

# AI FOR CYBERSECURITY WITH IBM QRADAR

## ASSIGNMENT – 2

NAME: Digvijay Patil

BRANCH: CSE – Cyber Security

COLLEGE: VIT – AP

Info regarding: Kali Linux Tools

1) Information gathering (Nslookup)

The screenshot displays the Super tool Beta/ interface. At the top, there is a search bar containing 'smartinternz.com/' and an 'HTTPS Lookup' button. Below this, the tool shows the certificate details for 'https://smartinternz.com/'. The interface includes a 'Monitor This' button and a 'Remind Me' button. The certificate information is presented in a table-like structure with three rows, each representing a different certificate level.

Certificate	
<p><b>Primary</b></p> <p>Common Name: smartinternz.com</p> <p>Issuer: Amazon RSA 2048 M01</p> <p>Serial: 075946D6B8738E96EA11C05A2FADBDBF</p> <p>Expires: 9 months</p> <p>Valid From: 4/20/2023</p> <p>Valid To: 5/19/2024</p> <p>Algorithm: sha256RSA</p>	<p>Remind Me</p>
<p>Common Name: Amazon RSA 2048 M01</p> <p>Issuer: Amazon Root CA 1</p> <p>Serial: 077312380B9D6688A33B1ED9BF9CCDA68E0E0F</p> <p>Expires: 7 years</p> <p>Valid From: 8/23/2022</p> <p>Valid To: 8/23/2030</p> <p>Algorithm: sha256RSA</p> <p>Organization: Amazon</p> <p>Location: US</p>	
<p>Common Name: Amazon Root CA 1</p> <p>Issuer: Amazon Root CA 1</p> <p>Serial: 066C9FCF99BF8C0A39E2F0788A43E696365BCA</p>	

Nslookup.io

smartinternz.com

Find DNS records

DNS records for **smartinternz.com**
[Cloudflare](#)
[Google DNS](#)
[OpenDNS](#)
[Authoritative](#)
[Local DNS](#)

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as this period, Cloudflare will update its cache by querying one of the authoritative name servers.

## A records

IPv4 address	Revalidate in
> <b>a</b> 35.154.227.143	1m
> <b>a</b> 13.234.22.171	1m

## AAAA records

No AAAA records found.

It helps to find static ip/ip on which site is hosted

## 2)Vulnerability scan(Nmap)

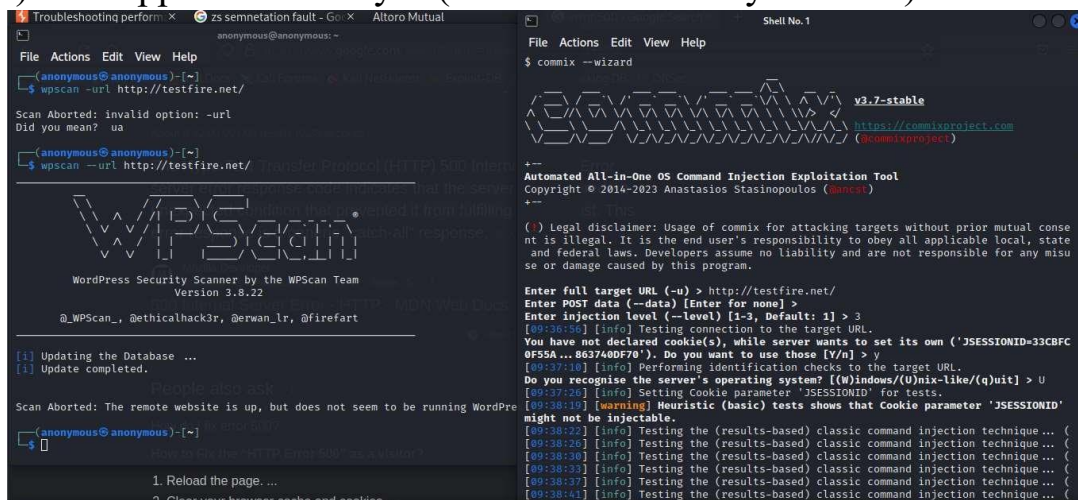
```
(anonymous@anonymous)-[~]
$ sudo nmap -Pn -O 35.154.227.143
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 02:04 IST
Nmap scan report for ec2-35-154-227-143.ap-south-1.compute.amazonaws.com (35.154.227.143)
Host is up (0.023s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    closed smtp
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (96%), Linux 4.4 (96%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (95%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT device (91%), BlueArc Titan 2100 NAS device (89%), DVTel DVT-9540DW network camera (88%), Toshiba e-STUDIO 280 printer (87%)
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 84.23 seconds
```

```
(anonymous@anonymous)-[~]
$ sudo nmap -Pn -O 13.234.22.171
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 02:06 IST
Nmap scan report for ec2-13-234-22-171.ap-south-1.compute.amazonaws.com (13.234.22.171)
Host is up (0.0012s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    closed smtp
110/tcp   open  pop3
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 30.32 seconds
```

It helps to find open ports (to perform attack) and version of packages related to port

### 3)Web Application analysis(WordPress Security Scanner)



```
WordPress Security Scanner by the WPScan Team
Version 3.8.22
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[1] Updating the Database ...
[1] Update completed.

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

How to fix the HTTP error 500 as a WordPress?

1. Reload the page. ...
2. Clear your browser cache and cookies.
```

It scan the wordpress website and find vulnerability in it. 4)Database assessment(SqlMap)

```
Shell No. 1
File Actions Edit View Help
$ sqlmap --wizard
  H
  |
  | [1.7.2#stable]
  | [V...]
  |
  | https://sqlmap.org
  |
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program

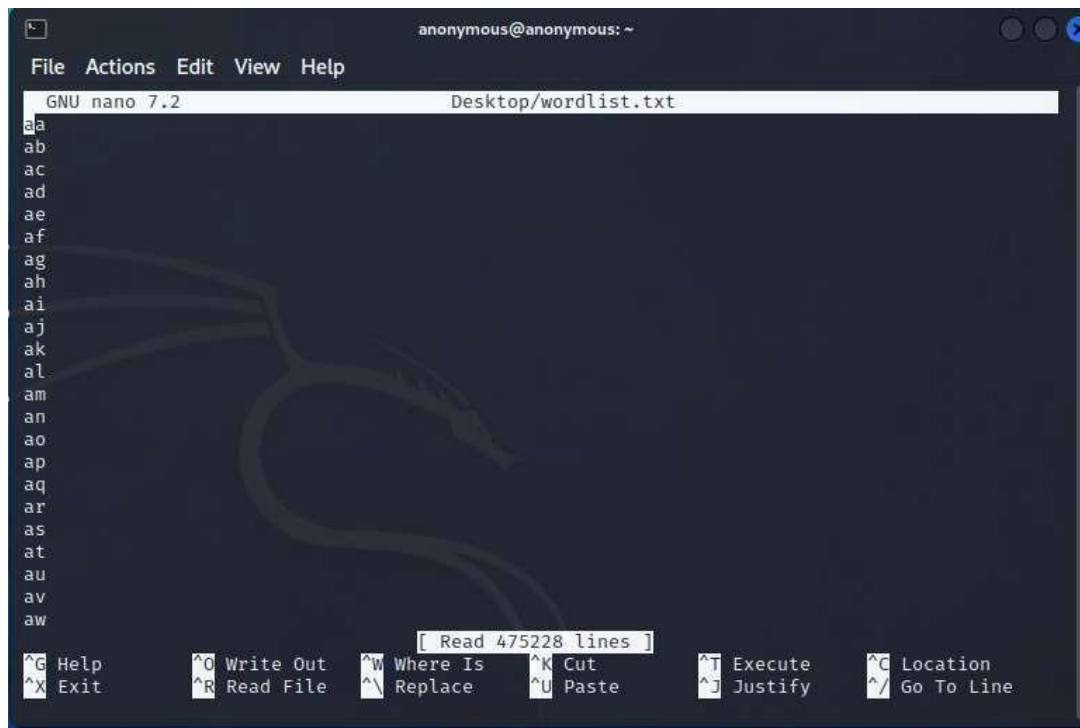
[*] starting @ 19:37:04 /2023-09-06/

[19:37:04] [INFO] starting wizard interface
Please enter full target URL (-u):
```

Sqlmap find vulnerability to attack on databases of given url.

## 5)Password Attacks(Crunch)

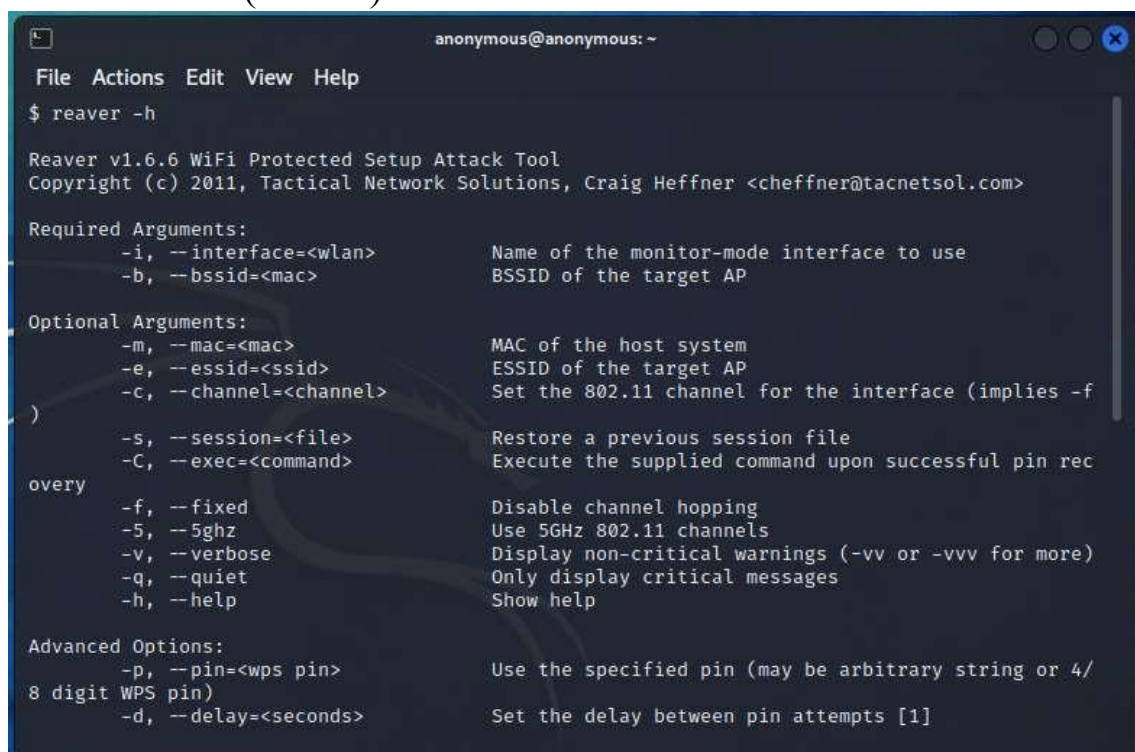
```
(anonymous@anonymous)-[~]
$ crunch 2 4 >Desktop/wordlist.txt
Crunch will now generate the following amount of data: 2357212 bytes
2 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 475228
```



```
anonymous@anonymous: ~
File Actions Edit View Help
GNU nano 7.2 Desktop/wordlist.txt
aa
ab
ac
ad
ae
af
ag
ah
ai
aj
ak
al
am
an
ao
ap
aq
ar
as
at
au
av
aw
[ Read 475228 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^/_ Go To Line
```

Crunch create a wordlist(dictionary) as user choice for brute force password attack

## 6)Wireless Attacks (Reaver)



```
anonymous@anonymous: ~
File Actions Edit View Help
$ reaver -h

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
  -i, --interface=<wlan>      Name of the monitor-mode interface to use
  -b, --bssid=<mac>          BSSID of the target AP

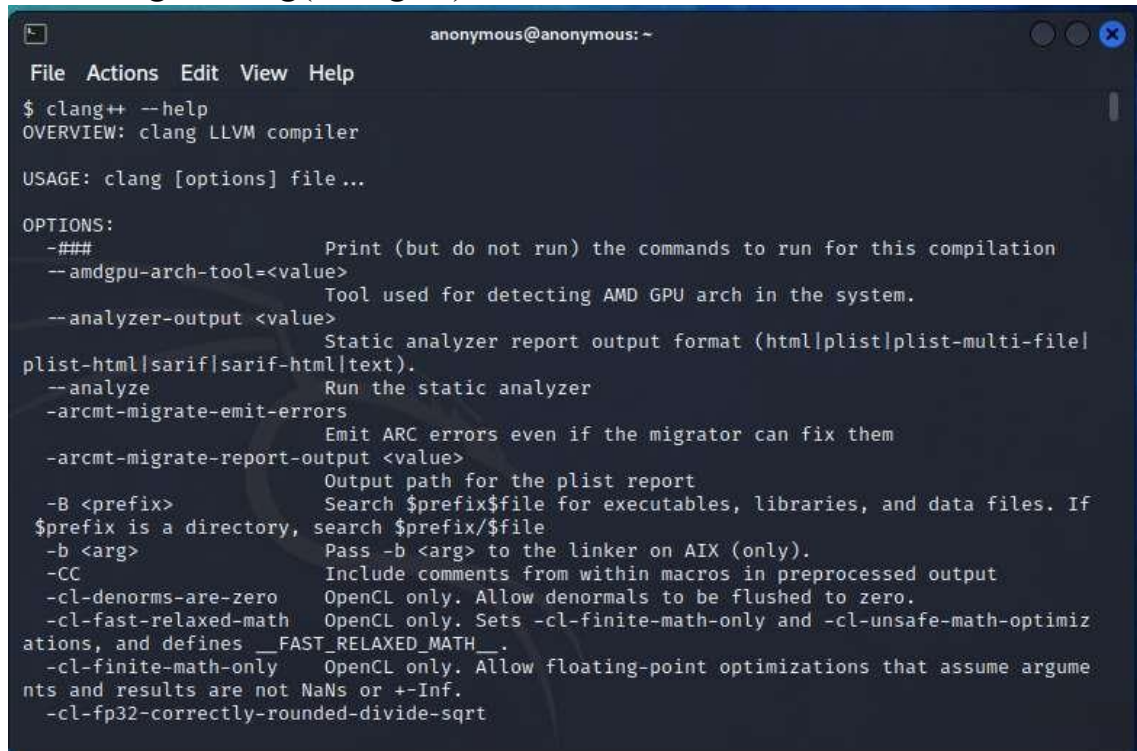
Optional Arguments:
  -m, --mac=<mac>            MAC of the host system
  -e, --essid=<ssid>         ESSID of the target AP
  -c, --channel=<channel>    Set the 802.11 channel for the interface (implies -f)
  -s, --session=<file>      Restore a previous session file
  -C, --exec=<command>      Execute the supplied command upon successful pin recovery
  -f, --fixed                Disable channel hopping
  -5, --5ghz                 Use 5GHz 802.11 channels
  -v, --verbose               Display non-critical warnings (-vv or -vvv for more)
  -q, --quiet                Only display critical messages
  -h, --help                 Show help

Advanced Options:
  -p, --pin=<wps pin>        Use the specified pin (may be arbitrary string or 4/8 digit WPS pin)
  -d, --delay=<seconds>     Set the delay between pin attempts [1]
```

Reaver is a wireless attack tool to get Wi-Fi credential. For ex for WPS ,it brute force WPS pin and can set to wait for particular time to continue again



## 7)Reverse Engineering(Clang++)



```
anonymous@anonymous: ~  
File Actions Edit View Help  
$ clang++ --help  
OVERVIEW: clang LLVM compiler  
  
USAGE: clang [options] file ...  
  
OPTIONS:  
-### Print (but do not run) the commands to run for this compilation  
--amdgpu-arch-tool=<value> Tool used for detecting AMD GPU arch in the system.  
--analyzer-output <value> Static analyzer report output format (html|plist|plist-multi-file|  
plist-html|sarif|sarif-html|text).  
--analyze Run the static analyzer  
-arcmt-migrate-emit-errors Emit ARC errors even if the migrator can fix them  
-arcmt-migrate-report-output <value> Output path for the plist report  
-B <prefix> Search $prefix$file for executables, libraries, and data files. If  
$prefix is a directory, search $prefix/$file  
-b <arg> Pass -b <arg> to the linker on AIX (only).  
-CC Include comments from within macros in preprocessed output  
-cl-denorms-are-zero OpenCL only. Allow denormals to be flushed to zero.  
-cl-fast-relaxed-math OpenCL only. Sets -cl-finite-math-only and -cl-unsafe-math-optimiz  
ations, and defines __FAST_RELAXED_MATH__.  
-cl-finite-math-only OpenCL only. Allow floating-point optimizations that assume argume  
nts and results are not NaNs or +-Inf.  
-cl-fp32-correctly-rounded-divide-sqrt
```

Clang++ helps to analyse packages to retrieve information code or process of development. TO develop crack of a software ,reverse engineering is done ,the according to code malicious dll or package is created to crack it

## 8)Exploitation Tools(Metasploit framework)

```
Shell No. 1
```

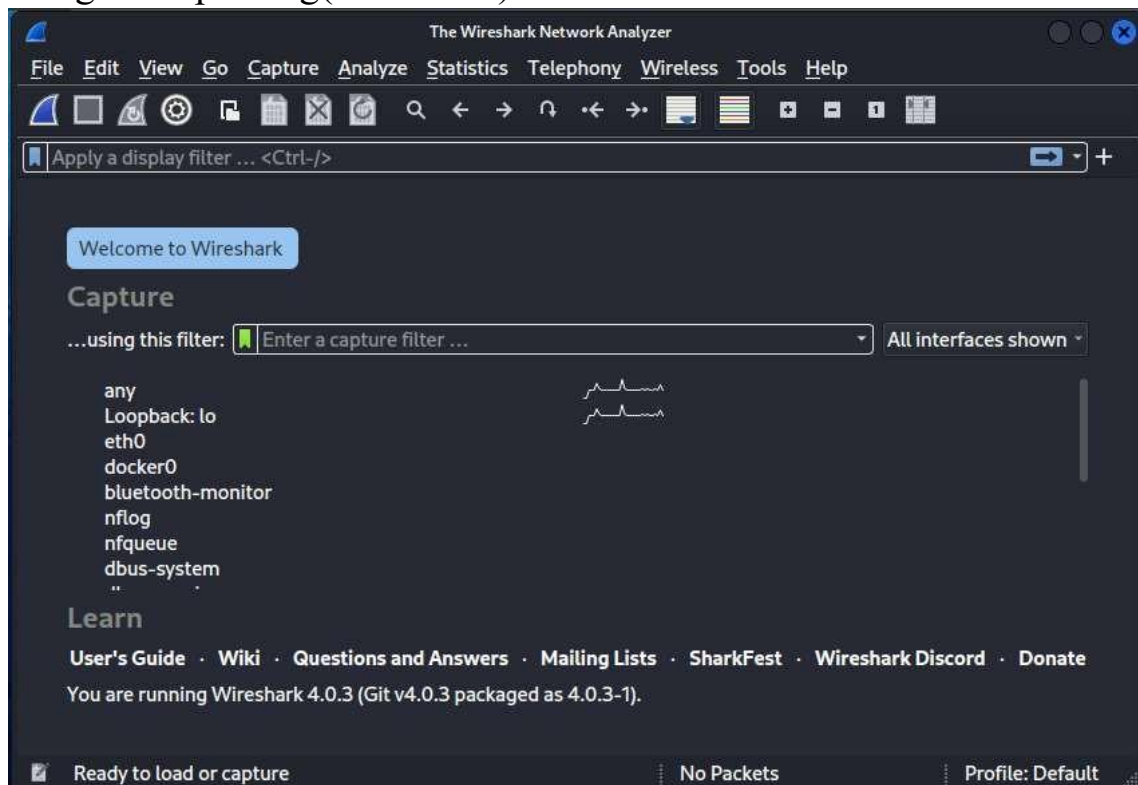
```
File Actions Edit View Help

$ sudo msfdb init && msfconsole
[sudo] password for anonymous:
[+] Starting database
[i] The database appears to be already configured, skipping initialization

##### ;;"
_..';di      di"; _..
' dddddd'.,'dd     dddddd',' dddddd ".
-.' dddddd dddddd    dddddd dddddd dd;
.'. dddddd dddddd    dddddd dddddd dddddd '.
"-..' dddd -.d       d '- ..'-
   "d'; di        di ':;'
 | dddd dddd      d .
'dddd dd  dd     ,
  'ddd      dd .
( 3 C )         /|__ \ Metasploit! \
;d'._*_.,"       \|___\
'(.,...."/

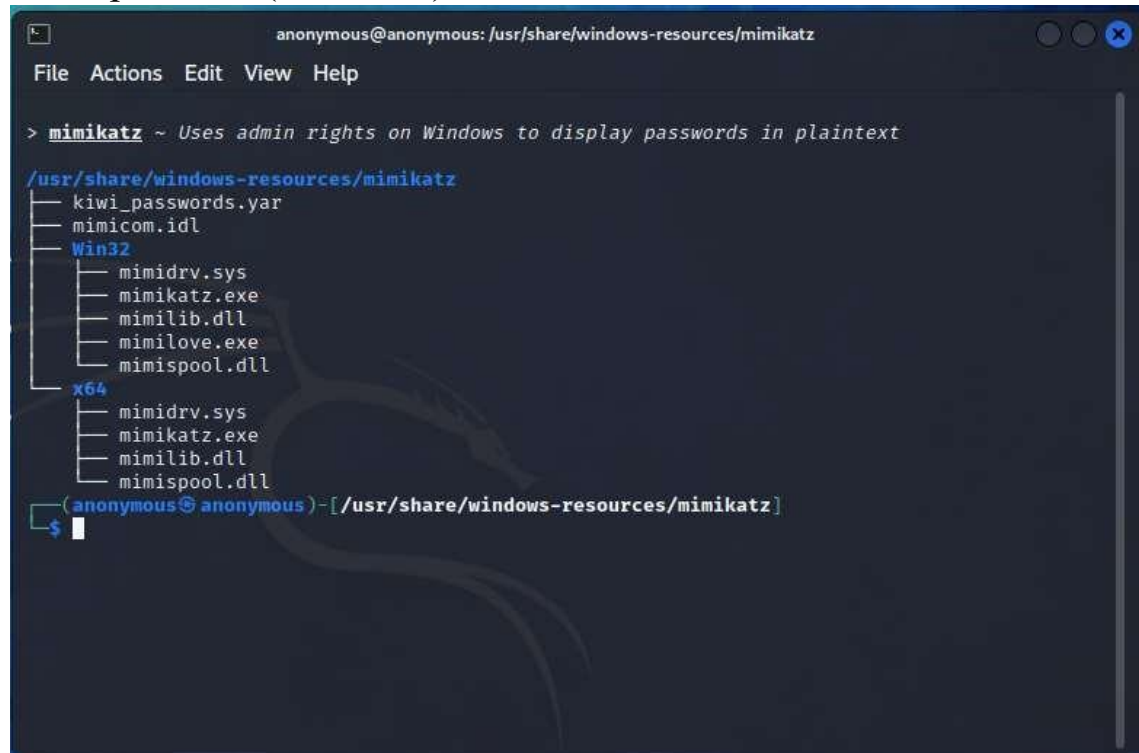
= [ metasploit v6.3.4-dev ]
+ -- ==[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- ==[ 968 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]
```

## 9)Sniffing and Spoofing(Wireshark)



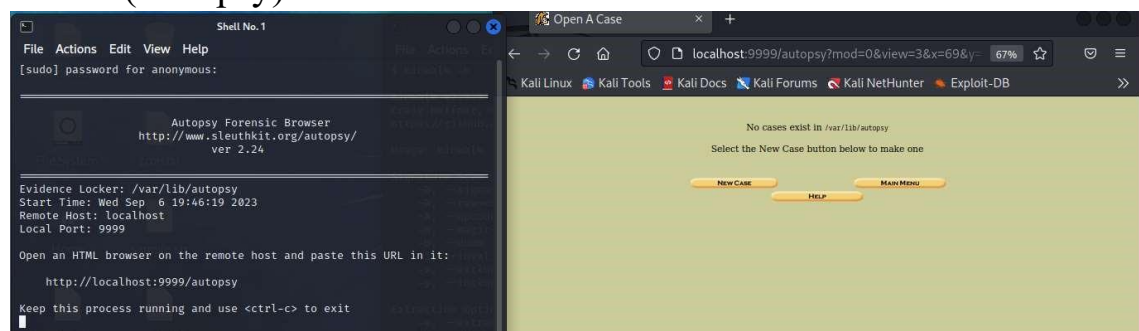
Wireshark helps to analyze or live monitoring of network to know the traffic or data transmission over network layer of packets. If data is transmitted by http, sniffer will get the actual data sent through it.

## 10) Post Exploitation(Mimikatz)



After execution of attack, if anyone want to trace , foot printing mimikatz can be used. It save the data in memory and perform operation to know how it perform. Sometimes it also help to retrieve password as password are saved in memory for useful purpose.

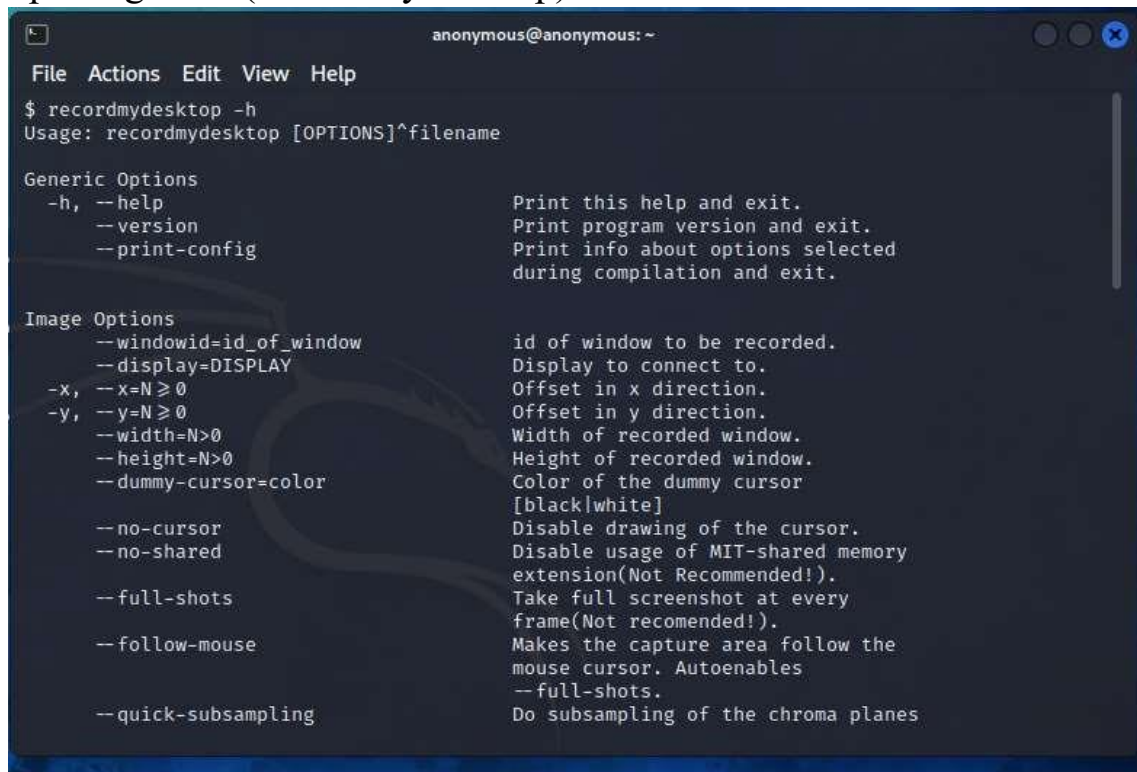
## 11)Forensic(Autopsy)



Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.



## 12)Reporting Tools(RecordmyDesktop)



```
anonymous@anonymous: ~
File Actions Edit View Help
$ recordmydesktop -h
Usage: recordmydesktop [OPTIONS]^filename

Generic Options
  -h, --help                Print this help and exit.
  --version                 Print program version and exit.
  --print-config             Print info about options selected
                             during compilation and exit.

Image Options
  --windowid=id_of_window  id of window to be recorded.
  --display=DISPLAY         Display to connect to.
  -x, --x=N>=0             Offset in x direction.
  -y, --y=N>=0             Offset in y direction.
  --width=N>0              Width of recorded window.
  --height=N>0             Height of recorded window.
  --dummy-cursor=color     Color of the dummy cursor
                             [black|white]
  --no-cursor              Disable drawing of the cursor.
  --no-shared              Disable usage of MIT-shared memory
                             extension(Not Recommended!).
  --full-shots             Take full screenshot at every
                             frame(Not recommended!).
  --follow-mouse           Makes the capture area follow the
                             mouse cursor. Autoenables
                             --full-shots.
  --quick-subsampling      Do subsampling of the chroma planes
```

Recordmydesktop is report creation in form of video with version of os with customized recording area of screen.

## 13)Social Engineering Tools(MSF Payload Creator)

```
anonymous@anonymous: ~  
File Actions Edit View Help  
$ msfpc  
[*] MSFvenom Payload Creator (MSFPC v1.4.5)  
  
[i] Missing TYPE or BATCH/LOOP mode  
  
/usr/bin/msfpc <TYPE> (<DOMAIN/IP>) (<PORT>) (<CMD/MSF>) (<BIND/REVERSE>) (<STAGED/STAGELESS>) (<TCP/HTTP/HTTPS/FIND_PORT>) (<BATCH/LOOP>) (<VERBOSE>)  
Example: /usr/bin/msfpc windows 192.168.1.10 # Windows & manual IP.  
         /usr/bin/msfpc elf bind eth0 4444 # Linux, eth0's IP & manual port.  
         /usr/bin/msfpc stageless cmd py https # Python, stageless command prompt.  
         /usr/bin/msfpc verbose loop eth1 # A payload for every type, using eth  
1's IP.  
using WAN IP. /usr/bin/msfpc msf batch wan # All possible Meterpreter payloads,  
tion. /usr/bin/msfpc help verbose # Help screen, with even more informa  
  
<TYPE>:  
+ APK  
+ ASP  
+ ASPX  
+ Bash [.sh]  
+ Java [.jsp]  
+ Linux [.elf]  
+ OSX [.macho]  
+ Perl [.pl]  
+ PHP  
+ Powershell [.ps1]  
+ Python [.py]  
+ Tomcat [.war]  
+ Windows [.exe // .exe // .dll]  
  
Rather than putting <DOMAIN/IP>, you can do a interface and MSFPC will detect that IP addre
```

To create malware for social engineering after reconnaissance, MSF payload creator is one of the tool customized malware of defined OS and file type.