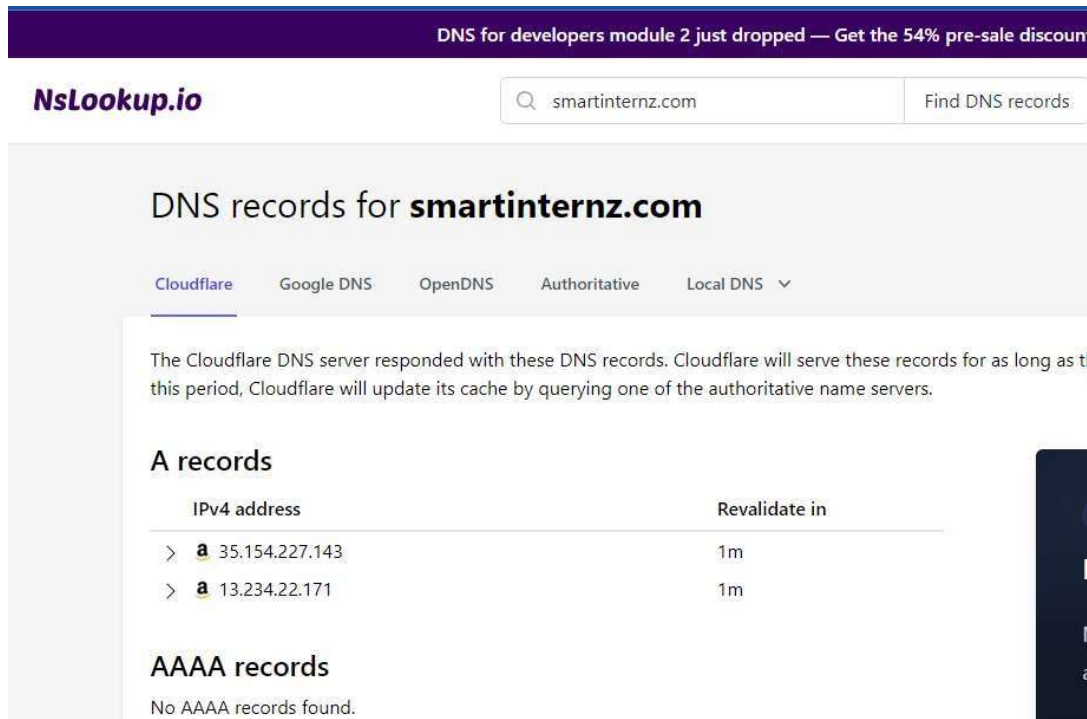
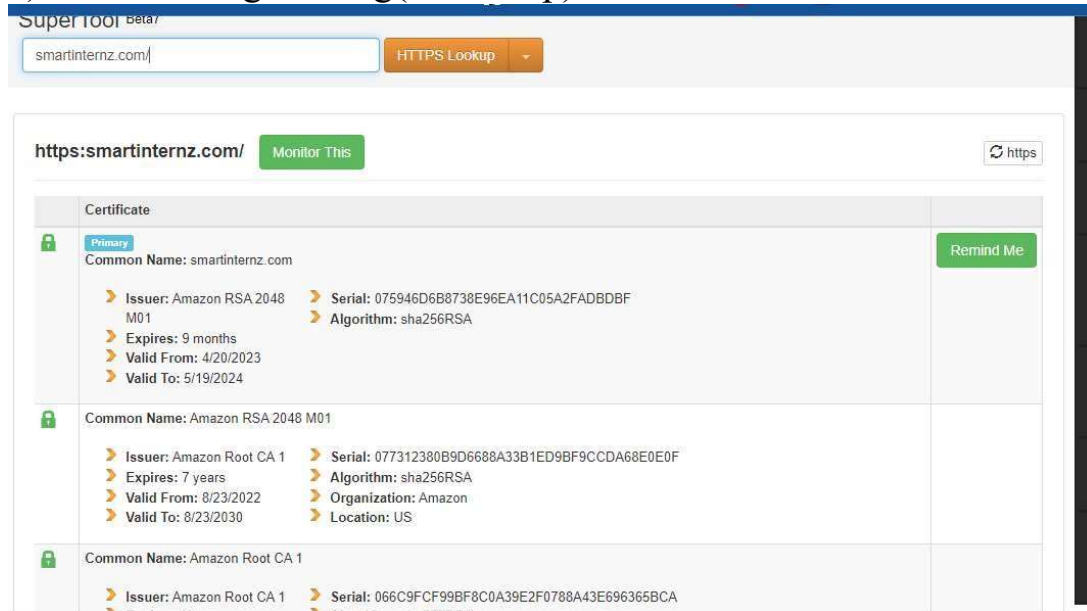


Kali Linux Tools

1) Information gathering(Nslookup):



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).

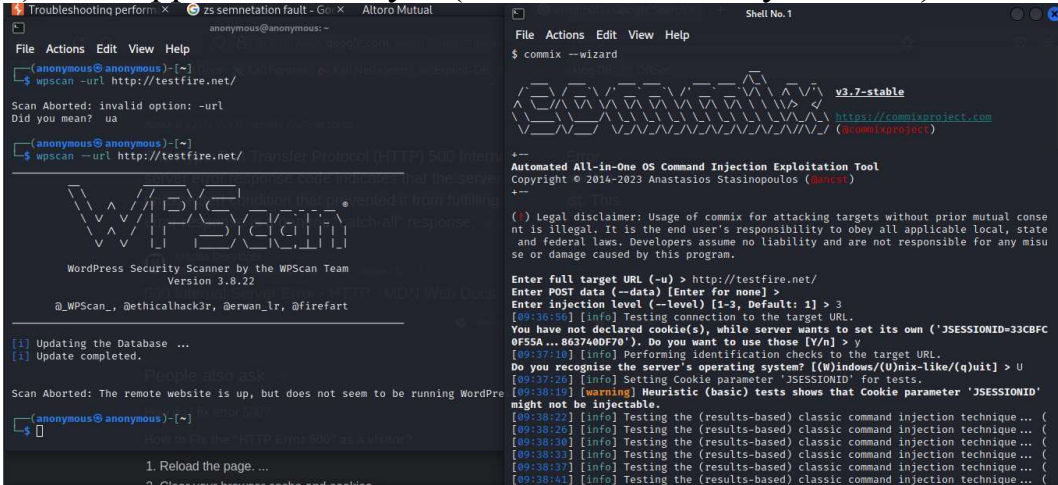
OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 84.23 seconds
```

```
(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 WPSec Team
Version 3.8.22
@_WPSec_, @ethicalhack3r, @erwan_lr, @firefart

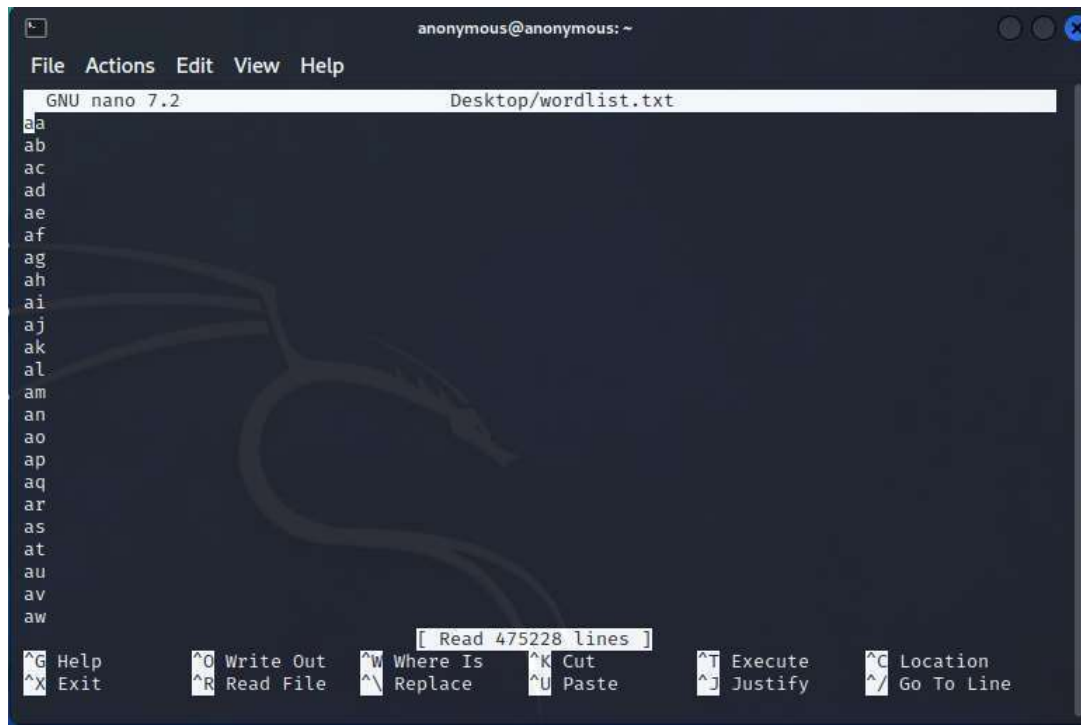
[4] Updating the Database ...
[1] Update completed.

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

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

It scan the wordpress website and find vulnerability in it.

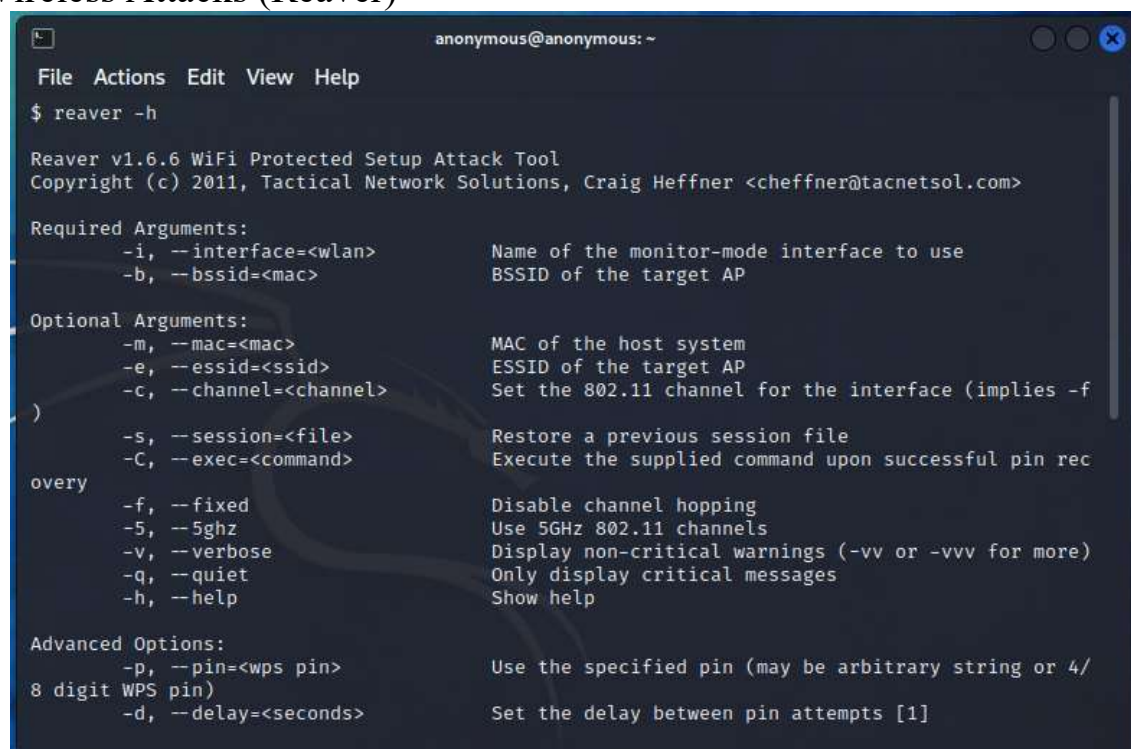
4) Database assessment (SqlMap)



```
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

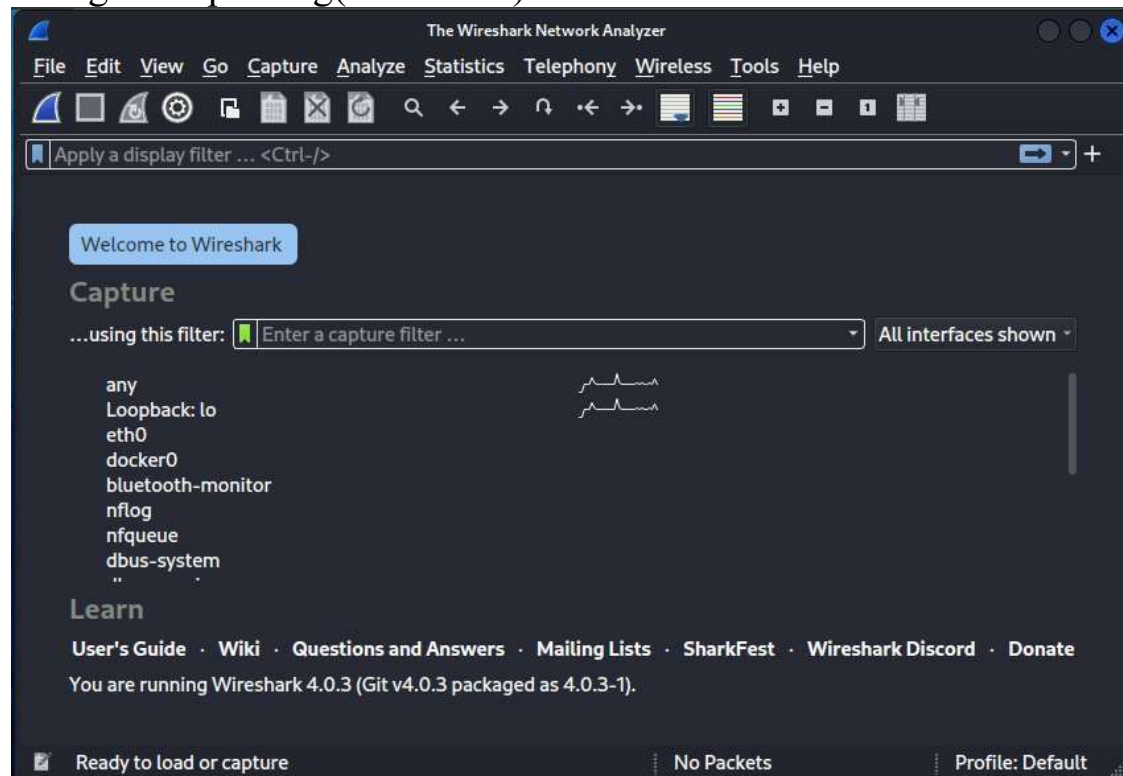
Optional Arguments:
  -m, --mac=<mac>            MAC of the host system
  -e, --essid=<ssid>          ESSID of the target AP
  -c, --channel=<channel>    Set the 802.11 channel for the interface (implies -f)
  -s, --session=<file>       Restore a previous session file
  -C, --exec=<command>       Execute 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

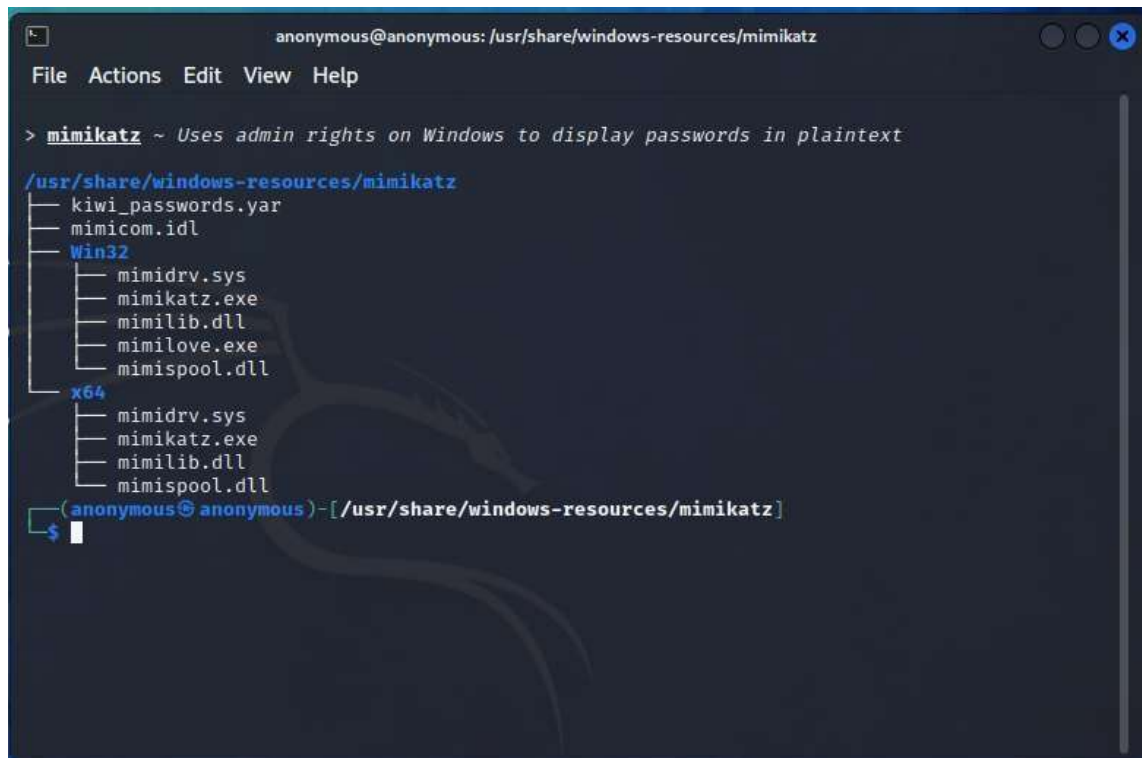
7)Reverse Engineering(Clang++)

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)



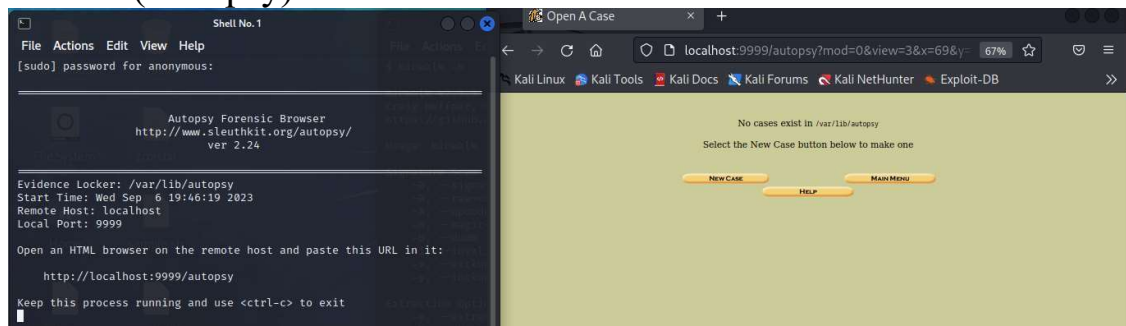
```
anonymous@anonymous: /usr/share/windows-resources/mimikatz
File Actions Edit View Help

> mimikatz ~ Uses admin rights on Windows to display passwords in plaintext

/usr/share/windows-resources/mimikatz
├── kiwi_passwords.yar
├── mimicom.idl
├── Win32
│   ├── mimidrv.sys
│   ├── mimikatz.exe
│   ├── mimilib.dll
│   ├── mimilove.exe
│   └── mimispool.dll
├── x64
│   ├── mimidrv.sys
│   ├── mimikatz.exe
│   ├── mimilib.dll
│   └── mimispool.dll
└── (anonymous@anonymous) - [ /usr/share/windows-resources/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.

