserID search box on the target 10.0.2.15 to locate the version identifier. Notice how the version identifier is at the end of the output right before the </pre>. closing HTML code.

d. Close the Follow HTTP Stream window.

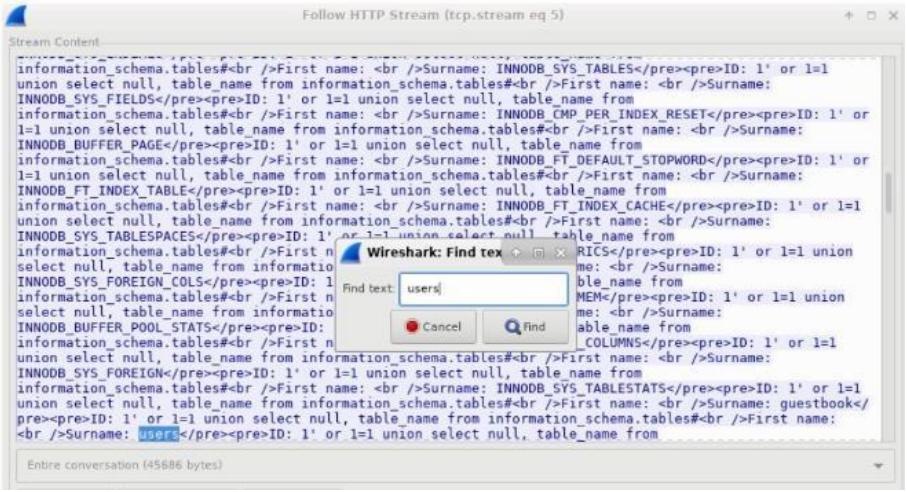
e. Click Clear to display the entire Wireshark conversation.

Step 5: The SQL Injection Attack and Table Information.

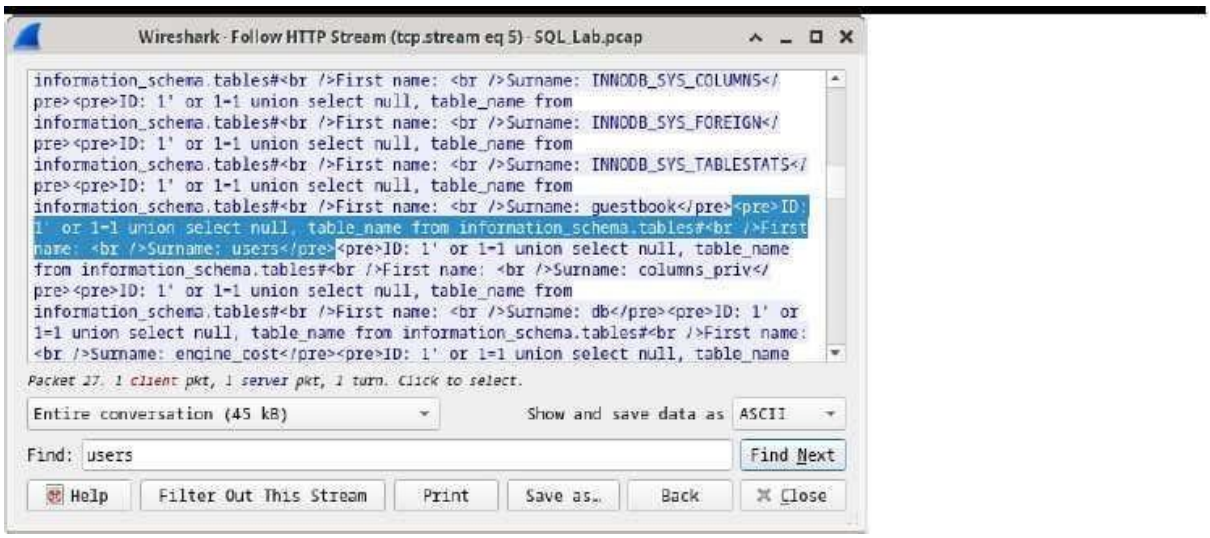
The attacker knows that there is a large number of SQL tables that are full of information. The attacker attempts to find them.

a. Within the Wireshark capture, right-click on line 25 and select Follow HTTP Stream. The source is shown in red. It has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source.

b. Click Find and enter users. Search for the entry displayed below. When the text is located, click Cancel in the Find text search box.



c. The attacker has entered a query (1'or 1=1 union select null, table_name from information_schema.tables) into a UserID search box on the target 10.0.2.15 to view all the tables in the database. This provides a huge output of many tables, as the attacker specified "null" without any further specifications.



d. Close the Follow HTTP Stream window.

e. Click Clear display filter to display the entire Wireshark conversation Step 6: The SQL Injection Attack Concludes.

The attack ends with the best prize of all; password hashes.

a. Within the Wireshark capture, right-click line 28 and select Follow HTTP Stream. The source is shown in red. It has sent a GET request to host 10.0.2.15. In blue, the destination device is responding back to the source

c.Click Find and type in 1=1. Search for this entry. When the text is located, click Cancel in the Find text search box.

The attacker has entered a query (1'or 1=1 union select user, password from users) into a UserID search box on the target 10.0.2.15 to pull usernames and password hashes! c. Close the Follow HTTP Stream window. Close any open windows.

Practical No: 6

Create your own syslog Server

Step 1: Install the syslog server

Open a terminal on your Ubuntu system.

Update the package repository:

sudo apt update

Install rsyslog, which is the default syslog daemon on most Linux distributions:

sudo apt install rsyslog -y

Step 2: Enable and start the rsyslog service Enable the service to start automatically on boot:

sudo systemctl enable rsyslog

Start the rsyslog service: **sudo systemctl start rsyslog** Verify that the service is running: **sudo systemctl status rsyslog**

```
snc@snc-VirtualBox:~$ sudo systemctl restart rsyslog
Warning: The unit file, source configuration file or drop-ins of rsyslog.service changed on disk. Run 'systemctl daemon-
reload' to reload units.
snc@snc-VirtualBox:~$ sudo tail -f /var/log/syslog
2025-01-19T14:06:42+05:30 snc-VirtualBox rsyslogd[60168]: rsyslog internal message (4,-3000): main Q: need to do hard ca
ncellation [v8.2312.0]
2025-01-19T14:06:42+05:30 snc-VirtualBox systemd[1]: rsyslog.service: Deactivated successfully.
2025-01-19T14:06:42+05:30 snc-VirtualBox systemd[1]: Stopped rsyslog.service - System Logging Service.
2025-01-19T14:06:42+05:30 snc-VirtualBox systemd[1]: rsyslog.service: Consumed 1.937s CPU time.
2025-01-19T14:06:42+05:30 snc-VirtualBox systemd[1]: Starting rsyslog.service - System Logging Service...
2025-01-19T14:06:42+05:30 snc-VirtualBox rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) f
rom systemd.  [v8.2312.0]
2025-01-19T14:06:42+05:30 snc-VirtualBox kernel: audit: type=1400 audit(1737275802.489:243): apparmor="STATUS" operation
="profile_replace" info="same as current profile, skipping" profile="unconfined" name="rsyslogd" pid=60518 comm="apparmo
r_parser"
2025-01-19T14:06:42+05:30 snc-VirtualBox systemd[1]: Started rsyslog.service - System Logging Service.
2025-01-19T14:06:42+05:30 snc-VirtualBox rsyslogd: rsyslogd's groupid changed to 102
2025-01-19T14:06:42+05:30 snc-VirtualBox rsyslogd[60168]: rsyslog internal message (4,-3000): main Q: need to do hard ca
ncellation [v8.2312.0]
```

Step 3: Configure rsyslog to receive remote logs

1. Open the rsyslog configuration file:

sudo nano /etc/rsyslog.conf

2. Locate the following lines and uncomment them (remove the):
   - For TCP logging:

module(load="imtcp")

input(type="imtcp" port="514")

   - For UDP logging:

module(load="imudp")

input(type="imudp" port="514")

3. Save the file and exit (in Nano, press CTRL+O, Enter, and CTRL+X).

Step 5: Restart the rsyslog service

Restart rsyslog to apply the configuration changes:

sudo systemctl restart rsyslog

```
  GNU nano 7.2                    /etc/rsyslog.conf
#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

*.* @0.0.0.0:514
*.* @@0.0.0.0:514

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Step 6: Verify the syslog server configuration

Check that the server is listening on the appropriate ports:

sudo netstat -tulnp | grep 514

You should see entries for both TCP and UDP on port 514.

Test logging from a remote client:

On the client machine, use the logger command to send a test message:

logger -n <syslog_server_ip> -P 514 "Test message from client" Replace <syslog_server_ip> with the IP address of your syslog server.

Check the logs on the syslog server to confirm receipt of the message: **sudo tail -f /var/log/syslog**

```
snc@snc-VirtualBox:~$ sudo ss -tulnp | grep 514
udp   UNCONN 0      0            0.0.0.0:514        0.0.0.0:*    users:(("rsyslogd",pid=59532,fd=5))
udp   UNCONN 0      0               [::]:514           [::]:*    users:(("rsyslogd",pid=59532,fd=6))
tcp   LISTEN 0      25           0.0.0.0:514        0.0.0.0:*    users:(("rsyslogd",pid=59532,fd=7))
tcp   LISTEN 0      25              [::]:514           [::]:*    users:(("rsyslogd",pid=59532,fd=8))
snc@snc-VirtualBox:~$ sudo nano /etc/rsyslog.conf
snc@snc-VirtualBox:~$ sudo nano /etc/rsyslog.conf
snc@snc-VirtualBox:~$ sudo systemctl restart rsyslog
Warning: The unit file, source configuration file or drop-ins of rsyslog.service changed on disk. Run 'systemctl daemon-
reload' to reload units.
snc@snc-VirtualBox:~$ sudo tail -f /var/log/syslog
2025-01-19T14:02:31+05:30 snc-VirtualBox kernel: audit: type=1400 audit(1737275551.765:242): apparmor="STATUS" operation
="profile_replace" info="same as current profile, skipping" profile="unconfined" name="rsyslogd" pid=60167 comm="apparmo
r_parser"
2025-01-19T14:02:31+05:30 snc-VirtualBox systemd[1]: Stopping rsyslog.service - System Logging Service...
2025-01-19T14:02:31+05:30 snc-VirtualBox systemd[1]: rsyslog.service: Deactivated successfully.
2025-01-19T14:02:31+05:30 snc-VirtualBox rsyslogd: [origin software="rsyslogd" swVersion="8.2312.0" x-pid="59532" x-info
="https://www.rsyslog.com"] exiting on signal 15.
2025-01-19T14:02:31+05:30 snc-VirtualBox systemd[1]: Stopped rsyslog.service - System Logging Service.
2025-01-19T14:02:31+05:30 snc-VirtualBox systemd[1]: Starting rsyslog.service - System Logging Service...
2025-01-19T14:02:31+05:30 snc-VirtualBox rsyslogd: [origin software="rsyslogd" swVersion="8.2312.0" x-pid="60168" x-info
="https://www.rsyslog.com"] start
2025-01-19T14:02:31+05:30 snc-VirtualBox kernel: audit: type=1400 audit(1737275551.765:242): apparmor="STATUS" operation
="profile_replace" info="same as current profile, skipping" profile="unconfined" name="rsyslogd" pid=60167 comm="apparmo
r_parser"
2025-01-19T14:02:31+05:30 snc-VirtualBox systemd[1]: Stopping rsyslog.service - System Logging Service...
2025-01-19T14:02:31+05:30 snc-VirtualBox systemd[1]: rsyslog.service: Deactivated successfully.
```

Practical no:7

Configure your Linux system to send syslog messages to a syslog server and Read them.

Step 1: Update the package repository

1. Install Required Packages:

Open the terminal and update your package list: **sudo**

apt update

Install rsyslog (if not already installed):

sudo apt install rsyslog

Check if the rsyslog service is running:

systemctl status rsyslog

2. Configure Rsyslog to Send Logs to a Remote Syslog Server:

- Edit the rsyslog configuration file on the client machine:

sudo nano /etc/rsyslog.conf

- Enable the preservation of FQDN (Fully Qualified Domain Name):

$PreserveFQDN on

- Add the following line to send logs to the remote syslog server (replace ip-addressof-rsyslog-server with the IP address or FQDN of your syslog server):
  - For UDP (use a single @):

. @ip-address-of-rsyslog-server:514 ○

For TCP (use double @@):

. @@ip-address-of-rsyslog-server:514

- (Optional) Add the following lines to handle cases where the syslog server is down:
- **$ActionQueueFileName queue**
- **$ActionQueueMaxDiskSpace 1g**
- **$ActionQueueSaveOnShutdown on**
- **$ActionQueueType LinkedList**

$ActionResumeRetryCount -1 •

Save and close the file.

3. Restart Rsyslog Service on the Client:

- Restart the rsyslog service to apply the changes:

sudo systemctl restart rsyslog

4. Verify Logs on the Syslog Server:

- On the syslog server, ensure that rsyslog is configured to receive logs (refer to the previous guide for setting up the syslog server).
- **Check the logs stored in /var/log/ on the syslog server:**

ls /var/log/

- Navigate to the directory corresponding to the client hostname to view its logs:

ls /var/log/client-hostname/

- Use cat, tail, or less to read the log files:

cat /var/log/client-hostname/syslog.log

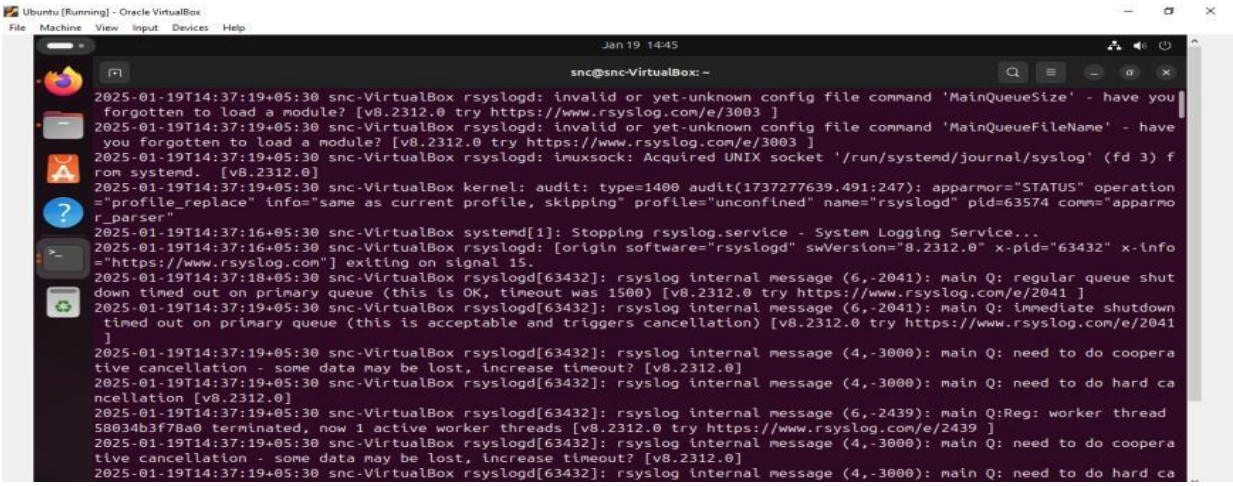
5. (Optional) Test Log Forwarding:

- On the client machine, generate a test log message:

logger "This is a test log message from the client."

- On the syslog server, check the logs to ensure the test message was received:

grep "This is a test log message" /var/log/client-hostname/syslog.log



Practical No:8

Install and Run Splunk on Linux

Step 1: Prerequisites

Before we begin, ensure that your Ubuntu system meets the following requirements:

- A supported version of Ubuntu (e.g., Ubuntu 20.04 LTS).
- Sufficient disk space and system resources.
- Access to the internet for downloading the Splunk Enterprise package.

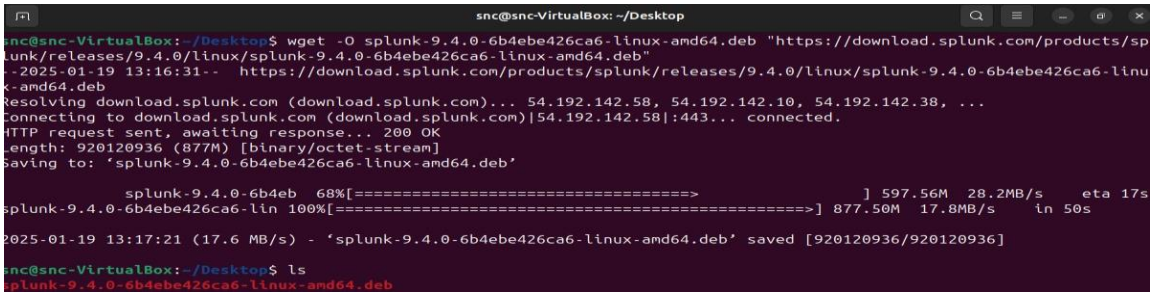
Step 2: Download Splunk Enterprise (SE)

Step 3: Install Splunk Enterprise

1. Open a terminal on your Ubuntu system.
2. Navigate to the Downloads directory where the Splunk Enterprise package is to be downloaded. (***cd Downloads***)
3. Paste and run the command gotten from the Splunk site to download Splunk Enterprise.
4. To view the downloaded file type:

Installer: wget -O splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb "https://download.splunk.com/products/splunk/releases/9.4.0/linux/splunk-9.4.0-6b4ebe426ca6 linux-amd64.deb"

ls



5. **Next, run this command to install Splunk Enterprise:**

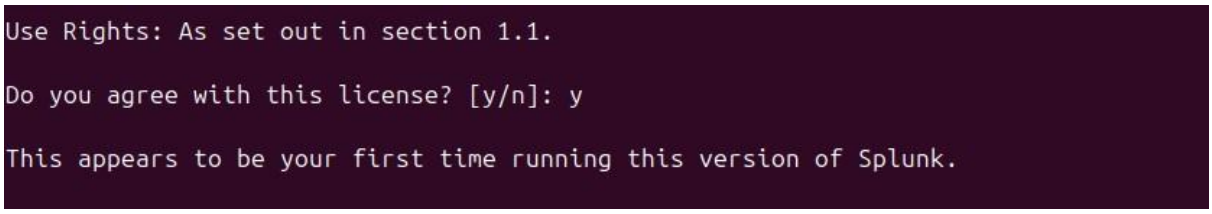
sudo apt install ./splunk<version>.deb

Note: Replace `<version>` with the actual version number of the downloaded Splunk Enterprise package. (tip: copy and paste the splunk file)

4. After the installation completes, start Splunk Enterprise by running:

***sudo /opt/splunk/bin/splunk start — accept-license* 5.**

Type ***'y'*** to agree with the license**.**



6.Splunk Enterprise will prompt you to create an administrator password. Follow the instructions to set a secure password.

Step 4: Access Splunk Enterprise Web Interface 1.

Start up the Splunk web interface by running:

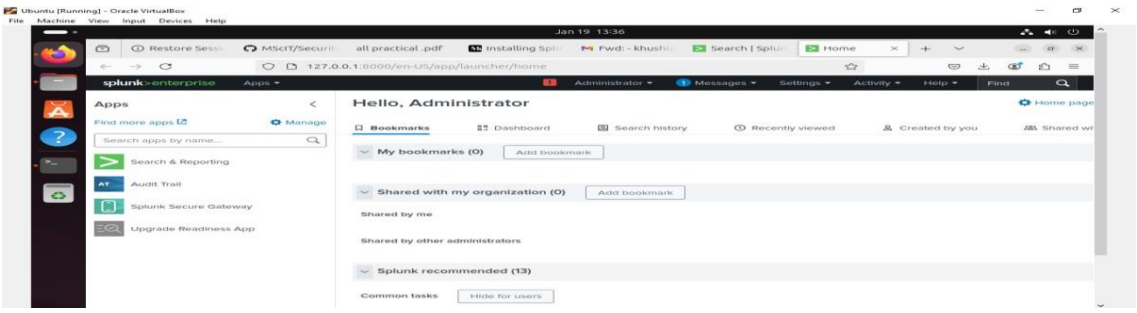
sudo /opt/splunk/bin/splunk start

```
Invalid mode "-".
snc@snc-VirtualBox:~/Desktop$ sudo /opt/splunk/bin/splunk start

Splunk> Needle. Haystack. Found.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
                Creating: /opt/splunk/var/lib/splunk
                Creating: /opt/splunk/var/run/splunk
                Creating: /opt/splunk/var/run/splunk/appserver/i18n
                Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunk/var/run/splunk/upload
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/run/splunk/search_log
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/var/lib/splunk/hashDb
```

3. After loading, right click on the link beside “The Splunk web interface is at” and click-on Open Link

```
Signature ok
subject=/CN=snc-VirtualBox/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib librarie
s shipped with the embedded Python interpreter; must be set to "1" for increased security
Done


Waiting for web server at http://127.0.0.1:8000 to be available..................................... Done
```

4. The Splunk Enterprise login page should appear. Enter the username and password you set in the Step 3 (6).
5. Once logged in, you can start using Splunk Enterprise to ingest, search, and analyze your data.



Practical No:9

Install and Configure ELK on Linux

Part A: Installing and Configuring Elasticsearch

Step 1: Install Java

Elasticsearch requires Java to run. Install the default JDK and JRE:

bash

sudo apt install default-jdk default-jre -y

Verify the installation:

bash

javac --version

Step 2: Add Elasticsearch Repository

1. Import the Elasticsearch GPG key:

   bash

   curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

2. Add the Elasticsearch repository:

   bash

   sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'

3. Update the package list:

   bash

   sudo apt update

Step 3: Install Elasticsearch

Install Elasticsearch using the following command:

bash

sudo apt install elasticsearch -y

Step 4: Configure Elasticsearch

4.1: Configure elasticsearch.yml

Edit the configuration file:

bash

sudo nano /etc/elasticsearch/elasticsearch.yml

Add or modify the following settings:

yaml

#Network settings

network.host: localhost

http.port: 9200

#Path settings

path.data: /var/lib/elasticsearch

path.logs: /var/log/elasticsearch

4.2: Configure JVM Options

1. Backup the original jvm.options file:

   bash

   sudo cp /etc/elasticsearch/jvm.options /etc/elasticsearch/jvm.options.backup

2. Edit the jvm.options file:

   bash

   sudo nano /etc/elasticsearch/jvm.options

3. Add or modify the following settings:

Heap Size Settings
-Xms512m
-Xmx512m
#GC Configuration
8-13:-XX:+UseConcMarkSweepGC
8-13:-XX:CMSInitiatingOccupancyFraction=75
8-13:-XX:+UseCMSInitiatingOccupancyOnly
G1GC Configuration
14-:-XX:+UseG1GC
#JVM Temporary Directory
-Djava.io.tmpdir=${ES_TMPDIR}
Heap Dumps
-XX:+HeapDumpOnOutOfMemoryError
-XX:HeapDumpPath=/var/lib/elasticsearch
Error Logs
-XX:ErrorFile=/var/log/elasticsearch/hs_err_pid%p.log
#GC Logging
9-:-
Xlog:gc,gc+age=trace,safepoint:file=/var/log/elasticsearch/gc.log:utctime,pid,tags:filecount=32,filesize=64m

Step 5: Set Proper Permissions

1. Set ownership and permissions for jvm.options:
   bash
   sudo chown root:elasticsearch /etc/elasticsearch/jvm.options
   sudo chmod 660 /etc/elasticsearch/jvm.options
2. Create and set permissions for the temporary directory:
   bash
   sudo mkdir -p /var/tmp/elasticsearch
   sudo chown elasticsearch:elasticsearch /var/tmp/elasticsearch
   sudo chmod 750 /var/tmp/elasticsearch
3. Set permissions for Elasticsearch directories:
   bash
   sudo chown -R elasticsearch:elasticsearch /var/lib/elasticsearch
   sudo chown -R elasticsearch:elasticsearch /var/log/elasticsearch
   sudo chmod -R 750 /var/lib/elasticsearch
   sudo chmod -R 750 /var/log/elasticsearch

Step 6: Start and Enable Elasticsearch

1. Reload the systemd daemon:
   bash
   sudo systemctl daemon-reload
2. Start Elasticsearch:
   bash
   sudo systemctl start elasticsearch
3. Enable Elasticsearch to start on boot:
   bash
   sudo systemctl enable elasticsearch
4. Check the status of Elasticsearch:
   Bash

sudo systemctl status elasticsearch

Step 7: Verify Installation

Test the Elasticsearch REST API:

bash

curl -X GET "localhost:9200"

Expected output:

```
json
{
  "name" : "Ideapad",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "...",
  "version" : {
    "number" : "7.17.27",
    ...
  },
  "tagline" : "You Know, for Search"
}
```

Part B: Installing and Configuring Logstash

Step 1: Install Logstash

Install Logstash using the following command:

bash

sudo apt install logstash -y

Step 2: Start and Enable Logstash

1. Start Logstash:
   bash
   sudo systemctl start logstash
2. Enable Logstash to start on boot:
   bash
   sudo systemctl enable logstash

Part C: Installing and Configuring Kibana

Step 1: Install Kibana

Install Kibana using the following command:

bash

sudo apt install kibana -y

Step 2: Configure Kibana

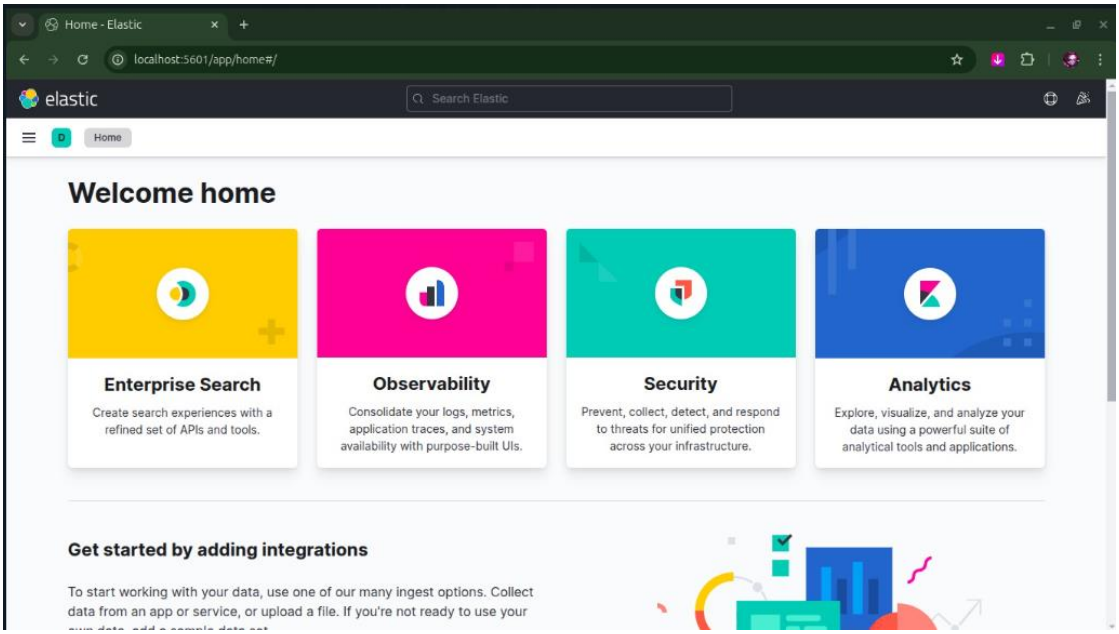
1. Edit the Kibana configuration file:
   bash
   sudo nano /etc/kibana/kibana.yml
   2. Uncomment and modify the following settings:
   yaml
   server.port: 5601
   server.host: "localhost"
   elasticsearch.hosts: ["http://localhost:9200"]

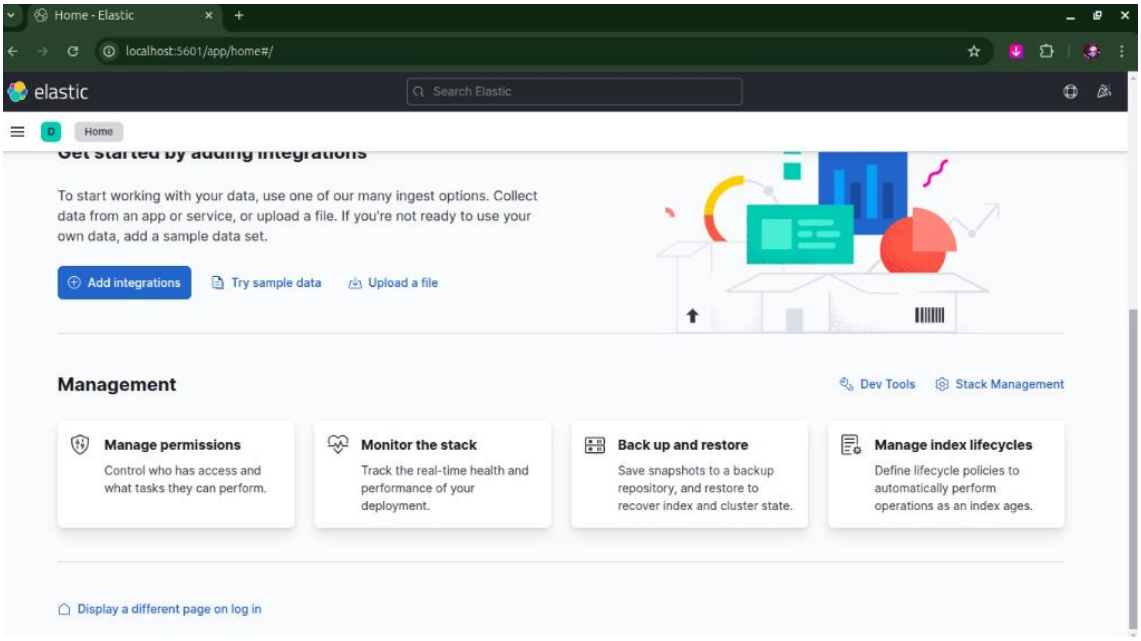
Step 3: Start and Enable Kibana

1. Start Kibana:
   sudo systemctl start kibana
2. Enable Kibana to start on boot:
   sudo systemctl enable kibana

Step 4: Access Kibana

1. Open a web browser and navigate to:
   http://localhost:5601
3. You should see the Kibana interface, indicating that the ELK Stack is running successfully.





Practical No: 10

Install and Configure GrayLog on Linux

1. First, install the prerequisites:

bash
sudo apt-get update
sudo apt-get install apt-transport-https openjdk-11-jre-headless uuid-runtime pwgen

2. Install MongoDB:

bash
sudo apt-get install mongodb-server

3. Install and configure Elasticsearch:

bash
Add Elasticsearch repository
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/oss-7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
# Install Elasticsearch
sudo apt-get update
sudo apt-get install elasticsearch-oss
# Configure Elasticsearch
sudo nano /etc/elasticsearch/elasticsearch.yml
Add these lines to elasticsearch.yml:
yaml
cluster.name: graylog
action.auto_create_index: false

4. Start and enable Elasticsearch:

bash
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch

5. Install Graylog:

bash
Add Graylog repository
wget https://packages.graylog2.org/repo/packages/graylog-4.3-repository_latest.deb
sudo dpkg -i graylog-4.3-repository_latest.deb
sudo apt-get update
Install Graylog server
sudo apt-get install graylog-server

6. Configure Graylog:

bash
Generate password secret
pwgen -N 1 -s 96
Generate admin password hash (replace 'your_password' with desired password)
echo -n "your_password" | sha256sum | cut -d" " -f1

7. Edit Graylog configuration:

bash
sudo nano /etc/graylog/server/server.conf

Add/modify these important settings:
conf
password_secret = <paste_generated_secret_here>
root_password_sha2 = <paste_password_hash_here>

http_bind_address = 0.0.0.0:9000

8. Start and enable Graylog:

bash

sudo systemctl daemon-reload

sudo systemctl enable graylog-server

sudo systemctl start graylog-server

9. Check the status:

bash

sudo systemctl status elasticsearch

sudo systemctl status mongodb

sudo systemctl status graylog-server

```
● mongod.service - MongoDB Database Server
     Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-01-22 12:19:07 IST; 2s ago
       Docs: https://docs.mongodb.org/manual
   Main PID: 17819 (mongod)
     Memory: 88.3M (peak: 88.6M)
        CPU: 748ms
     CGroup: /system.slice/mongod.service
             └─17819 /usr/bin/mongod --config /etc/mongod.conf

Jan 22 12:19:07 Ideapad systemd[1]: Started mongod.service - MongoDB Database Server.
Jan 22 12:19:07 Ideapad mongod[17819]: {"t":{"$date":"2025-01-22T06:49:07.525Z"},"s":"I",  "c":"CONTROL",  "id":7484500, "ctx":"main",>
❯ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-01-22 12:00:56 IST; 18min ago
       Docs: https://www.elastic.co
   Main PID: 1813 (java)
      Tasks: 94 (limit: 9265)
     Memory: 1.3G (peak: 1.6G swap: 2.8M swap peak: 2.8M)
        CPU: 1min 30.217s
     CGroup: /system.slice/elasticsearch.service
             ├─1813 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.nega>
             └─3000 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jan 22 12:53:59 Ideapad systemd[1]: Starting elasticsearch.service - Elasticsearch...
Jan 22 12:00:33 Ideapad systemd-entrypoint[1813]: Jan 22, 2025 12:00:33 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
Jan 22 12:00:33 Ideapad systemd-entrypoint[1813]: WARNING: COMPAT locale provider will be removed in a future release
Jan 22 12:00:56 Ideapad systemd[1]: Started elasticsearch.service - Elasticsearch.
❯ sudo systemctl status graylog-server

● graylog-server.service - Graylog server
     Loaded: loaded (/usr/lib/systemd/system/graylog-server.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-01-22 12:53:59 IST; 33min left
       Docs: http://docs.graylog.org/
   Main PID: 1815 (graylog-server)
      Tasks: 129 (limit: 9265)
     Memory: 939.7M (peak: 940.2M)
        CPU: 54.416s
     CGroup: /system.slice/graylog-server.service
             ├─1815 /bin/sh /usr/share/graylog-server/bin/graylog-server
             └─1965 /usr/bin/java -Xms1g -Xmx1g -XX:NewRatio=1 -server -XX:+ResizeTLAB -XX:-OmitStackTraceInFastThrow -Djdk.tls.acknow>
```

10. Configure firewall (if enabled):

bash

sudo ufw allow 9000/tcp # Web interface

sudo ufw allow 12201/udp # GELF UDP

sudo ufw allow 12201/tcp # GELF TCP

11. Access the web interface:

Open a web browser and navigate to:

http://your_server_ip:9000

Default login credentials:

- Username: admin

- Password: (the password you set earlier)

Additional Configuration Tips:

1. To increase memory limits for Elasticsearch:

bash

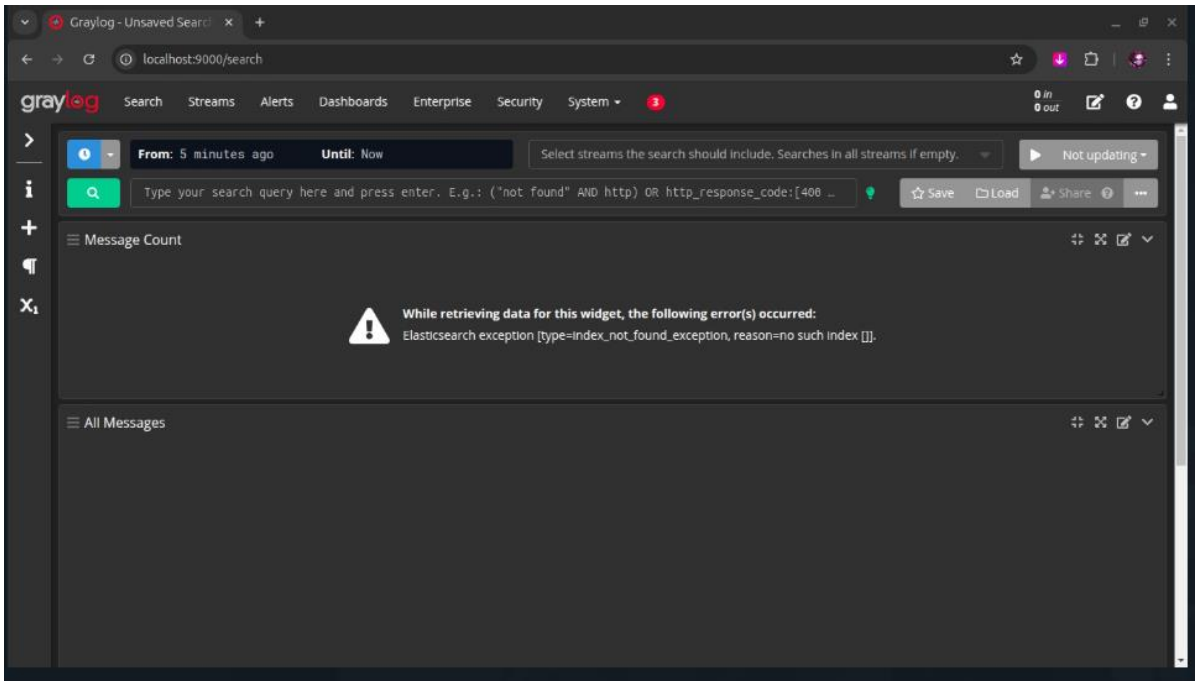
sudo nano /etc/elasticsearch/jvm.options

Modify these lines:

-Xms2g

-Xmx2g

2. To configure system limits:
   bash
   sudo nano /etc/security/limits.conf

Add these lines:
   elasticsearch soft nofile 65536
   elasticsearch hard nofile 65536

3. To view logs if there are issues:
   bash
   sudo tail -f /var/log/graylog-server/server.log