KALASALINGAM
ACADEMY OF RESEARCH & EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A" Grade

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

LAB RECORD NOTE BOOK

(Academic Year 2021 – 2022/EVEN Semester)

INFORMATION SECURITY FUNDAMENTALS LAB (213CSE1302)

Name of the Student :	**Register No :**
Branch :	**Year :**
Semester :	**Section :**

Name of the Course Teacher	Dr. N. C. Brintha, Associate Professor / CSE

TABLE OF CONTENTS

KALASALINGAM
ACADEMY OF RESEARCH & EDUCATION
(DEEMED TO BE UNIVERSITY)

Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A" Grade

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Bonafide record of work done by _____ of **COMPUTER SCIENCE AND ENGINEERING** department in **INFORMATION SECURITY FUNDAMENTALS LAB (213CSE1302)** during even/odd semester in academic year 2021 - 2022.

Staff In-charge **Head of the Department**

Submitted to the practical Examination held at Kalasalingam Academy of Research and Education, Anandnagar, Krishnankoil on _____

_____

REGISTER NUMBER

Internal Examiner **External Examiner**

EXPERIMENT EVALUATION SUMMARY

Name: **Reg No:**

Class:

Experiments			
S. No	**Topic**	**Marks**	**Signature**
1	Encryption/Decryption process using VeraCrypt		
2	Hide and Unhide Sensitive Information using Steghide		
3	Cryptography using Cryptol-online		
4	Hashing data using QuickHash-GUI		
5	Cryptographic attack using Hashcat		
6	Operations Security using ClamWin		
7	Vulnerability analysis using Legion		
8	Network Security using Wireshark		
9	Assessing threats and vulnerabilities using Legion		
10	Secure Network Administration using Nmap		
11	Securing Windows OS using Windows Security		
12	Security Assessment using Nikto		
13	Log Management using Logwatch		
14	Logs Management in Linux		
15	Antivirus installations, configuration, and management using ClamAV		

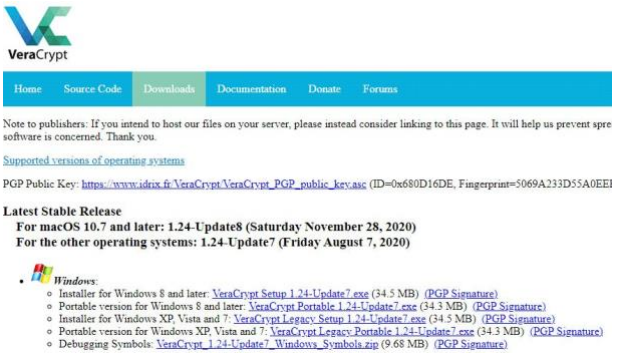
Ex. No. 1	Encryption/Decryption process using VeraCrypt

Aim:

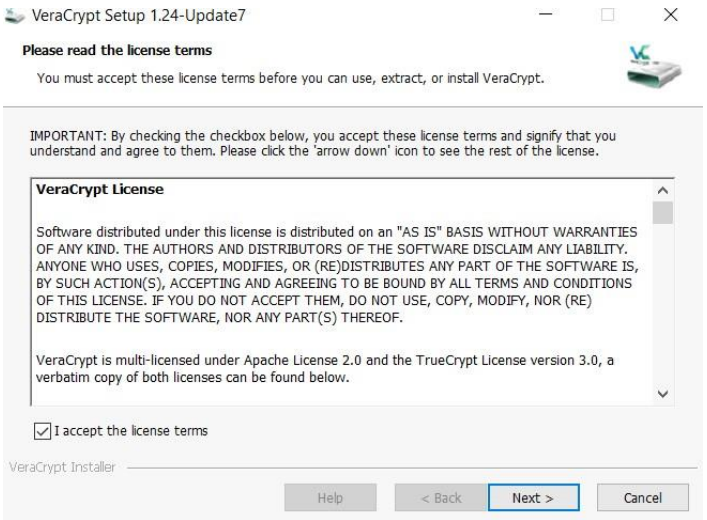
To analyze the Encryption/Decryption process using Vera Crypt tool.

Procedure:

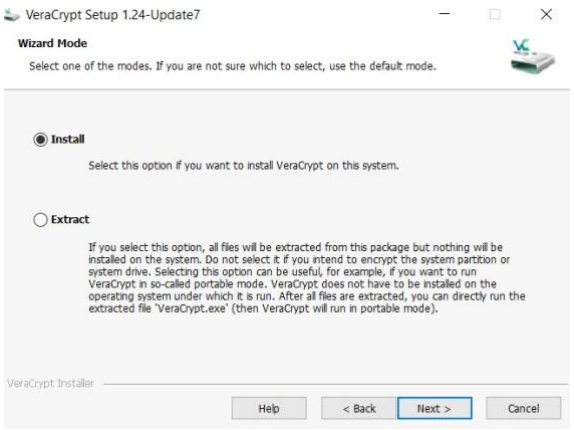
Step 1: Download VeraCrypt for Windows from the official website using URL:https://veracrypt.fr/en/Downloads.html



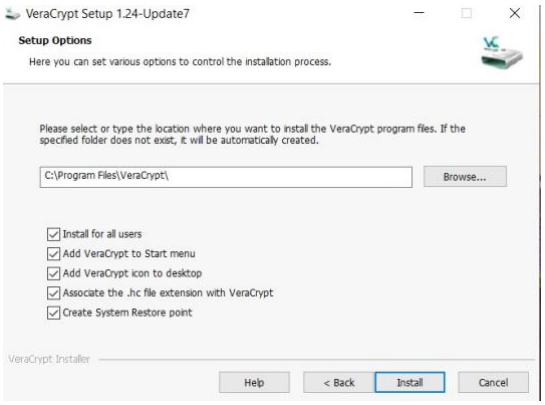
Step 2: Click on the setup file and start Installation, then accept the license, and then click on Next.



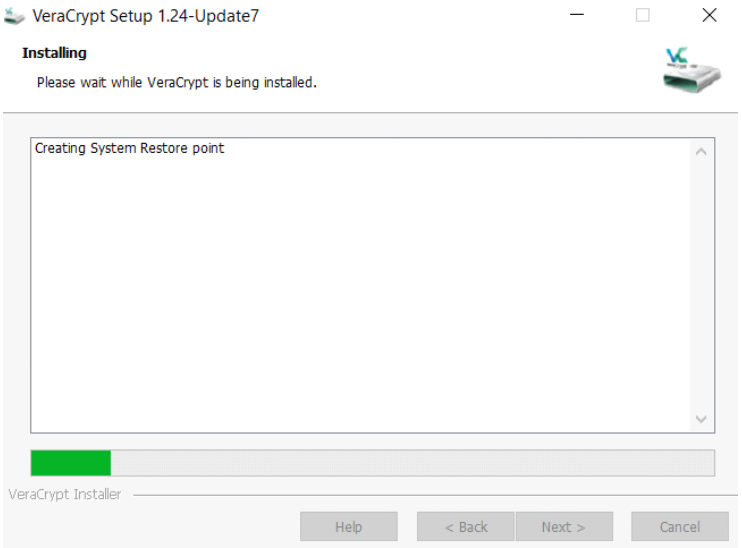
Step 3: Select install and click on the Next button.



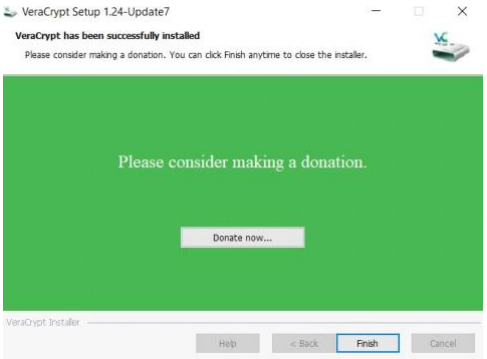
Step 4: Select the location where you want to VeraCrypt install program files. Select all options and clickInstall.



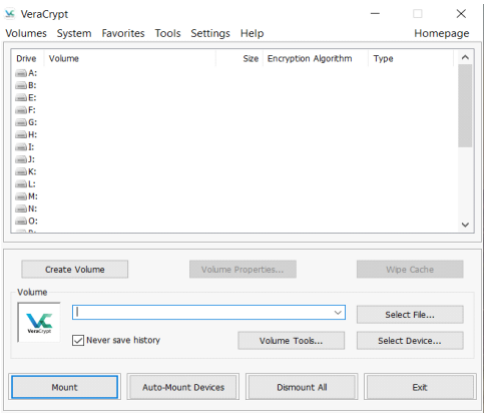
Step 5: Now the installation process is started. After successful installation click on OK.



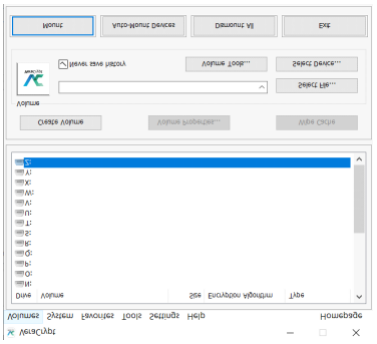
Step 6: Click on Finish to complete the installation process of VeraCrypt.



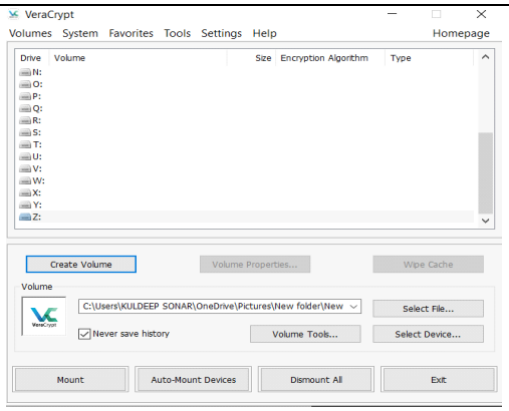
Step 7: After installation of VeraCrypt, now we start encryption of the drive.



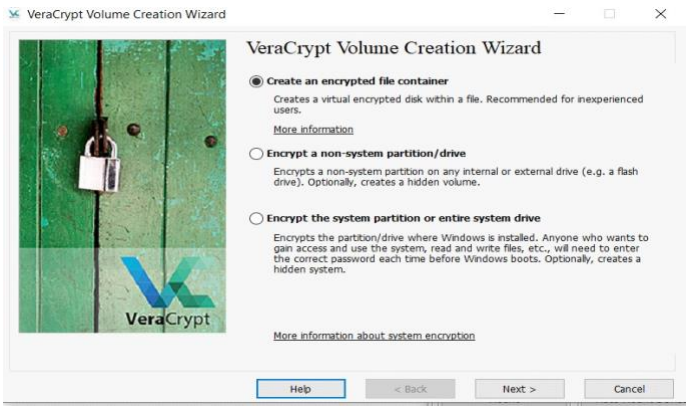
Step 8: Select a Specific drive to encrypt. For example, Drive “Z” is selected.



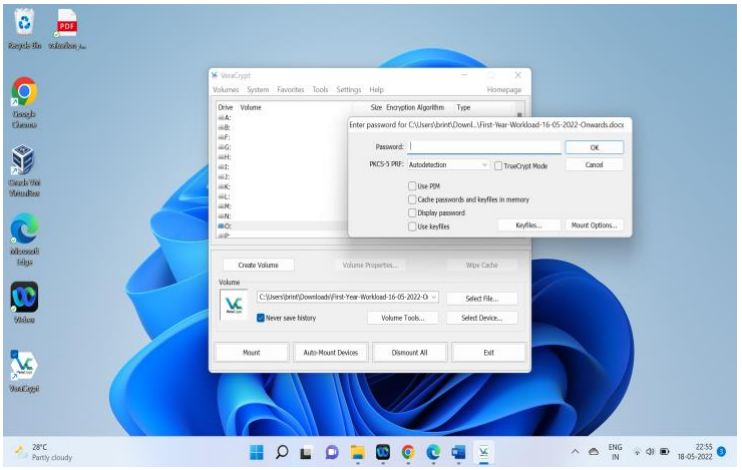
Step 9: Select location to create volume for the encrypted drive.



Step 10: Select create an encrypted file container to create a virtual encrypted disk. Then, click next to thedrive encryption process.



Sample Output Screenshot:



Result:

Thus, the veracrypt tool was used to encrypt and decrypt a system volume successfully

Ex. No. 2	Hide and Unhide Sensitive Information using Steghide

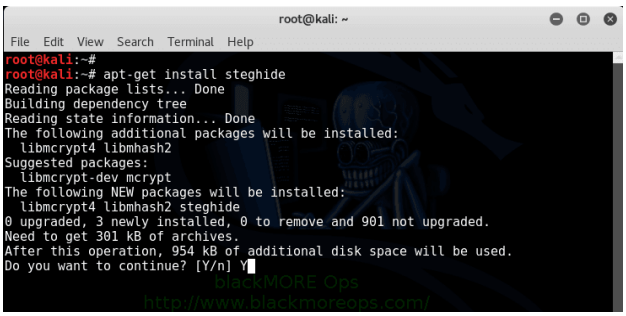
Aim:

To Hide and Unhide sensitive data using Steghide.

Procedure:

Step 1: Open Kali Linux terminal.

Step 2: To Install Steghide type command: **apt-get install steghide**



Step 3: To change the working directory to Desktop-type command: **cd Desktop** in Kali Linux terminal.

Step 4: Create a text file example **secret.txt** and Download an image file in which we will hide out text filesinside it, for example, **girl.jpg**.

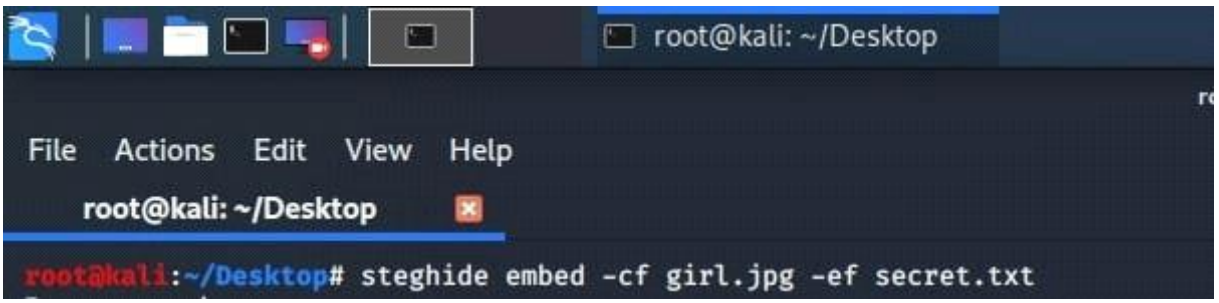
Step 5: Make sure that both the files i.e JPG Image file and the text file in the same working directory.

Step 6: Type steghide or steghide -h to show all the option of steghide.

```
the first argument must be one of the following:
embed, --embed embed data
extract, --extract extract data
info, --info display information about a cover- or stego-file
info <filename> display information about <filename>
encinfo, --encinfo display a list of supported encryption algorithms
version, --version display version information
license, --license display steghide's license
help, --help display this usage information

embedding options:
-ef, --embedfile select file to be embedded
-ef <filename> embed the file <filename>
-cf, --coverfile select cover-file
-cf <filename> embed into the file <filename>
-p, --passphrase specify passphrase
-p <passphrase> use <passphrase> to embed data
-sf, --stegofile select stego file
-sf <filename> write result to <filename> instead of cover-file
-e, --encryption select encryption parameters
-e <a>[<m>][<m>[<a>] specify an encryption algorithm and/or mode
-e none do not encrypt data before embedding
-z, --compress compress data before embedding (default)
-z <l> using level <l> (1 best speed...9 best compression)
-Z, --dontcompress do not compress data before embedding
-K, --nochecksum do not embed crc32 checksum of embedded data
-N, --dontembedname do not embed the name of the original file
-f, --force overwrite existing files
-q, --quiet suppress information messages
-v, --verbose display detailed information
```

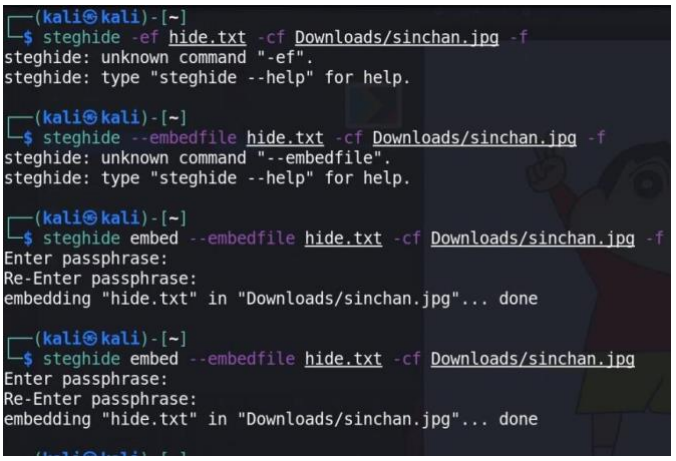
Step 7: Now type the command: **steghide embed -cf girl.jpg -ef secret.txt** to embed the text File into theImage File with a password.



Step 8: Now, Enter a Passphrase/password. Then re-enter the same passphrase to confirm and hit enter.

Step 9: Finally get output on terminal.

Sample Output Screenshot:



```
┌──(kali㉿kali)-[~]
└─$ steghide -ef hide.txt -cf Downloads/sinchan.jpg -f
steghide: unknown command "-ef".
steghide: type "steghide --help" for help.

┌──(kali㉿kali)-[~]
└─$ steghide --embedfile hide.txt -cf Downloads/sinchan.jpg -f
steghide: unknown command "--embedfile".
steghide: type "steghide --help" for help.

┌──(kali㉿kali)-[~]
└─$ steghide embed --embedfile hide.txt -cf Downloads/sinchan.jpg -f
Enter passphrase:
Re-Enter passphrase:
embedding "hide.txt" in "Downloads/sinchan.jpg"... done

┌──(kali㉿kali)-[~]
└─$ steghide embed --embedfile hide.txt -cf Downloads/sinchan.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "hide.txt" in "Downloads/sinchan.jpg"... done
```

Result:

Thus, the steghide is used to Hide and Unhide sensitive data Successfully

Ex. No. 3	Cryptography using Cryptool-online

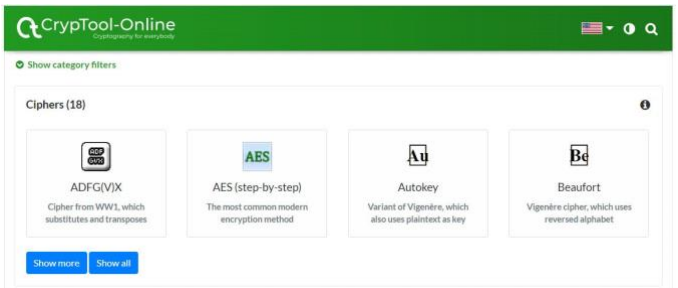
Aim:

To cryptograph the text using Cryptool-online.

Procedure:

Step 1: Click on the URL to open CrypTool-Online: https://www.cryptool.org/en/cto/

Step 2: Click on ADFGX is to start the encoding procedure.

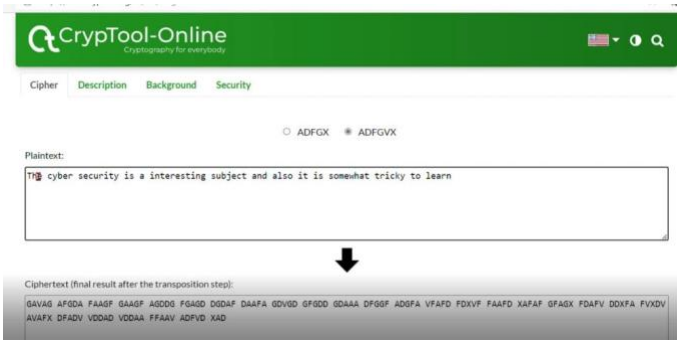


Step 3: Select ADFGVX in cipher.

Step 4: Select blocks "Blocks of 5" mentioned below to see the ciphertext in a specific set of characters.

Step 5: Type or paste text in the plaintext area. In Ciphertext area final result of the text will be shownautomatically in Cryptography form.

Sample Output Screenshot:



Result:

Finally Converted Plain Text into cipher text using Cryptool-online.

Ex. No. 4	Hashing data using QuickHash-GUI

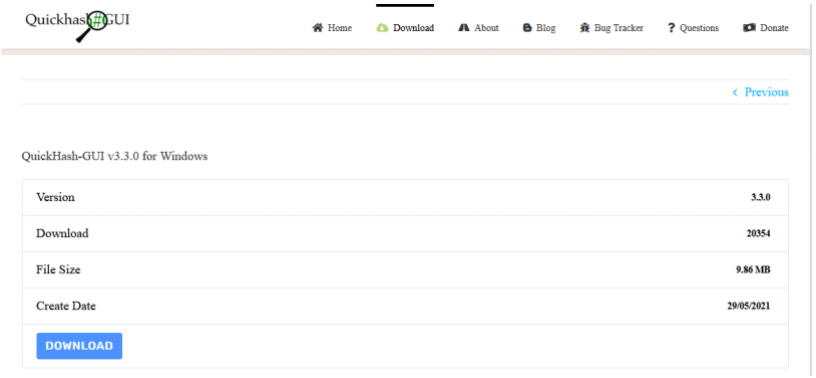
Aim:

To hash data by using Quick-hash-GUIptool-online.

Procedure:

Step 1: To install QuickHash-GUI for Windows click on URL:
https://www.quickhash-gui.org/download/quickhash-gui-v3-3-0-windows/

Step 2: Click on download and follow the instruction to complete the installation process.

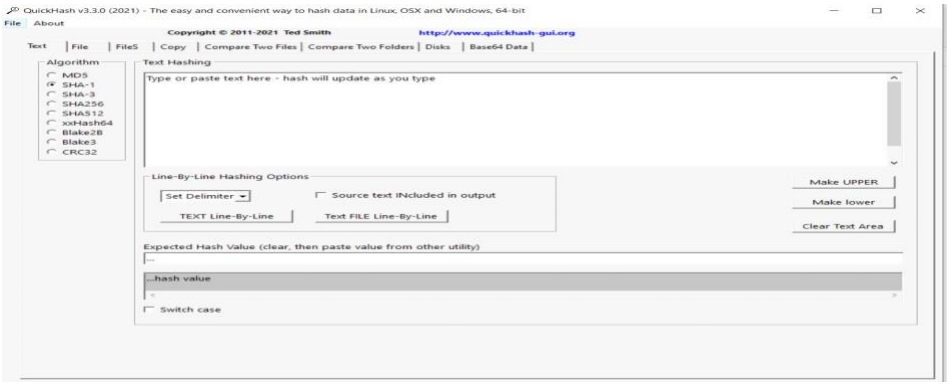


Step 3: Select an algorithm from the left-side algorithms panel.

Step 4: Type or paste text in the text hashing panel.

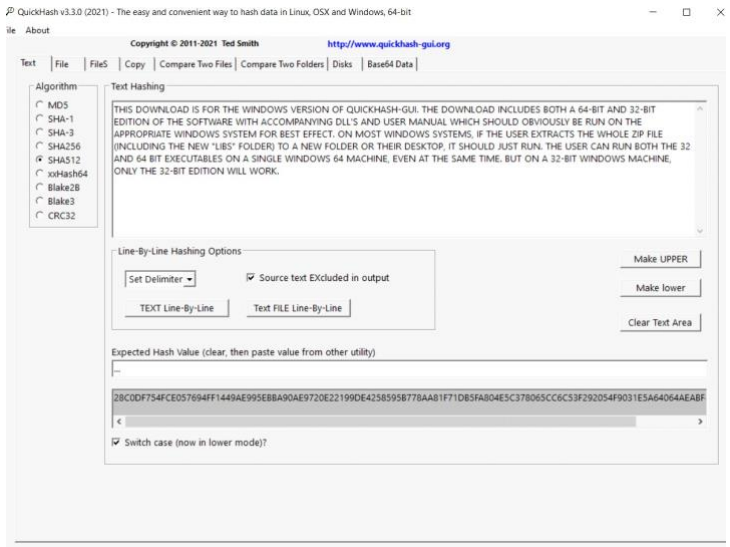
Step 5: Get a hash value at the bottom.

Step 6: Here we select: SHA-1 algorithm.



Step 7: Here we select: SHA512 algorithm.

Sample Output Screenshot:



Result:

Learned hashing text data with two different algorithms using the QuickHash-GUI tool Successfully.

Ex. No. 5	Cryptographic attack using Hashcat

Aim:

This exercise is about use of Hashcat for the cryptographic attack.

Procedure:

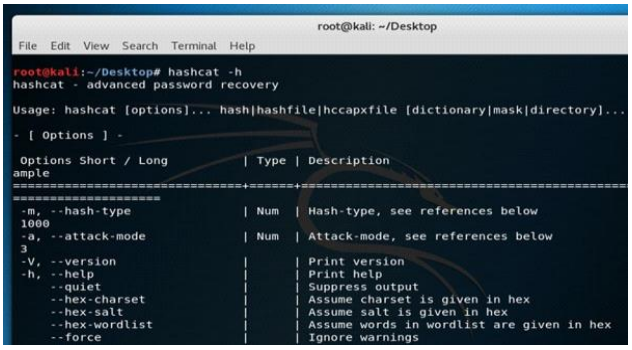
Step 1: To install Hashcat download the Hashcat tool using the URL: https://hashcat.net/hashcat/

Download

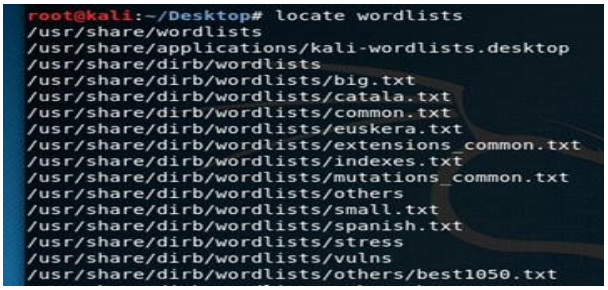
Name	Version	Date	Download	Signature
hashcat binaries	v6.2.4	2021.08.29	Download	PGP
hashcat sources	v6.2.4	2021.08.29	Download	PGP

Step 2: After installation, open the Kali Linux terminal to perform the cryptographic attack.

Step 3: Some of the most important hashcat options are **-m** (the hashtype) and **-a** (attack mode).



Step 4: To find the Kali Linux numerous wordlists type command line: **locate wordlists.**



Step 5: Here, for example, create a “rockyou.txt” that contains seven hashes and find in wordlists.

```
root@kali:~/Desktop# locate rockyou.txt
/usr/share/wordlists/rockyou.txt
```

Step 6: To cracking the hashes in rockyou.txt use the command: **target_hashes.txt**

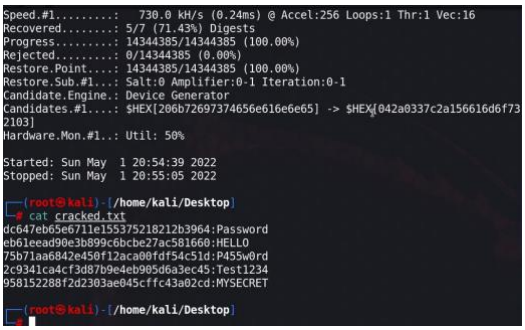
```
root@kali:~/Desktop# hashcat -m 0 -a 0 -o cracked.txt target_hashes.txt /usr/share
/wordlists/rockyou.txt
```

Step 7: Explanation of terms used in the above command line:

- -m 0 designates the type of hash we are cracking (MD5).
- -a 0 designates a dictionary attack.
- -o cracked.txt is the output file for the cracked passwords.
- target_hashes.txt is our input file of hashes.
- /usr/share/wordlists/rockyou.txt is the absolute path to the wordlist file for this dictionary attack.

Step 8: Finally get the results, we have cracked five out of seven targeted hashes.

Sample Output Screenshot:



```
Speed.#1.........:   730.0 kH/s (0.24ms) @ Accel:256 Loops:1 Thr:1 Vec:16
Recovered........: 5/7 (71.43%) Digests
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f73
2103]
Hardware.Mon.#1..: Util: 50%

Started: Sun May  1 20:54:39 2022
Stopped: Sun May  1 20:55:05 2022

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat cracked.txt
dc647eb65e6711e155375218212b3964:Password
eb61eead90e3b899c6bcbe27ac581660:HELLO
75b71aa6842e450f12aca00fdf54c51d:P455w0rd
2c9341ca4cf3d87b9e4eb905d6a3ec45:Test1234
958152288f2d2303ae045cffc43a02cd:MYSECRET

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

Result:

Performed Cryptographic attack Successfully by using hashcat.

Ex. No. 6	Operations Security using ClamWin

Aim:

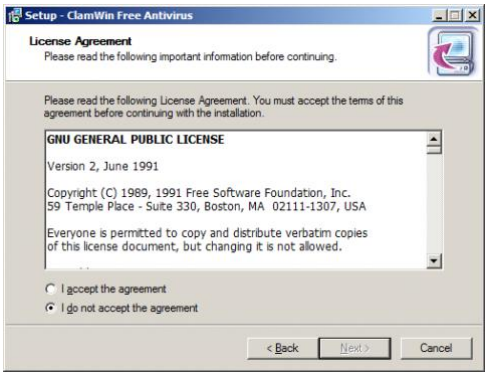
Understanding the operating of ClamWin security tool.

Procedure:

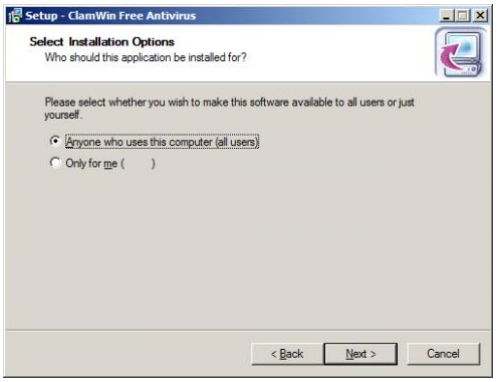
Step 1: To Install ClamWin in Windows click on the URL: https://clamwin.com/content/view/18/46/

Step 2: Run the downloaded setup exe file and click on Next.

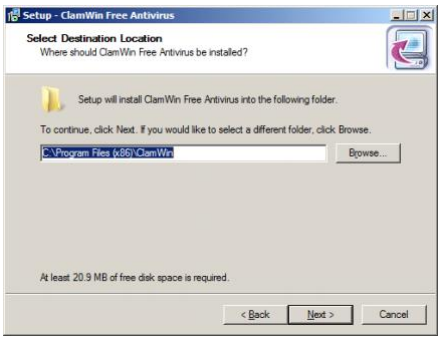
Step 3: Accept the license and click on the Next.



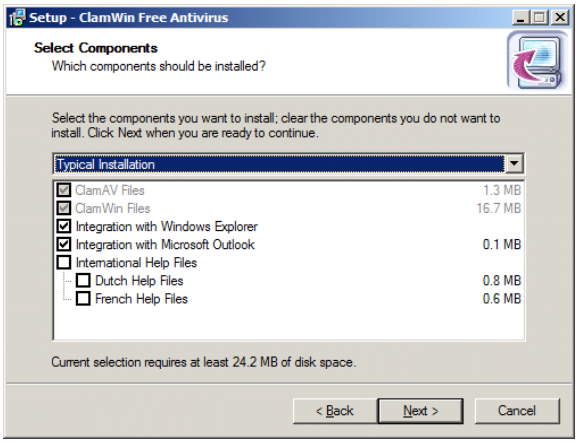
Step 4: Select an option and click on Next.



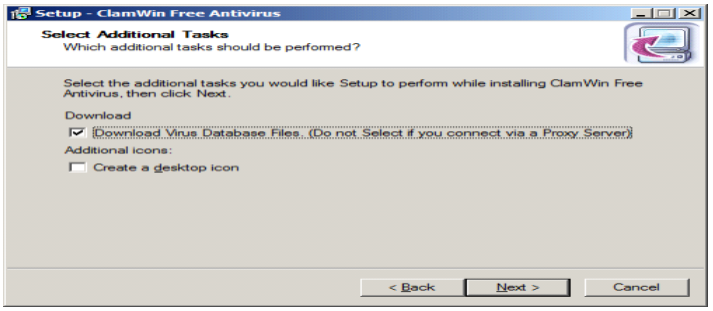
Step 5: Choose a location and click on Next.



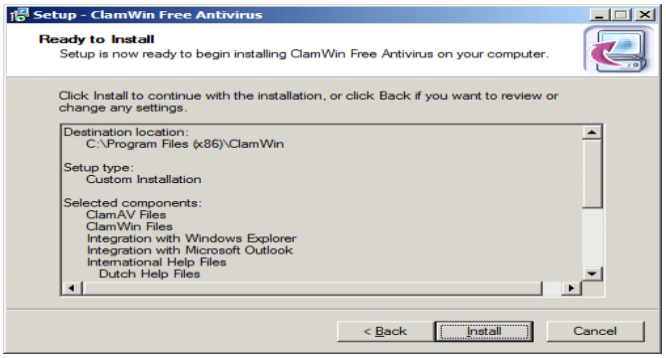
Step 6: Select the components and click on Next.



Step 7: Select an additional task and click on Next.



Step 8: Click on Install to run the installation process.

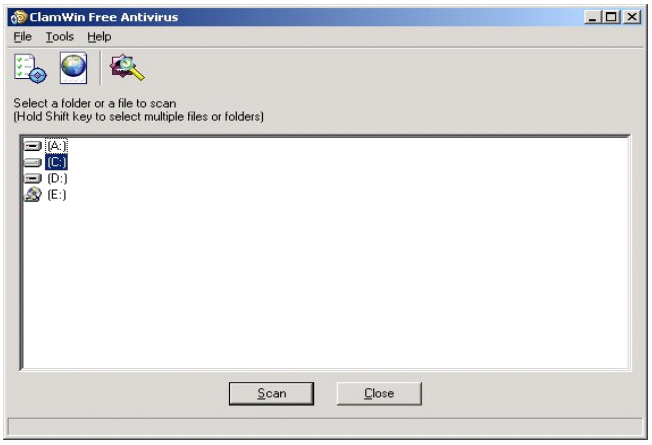


Step 9: Click on the Finish button to complete the installation process.

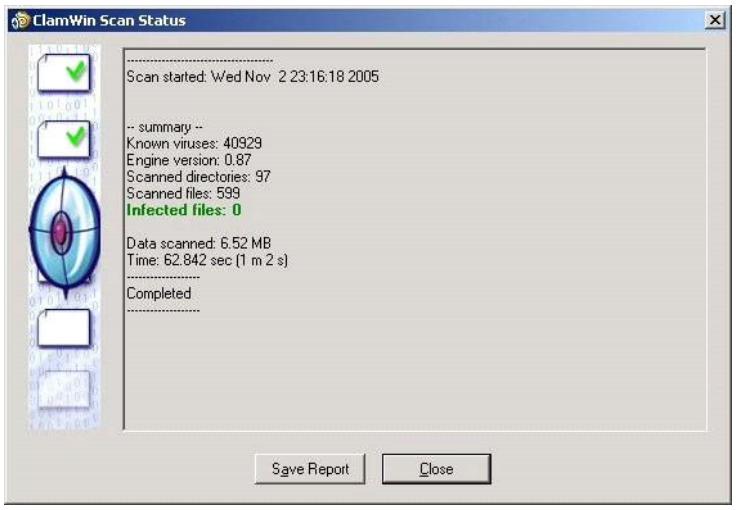
Step 10: After finishing installation open the ClamWin Tool to scan a drive.

Step 11: Select a Drive from computer Example: C drive.

Step 12: Click on Scan.



Sample Output Screenshot:



Result:

Learned security tool and scanningwith Clam-win successfully

Ex. No. 7	Vulnerability analysis using Legion

Aim:

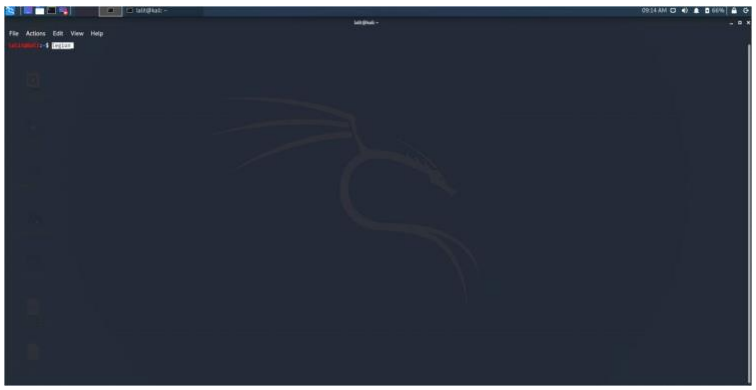
Scanning a website by using legion tool.

Procedure:

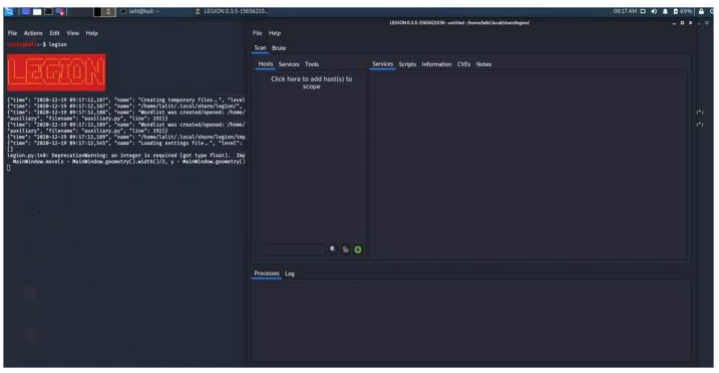
Step 1: To install Legion tool run the command in the Kali Linux terminal.

```
sudo apt-get install legion -y
```

Step 2: After installation, to start the legion tool from terminal type command: **legion.**

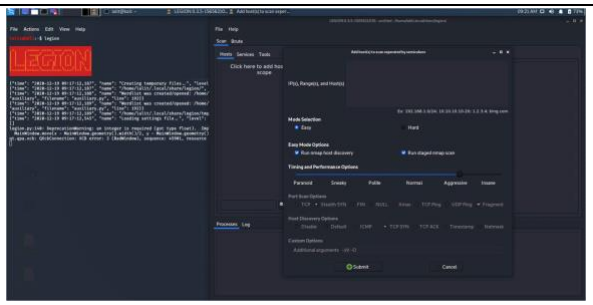


Step 3: Now, Legion tool is open to perform the scanning task.

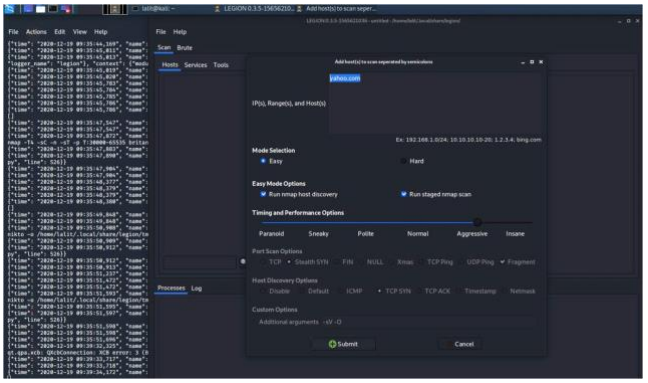


Step 4: Here, to perform an easy mode scan on yahoo.com with **-sV** and -O arguments.

Step 5: Click on host section.

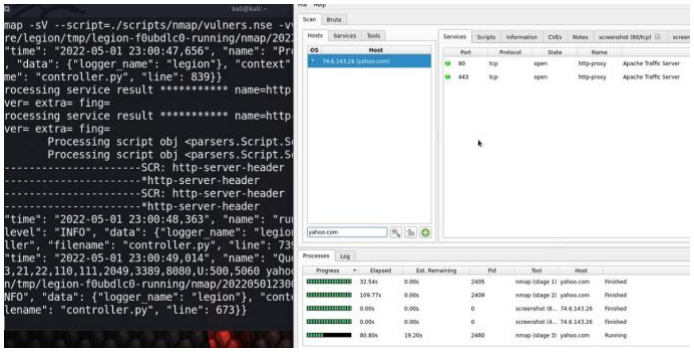


Step 6: Add “yahoo.com” as host and click on submit button.



Step 7: Get a scanning result.

Sample Output Screenshot:



Result:

Learned the process of installation of Legion tool and the procedure of finding vulnerabilities in a website.

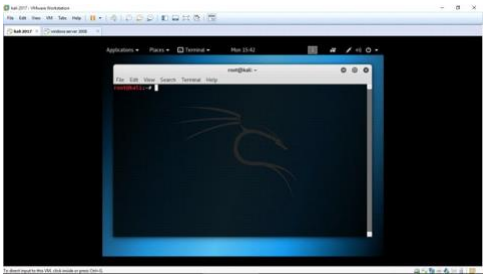
Ex. No. 8	Network Security using Wire shark

Aim:

Securing network with Wire shark

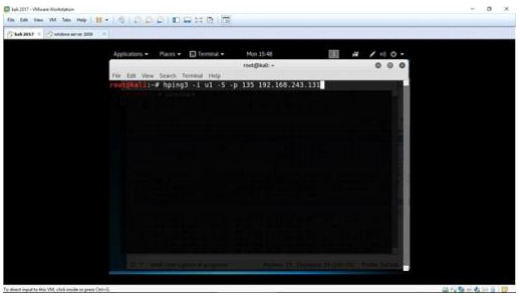
Procedure:

Step 1: Open Kali Linux.

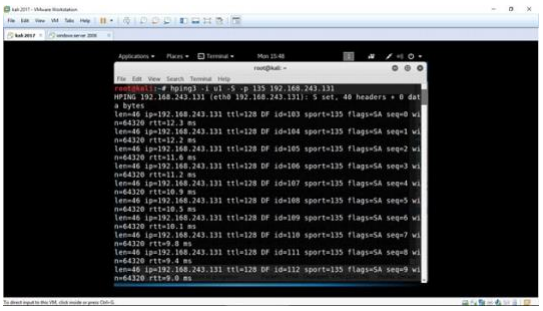


Step 2: Type command: hping3 -i u1 -S -p 80 **192.168.243.131** (IP address of target machine) in terminal and press enter, where:

- i — interval wait.
- u1- 1 microsecond.
- -S — Syn packet.
- -p — port number.

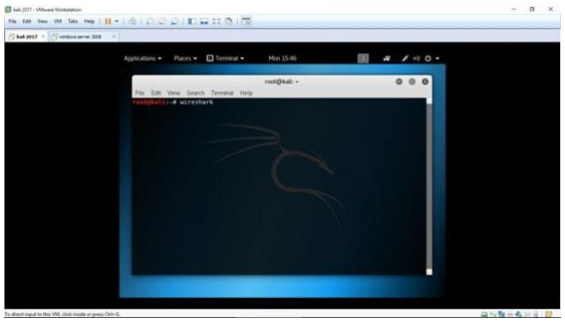


Step 3: Now, the following results will get.

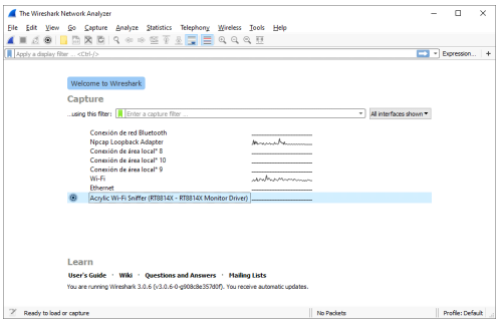


Step 4: Now, to check the result in Wireshark.

Step 5: To open Wireshark in kali Linux type command: Wireshark.

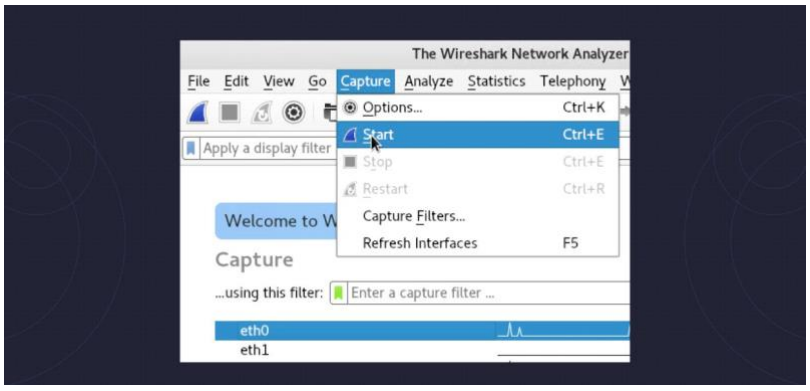


Step 6: Now, Wireshark is open.



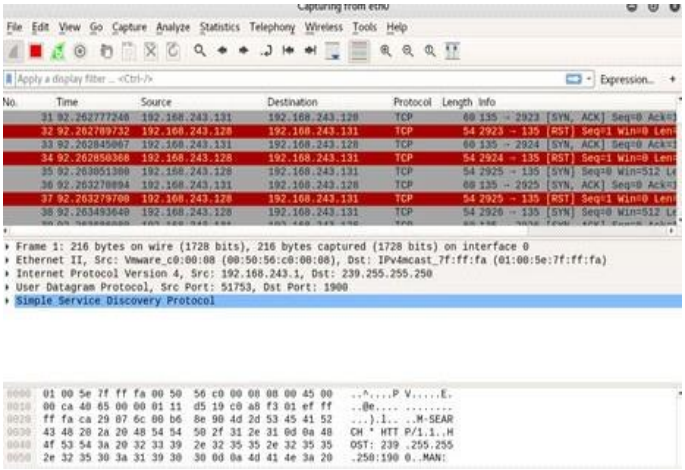
Step 7: Click on the Start Capturing Packets icon on the toolbar.

Step 8: Click on menu item and select Capture and click on start.



Step 9: Now, Wireshark will show the packets that it captures in real-time.

Sample Output Screenshot:



Result:

Performed a network security check with Wireshark

Ex. No. 9	Assessing threats and vulnerabilities using Legion

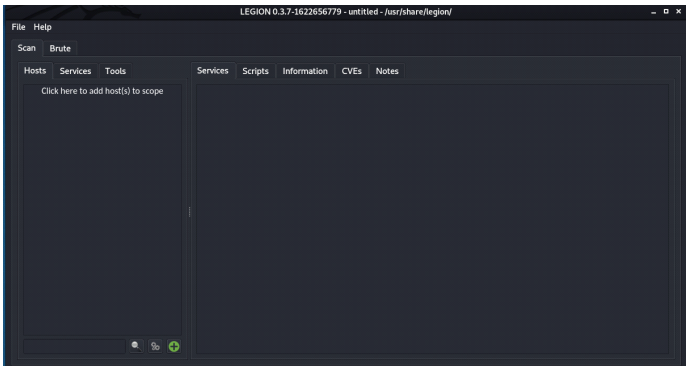
Aim:

Scanning vulnerabilities in a website network using Legion Tool.

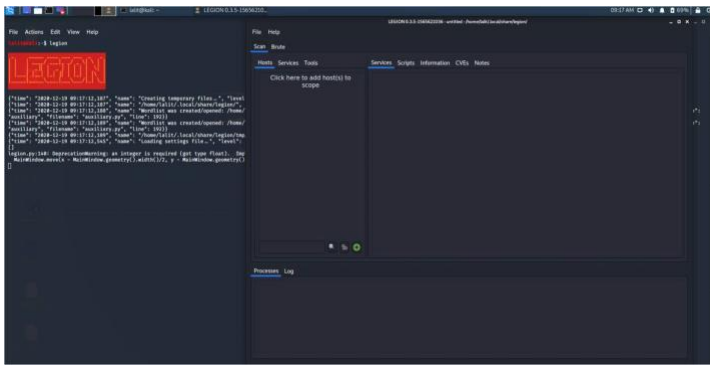
Procedure:

Step 1: To start the Legion tool in Kali Linux terminal use command: **Legion**

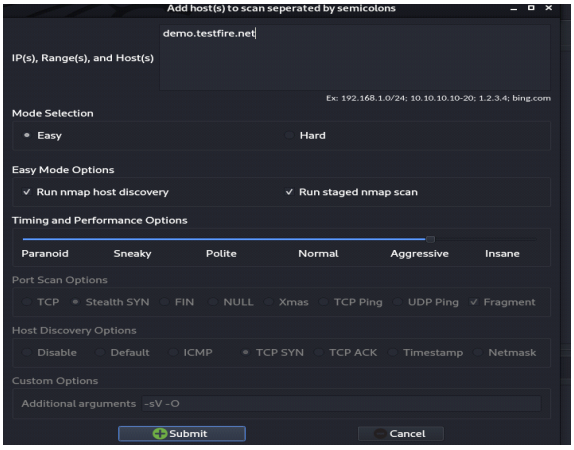
Step 2: To do an Easy mode scan on demo.testfire.net



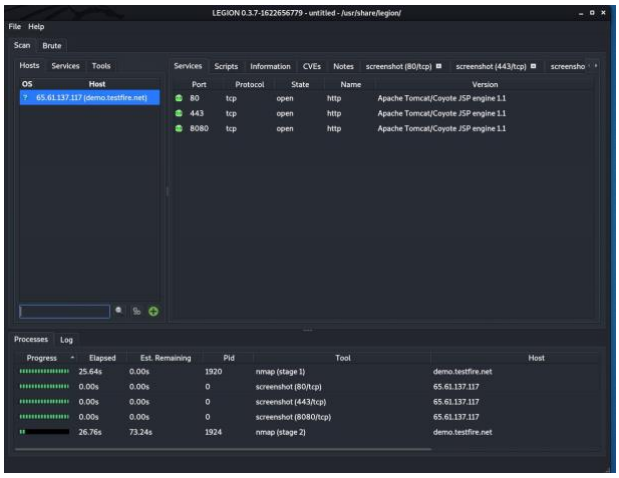
Step 3: Click on host section.



Step 4: Add host example: **"demo.testfire.net"**, choose Easy and click on submit button

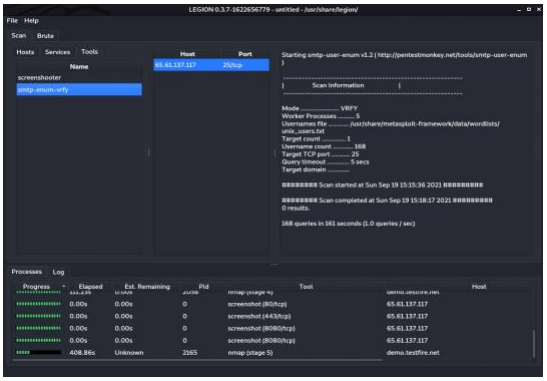


Step 5: Now, get the scanning result.



Step 6: Now, get the scanning result and click on **smtp-enum-vrfy** in Tools tab to view full scan information.

Sample Output Screenshot:



Result:

Scanned a website network vulnerabilities using Legion tool successfully

Ex. No. 10	Secure Network Administration using Nmap

Aim:

Scanning a website network using Nmap Tool

Procedure:

Step 1: IP Address of site and OS for this Lab.

- Kali Linux = 192.168.43.236
- Windows 7 = 192.168.43.29
- Facebook site = 31.13.79.35

Step 2: Open Kali Linux and to configure IP address of Kali Linux type command: **ifconfig.**

```
root@drona:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.236  netmask 255.255.255.0  broadcast 192
        inet6 fe80::a00:27ff:fe39:8bf2  prefixlen 64  scopeid 0x2
        ether 08:00:27:39:8b:f2  txqueuelen 1000  (Ethernet)
        RX packets 2730  bytes 186283 (181.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 157644  bytes 9579610 (9.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
```

Step 3: To configure IP address in Window 7. Open cmd prompt and type command: **ipconfig.**

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::291e:e45e:6838:49f2%11
   IPv4 Address. . . . . . . . . . . : 192.168.43.29
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1

Tunnel adapter isatap.{6FADE99E-AD12-4C69-92DE-E858A66AD176}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Step 4: To get IP address of the Facebook site. In Kali Linux type command: **ping www.facebook.com.**

```
root@drona:~# ping www.facebook.com
PING star-mini.c10r.facebook.com (31.13.79.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=1
ttl=51 time=38.9 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=2
ttl=51 time=76.2 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=3
ttl=51 time=69.4 ms
^C
```

Step 5: To Nmapping of Facebook site type command: **nmap 31.13.79.35** (IP address of website).

```
root@drona:~# nmap 31.13.79.35
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-12 12:18 EDT
Nmap scan report for edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35)
Host is up (0.049s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
843/tcp  closed unknown
5222/tcp closed xmpp-client

Nmap done: 1 IP address (1 host up) scanned in 5.76 seconds
```

Step 6: Here 996 filtered ports show the firewall is working behind this site. Also, TCP ports are open withhttp and https services. Even xmp-client and some unknown services are in a closed state.

Step 7: Hence we have successfully scan Networks using Nmap and obtained useful information andvulnerabilities from targeted sites.

Sample Output Screenshot:

```
┌──(root㉿kali)-[/home/kali]
└─# ping www.facebook.com
PING star-mini.c10r.facebook.com (157.240.228.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35): icmp_seq=
64 bytes from edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35): icmp_seq=
64 bytes from edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35): icmp_seq=
64 bytes from edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35): icmp_seq=
64 bytes from edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35): icmp_seq=
^C
--- star-mini.c10r.facebook.com ping statistics ---
7 packets transmitted, 5 received, 28.5714% packet loss, time 7142ms
rtt min/avg/max/mdev = 63.693/73.645/107.051/16.799 ms

┌──(root㉿kali)-[/home/kali]
└─# nmap 157.240.228.35
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-16 21:41 IST
Nmap scan report for edge-star-mini-shv-01-tir2.facebook.com (157.240.228.35)
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 45.71 seconds
```

Result:

Scanned a website network using Nmap too

Ex. No. 11	Securing Windows OS using Windows Security

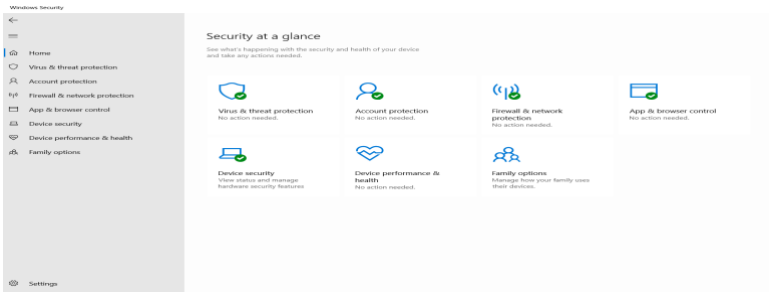
Aim:

Understanding the features of Windows security in the Windows Operating System.

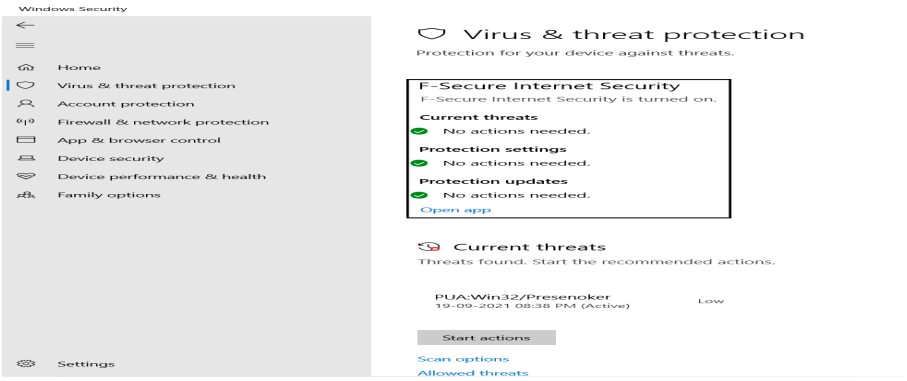
Procedure:

Step 1: Click on the start menu. Go to Windows Security.

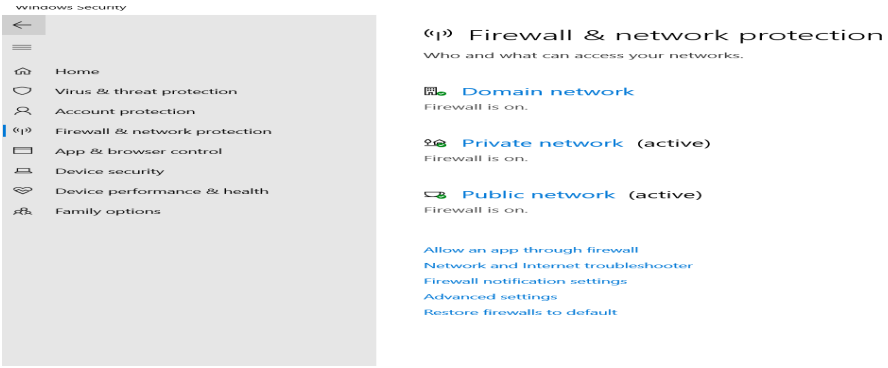
Step 2: Click on Home for a Windows security quick view



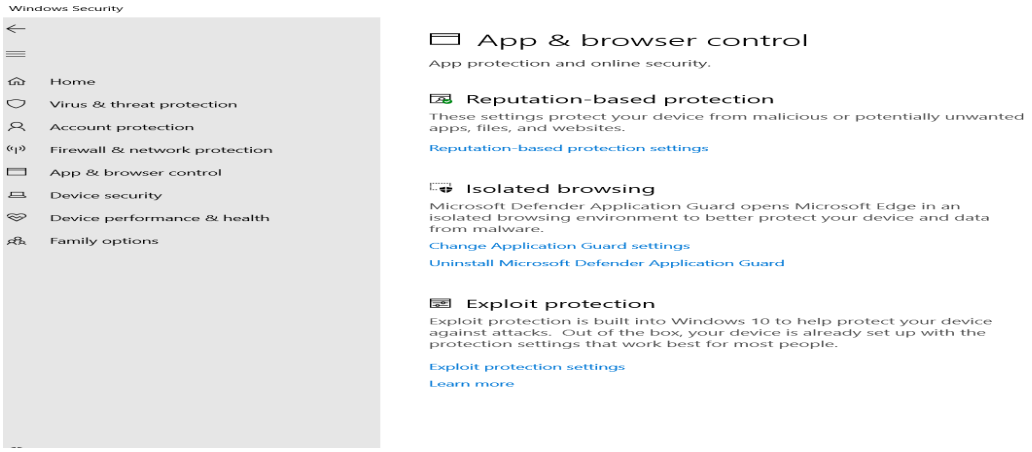
Step 3: Click on virus and threat protection to scan the device against threats.



Step 4: Click on firewall and protection to know who and what can access your network.

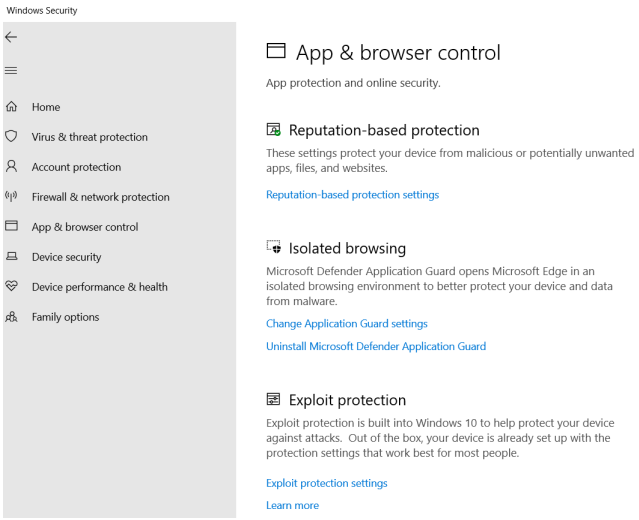


Step 5: Click on app and browser control for app and online protection.



Step 6: Click on device security to control the security settings that come with the device.

Sample Output Screenshot:



Result:

Verified security features in Windows OS.

Ex. No. 12	Security Assessment using Nikto

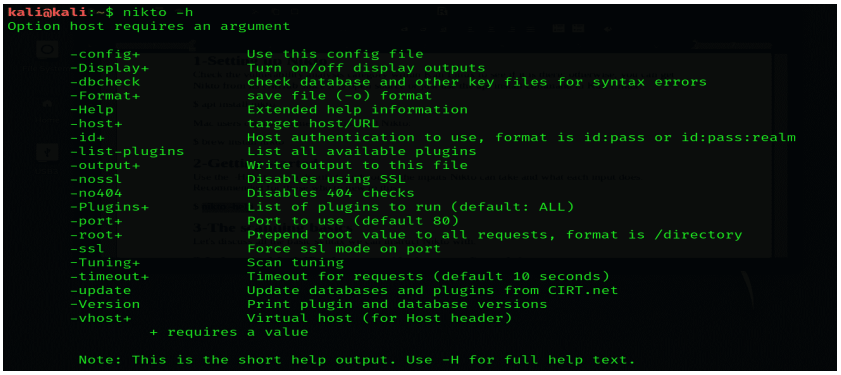
Aim:

Scanning web vulnerabilities using Nikto

Procedure:

Step 1: Open Kali Linux Terminal open Nikto.

Step 2: To see a detailed guide on all the inputs of Nikto use command: "$ nikto -h"



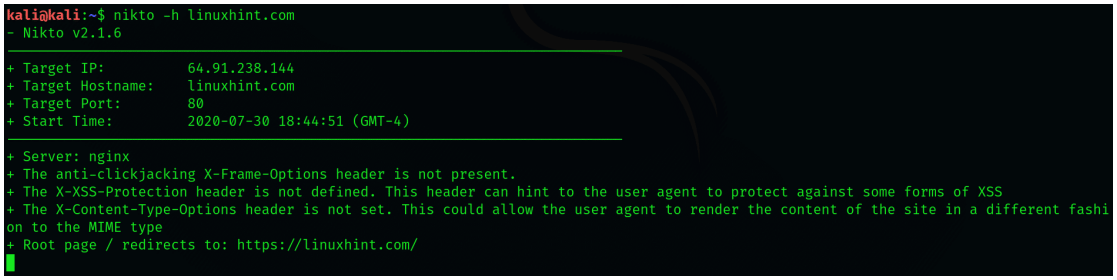
```
kali@kali:~$ nikto -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```

Step 3: Substitute the default IP with a hostname: linuxhint.com

Step 4: Use command: $ nikto -h linuxhint.com



```
kali@kali:~$ nikto -h linuxhint.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          64.91.238.144
+ Target Hostname:    linuxhint.com
+ Target Port:        80
+ Start Time:         2020-07-30 18:44:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashi
on to the MIME type
+ Root page / redirects to: https://linuxhint.com/
```

Step 5: Scanning SSL enabled websites Example: pbs.org

Step 6: Use command line: $ nikto -h pbs.org –ssl

Step 7: We've performed a quick scan of pbs.org

Sample Output Screenshot:

```
┌──(kali㉿kali)-[~]
└─$ nikto -h pbs.org -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          54.225.198.196
+ Target Hostname:    pbs.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.pbs.org
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Message:            Multiple IP addresses found: 54.225.198.196, 54.225.206.15
+ Start Time:         2022-05-16 22:00:53 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
+ Uncommon header 'x-pbs-fwsrvname' found, with contents: fwcacheproxy1
+ The site uses SSL and the Strict-Transport-Security HTTP header is not definec
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent
 to the MIME type
+ Root page / redirects to: https://www.pbs.org/
```

Result:

Scanned vulnerabilities successfully by using Nikto

Ex. No. 13	Log Management using Logwatch

Aim: How to install Logwatch Tool in Kali Linux

Procedure:

Step 1: Before start, prerequisites are:

- Ensure email is working. Instructions for doing so may be found in MailServer.
- Turn on the universe repository. Instructions for doing so may be found in Repositories.

Step 2: Open ubuntu terminal and to install Logwatch run the Command: **~# apt-get -y install logwatch**

```
root@ubuntu-14:~#
root@ubuntu-14:~# apt-get -y install logwatch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  postfix ssl-cert
Suggested packages:
  fortune-mod procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre
  sasl2-bin dovecot-common postfix-cdb mail-reader postfix-doc
  openssl-blacklist
Recommended packages:
  libdate-manip-perl
The following NEW packages will be installed:
  logwatch postfix ssl-cert
0 upgraded, 3 newly installed, 0 to remove and 52 not upgraded.
Need to get 1,569 kB of archives.
After this operation, 5,851 kB of additional disk space will be used.
```

Step 3: After installation we will get the end result.

```
Running newaliases
 * Stopping Postfix Mail Transport Agent postfix
 * Starting Postfix Mail Transport Agent postfix
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
Setting up logwatch (7.4.0+svn20130529rev144-1ubuntu1) ...
Processing triggers for libc-bin (2.19-0ubuntu6.6) ...
root@ubuntu-14:~#
```

Step 4: The local configurations file is located in /etc/logwatch/conf/logwatch.conf

Step 5: Default configurations file can be configured in

/usr/share/logwatch/default.conf/logwatch.conf.

Step 6: Open the file using command: **~# vim /usr/share/logwatch/default.conf/logwatch.conf**

Step 7: To test Logwatch run command: **~# logwatch.**

Step 9: Get a report of each service running and application installed.

Sample Output Screenshot:

```
root@ubuntu-14:~#
root@ubuntu-14:~# logwatch

 ################### Logwatch 7.4.0 (05/29/13) ####################
        Processing Initiated: Sat Jul 18 15:22:37 2015
        Date Range Processed: today
                              ( 2015-Jul-18 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: ubuntu-14
 ##################################################################

 -------------------- Cron Begin ------------------------
```

Result:

Logwatch is installed and Located the configurations of Logwatch.

Ex. No. 14	Logs Management in Linux

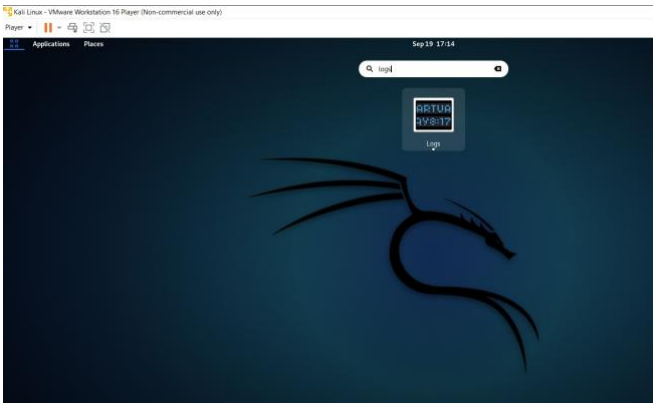
Aim: To manage logs in kali linux.

Procedure:

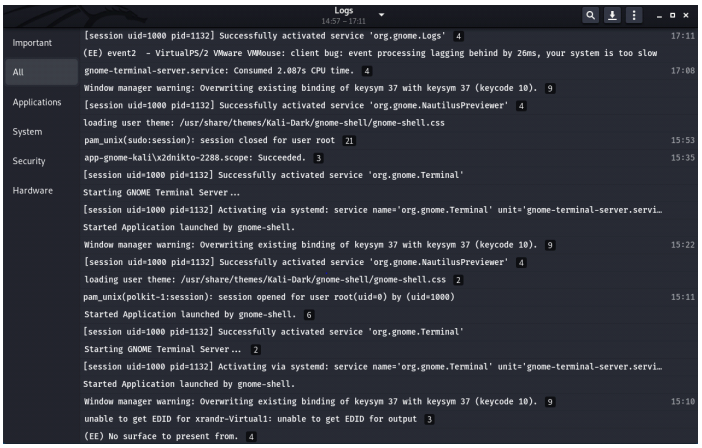
Step 1: Open Installed Kali Linux.

Step 2: Type logs in the search bar.

Step 3: Click on logs to open the log management.

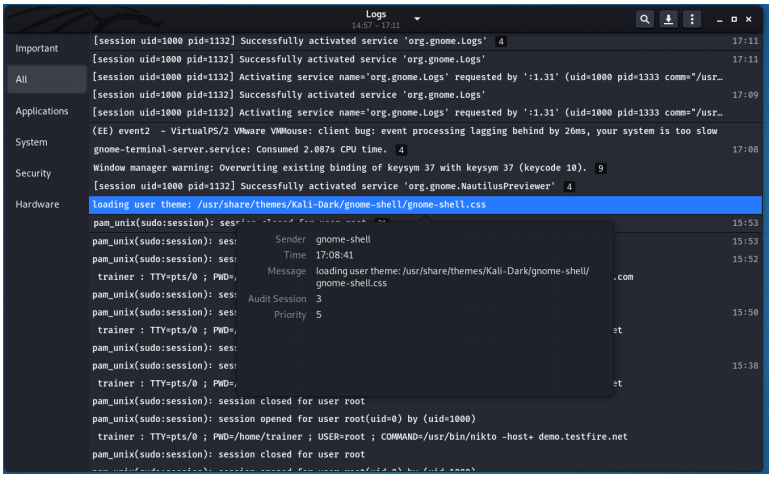


Step 4: Click on All to see all system logs.



Step 5: Click on a particular log to check the log activity.

Sample Output Screenshot:



Result:

Successfully Managed logs in Kali Linux

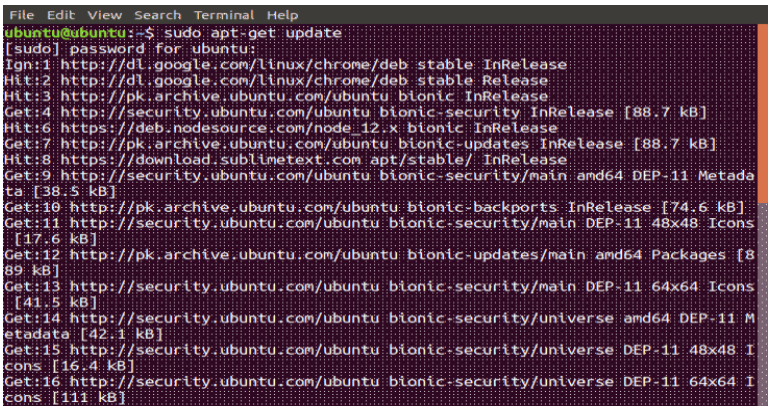
Ex. No. 15	Antivirus installations, configuration, and management using ClamAV

Aim: Installation of ClamAV Antivirus and performing ascan for viruses.

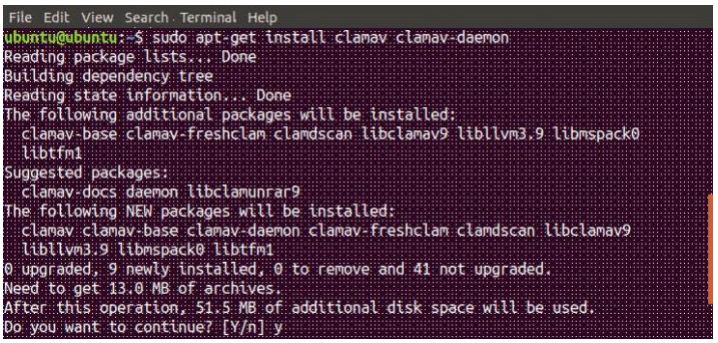
Procedure:

Step 1: To install ClamAV open the terminal and update the system.

Step 2: To update the system run the command: run the command: **~$sudo apt-get update**



Step 3: To install ClamAV run the command: ~$ sudo apt-get install clamav clamav-daemon and press Enterand choose Y.



Step 4: To check whether ClamAV installed or run the command: **~$ clamscan - - version.**

Step 5: If the above command gives the version of ClamAV then it has been installed successfully.

Step 6: After installation of ClamAV, you need to update the ClamAV signature database using command run the command: **~$ sudo freshclam.**

Step 7: To check the other ClamAV utility options type command: **$ clamscan –h.**

```
root@pentest-vm:~# clamscan -h

                      Clam AntiVirus: Scanner 0.100.1
          By The ClamAV Team: https://www.clamav.net/about.html#credits
          (C) 2007-2018 Cisco Systems, Inc.

    clamscan [options] [file/directory/-]

    --help                -h             Show this help
    --version             -V             Print version number
    --verbose             -v             Be verbose
    --archive-verbose     -a             Show filenames inside scanned archives
    --debug                              Enable libclamav's debug messages
    --quiet                              Only output error messages
    --stdout                             Write to stdout instead of stderr
    --no-summary                         Disable summary at end of scanning
    --infected            -i             Only print infected files
    --suppress-ok-results -o             Skip printing OK files
    --bell                               Sound bell on virus detection

    --tempdir=DIRECTORY                  Create temporary files in DIRECTORY
    --leave-temps[=yes/no(*)]            Do not remove temporary files
```

Step 8: Now ClamAV is ready to use. Here, for example, to scan the current user's Pictures folder run thecommand: **$ sudo clamscan --infected --remove --recursive /home/sana/Pictures.**

Step 9: Get the scan summary report.

Sample Output Screenshot:

```
sana@sana-HP-ProBook-4530s:~$ sudo clamscan --infected --remove --recursive /hom
e/sana/Pictures

----------- SCAN SUMMARY -----------
Known viruses: 6106139
Engine version: 0.100.3
Scanned directories: 1
Scanned files: 2
Infected files: 0
Data scanned: 0.05 MB
Data read: 0.05 MB (ratio 1.00:1)
Time: 63.456 sec (1 m 3 s)
```

Result:

Successfully Installed Clamav and Performed a scan for virus and got report.