EXP. NO: 1

DATE:

IMPLEMENTATION OF CONFIDENTIALITY

AIM:

ALGORITHM:

PROGRAM:

```
#include <stdio.h>
#include<stdlib.h>
int encrypt() {
char str[100];
printf("\t\tInput String: ");
scanf("%s",str);
printf("\n\t\tEncrypted String: ");
for(inti=0;str[i]!='\0';i++)
printf("%c",str[i]+3);
}
int decrypt() {
char str[100];
printf("\t\tInput String: ");
scanf("%s",str);
printf("\n\t\tDecrypted String: ");
for(inti=0;str[i]!='\0';i++)
printf("%c",str[i]-3);
}
int main() {
int choice;
char ch;
printf("\t\tConfidentiality\n");
do{
printf("\t\tChoose operation\n\t\t1. Encryption\n\t\t2. Decryption\n\t\t3. Exit\n\t\t\n\t\t");
scanf("%d",&choice);
switch(choice) {
case 1:
encrypt();
break;
case 2:
decrypt();
```

```
break;
case 3:
exit(0);
break;
default:
break;
}
printf("\n\t\tDo you want to continue (Y/N): ");
scanf(" %c",&ch);
} while(ch=='y' || ch=='Y');
return 0;
}
```

OUTPUT:

```
Confidentiality
        Choose operation
        1. Encryption
        2. Decryption
        3. Exit

        1
        Input String: abc
        Encrypted String: def
        Do you want to continue (Y/N): Y
        Choose operation
        1. Encryption
        2. Decryption
        3. Exit

        2
        Input String: def
        Decrypted String: abc
        Do you want to continue (Y/N): N
```


RESULT:

EXP. NO: 2

DATE:

IMPLEMENTATION OF INTEGRITY

AIM:

ALGORITHM:

PROGRAM:

```
import hashlib
a=input("Enter a string:\n")
result=hashlib.md5()
print("The byte equivalent of hash is:",end="
print(result.digest())
import haslib
print("The available algorithms are:",end="")
print(hashlib.algorithms_guaranteed)
```

OUTPUT:

```
Enter a string:
integrity
The byte equivalent of hash is:
b'\xd4\x1d\x8c\xd9\x8f\x00\xb2\x04\xe9\x80\t\x98\xec\xf8B~'
>
```

```
The available algorithms are:
{'blake2b', 'blake2s', 'sha1', 'shake_128', 'sha3_384', 'sha224', 'sha384', 'sha3_256'
    , 'sha512', 'sha3_224', 'md5', 'shake_256', 'sha256', 'sha3_512'}
>
```


RESULT:

EXP. NO: 3

DATE:

ADMINISTRATION OF USERS, PASSWORDS, POLICIES, PRIVILEGES AND ROLES

AIM:

ALGORITHM:

COMMANDS:

1. Find out the users who are currently logged in and find out the particular user too

whoami

2. Display the name of your home directory

pwd

3. Create a user and display the user details

addusersanjana

cat /etc/passwd

4. Display the details of encrypted user passwords

cat /etc/shadow

5. Create a group name as “Third Year” and display the details

addgroup Third year

cat /etc/group

6. Create a file name “sam.sh” and list the permissions of the file and directories

vi sam.sh

ls -l

7. Display hidden files

ls -a

8. Create a file and do the following :

vi sample.txt

ls -l

1. Others can’t read it :

chmod o-r sample.txt

2. Group members can execute it

chmodg+x sampl.txt

3. Others cannot read or write it.

chmod o-r-w sample.txt

4. Group members & Others can read and write it.

Chmodo+r+w sample.txt

5. Everyone has full access.

chmod 777 sample.txt

6. Deny all access from everyone.

chmod 000 sample.txt

7. Change the permissions to 600 to prevent group members or others from reading the file.

chmod 600 sample.txt

9. Write a shell script to greet the user on the screen

vi greet.sh

echo “What is your name?”

read user

echo “Hello $user!!”

10. Write a shell script to perform basic Arithmetic Operation

vi math.sh

echo “Enter 1st number:”

read a

echo “Enter 2nd number:”

read b

echo “sum=” $((a+b))

echo “difference=”$((a-b))

echo “Multiplication=”((a*b))

echo “Division=”((a/b))

OUTPUT:

```
abi  .bash_profile  .config  Downloads  Music     Sam.sh
[ameen_07@fedora ~]$ nano sample.txt
[ameen_07@fedora ~]$ chmod o-r sample.txt
[ameen_07@fedora ~]$ ls -l
total 8
drwxr-xr-x. 1 ameen_07 ameen_07 28 Feb 14 23:10 abi
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Desktop
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Documents
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Downloads
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Music
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Pictures
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Public
-rw-r-----. 1 ameen_07 ameen_07  9 Mar  9 22:34 sample.txt
-rw-r--r--. 1 ameen_07 ameen_07 12 Mar  9 22:29 Sam.sh
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Templates
drwxr-xr-x. 1 ameen_07 ameen_07  0 Jan 31 22:01 Videos
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-r-----. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod g+x sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-r-x---. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
```

```
[ameen_07@fedora ~]$ w
 22:17:16 up 15 min,  1 user,  load average: 1.20, 0.29, 0.10
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
ameen_07 tty2      22:16   15:30   0.03s  0.03s /usr/libexec/gnome-session-bina
[ameen_07@fedora ~]$ pwd
/home/ameen_07
[ameen_07@fedora ~]$ sudo adduser third
[sudo] password for ameen_07:
[ameen_07@fedora ~]$ sudo cat /etc/shadow |grep third
third:!!:19426:0:99999:7:::
[ameen_07@fedora ~]$ sudo addgrp
sudo: addgrp: command not found
[ameen_07@fedora ~]$ sudo groupadd thirdyear
[ameen_07@fedora ~]$ cat /etc/passwd |grep thirdyear
[ameen_07@fedora ~]$ sudo cat /etc/group |grep thirdyear
thirdyear:x:1002:
[ameen_07@fedora ~]$ ls -l Sam.sh
ls: cannot access 'Sam.sh': No such file or directory
[ameen_07@fedora ~]$ nano Sam.sh
[ameen_07@fedora ~]$ ls -l Sam.sh
-rw-r--r--. 1 ameen_07 ameen_07 12 Mar  9 22:29 Sam.sh
[ameen_07@fedora ~]$ ls -a
.  .bash_history  .bashrc  Desktop  .local  Pictures  Templates
..  .bash_logout  .cache  Documents  .mozilla  Public  Videos
```

```
[ameen_07@fedora ~]$ chmod g= sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-------. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod g+r+w sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw----. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod o+r+x sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw-r-x. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod o= sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw----. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod o+r+w sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw-rw-. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod 777 sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rwxrwxrwx. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod 000 sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
[ameen_07@fedora ~]$ chmod g+r+w sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw----. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod o+r+x sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw-r-x. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod o= sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw----. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod o+r+w sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rw-rw-rw-. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod 777 sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
-rwxrwxrwx. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod 000 sample.txt
[ameen_07@fedora ~]$ ls -l sample.txt
----------. 1 ameen_07 ameen_07 9 Mar  9 22:34 sample.txt
[ameen_07@fedora ~]$ chmod 600 sample.txt
```

```
[ameen_07@fedora ~]$ nano first.sh
[ameen_07@fedora ~]$ chmod +x sample.txt
[ameen_07@fedora ~]$ ./sample.sh\
>
Display all 2612 possibilities? (y or n)
> ^C
[ameen_07@fedora ~]$ ./sample.sh
bash: ./sample.sh: No such file or directory
[ameen_07@fedora ~]$ chmod +x first.sh
[ameen_07@fedora ~]$ ./first.sh\
> ^C
[ameen_07@fedora ~]$ chmod +x first.sh
[ameen_07@fedora ~]$ ./first.sh
Enter name
senthil
WELCOME senthil
[ameen_07@fedora ~]$ nano arithmetic.sh
[ameen_07@fedora ~]$ nano arithmetic.sh
[ameen_07@fedora ~]$ chmod +x arithmetic.sh
[ameen_07@fedora ~]$ ./arithmetic.sh
Enter the number 1
23
Enter the number 2
34
The addition is  23+34
The difference is 23+34
The product is 23*34
The quotient is 23/34
The remainder is 23%34
[ameen_07@fedora ~]$ nano aritmetic.sh
[ameen_07@fedora ~]$ nano arithmethic.sh
```


RESULT:

EXP. NO: 4

DATE:

MANDATORY ACCESS CONTROL USING LINUX

AIM:

ALGORITHM:

DESCRIPTION:

Security-Enhanced Linux (SELinux) is a security architecture for Linux systems that allowsadministrators to have more control over who can access the system. SELinux defines access controlsfor the applications, processes,

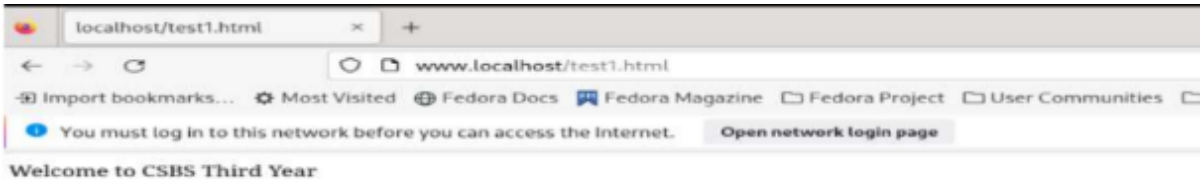
which are a set of rulesthat tell SELinux what can or can't be accessed, to enforce the access allowed by a policy. When anapplication or process, known as a subject, makes a request to access an object, like a file, SELinuxchecks with an access vector cache (AVC), where permissions are cached for subjects and objects. IfSELinux is unable to make a decision about access based on the cached permissions, it sends the requestto the security server. The security server checks for the security context of the app or process and thefile. Security context is applied from the SELinux policy database. Permission is then granted or denied.If permission is denied, an "avc: denied" message will be available in /var/log/m

SELinux can operate in any of the 3 modes :

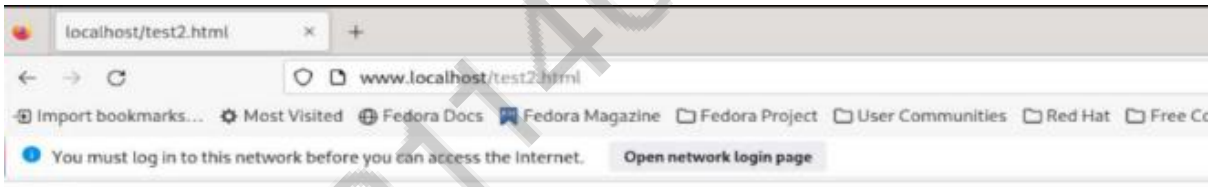
1. Enforced : Actions contrary to the policy are blocked and a corresponding event is logged inthe audit log.
2. Permissive : Permissive mode loads the SELinux rules, onlylogging is performed.
3. Disabled : The SELinux is disabled entirely.

OUTPUT:

```
[student@fedora ~]$ su
Password:
[root@fedora student]# yum install httpd
Last metadata expiration check: 0:37:03 ago on Thu 30 Mar 2023 11:13:52 PM EDT.
Package httpd-2.4.56-1.fc36.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@fedora student]# systemctl start httpd
[root@fedora student]# vi test1.html
[root@fedora student]# cat test1.html
This is test1 webpage

[root@fedora student]# vi test2.html
[root@fedora student]# cat test2.html
This is second webpage
[root@fedora student]# ls
Desktop    Downloads  Pictures  Templates   test2.html
Documents  Music      Public    test1.html  Videos
[root@fedora student]# cp test1.html /var/www/html
cp: overwrite '/var/www/html/test1.html'? ^C
[root@fedora student]# ls -lZ /var/www/html/test*
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 Mar 30 23
```




```
[root@fedora html]# chcon -R -t httpd_sys_content_t test2.html
[root@fedora html]# ls -lZ test2.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 23 Mar 30 2
3:51 test2.html
[root@fedora html]#
```



RESULT:

EXP. NO: 5

DATE:

SNORT IDS

AIM:

ALGORITHM:

DESCRIPTION:

Snort is a powerful open-source intrusion detection system (IDS) and intrusion preventionsystem (IPS) that provides real-time network traffic analysis and data packet logging. It uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detectpotentially malicious activity. Using snort, network admins can spot denial-of-service (DoS) attacksand distributed DoS (DDoS) attacks, Common Gateway Interface (CGI) attacks, buffer overflows,and stealth port scans. Snort creates a series of rules that define malicious network activity, identifymalicious packets, and send alerts to users.

There are 3 types of rules in SNORT, those are

1. Alert Rules: This uses the alert technique to produce notifications.
2. Logging Rules: It logs each individual alert as soon as it is generated.
3. Pass Rules: If the packet is deemed malicious, it is ignored and dropped.

Basic Usages of Snort

Packet Sniffing: The way traffic is being transmitted can be thoroughly examined by gatheringthe individual packets that travel to and from devices on the network.

Generates Alerts: It generates warnings based on the configuration file's rules when it discoversunusual or malicious activity, the possibility of a vulnerability being exploited, or a network threatthat compromises the organization's security policy.

Debug Traffic: After the traffic has been logged, any malicious packets and configurationproblems are checked.

Wget:

Command wget stands for web get.

- The wget is a free non-interactive file downloader command.
- Non-interactive means it can work in background when user is not logged in.

Thisallows user to get disconnected with the system while wget finish its work.

- It can even download entire website as a local version of remote websites, fully recreating the structure of original website. In short, you can mirror an entire websitewith wget.
- wget<URL>

tar:

A tar (tape archive) file format is an archive created by tar, a UNIX-based utility used topackage files together for backup or distribution purposes.

--gzip -------- Read or write compressed archives through gzip format.

Libpcap:

Packet capture library (libpcap)

- ibpcap.----are libraries used for user-level packet capture
- libpcap is an open source C-language library for capturing network packets. libpcap is

available for a number of different platforms, including most Unix and Unix-likeplatforms (such as Linux and BSD), as well as for Windows.

- Although libpcap is primarily a packet-capturing tool, it also can create and manipulate

packets from saved files, which can then be used in the wide variety of tools that supportthe libpcap format.

PCRE:

PCRE - Perl-compatible regular expressions.

- The PCRE library is a set of functions that implement regularexpression pattern matching.

Libdnet:

- The libdnet package is designed for, Simple portable interface to lowlevel networking routines.
- libdnet provides a simplified, portable interface to several low-level networking

routines, including network address manipulation, kernel arp(4) cache and route(4) table lookup and manipulation, network firewalling (IP filter, ipfw, ipchains, pf, ...), network interfacelookup and manipulation, raw IP packet and Ethernet frame, and data transmission.

COMMANDS:

[root@localhost security lab]# cd /usr/src

[root@localhost security lab]# wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

[root@localhost security lab]# wget https://www.snort.org/downloads/snort/snort-2.9.16.1.tar.gz

```
[root@localhost security lab]# tar xvzf daq-2.0.7.tar.gz
[root@localhost security lab]# tar xvzf snort-2.9.16.1.tar.gz
[root@localhost security lab]# yum install libpcap* pcre* libdnet* -y
[root@localhost security lab]# cd daq-2.0.7
[root@localhost security lab]# . /configure
[root@localhost security lab]# make
[root@localhost security lab]# make install
[root@localhost security lab]# cd snort-2.9.16.1
[root@localhost security lab]# . /configure
[root@localhost security lab]# make
[root@localhost security lab]# make install
[root@localhost security lab]# snort --version_ -*> Snort! <*- o" )~ Version 2.9.8.2 GRE
(Build 335)
"" By Martin Roesch& The SnortTeam: http://www.snort.org/contact#team
Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.3
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8
[root@localhost security lab]# mkdir /etc/snort
[root@localhost security lab]# mkdir /etc/snort/rules
[root@localhost security lab]# mkdir /var/log/snort
[root@localhost security lab]# vi /etc/snort/snort.conf
add this line- include /etc/snort/rules/icmp.rules
[root@localhost security lab]# vi /etc/snort/rules/icmp.rules
alerticmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)
[root@localhost security lab]# snort -i enp3s0 -c /etc/snort/snort.conf -l /var/log/snort/
Another terminal
[root@localhost security lab]# ping www.yahoo.com
Ctrl + C
[root@localhost security lab]# vi /var/log/snort/alert
[**] [1:477:3] ICMP Packet [**]
```

[Priority: 0]

10/06-15:03:11.187877 192.168.43.148 -> 106.10.138.240

ICMP TTL:64 TOS:0x0 ID:45855 IpLen:20 DgmLen:84 DF

Type:8 Code:0 ID:14680 Seq:64 ECHO

[**] [1:477:3] ICMP Packet [**]

[Priority: 0]

10/06-15:03:11.341739 106.10.138.240 -> 192.168.43.148

ICMP TTL:52 TOS:0x38 ID:2493 IpLen:20 DgmLen:84

Type:0 Code:0 ID:14680 Seq:64 ECHO REPLY

[**] [1:477:3] ICMP Packet [**]

[Priority: 0]

10/06-15:03:12.189727 192.168.43.148 -> 106.10.138.240

ICMP TTL:64 TOS:0x0 ID:46238 IpLen:20 DgmLen:84 DF

Type:8 Code:0 ID:14680 Seq:65 ECHO

[**] [1:477:3] ICMP Packet [**]

[Priority: 0]

10/06-15:03:12.340881 106.10.138.240 -> 192.168.43.148

ICMP TTL:52 TOS:0x38 ID:7545 IpLen:20 DgmLen:84

Type:0 Code:0 ID:14680 Seq:65 ECHO REPLY

RESULT:

EXP. NO: 6

DATE:

LINUX AUDITING USING LYNIS

AIM:

ALGORITHM:

DESCRIPTION:

Lynis is an open-source and much powerful auditing tool for Unix/Linux-like operatingsystems. It scans the system for security information, general system information, installed andavailable software information, configuration mistakes, security issues, user accounts without apassword, wrong file permissions, firewall auditing, etc. Since Lynis is flexible, it is used for variousdifferent purposes that include:

• Security auditing

• Compliance testing

• Penetration testing

• Vulnerability detection

• System hardening

Lynis has color-coding:

Green: which means everything works fine or is disabled

Yellow: Skipped, NOT FOUND, might have a suggestion

Red: It shows that the particular test or scan is unsafe or needs more attention.

White (No color code): Regular File or Normal File

Blue: Directory

Bright Green: Executable File

Bright Red: Archive file or Compressed File

Magenta: Image File

Cyan: Audio File

Sky Blue: Symbolic Link File

OUTPUT:

```
[root@fedora ~]# git clone https://github.com/CISOfy/lynis
Cloning into 'lynis'...
remote: Enumerating objects: 14638, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 14638 (delta 21), reused 30 (delta 13), pack-reused 14594
Receiving objects: 100% (14638/14638), 7.77 MiB | 7.50 MiB/s, done.
Resolving deltas: 100% (10787/10787), done.
[root@fedora ~]# cd lynis
[root@fedora lynis]# ls
CHANGELOG.md        CONTRIBUTING.md  db          developer.prf  FAQ            include  LICENSE  lynis.8  README     SECURITY.md
CODE_OF_CONDUCT.md  CONTRIBUTORS.md  default.prf extras         HAPPY_USERS.md INSTALL  lynis    plugins  README.md  TODO.md
[root@fedora lynis]# ls -l lynis
-rwxr-xr-x. 1 root root 51784 Mar 22 08:49 lynis
[root@fedora lynis]#
```

```
[root@fedora lynis]# lynis show tests ACCT-9626
ACCT-9626
==================================

Type: test

Description:
Check for sysstat accounting data

Category: security, Group: accounting

Test Execution:
  Operating System:    Yes (Linux only)
  Profile:             Yes (not configured)


[root@fedora lynis]#
```

```
[root@fedora lynis]# lynis show tests TOOL-5190
TOOL-5190
==================================

Type: test

Description:
Check presence of available IDS/IPS tooling

Category: security, Group: tooling

Test Execution:
  Operating System:    Yes (all systems)
  Profile:             Yes (not configured)


[root@fedora lynis]#
```

```
[root@fedora lynis]# ./lynis update info

 == Lynis ==

  Version           : 3.0.8
  Status            : Up-to-date
  Release date      : 2022-05-17
  Project page      : https://cisofy.com/lynis/
  Source code       : https://github.com/CISOfy/lynis
  Latest package    : https://packages.cisofy.com/


2007-2021, CISOfy - https://cisofy.com/lynis/

[root@fedora lynis]#
```

```
Hardening index : 69 [##############        ]
Tests performed : 258
Plugins enabled : 0

Components:
- Firewall               [V]
- Malware scanner        [V]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat

================================================================================

  Lynis 3.0.8

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================
```


RESULT:

EXP. NO: 7

DATE:

INSTALL AND CONFIGURE IPTABLES FIREWALL

AIM:

ALGORITHM:

DESCRIPTION:

Iptables is a generic table structure that defines rules and commands as part of the netfilterframework that facilitates Network Address Translation (NAT), packet filtering, and packet manglingin the Linux operating system. NAT is the process of converting an Internet Protocol address (IPaddress) into another IP address. Packet filtering is the process of passing or blocking packets at anetwork interface based on source and destination addresses, ports, or protocols. Packet mangling isthe ability to alter or modify packets before and/or after routing. The firewall matches packets with rules defined in these tables and thentakes the specified action on a possible match.

• Tables is the name for a set of chains.

• Chain is a collection of rules.

• Rule is condition used to match packet.

• Target is action taken when a possible rule matches. Examples of the targetare ACCEPT, DROP, QUEUE.

• Policy is the default action taken in case of no match with the inbuilt chain and can be ACCEPT or DROP.

Syntax

iptables --table TABLE -A/-C/-D... CHAIN rule --jump Target

TABLE

There are five possible tables:

• filter: Default used table for packet filtering. It includes chains like INPUT,OUTPUT and FORWARD.

• nat : Related to Network Address Translation. It includesPREROUTING and POSTROUTING chains.

• mangle : For specialised packet alteration. Inbuilt chains includePREROUTING and OUTPUT.

• raw : Configures exemptions from connection tracking. Built-in chains arePREROUTING and OUTPUT.

• security : Used for Mandatory Access Control

CHAINS

There are few built-in chains that are included in tables.

• They are:

1.INPUT :set of rules for packets destined to localhost sockets.

2.FORWARD :for packets routed through the device.

3.OUTPUT :for locally generated packets, meant to be transmitted outside.

4.PREROUTING :for modifying packets as they arrive.

5.POSTROUTING :for modifying packets as they are leaving.

- While trying out the commands, Remove all filtering rules and user createdchains.
  sudoiptables --flush
- To save the iptables configuration use:
  sudoiptables-save
- Restoring iptablesconfig can be done with:
  sudoiptables-restore

OPTIONS

-A, –append : Append to the chain provided in parameters.

Syntax:

iptables [-t table] --append [chain] [parameters]

Example: This command drops all the traffic coming on any port.

iptables -t filter --append INPUT -j DROP

PARAMETERS

-s, –source: is used to match with the source address of the packet.

Syntax:

iptables [-t table] -A [chain] -s {source_address} [target]

Example: This command appends a rule in the INPUT chain to accept all packetsoriginating from 192.168.1.230.

iptables -t filter -A INPUT -s 192.168.1.230 -j ACCEPT

-d, –destination : is used to match with the destination address of the packet.

Syntax:

iptables [-t table] -A [chain] -d {destination_address} [target]

Example: This command appends a rule in the OUTPUT chain to drop allpackets destined for 192.168.1.123.

iptables -t filter -A OUTPUT -d 192.168.1.123 -j DROP

-j, –jump : this parameter specifies the action to be taken on a match.

Syntax:

iptables [-t table] -A [chain] [parameters]

Example: This command adds a rule in the FORWARD chain to drop all packets.

iptables -t filter -A FORWARD – j DROP

OUTPUT:

```
computer@computer:~$ sudo iptables -t filter --append INPUT -j DROP
computer@computer:~$ ping www.google.com
ping: unknown host www.google.com
computer@computer:~$ sudo iptables -t filter --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
Terminal File Edit View Search Terminal Help
computer@computer:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  192.168.1.123        anywhere
2    DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain DOCKER-USER (0 references)
num  target     prot opt source               destination
computer@computer:~$ sudo iptables -t filter --delete INPUT 2
computer@computer:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  thinkpad-e470.lan    anywhere

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain DOCKER-USER (0 references)
num  target     prot opt source               destination
computer@computer:~$
```

```
computer@computer:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain DOCKER-USER (0 references)
num  target     prot opt source               destination
computer@computer:~$ sudo iptables -t filter --check INPUT -s 192.168.1.123 -j DROP ; echo $?
iptables: Bad rule (does a matching rule exist in that chain?).
1
computer@computer:~$ sudo iptables -t filter --check INPUT -j DROP ; echo $?
0
computer@computer:~$
```

```
Terminal  File  Edit  View  Search  Terminal  Help
computer@computer:~$ sudo iptables -t filter -A INPUT -p udp -j DROP
computer@computer:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       udp  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DOCKER-USER (0 references)
target     prot opt source               destination
computer@computer:~$
```

```
computer@computer:~$ sudo iptables -t filter -A FORWARD -j DROP
computer@computer:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       udp  --  anywhere             anywhere
ACCEPT     all  --  192.168.1.230        anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.123
computer@computer:~$
```

RESULT:

EXP. NO: 8a

DATE:

LIVE DATA ACQUISITION OF RAM

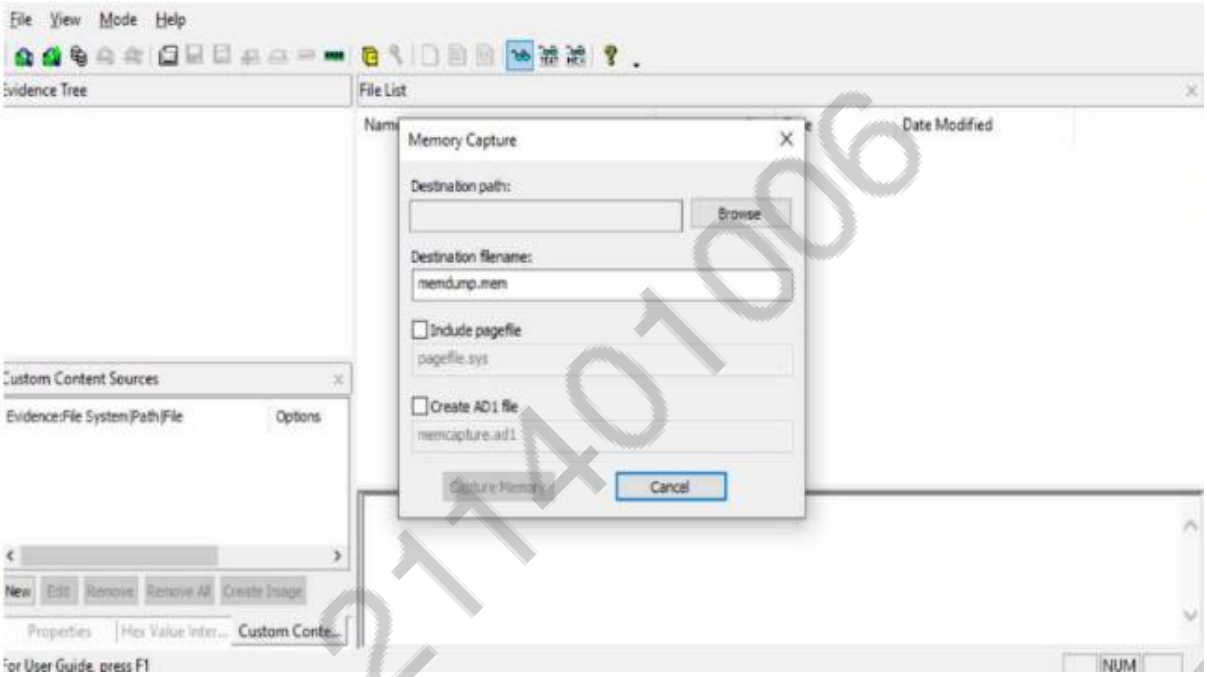
AIM:

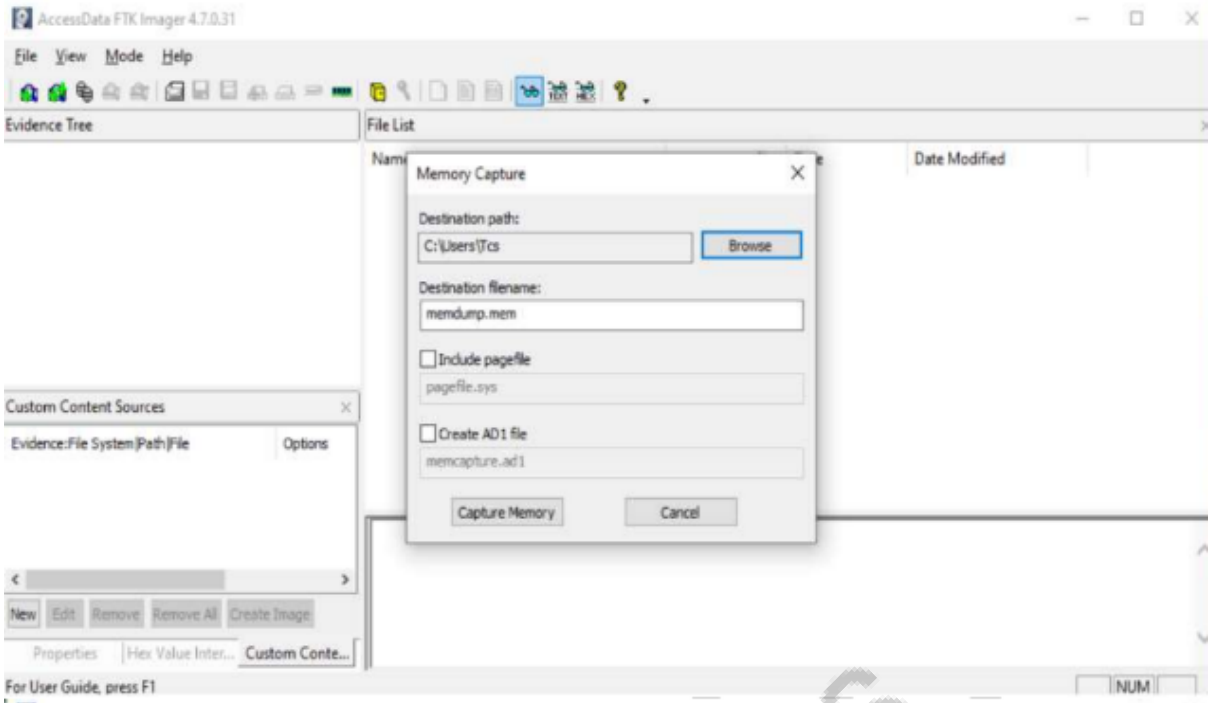
ALGORITHM:

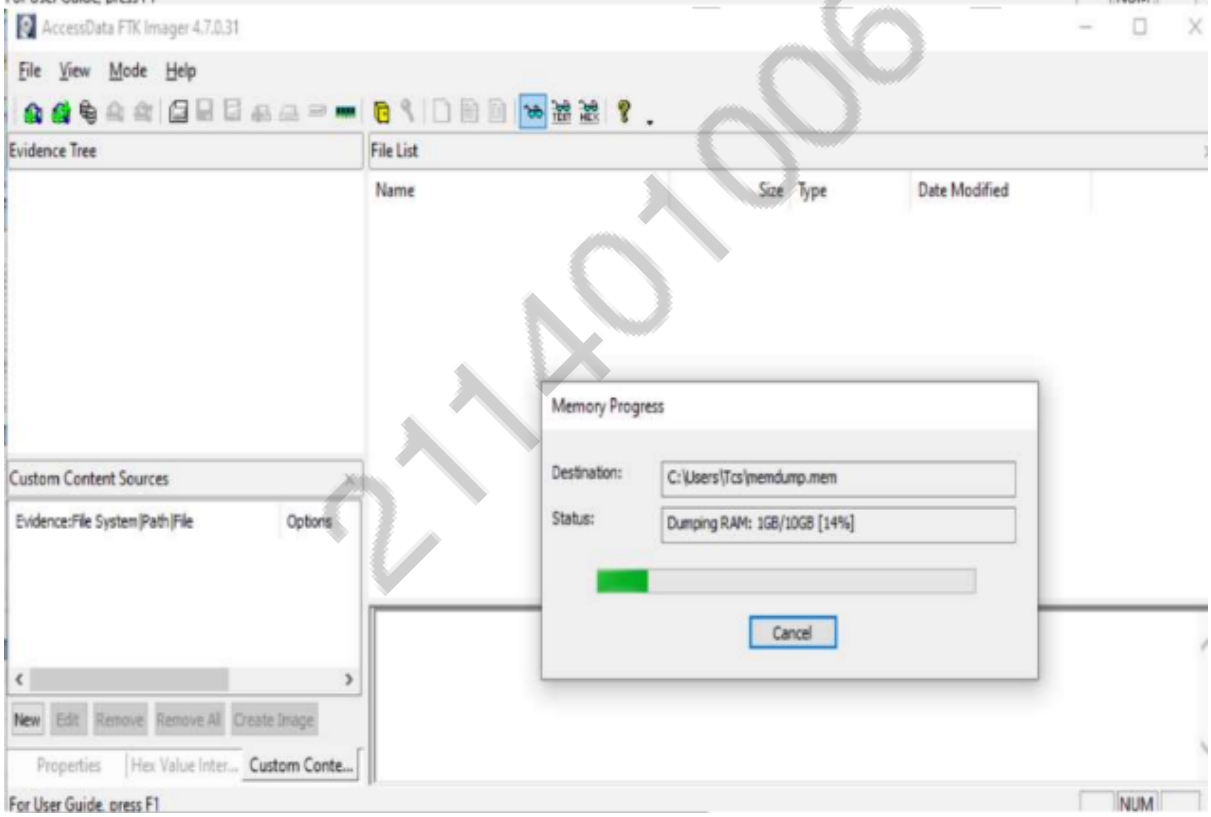
DESCRIPTION:

FTK Imager is an open-source software by AccessData that is used for creating accurate copiesof the original evidence without actually making any changes to it. The Image of the original evidenceis remaining the same and allows us to copy data at a much faster rate, which can be soon be preservedand can be analyzed further.The FTK imager also provides you with the inbuilt integrity checking function which generatesa hash report which helps matching the hash of the evidence before and after creating the image ofthe original Evidence.

OUTPUT:




AccessData FTK Imager 4.7.0.31
File View Mode Help
Evidence Tree
File List
Date Modified
Memory Capture
Destination path:
C:\Users\Tcs
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM


AccessData FTK Imager 4.7.0.31
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Memory Progress
Destination:
C:\Users\Tcs\memdump.mem
Status:
Dumping RAM: 1GB/10GB [14%]
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM

```
C:\Users\Tcs>dir
 Volume in drive C has no label.
 Volume Serial Number is 1E1A-02BD

 Directory of C:\Users\Tcs

18-04-2023  01.07 PM    <DIR>          .
18-04-2023  01.07 PM    <DIR>          ..
21-03-2023  02.15 PM    <DIR>          .android
20-02-2019  11.32 AM    <DIR>          .AndroidStudio3.3
12-11-2019  11.09 AM    <DIR>          .appsb
25-08-2018  03.23 PM    <DIR>          .argouml
18-10-2022  11.03 AM    <DIR>          .cache
25-01-2018  02.49 PM                 0 .cdtclient
26-08-2022  02.03 PM    <DIR>          .config
18-10-2022  11.03 AM    <DIR>          .eclipse
27-02-2018  02.29 PM                16 .emulator_console_auth_token
25-03-2022  10.44 AM               207 .gitconfig
09-08-2022  12.31 PM    <DIR>          .gradle
17-01-2018  10.49 AM    <DIR>          .idlerc
09-08-2022  12.54 PM    <DIR>          .m2
24-06-2022  11.00 AM    <DIR>          .ms-ad
30-06-2018  09.45 AM    <DIR>          .nbi
18-10-2022  11.03 AM    <DIR>          .p2
22-08-2022  10.10 AM               184 .packettracer
04-04-2023  10.33 AM    <DIR>          .spss
12-11-2019  11.09 AM    <DIR>          .swt
```

```
The directory name is invalid.

C:\Users\Tcs>CertUtil -hashfile
Expected at least 1 args, received 0
CertUtil: Missing argument

Usage:
  CertUtil [Options] -hashfile InFile [HashAlgorithm]
  Generate and display cryptographic hash over a file

Options:
  -Unicode          -- Write redirected output in Unicode
  -gmt              -- Display times as GMT
  -seconds          -- Display times with seconds and milliseconds
  -v                -- Verbose operation
  -privatekey       -- Display password and private key data
  -pin PIN                  -- Smart Card PIN
  -sid WELL_KNOWN_SID_TYPE  -- Numeric SID
            22 -- Local System
            23 -- Local Service
            24 -- Network Service

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

CertUtil -?              -- Display a verb list (command list)
CertUtil -hashfile -?    -- Display help text for the "hashfile" verb
CertUtil -v -?           -- Display all help text for all verbs


C:\Users\Tcs>
```


RESULT:

EXP. NO: 8b

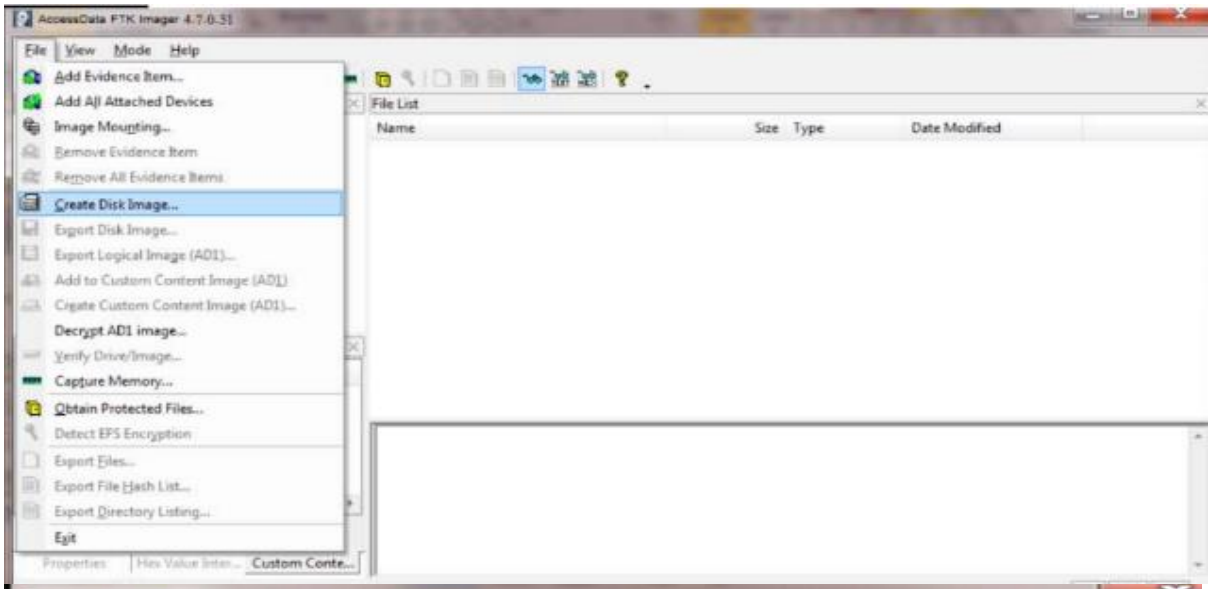
DATE:

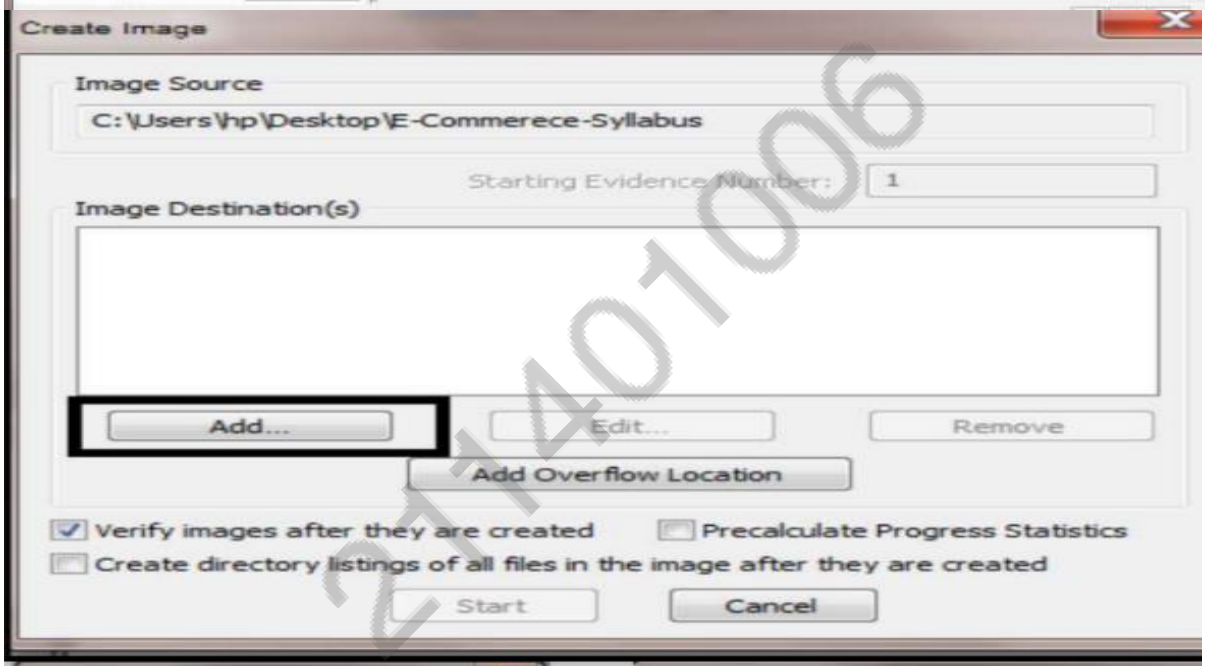
LIVE DATA AQCUISITION OF A FOLDER

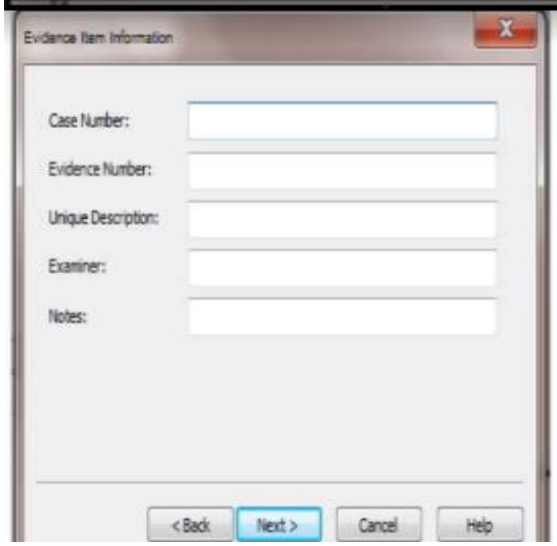
AIM:

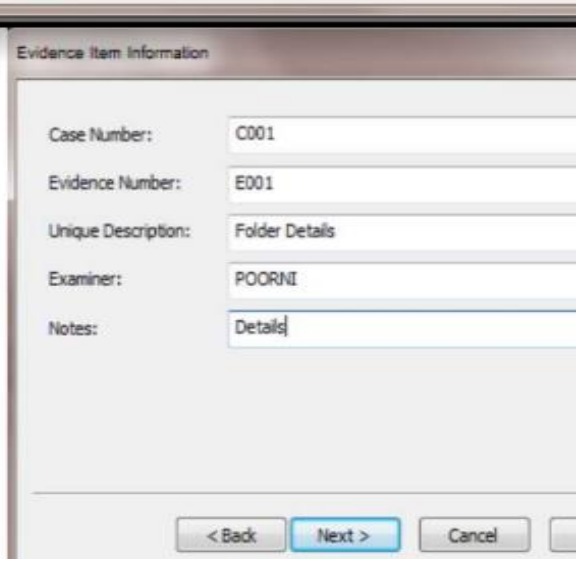
ALGORITHM:

OUTPUT:


AccessData FTK Imager 4.7.0.51
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EPS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name
Size
Type
Date Modified


Create Image
Image Source
C:\Users\hp\Desktop\E-Commerece-Syllabus
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel
21T401006


Evidence Item Information
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:
< Back
Next >
Cancel
Help


Evidence Item Information
Case Number:
C001
Evidence Number:
E001
Unique Description:
Folder Details
Examiner:
POORNI
Notes:
Details
< Back
Next >
Cancel

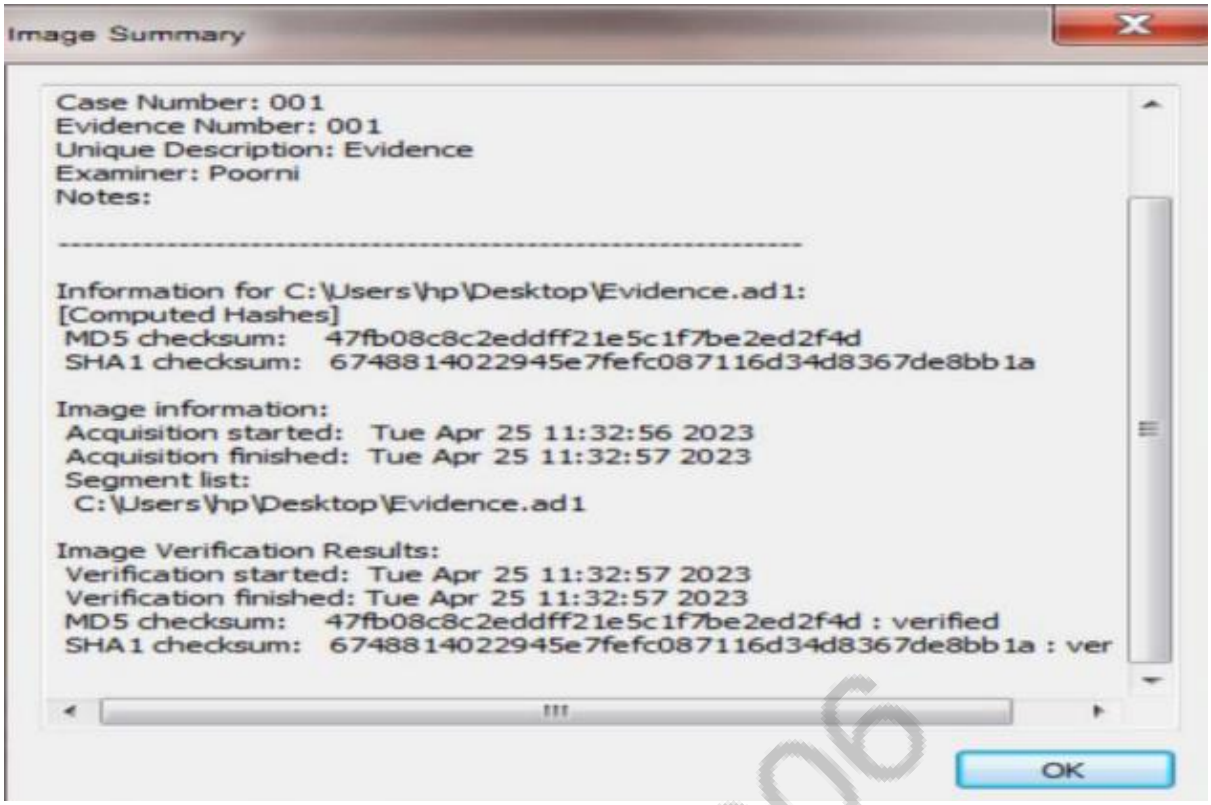


Image Summary

```
Case Number: 001
Evidence Number: 001
Unique Description: Evidence
Examiner: Poorni
Notes:

--------------------------------------------------------------

Information for C:\Users\hp\Desktop\Evidence.ad1:
[Computed Hashes]
 MD5 checksum:    47fb08c8c2eddff21e5c1f7be2ed2f4d
 SHA1 checksum:   6748814022945e7fefc087116d34d8367de8bb1a

Image information:
 Acquisition started:   Tue Apr 25 11:32:56 2023
 Acquisition finished:  Tue Apr 25 11:32:57 2023
 Segment list:
  C:\Users\hp\Desktop\Evidence.ad1

Image Verification Results:
 Verification started:  Tue Apr 25 11:32:57 2023
 Verification finished: Tue Apr 25 11:32:57 2023
 MD5 checksum:    47fb08c8c2eddff21e5c1f7be2ed2f4d : verified
 SHA1 checksum:   6748814022945e7fefc087116d34d8367de8bb1a : ver
```

OK

RESULT:

EXP. NO: 9

DATE:

LINUX OS HARDENING

AIM:

ALGORITHM:

DESCRIPTION:

- To harden the Linux operating system through various configurations and reducing

the attack surface.

- The chkconfig command tool allows to configure services start and stop automatically

through command line.

--list Parameter will displayed all services and their current start-up status in each

run-level configuration.

grep - Global Search for Regular Expression and Print out.

The grep filter searches a file for a particular pattern of characters, anddisplays all lines that

contain that pattern.

To disable USB storage, create the following file and edit it with yourfavourite text editor.

/etc/modprobe.d/usb-storage.conf

Within this file, add the following line.

installusb-storage /bin/true

After saving that line to the /etc/modprobe.d/usb-storage.conf file youwill need to perform a

reboot to complete the process.

After rebooting if you plug in a USB storage device you should not be

able to access it.

Awk is abbreviated from the names of the developers – Aho, Weinberger, and

Kernighan.

- Awk is a scripting language used for manipulating data and generating

reports.

- The awk command programming language requires no compiling and allows

the user to use variables, numeric functions, string functions, and logical

operators.

- Awk is mostly used for pattern scanning and processing.

Lockdown cron jobs by putting the name into the cron.deny file

- Cron is a system that helps Linux users to schedule any task. However, a cron job is

any defined task to run in a given timeperiod.

- It can be a shell script or a simple bash command.
- Cron job helps us automate our routine tasks, it can be hourly,daily, monthly, etc.
- The crontab stands for cron table.

 It is a Linux system file that contains a list of the cron job.

 The control access to the crontab command by using two files inthe /etc/cron.d

directory:

cron.deny and cron.allow. To harden the Linux operating system through various configurations and reducing

the attack surface.

- The chkconfig command tool allows to configure services start and stop automatically

through command line.

--list Parameter will displayed all services and their current start-up status in each

run-level configuration.

grep - Global Search for Regular Expression and Print out.

The grep filter searches a file for a particular pattern of characters, anddisplays all lines that

contain that pattern.

To disable USB storage, create the following file and edit it with yourfavourite text editor.

/etc/modprobe.d/usb-storage.conf

Within this file, add the following line.

installusb-storage /bin/true

After saving that line to the /etc/modprobe.d/usb-storage.conf file youwill need to perform a

reboot to complete the process.

After rebooting if you plug in a USB storage device you should not be

able to access it.

Awk is abbreviated from the names of the developers – Aho, Weinberger, and

Kernighan.

- Awk is a scripting language used for manipulating data and generating

reports.

- The awk command programming language requires no compiling and allows

the user to use variables, numeric functions, string functions, and logical

operators.

- Awk is mostly used for pattern scanning and processing.

Lockdown cron jobs by putting the name into the cron.deny file

- Cron is a system that helps Linux users to schedule any task. However, a cron job is

any defined task to run in a given timeperiod.

- It can be a shell script or a simple bash command.
- Cron job helps us automate our routine tasks, it can be hourly,daily, monthly, etc.
- The crontab stands for cron table.
- It is a Linux system file that contains a list of the cron job.
- The control access to the crontab command by using two files inthe /etc/cron.d directory: cron.deny and cron.allow.

OUTPUT:

```
[student@fedora ~]$ su
Password:
[root@fedora student]# chkconfig --list

Note: This output shows SysV services only and does not include native
      systemd services. SysV configuration data might be overridden by native
      systemd configuration.

      If you want to list systemd services use 'systemctl list-unit-files'.
      To see services enabled on particular target use
      'systemctl list-dependencies [target]'.

livesys         0:off   1:off   2:off   3:on    4:on    5:on    6:off
livesys-late    0:off   1:off   2:off   3:on    4:on    5:on    6:off
[root@fedora student]#
```

```
[root@fedora student]# chkconfig --list | grep livesys

Note: This output shows SysV services only and does not include native
      systemd services. SysV configuration data might be overridden by native
      systemd configuration.

      If you want to list systemd services use 'systemctl list-unit-files'.
      To see services enabled on particular target use
      'systemctl list-dependencies [target]'.

livesys         0:off   1:off   2:off   3:off   4:off   5:off   6:off
livesys-late    0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

```
[root@fedora student]# yum update all
Fedora 36 - x86_64                          4.6 kB/s | 5.6 kB     00:01
Fedora Modular 36 - x86_64                  7.4 kB/s | 5.5 kB     00:00
Fedora 36 - x86_64 - Updates                8.0 kB/s | 6.0 kB     00:00
Fedora 36 - x86_64 - Updates                2.5 MB/s |  17 MB     00:06
Fedora Modular 36 - x86_64 - Updates        7.6 kB/s | 5.4 kB     00:00
Fedora Modular 36 - x86_64 - Updates        137 kB/s | 597 kB     00:04
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are pro
tected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

```
[root@localhost ~]# echo ALL >>/etc/cron.deny
[root@localhost ~]# cat  /etc/cron.deny
ALL
ALL
ALL
```


RESULT:

EXP. NO: 10

DATE:

N-STALKER

AIM:

ALGORITHM:

DESCRIPTION:

N-Stalker is a leader on Web Application Security Assessment technology. It currently developsand maintains N-Stalker Web Application Security Scanner suite, a software product aimed onscanning and finding security vulnerabilities in Web Applications. It can play significant role inapplication security testing. This is trusted when it comes to browser level vulnerabilities. Some of thefeatures are-

• HTTP Fingerprinting
• Parallel Web Crawling
• Server-side technology discoverer
• Automatic False Positive Prevention Engine
• Component-oriented Web Crawler
• Component-oriented Scanning Engine
• IDS Evasion Fuzzing Test
• Web form autocomplete mechanism

Development & QA Profile

1. A deep approach in the Web Application structure and output code (HTML),enabling N-Stalker to sweep out transaction brokers andcommon application areas to identify development security flaws.
2. A QA approach can be used to certify internal or third-party development code and give the level of trust needed to promote webapplications to production level.

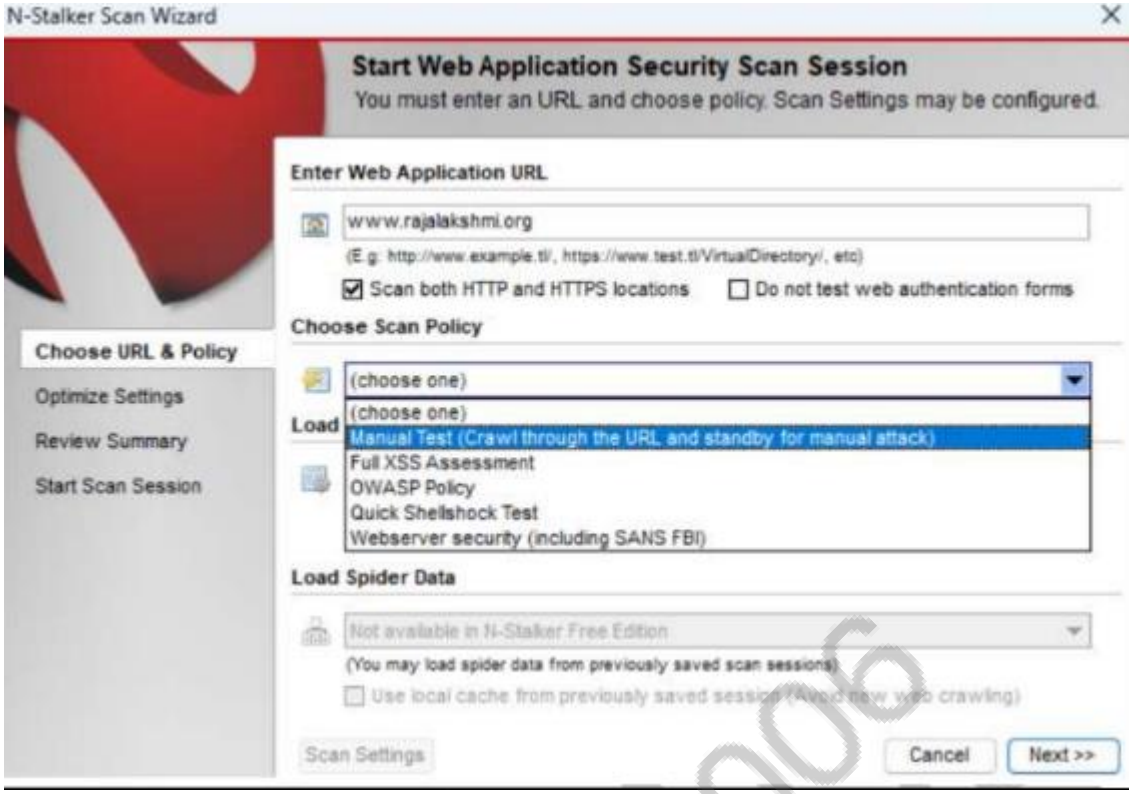
Infrastructure & Deploy Profile:

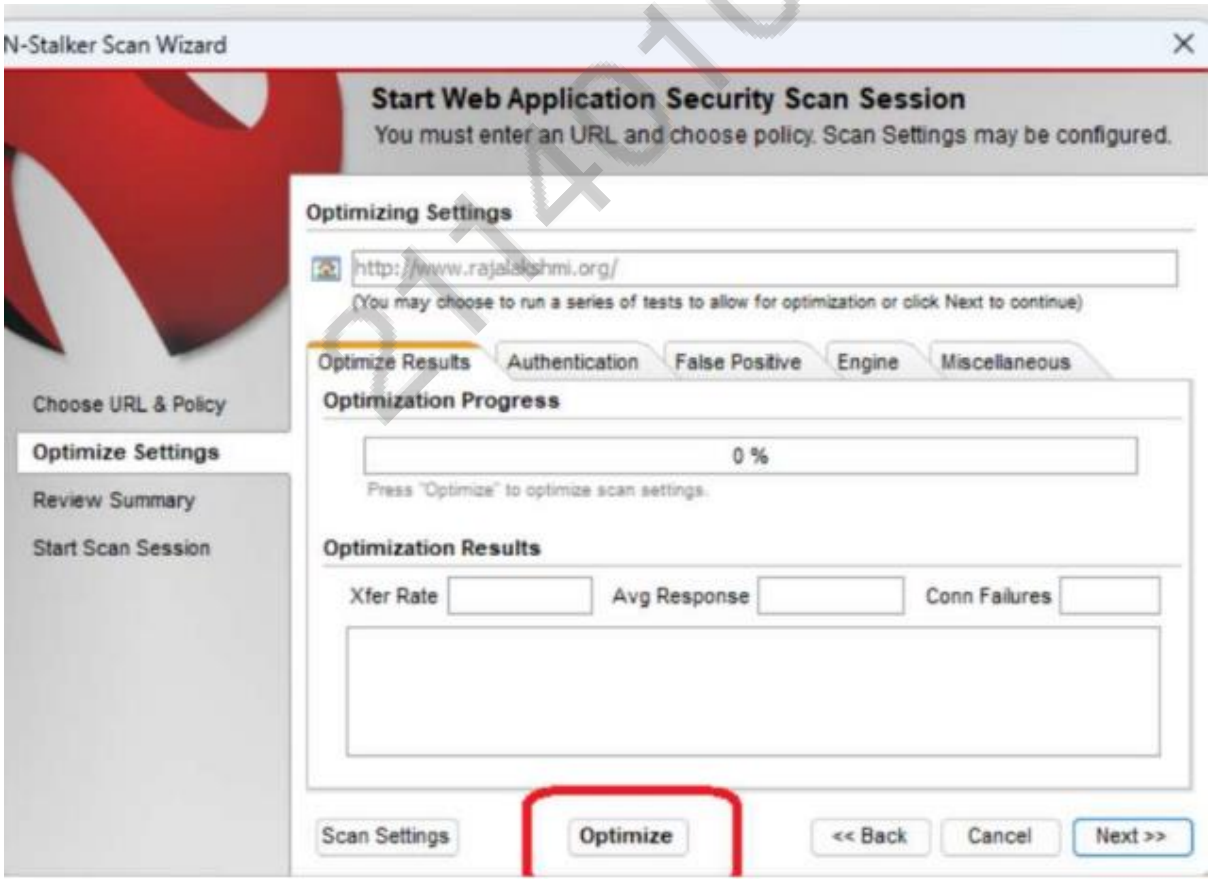
N-Stalker is the only vendor to provide more than 35,000 attack signatures toassess your Web server infrastructure and guarantee a safe hostingenvironment.

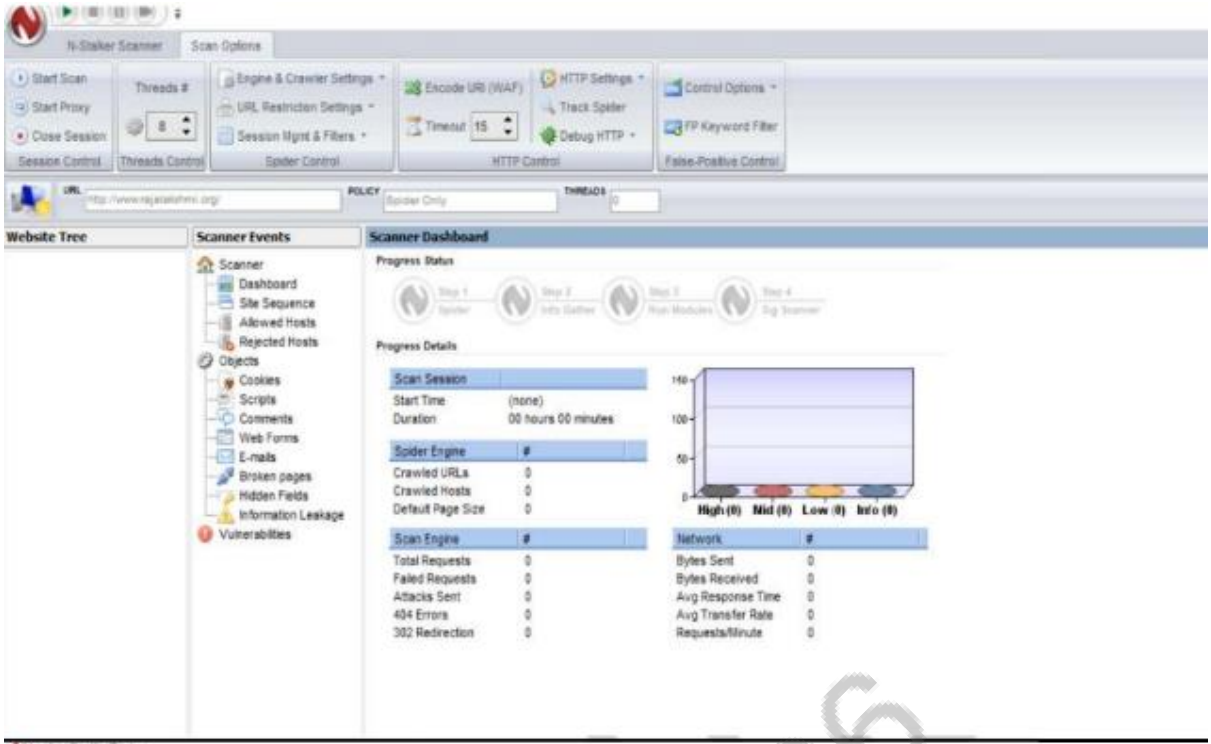
Pen-test and Security Audit Profile:

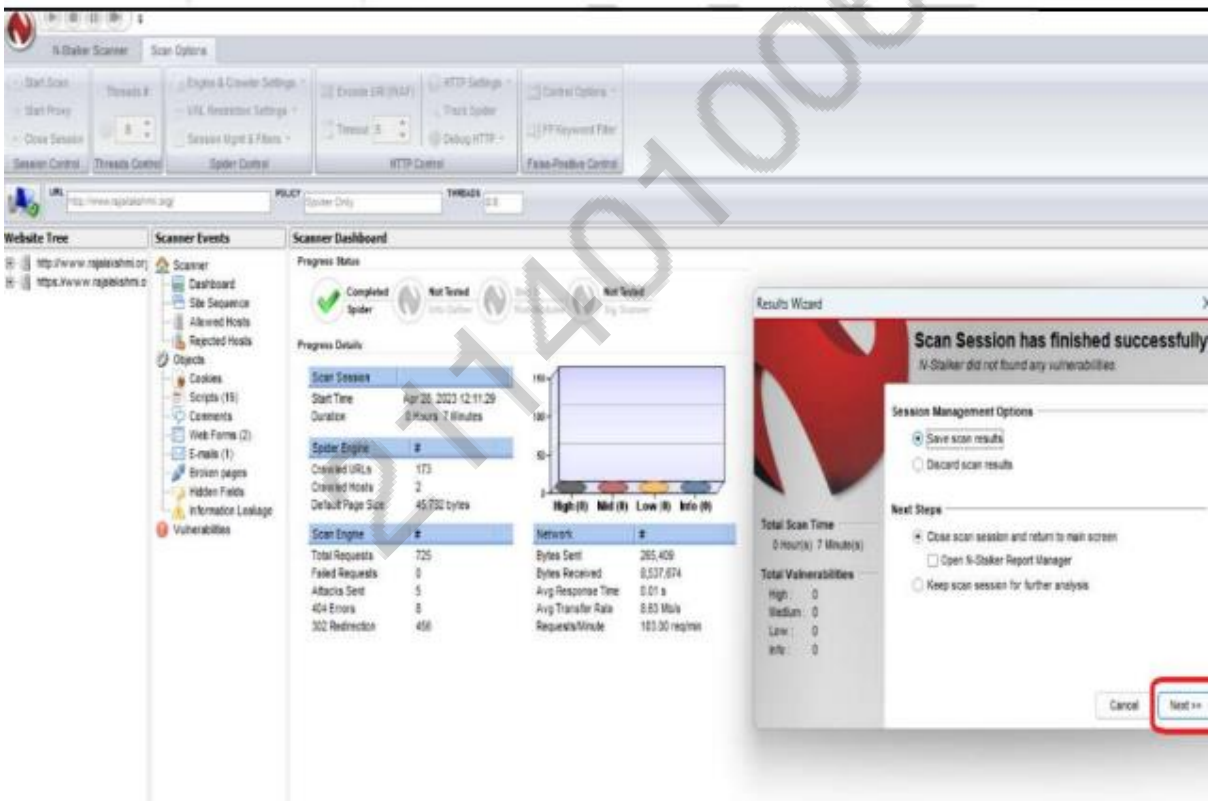
A complete analysis of your web application, includingdevelopment, infrastructure and production aspects thatcan be used to assess the current level of security of WebApplications currently in use.

OUTPUT:









RESULT:

EXP. NO: 11

DATE:

WEB VULNERABILITIES USING O-SAFT

AIM:

ALGORITHM:

DESCRIPTION:

O-Saft is easy to use tool to show informationabout SSL certificate and tests the SSLconnection according to given list of ciphers andvarious SSL configurations.

O-Saft - OWASP SSL advanced forensic toolOWASP SSL audit for testers

List the contents of an archive file.

 The “-t” option can be used to list the contents of an archive file without extracting it.

+cipher

Check target for ciphers, either all ciphers, or ciphers specifiedwith --cipher=CIPHER option.

+version

Show version information for both theprogram and the Perl modules that it uses.

A TLD (top-level domain) is the most generic domain in the Internet's hierarchical DNS domain namesystem).

TLD is everything that follows the final dot of a domain name. For example, in the domain name 'google.com','.com' is the TLD. Some other popular TLDs include '. org', '. uk', and '.

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server

TLS (Transport Layer Security)

SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data andcertificate.

The RSA algorithm (Rivest-Shamir-Adleman) is the basis of a cryptosystem -- a suite of cryptographicalgorithms that are used for specific security services or purposes.

AES stands for Advanced Encryption Standard.

DES stands for Data Encryption Standard.

Camellia is a symmetric block cipher with secret key of size of 128, 192 or 256 bits.

ARIA is a block cipher.uses a substitution–permutation network structure based on AES.

The Diffie-Hellman algorithm (DHA)

Ephemeral Diffie-Hellman (DHE)

OUTPUT:

```
[root@fedora student]# wget -c https://github.com/OWASP/O-Saft/raw/master/o-saft.tgz
--2023-05-02 14:53:10--  https://github.com/OWASP/O-Saft/raw/master/o-saft.tgz
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/OWASP/O-Saft/master/o-saft.tgz [following]
--2023-05-02 14:53:10--  https://raw.githubusercontent.com/OWASP/O-Saft/master/o-saft.tgz
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2455024 (2.3M) [application/octet-stream]
Saving to: 'o-saft.tgz'

o-saft.tgz          100%[===================>]   2.34M   495KB/s    in 4.8s

2023-05-02 14:53:16 (495 KB/s) - 'o-saft.tgz' saved [2455024/2455024]

[root@fedora student]#
```

```
[root@fedora student]# ls -lrt
total 4280
-rw-r--r--. 1 student student 1890015 Jul 21  2022 7th-Std-Tamil-Book-Back-Questions.pdf
drwxr-xr-x. 1 student student       0 Jan 27 09:43 Videos
drwxr-xr-x. 1 student student       0 Jan 27 09:43 Templates
drwxr-xr-x. 1 student student       0 Jan 27 09:43 Public
drwxr-xr-x. 1 student student       0 Jan 27 09:43 Music
drwxr-xr-x. 1 student student       0 Jan 27 09:43 Desktop
drwxr-xr-x. 1 student student      56 Feb 15 08:18 Documents
-rw-rw-r--. 1 student student       0 Mar 10 09:06 Sam.sh
-rw-rw-r--. 1 student student       0 Mar 10 09:06 Sam1.txt
--w-rw-r--. 1 student student       0 Mar 10 09:08 Sample.txt
-rwxrwxr-x. 1 student student   26808 Apr 12 09:01 a.out
-rw-rw-r--. 1 student student    1518 Apr 12 09:13 sjfscheduling.c
drwxr-xr-x. 1 student student      58 May  2 14:43 Downloads
-rw-r--r--. 1 root    root    2455024 May  2 14:53 o-saft.tgz
drwxr-xr-x. 1 student student      22 May  2 14:53 Pictures
[root@fedora student]#
```

```
[root@fedora student]# tar -tf o-saft.tgz
O-Saft/o-saft.pl
O-Saft/o-saft.tcl
O-Saft/o-saft-img.tcl
O-Saft/checkAllCiphers.pl
O-Saft/yeast.pl
O-Saft/o-saft
O-Saft/o-saft.cgi
O-Saft/o-saft.php
O-Saft/contrib/o-saft-standalone.pl
O-Saft/o-saft-docker
O-Saft/o-saft-docker-dev
O-Saft/Dockerfile
O-Saft/osaft.pm
O-Saft/Net/SSLinfo.pm
O-Saft/Net/SSLhello.pm
O-Saft/OSaft/Ciphers.pm
O-Saft/OSaft/Data.pm
O-Saft/OSaft/Text.pm
O-Saft/OSaft/error_handler.pm
O-Saft/o-saft-dbx.pm
```

```
O-Saft/t/Makefile.opt
O-Saft/t/Makefile.cmd
O-Saft/t/Makefile.ext
O-Saft/t/Makefile.exit
O-Saft/t/Makefile.cgi
O-Saft/t/Makefile.tcl
O-Saft/t/Makefile.misc
O-Saft/t/Makefile.warnings
O-Saft/t/Makefile.critic
O-Saft/t/Makefile.dev
O-Saft/t/Makefile.etc
O-Saft/t/Makefile.template
O-Saft/t/Makefile.docker
O-Saft/t/Makefile.FQDN
O-Saft/t/Makefile.examples
O-Saft/t/SSLinfo.pl
O-Saft/t/o-saft_bench.sh
O-Saft/t/cloc-total.awk
O-Saft/t/critic_345.sh
O-Saft/t/gen-graph-annotations.sh
O-Saft/t/gen-graph-sub-calls.sh
O-Saft/t/test-bunt.pl.txt
O-Saft/t/.perlcriticrc
O-Saft/contrib/bash_completion_o-saft
```

```
O-Saft/contrib/HTML-table.awk
O-Saft/contrib/JSON-struct.awk
O-Saft/contrib/JSON-array.awk
O-Saft/contrib/XML-attribute.awk
O-Saft/contrib/XML-value.awk
O-Saft/contrib/lazy_checks.awk
O-Saft/contrib/Cert-beautify.pl
O-Saft/contrib/alertscript.pl
O-Saft/contrib/alertscript.cfg
O-Saft/contrib/bunt.pl
O-Saft/contrib/bunt.sh
O-Saft/contrib/symbol.pl
O-Saft/contrib/cipher_check.sh
O-Saft/contrib/critic.sh
O-Saft/contrib/gen_standalone.sh
O-Saft/contrib/distribution_install.sh
O-Saft/contrib/install_openssl.sh
O-Saft/contrib/install_perl_modules.pl
O-Saft/contrib/INSTALL-template.sh
O-Saft/contrib/Dockerfile.alpine-3.6
O-Saft/contrib/zap_config.sh
O-Saft/contrib/zap_config.xml
O-Saft/INSTALL.sh
[root@fedora student]#
```

```
[root@fedora O-Saft]# yum install perl
Fedora 36 - x86_64                                6.8 kB/s | 5.6 kB     00:00
Fedora 36 openh264 (From Cisco) - x86_64          1.2 kB/s | 989  B     00:00
Fedora Modular 36 - x86_64                        7.0 kB/s | 5.5 kB     00:00
Fedora 36 - x86_64 - Updates                      7.4 kB/s | 5.8 kB     00:00
Fedora 36 - x86_64 - Updates                      2.3 MB/s |  17 MB     00:07
Fedora Modular 36 - x86_64 - Updates              5.4 kB/s | 5.1 kB     00:00
Fedora Modular 36 - x86_64 - Updates              223 kB/s | 596 kB     00:02
Dependencies resolved.
================================================================================
 Package                      Arch     Version                Repo       Size
================================================================================
Installing:
 perl                         x86_64   4:5.34.1-486.fc36      fedora     18 k
Installing dependencies:
 annobin-docs                 noarch   12.02-1.fc36           updates    93 k
 annobin-plugin-gcc           x86_64   12.02-1.fc36           updates   896 k
```

```
 perl-Time                    noarch   1.03-486.fc36          fedora     23 k
 perl-Time-HiRes              x86_64   4:1.9767-480.fc36      fedora     57 k
 perl-Time-Piece              x86_64   1.3401-486.fc36        fedora     46 k
 perl-Unicode-Collate         x86_64   1.31-1.fc36            fedora    737 k
 perl-Unicode-Normalize       x86_64   1.28-479.fc36          fedora     91 k
 perl-Unicode-UCD             noarch   0.75-486.fc36          fedora     83 k
 perl-User-pwent              noarch   1.03-486.fc36          fedora     25 k
 perl-autodie                 noarch   2.34-480.fc36          fedora     94 k
 perl-autouse                 noarch   1.11-486.fc36          fedora     19 k
 perl-bignum                  noarch   0.65-1.fc36            updates    50 k
 perl-blib                    noarch   1.07-486.fc36          fedora     17 k
 perl-debugger                noarch   1.60-486.fc36          fedora    139 k
 perl-deprecate               noarch   0.04-486.fc36          fedora     19 k
 perl-devel                   x86_64   4:5.34.1-486.fc36      fedora    677 k
 perl-diagnostics             noarch   1.37-486.fc36          fedora    216 k
 perl-doc                     noarch   5.34.1-486.fc36        fedora    4.7 M
 perl-encoding                x86_64   4:3.00-485.fc36        updates    63 k
```

```
Target supports PSK Identity Hint:
Target's OCSP Response:
Target's supported ALPNs:
Target's supported  NPNs:
Target's selected protocol (ALPN):
Target's selected protocol  (NPN):
Target's advertised protocols:
Target's Server public key length:
Target's DH Parameter:
Target's Master-Key:
Target's Session-ID:
Target's Session-ID-ctx:
Target's TLS Session Ticket:
Target's TLS Session Ticket Lifetime:
Target's TLS Session Start Time locale:
Target's TLS Session Start Time EPOCH:  139746545144144
Target's fallback SSL Protocol:         TLSv1_3
Selected SSL Protocol:                  TLSv12
HTTP Status line:                       HTTP/1.1 302 Found
HTTP Location header:                   https://rajalakshmi.org/
HTTP Refresh header:
HTTP STS header:
HTTPS Server banner:                    Apache/2.4.46 (Win64) OpenSSL/1.1.1h PH
P/8.0.0
HTTPS Status line:                      HTTP/1.1 200 OK
HTTPS Location header:
HTTPS Refresh header:
HTTPS Error alerts:
HTTPS STS header:
HTTPS STS MaxAge:
HTTPS STS include sub-domains:
```

```
[root@fedora O-Saft]# ./o-saft +cipher rajalakshmi.org
./o-saft.pl   +cipher rajalakshmi.org  | cat
!!Hint: +cipher : functionality changed, please see 'o-saft.pl --help=TECHNIC'
**WARNING: 149: no executable for '/usr/local/openssl/bin/openssl' found; all o
penssl functionality disabled
!!Hint: consider using '--openssl=/path/to/openssl'
**WARNING: 409: SSLv2 does not support SNI; cipher checks are done without SNI

=== Ciphers: Checking SSLv2 ===
=   Total number of checked ciphers      59
**WARNING: 409: SSLv3 does not support SNI; cipher checks are done without SNI

=== Ciphers: Checking SSLv3 ===
=   Total number of checked ciphers      2640

=== Ciphers: Checking TLSv1 ===
    ECDHE-RSA-AES256-SHA                 yes     HIGH
    DHE-RSA-AES256-SHA                   yes     HIGH
    DHE-RSA-CAMELLIA256-SHA              yes     HIGH
    ECDHE-RSA-AES128-SHA                 yes     HIGH
    DHE-RSA-AES128-SHA                   yes     HIGH
    DHE-RSA-CAMELLIA128-SHA              yes     HIGH
    AES256-SHA                           yes     HIGH
    CAMELLIA256-SHA                      yes     HIGH
    AES128-SHA                           yes     HIGH
    CAMELLIA128-SHA                      yes     HIGH
    DHE-RSA-SEED-SHA                     yes     MEDIUM
    SEED-SHA                             yes     MEDIUM
    IDEA-CBC-SHA                         yes     weak
```

```
[root@fedora O-Saft]# ./o-saft +version
./o-saft.pl   +version  | cat
**WARNING: 149: no executable for '/usr/local/openssl/bin/openssl' found; all o
penssl functionality disabled
!!Hint: consider using '--openssl=/path/to/openssl'
**ERROR: 007: Can't locate Net/DNS.pm in @INC (you may need to install the Net
:DNS module) (@INC contains: .. /home/student/O-Saft . lib bin /usr/local/lib64
/perl5/5.34 /usr/local/share/perl5/5.34 /usr/lib64/perl5/vendor_perl /usr/share
/perl5/vendor_perl /usr/lib64/perl5 /usr/share/perl5) at ./o-saft.pl line 309.
at ./o-saft.pl line 1205.
**WARNING: 101: 'require Net/DNS.pm' failed
**WARNING: 111: option '--mx disabled
=== started in: /home/student/O-Saft ===
=== ./o-saft.pl 23.04.23 ===
    Net::SSLeay::
       ::OPENSSL_VERSION_NUMBER()    0x30000000 (805306368)
       ::SSLeay()                    0x30000020 (805306400)
    Net::SSLeay::SSLeay_version()    OpenSSL 3.0.2 15 Mar 2022
= openssl =
    external executable              <<executable not found>>
    external executable (TLSv1.3)    openssl
    version of external executable   <<openssl>>
    used environment variable (name) LD_LIBRARY_PATH
    environment variable (content)   <<undef>>
    path to shared libraries
    full path to openssl.cnf file    /usr/local/openssl/ssl/openssl.cnf
    common openssl.cnf files         /etc/ssl/openssl.cnf /usr/lib/ssl/openssl
```

```
    common openssl.cnf files         /etc/ssl/openssl.cnf /usr/lib/ssl/openssl.
cnf /System//Library/OpenSSL/openssl.cnf /usr/ssl/openssl.cnf
    URL where to find CRL file       <<undef>>
    directory with PEM files for CAs /etc/ssl/certs/
    PEM format file with CAs         /etc/ssl/certs//ca-certificates.crt
    common paths to PEM files for CAs /etc/ssl/certs /usr/lib/certs /System/Lib
rary/OpenSSL /etc/tls/certs
    common PEM filenames for CAs     ca-certificates.crt certificates.crt certs
.pem cert.pem
= o-saft.pl =
    list of supported elliptic curves prime192v1 prime256v1 sect163k1 sect163r1
 sect193r1 sect233k1 sect233r1 sect283k1 sect283r1 sect409k1 sect409r1 sect571k
1 sect571r1 secp160k1 secp160r1 secp160r2 secp192k1 secp224k1 secp224r1 secp256
k1 secp384r1 secp521r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1
    list of supported ALPN, NPN      http/1.1,h2c,h2c-14,spdy/1,npn-spdy/2,spdy
/2,spdy/3,spdy/3.1,spdy/4a2,spdy/4a4,grpc-exp,h2-14,h2-15,http/2.0,h2
= o-saft.pl +cipher --ciphermode=openssl or --ciphermode=ssleay =
    number of supported ciphers      0
!!Hint: use '--v' to get list of ciphers
    openssl supported SSL versions
    o-saft.pl known SSL versions     SSLv2 SSLv3 TLSv1 TLSv11 TLSv12 TLSv13 DTL
Sv09 DTLSv1 DTLSv11 DTLSv12 DTLSv13
**WARNING: 841: used openssl version '805306368' differs from compiled Net:SSLe
ay '805306400'; ignored
= o-saft.pl +cipher --ciphermode=intern =
    used cipherrange                 intern
    number of supported ciphers      2640
    default list of ciphers          0x03000100 .. 0x0300013F, 0x0300FE00 .. 0x
0300FEFF,0x03000000 .. 0x030000FF, 0x03001300 .. 0x030013FF,
```

```
= o-saft.pl +cipher --ciphermode=intern =
    used cipherrange                intern
    number of supported ciphers     2640
    default list of ciphers         0x03000100 .. 0x0300013F, 0x0300FE00 .. 0x
0300FFFF,0x03000000 .. 0x030000FF, 0x03001300 .. 0x030013FF,
        0x0300C000 .. 0x0300C1FF, 0x0300CC00 .. 0x0300CCFF,
        0x0300D000 .. 0x0300D0FF,
        0x0300FE00 .. 0x0300FFFF,
        0x03000A0A, 0x03001A1A, 0x03002A2A, 0x03003A3A, 0x03004A4A,
        0x03005A5A, 0x03006A6A, 0x03007A7A, 0x03008A8A, 0x03009A9A,
        0x0300AAAA, 0x0300BABA, 0x0300CACA, 0x0300DADA, 0x0300EAEA, 0x0300FAFA

= Required (and used) Modules =
    @INC                  .. /home/student/O-Saft . lib bin /usr/local/lib64/per
l5/5.34 /usr/local/share/perl5/5.34 /usr/lib64/perl5/vendor_perl /usr/share/per
l5/vendor_perl /usr/lib64/perl5 /usr/share/perl5
=   module name            VERSION  found in
=   ----------------------+--------+-----------------------------------------
    IO::Socket::INET       1.46     /usr/lib64/perl5/IO/Socket/INET.pm
    IO::Socket::SSL        2.074    /usr/share/perl5/vendor_perl/IO/Socket/SSL
pm
    Time::Local            1.30     /usr/share/perl5/vendor_perl/Time/Local.pm
    Net::DNS
    Net::SSLeay            1.92     /usr/lib64/perl5/vendor_perl/Net/SSLeay.pm
    Net::SSLinfo           23.04.23 /home/student/O-Saft/Net/SSLinfo.pm
    Net::SSLhello          23.04.23 /home/student/O-Saft/Net/SSLhello.pm
    OSaft::Ciphers         23.04.23 /home/student/O-Saft/OSaft/Ciphers.pm
    osaft                  23.04.23 /home/student/O-Saft/osaft.pm
```


RESULT:

EXP. NO: 12

DATE:

STUDY OF KALI LINUX DISTRIBUTION

AIM:

ALGORITHM:

DESCRIPTION:

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing andSecurity Auditing. Kali Linux contains several hundred tools aimed at various information securitytasks, such as Penetration Testing, Forensics and Reverse Engineering. Kali Linux is developed,funded and maintained by Offensive Security, a leading information security training company.

Kali Linux was released on the 13th March, 2013 as a complete, top-to-bottom rebuild ofBackTrack Linux, adhering completely toDebian development standards. Features are listed below-

• More than 600 penetration testing tools

• Free and Open Source Software

• Open source Git tree: All of the source code which goes into Kali Linux is available foranyone who wants to tweak or rebuild packages to suit their specific needs.

• FHS compliant: It adheres to the Filesystem Hierarchy Standard, allowing Linux users toeasily locate binaries, support files, libraries, etc.

• Wide-ranging wireless device support: A regular sticking point with Linux distributionshas been support for wireless interfaces. Kali Linux supports many wireless devices.

• Custom kernel, patched for injection: As penetration testers, the development team oftenneeds to do wireless assessments and Kali Linux kernel has the latest injection patchesincluded.

• Developed in a secure environment: The Kali Linux team is made up of a small group ofindividuals who are the only ones trusted to commit packages and interact with therepositories, all of which is done using multiple secure protocols.

• GPG signed packages and repositories: Every package in Kali Linux is signed by eachindividual developer who built and committed it, and the repositories subsequently sign thepackages as well.

• Multi-language support: It has multilingual support, allowing more users to operate intheir native language and locate the tools they need for the job.

• Completely customizable: It can be customized to the requirements of the users.

• ARMEL and ARMHF support: It is suitable for ARM-based single-board systems likethe Raspberry Pi and BeagleBone Black.

Security Tools:

Kali Linux includes many well known security tools and are listed below-

• Nmap

• Aircrack-ng

• Kismet

• Wireshark

• Metasploit Framework

• Burp suite

• John the Ripper

• Social Engineering Toolkit

• Airodump-ng

Aircrack-ng Suite:

It is a complete suite of tools to assess WiFi network security. It focuses on different areasof WiFi security:

• Monitoring: Packet capture and export of data to text files for further processing by thirdparty tools.

• Attacking: Replay attacks, deauthentication, fake access points and others via packetinjection.

• Testing: Checking WiFi cards and driver capa

• Cracking: WEP and WPA PSK (WPA 1 and2).

OUTPUT:

```
root@kali:~# apt-get install bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  bettercap
0 upgraded, 1 newly installed, 0 to remove and 1902 not upgraded.
Need to get 6,794 kB of archives.
After this operation, 25.2 MB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-last-snapshot/main amd64 bettercap amd64 2.
32.0-1+b7 [6,794 kB]
Fetched 6,794 kB in 2s (3,428 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 339769 files and directories currently installed.)
Preparing to unpack .../bettercap_2.32.0-1+b7_amd64.deb ...
Unpacking bettercap (2.32.0-1+b7) ...
Setting up bettercap (2.32.0-1+b7) ...
bettercap.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2022.3.1) ...
root@kali:~# S
```

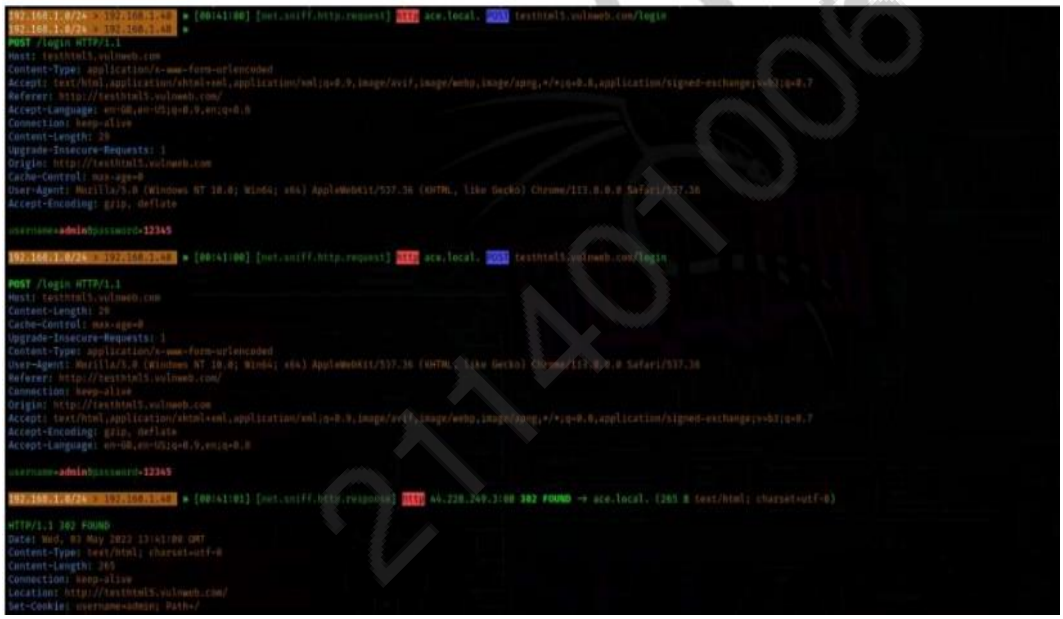
```
> 192.168.135.128 > help

          help MODULE : List available commands or show module specific help if no module na
e is provided.
                active : Show information about active modules.
                  quit : Close the session and exit.
         sleep SECONDS : Sleep for the given amount of seconds.
              get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a w
ildcard.
        set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VA
RIABLE.
                 clear : Clear the screen.
        include CAPLET : Load and run this caplet in the current session.
             ! COMMAND : Execute a shell command and print its output.
        alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

      any.proxy > not running
       api.rest > not running
      arp.spoof > not running
             c2 > not running
        caplets > not running
    dhcp6.spoof > not running
       dns.spoof > not running
  events.stream > running
            hid > not running
     http.proxy > not running
    http.server > not running
    https.proxy > not running
   https.server > not running
    mac.changer > not running
     mdns.server > not running
   mysql.server > not running
       ndp.spoof > not running
       net.probe > not running
       net.recon > not running
       net.sniff > not running
   packet.proxy > not running
       syn.scan > not running
       tcp.proxy > not running
          ticker > not running
              ui > not running
          update > not running
            wifi > not running
             wol > not running
```

acunetix

Vulnerable test websites for Acunetix Web Vulnerability Scanner.

Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help you test Acunetix but you may also use it for manual penetration testing or for educational purposes. It will help you learn about vulnerabilities such as SQL Injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and many more.



RESULT:

EXP. NO: 13

DATE:

MALWARE ANALYSIS

AIM:

ALGORITHM:

DESCRIPTION:

YARA is the name of a tool primarily used in malware research and detection.It provides a rule-based approach to create descriptions of malware families based on textual or binary patterns. Adescription is essentially a YARA rule name, where these rules consist of sets of strings and a Boolean expression. The language used has traits of Perl compatible regular expressions. YARA by defaultcomes with modules to process PE, ELF analysis, as well as support for the open-source Cuckoosandbox.

Yara Script:

```
rulespyeye : banker
{
meta:
author = "Ben"
description = "SpyEye X.Y memory"
date = "2022-05-25"
version = "1.0"
filetype = "memory"
strings:
$g = "bot_version"
$h = "bot_guid"
condition:
any of ($g,$h) and filesize>50000
```

OUTPUT:

```
[root@localhost Downloads]# ll malware.exe
-rw-r--r--. 1 root root 148480 May 26 11:17 malware.exe
[root@localhost Downloads]# yaraspyeye.yara malware.exe
spyeye malware.exe
```

RESULT: