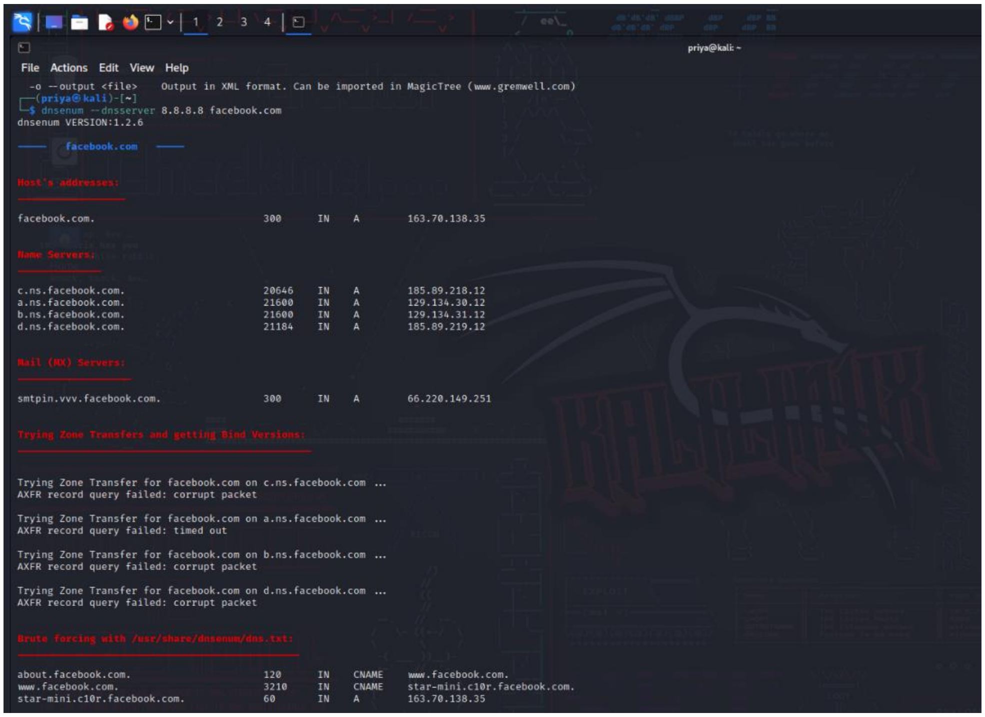
ASSIGNMENT – 2

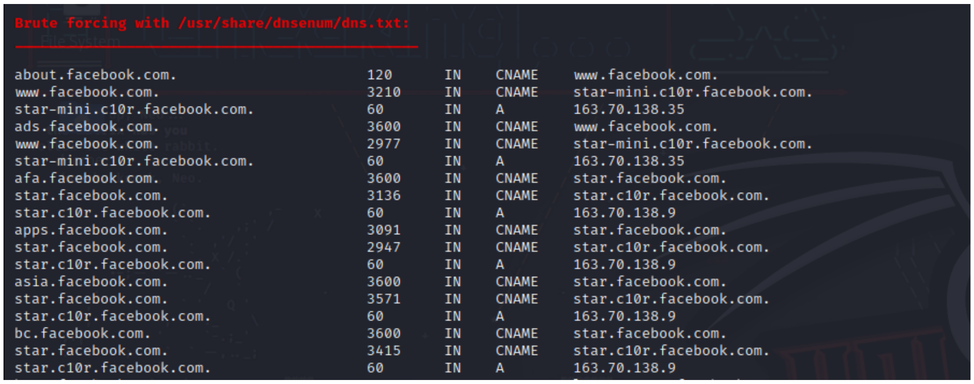
1. Exploring tools in Kali Linux.

01 – Information Gathering.

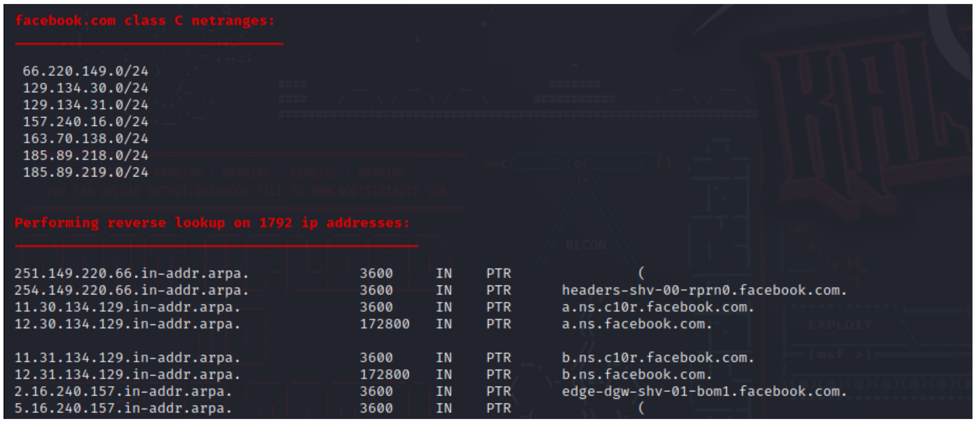
Dnsenum: DNSenum is a command-line network reconnaissance tool designed for domain analysis and reconnaissance. It assists in gathering critical information about a target domain's DNS infrastructure. It helps in subdomain enumeration, brute-force subdomain discovery, and DNS zone transfer attempts. It's valuable for identifying hidden entry points and potential vulnerabilities within a domain. By systematically probing a domain's DNS records, it aids in assessing the overall security posture.



```
  -o --output <file>    Output in XML format. Can be imported in MagicTree (www.gremwell.com)
┌──(priya㉿kali)-[~]
└─$ dnsenum --dnsserver 8.8.8.8 facebook.com
dnsenum VERSION:1.2.6

-----   facebook.com   -----


Host's addresses:
__________________

facebook.com.                            300      IN    A        163.70.138.35


Name Servers:
______________

c.ns.facebook.com.                       20646    IN    A        185.89.218.12
a.ns.facebook.com.                       21600    IN    A        129.134.30.12
b.ns.facebook.com.                       21600    IN    A        129.134.31.12
d.ns.facebook.com.                       21184    IN    A        185.89.219.12


Mail (MX) Servers:
___________________

smtpin.vvv.facebook.com.                 300      IN    A        66.220.149.251


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for facebook.com on c.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on a.ns.facebook.com ...
AXFR record query failed: timed out

Trying Zone Transfer for facebook.com on b.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on d.ns.facebook.com ...
AXFR record query failed: corrupt packet


Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

about.facebook.com.                      120      IN    CNAME    www.facebook.com.
www.facebook.com.                        3210     IN    CNAME    star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.             60       IN    A        163.70.138.35
```

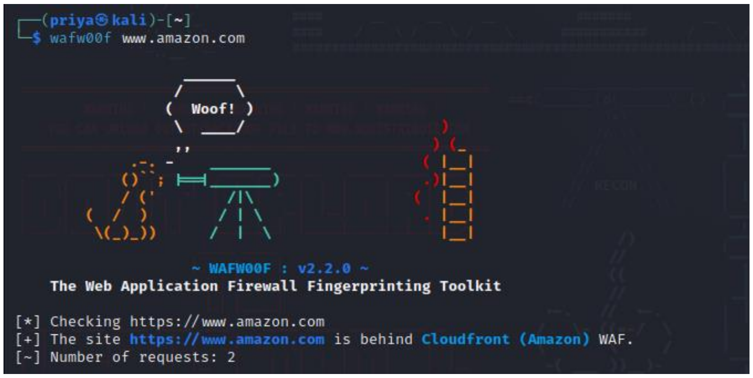


```
Brute forcing with /usr/share/dnsenum/dns.txt:
______________________________________________

about.facebook.com.                      120      IN    CNAME    www.facebook.com.
www.facebook.com.                        3210     IN    CNAME    star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.             60       IN    A        163.70.138.35
ads.facebook.com.                        3600     IN    CNAME    www.facebook.com.
www.facebook.com.                        2977     IN    CNAME    star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.             60       IN    A        163.70.138.35
afa.facebook.com.                        3600     IN    CNAME    star.facebook.com.
star.facebook.com.                       3136     IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.                  60       IN    A        163.70.138.9
apps.facebook.com.                       3091     IN    CNAME    star.facebook.com.
star.facebook.com.                       2947     IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.                  60       IN    A        163.70.138.9
asia.facebook.com.                       3600     IN    CNAME    star.facebook.com.
star.facebook.com.                       3571     IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.                  60       IN    A        163.70.138.9
bc.facebook.com.                         3600     IN    CNAME    star.facebook.com.
star.facebook.com.                       3415     IN    CNAME    star.c10r.facebook.com.
star.c10r.facebook.com.                  60       IN    A        163.70.138.9
```



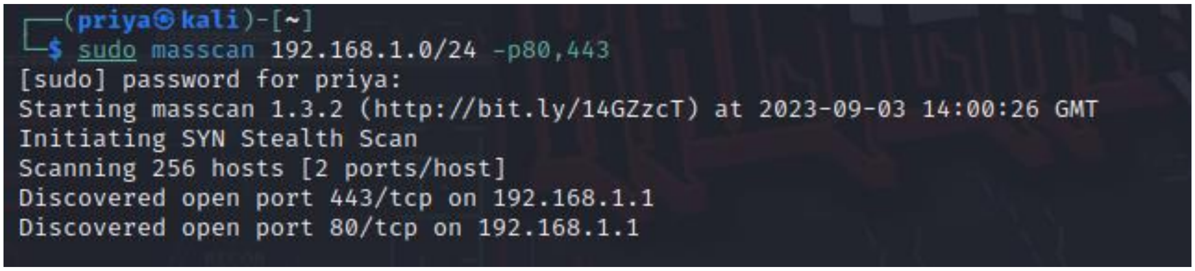
```
facebook.com class C netranges:
_______________________________

 66.220.149.0/24
 129.134.30.0/24
 129.134.31.0/24
 157.240.16.0/24
 163.70.138.0/24
 185.89.218.0/24
 185.89.219.0/24

Performing reverse lookup on 1792 ip addresses:
_______________________________________________

251.149.220.66.in-addr.arpa.            3600     IN    PTR          (
254.149.220.66.in-addr.arpa.            3600     IN    PTR      headers-shv-00-rprn0.facebook.com.
11.30.134.129.in-addr.arpa.             3600     IN    PTR      a.ns.c10r.facebook.com.
12.30.134.129.in-addr.arpa.             172800   IN    PTR      a.ns.facebook.com.

11.31.134.129.in-addr.arpa.             3600     IN    PTR      b.ns.c10r.facebook.com.
12.31.134.129.in-addr.arpa.             172800   IN    PTR      b.ns.facebook.com.
2.16.240.157.in-addr.arpa.              3600     IN    PTR      edge-dgw-shv-01-bom1.facebook.com.
5.16.240.157.in-addr.arpa.              3600     IN    PTR          (
```

Wafw00f: Wafw00f is a security tool used to identify and profile web application firewalls (WAFs). By sending HTTP requests to a target website and analyzing the responses, it can detect if a WAF is actively protecting the web application. This information is invaluable as it helps in understanding the defensive measures in place and assess the security of web applications. Wafw00f aids in penetration testing by revealing the presence of WAFs and can assist in bypassing them for legitimate security assessments and testing purposes.



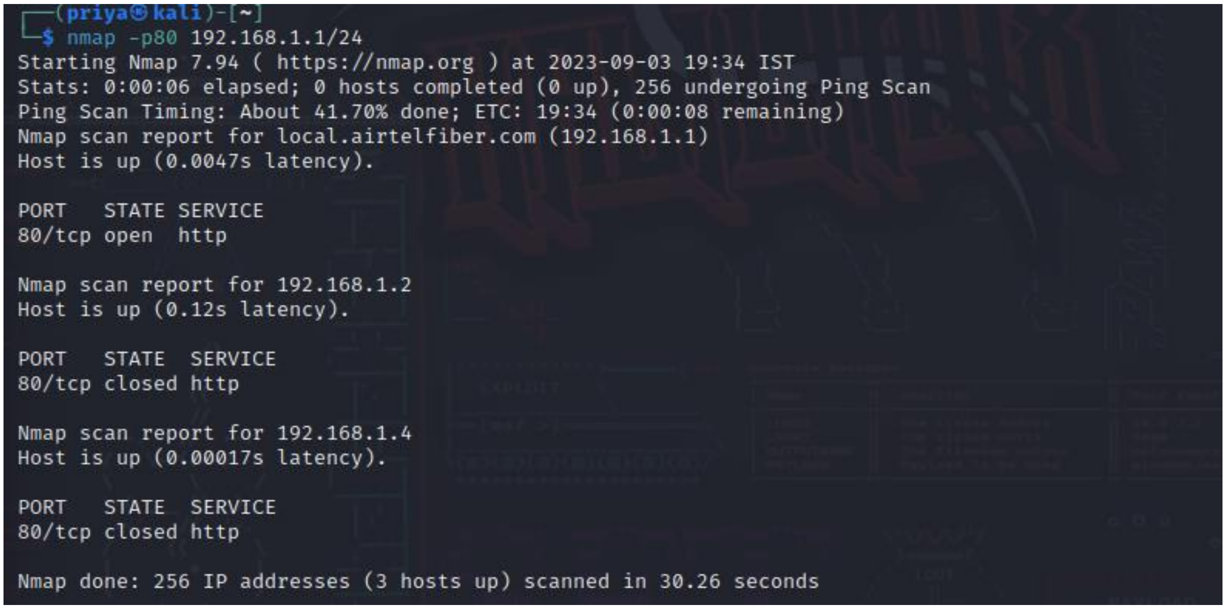
```
┌──(priya㉿kali)-[~]
└─$ wafw00f www.amazon.com

                 ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.amazon.com
[+] The site https://www.amazon.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

Masscan: Masscan is a high-speed network port scanner designed for large-scale scans of IP addresses and ports. It's optimized for quick and efficient scanning, making it useful for discovering open ports and services across vast IP ranges. Masscan's speed and flexibility makes it valuable.



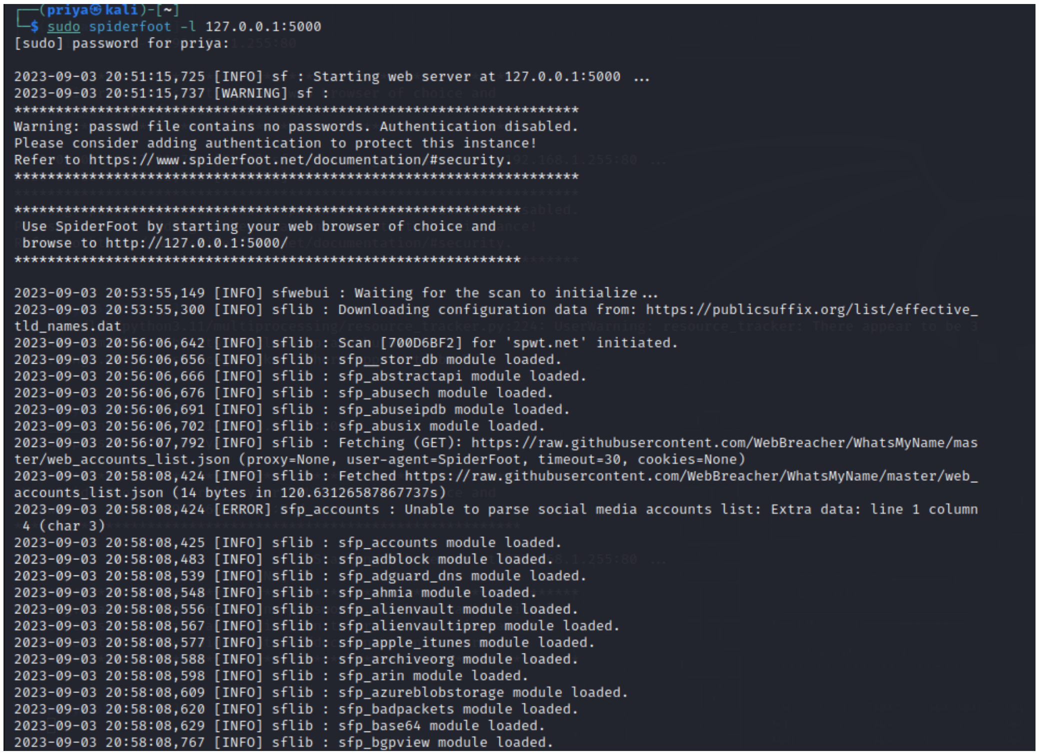
```
┌──(priya㉿kali)-[~]
└─$ sudo masscan 192.168.1.0/24 -p80,443
[sudo] password for priya:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-09-03 14:00:26 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [2 ports/host]
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
```

Nmap: Nmap (Network Mapper) is a versatile open-source network scanning tool. It's used for discovering devices, services, and vulnerabilities on a network. Nmap can perform tasks like port scanning, host discovery, version detection, and OS fingerprinting. It is used for network reconnaissance and security auditing.



```
┌──(priya㉿kali)-[~]
└─$ nmap -p80 192.168.1.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-03 19:34 IST
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 41.70% done; ETC: 19:34 (0:00:08 remaining)
Nmap scan report for local.airtelfiber.com (192.168.1.1)
Host is up (0.0047s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.1.2
Host is up (0.12s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 192.168.1.4
Host is up (0.00017s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 30.26 seconds
```

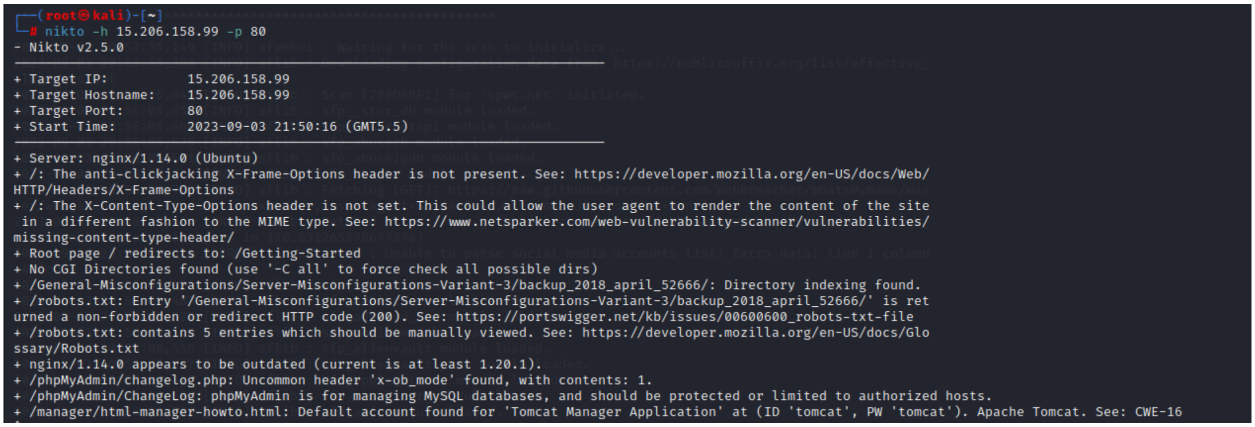
SpiderFoot: SpiderFoot is an open-source intelligence gathering tool for reconnaissance. It automates the process of collecting information from various sources, including search engines, social media, DNS, and more. SpiderFoot helps in gathering data about domains, IP addresses, email addresses, and entities to assess potential threats and vulnerabilities.



```
┌──(priya㉿kali)-[~]
└─$ sudo spiderfoot -l 127.0.0.1:5000
[sudo] password for priya:

2023-09-03 20:51:15,725 [INFO] sf : Starting web server at 127.0.0.1:5000 ...
2023-09-03 20:51:15,737 [WARNING] sf :
********************************************************************
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
********************************************************************

*************************************************************
 Use SpiderFoot by starting your web browser of choice and
 browse to http://127.0.0.1:5000/
*************************************************************

2023-09-03 20:53:55,149 [INFO] sfwebui : Waiting for the scan to initialize...
2023-09-03 20:53:55,300 [INFO] sflib : Downloading configuration data from: https://publicsuffix.org/list/effective_
tld_names.dat
2023-09-03 20:56:06,642 [INFO] sflib : Scan [700D6BF2] for 'spwt.net' initiated.
2023-09-03 20:56:06,656 [INFO] sflib : sfp__stor_db module loaded.
2023-09-03 20:56:06,666 [INFO] sflib : sfp_abstractapi module loaded.
2023-09-03 20:56:06,676 [INFO] sflib : sfp_abusech module loaded.
2023-09-03 20:56:06,691 [INFO] sflib : sfp_abuseipdb module loaded.
2023-09-03 20:56:06,702 [INFO] sflib : sfp_abusix module loaded.
2023-09-03 20:56:07,792 [INFO] sflib : Fetching (GET): https://raw.githubusercontent.com/WebBreacher/WhatsMyName/mas
ter/web_accounts_list.json (proxy=None, user-agent=SpiderFoot, timeout=30, cookies=None)
2023-09-03 20:58:08,424 [INFO] sflib : Fetched https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_
accounts_list.json (14 bytes in 120.63126587867737s)
2023-09-03 20:58:08,424 [ERROR] sfp_accounts : Unable to parse social media accounts list: Extra data: line 1 column
 4 (char 3)
2023-09-03 20:58:08,425 [INFO] sflib : sfp_accounts module loaded.
2023-09-03 20:58:08,483 [INFO] sflib : sfp_adblock module loaded.
2023-09-03 20:58:08,539 [INFO] sflib : sfp_adguard_dns module loaded.
2023-09-03 20:58:08,548 [INFO] sflib : sfp_ahmia module loaded.
2023-09-03 20:58:08,556 [INFO] sflib : sfp_alienvault module loaded.
2023-09-03 20:58:08,567 [INFO] sflib : sfp_alienvaultiprep module loaded.
2023-09-03 20:58:08,577 [INFO] sflib : sfp_apple_itunes module loaded.
2023-09-03 20:58:08,588 [INFO] sflib : sfp_archiveorg module loaded.
2023-09-03 20:58:08,598 [INFO] sflib : sfp_arin module loaded.
2023-09-03 20:58:08,609 [INFO] sflib : sfp_azureblobstorage module loaded.
2023-09-03 20:58:08,620 [INFO] sflib : sfp_badpackets module loaded.
2023-09-03 20:58:08,629 [INFO] sflib : sfp_base64 module loaded.
2023-09-03 20:58:08,767 [INFO] sflib : sfp_bgpview module loaded.
```

02 Vulnerability Analysis:

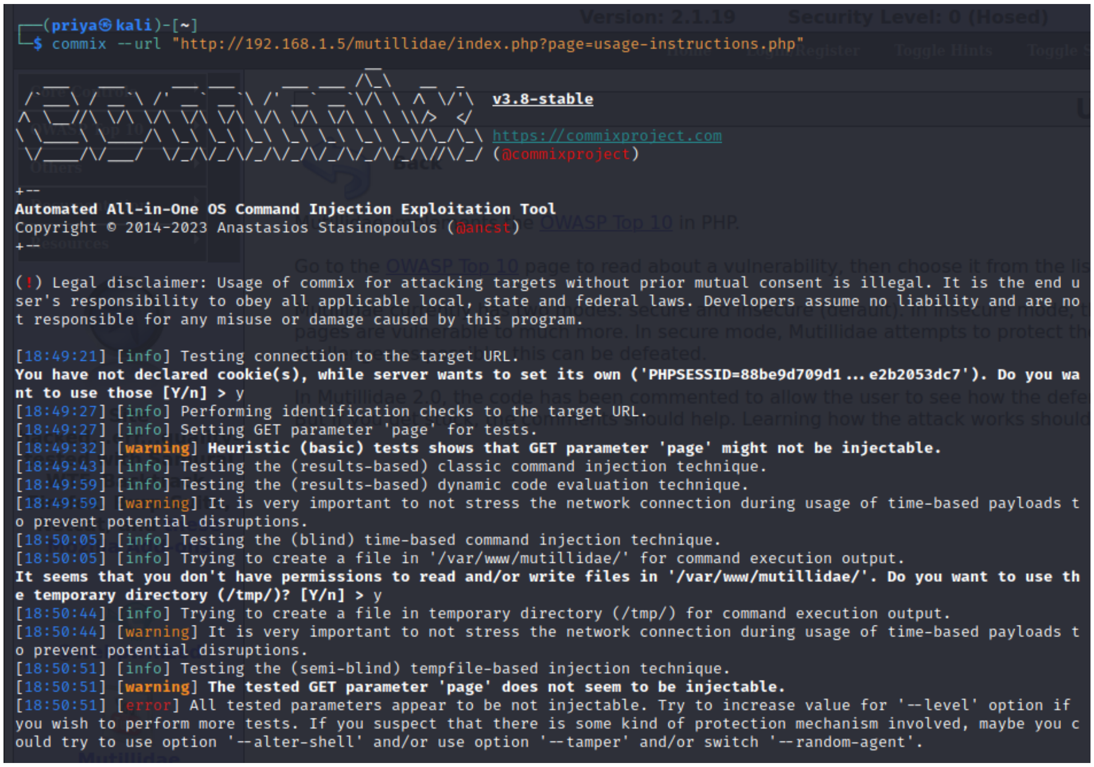
Nikto: Nikto is a web server vulnerability scanner used to identify security issues on web servers and applications. It checks for known vulnerabilities, outdated software, and common misconfigurations. Security professionals use Nikto to assess the security of web servers and prioritize remediation efforts, making it a valuable tool for web security assessments.



```
┌──(root㉿kali)-[~]
└─# nikto -h 15.206.158.99 -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          15.206.158.99
+ Target Hostname:    15.206.158.99
+ Target Port:        80
+ Start Time:         2023-09-03 21:50:16 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.14.0 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/
HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
missing-content-type-header/
+ Root page / redirects to: /Getting-Started
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /General-Misconfigurations/Server-Misconfigurations-Variant-3/backup_2018_april_52666/: Directory indexing found.
+ /robots.txt: Entry '/General-Misconfigurations/Server-Misconfigurations-Variant-3/backup_2018_april_52666/' is ret
urned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glo
ssary/Robots.txt
+ nginx/1.14.0 appears to be outdated (current is at least 1.20.1).
+ /phpMyAdmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /manager/html-manager-howto.html: Default account found for 'Tomcat Manager Application' at (ID 'tomcat', PW 'tomcat'). Apache Tomcat. See: CWE-16
```

03 Web Application Analysis:

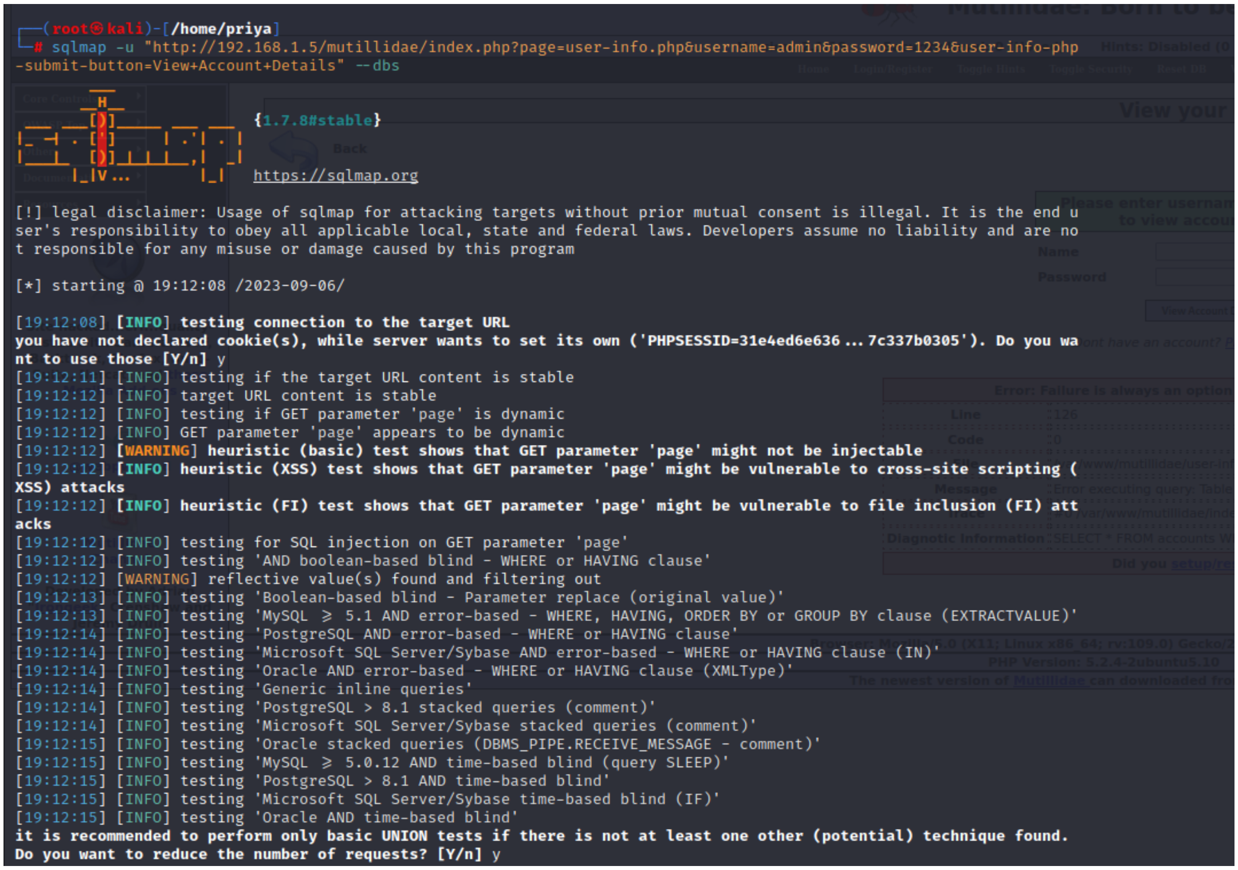
Commix: Commix is an open-source tool designed for automated web application security testing. It specializes in finding and exploiting vulnerabilities in web applications that involve command injection attacks. Commix helps in discovering and assess security flaws in web applications, aiding in their protection and improvement.



```
┌──(priya㉿kali)-[~]
└─$ commix --url "http://192.168.1.5/mutillidae/index.php?page=usage-instructions.php"
                                      __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v3.8-stable
/\ \__//\ \L\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2023 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program.

[18:49:21] [info] Testing connection to the target URL.
You have not declared cookie(s), while server wants to set its own ('PHPSESSID=88be9d709d1...e2b2053dc7'). Do you wa
nt to use those [Y/n] > y
[18:49:27] [info] Performing identification checks to the target URL.
[18:49:27] [info] Setting GET parameter 'page' for tests.
[18:49:32] [warning] Heuristic (basic) tests shows that GET parameter 'page' might not be injectable.
[18:49:43] [info] Testing the (results-based) classic command injection technique.
[18:49:59] [info] Testing the (results-based) dynamic code evaluation technique.
[18:49:59] [warning] It is very important to not stress the network connection during usage of time-based payloads t
o prevent potential disruptions.
[18:50:05] [info] Testing the (blind) time-based command injection technique.
[18:50:05] [info] Trying to create a file in '/var/www/mutillidae/' for command execution output.
It seems that you don't have permissions to read and/or write files in '/var/www/mutillidae/'. Do you want to use th
e temporary directory (/tmp/)? [Y/n] > y
[18:50:44] [info] Trying to create a file in temporary directory (/tmp/) for command execution output.
[18:50:44] [warning] It is very important to not stress the network connection during usage of time-based payloads t
o prevent potential disruptions.
[18:50:51] [info] Testing the (semi-blind) tempfile-based injection technique.
[18:50:51] [warning] The tested GET parameter 'page' does not seem to be injectable.
[18:50:51] [error] All tested parameters appear to be not injectable. Try to increase value for '--level' option if
you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved, maybe you c
ould try to use option '--alter-shell' and/or use option '--tamper' and/or switch '--random-agent'.
```

04 Database Assessment:

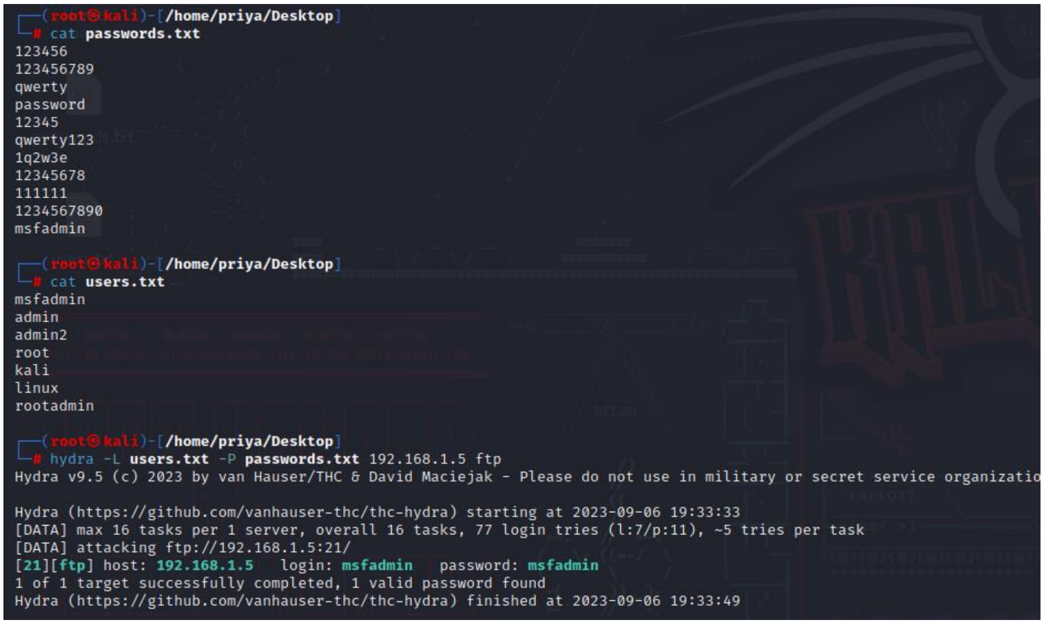
SQLmap: SQLmap is a popular open-source penetration testing tool for automating the detection and exploitation of SQL injection vulnerabilities in web applications. It helps security professionals identify and assess database-related security weaknesses, enabling them to better secure web applications against SQL injection attacks and other database-related threats.



```
┌──(root㉿kali)-[/home/priya]
└─# sqlmap -u "http://192.168.1.5/mutillidae/index.php?page=user-info.php&username=admin&password=1234&user-info-php
-submit-button=View+Account+Details" --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.8#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 19:12:08 /2023-09-06/

[19:12:08] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=31e4ed6e636...7c337b0305'). Do you wa
nt to use those [Y/n] y
[19:12:11] [INFO] testing if the target URL content is stable
[19:12:12] [INFO] target URL content is stable
[19:12:12] [INFO] testing if GET parameter 'page' is dynamic
[19:12:12] [INFO] GET parameter 'page' appears to be dynamic
[19:12:12] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[19:12:12] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (
XSS) attacks
[19:12:12] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) att
acks
[19:12:12] [INFO] testing for SQL injection on GET parameter 'page'
[19:12:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:12:12] [WARNING] reflective value(s) found and filtering out
[19:12:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:12:13] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:12:14] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:12:14] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:12:14] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:12:14] [INFO] testing 'Generic inline queries'
[19:12:14] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:12:14] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:12:15] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:12:15] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[19:12:15] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:12:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:12:15] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found.
Do you want to reduce the number of requests? [Y/n] y
```

05 password attacks:

Hydra: Hydra is a powerful and versatile password-cracking tool used to perform brute-force and dictionary attacks on various network protocols, such as SSH, FTP, HTTP, and more. Security professionals use Hydra to test the strength of passwords and identify weak authentication mechanisms, aiding in system and network security assessments.



```
┌──(root㉿kali)-[/home/priya/Desktop]
└─# cat passwords.txt
123456
123456789
qwerty
password
12345
qwerty123
1q2w3e
12345678
111111
1234567890
msfadmin

┌──(root㉿kali)-[/home/priya/Desktop]
└─# cat users.txt
msfadmin
admin
admin2
root
kali
linux
rootadmin

┌──(root㉿kali)-[/home/priya/Desktop]
└─# hydra -L users.txt -P passwords.txt 192.168.1.5 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-06 19:33:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:7/p:11), ~5 tries per task
[DATA] attacking ftp://192.168.1.5:21/
[21][ftp] host: 192.168.1.5   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-06 19:33:49
```

06 Wireless Attacks:

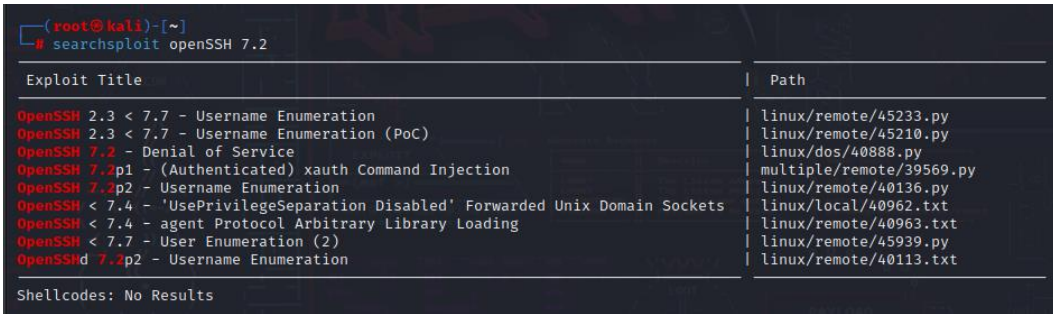
Pixiewps: Pixiewps is a tool used for auditing and retrieving WPS (Wi-Fi Protected Setup) PINs. It identifies vulnerable WPS-enabled Wi-Fi networks, attempts to crack their PINs, and recover the WPA/WPA2 PSK (Pre-Shared Key). Security experts and pentesters use Pixiewps to assess the security of Wi-Fi networks and strengthen their configurations against attacks.

07 Reverse Engineering:

Radare2: Radare2 is a powerful open-source framework for reverse engineering and binary analysis. It provides a wide range of tools and utilities for disassembling, debugging, analyzing, and patching binary code across various platforms and architectures. Security researchers, hackers, and developers use Radare2 for tasks like malware analysis and vulnerability research.

08 Exploitation Tools:

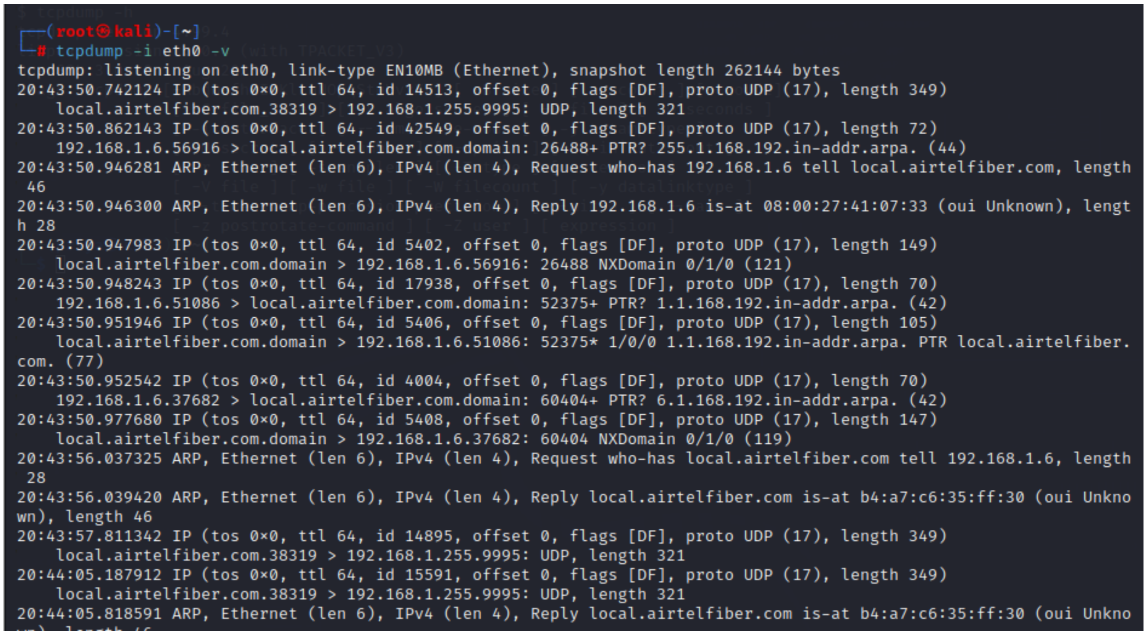
Searchsploit: Searchsploit is a command-line tool that searches the Exploit Database (Exploit-DB) for known vulnerabilities and exploits. It simplifies the process of finding and accessing relevant exploit code, making it a valuable resource for security professionals and penetration testers looking to assess and secure systems by identifying and mitigating known vulnerabilities.



```
┌──(root㉿kali)-[~]
└─# searchsploit openSSH 7.2
 ------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                            |  Path
 ------------------------------------------------------------------------ ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                  | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                            | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service                                           | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                   | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                      | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                  | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                      | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration                                     | linux/remote/40113.txt
 ------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

09 Sniffing and Spoofing:

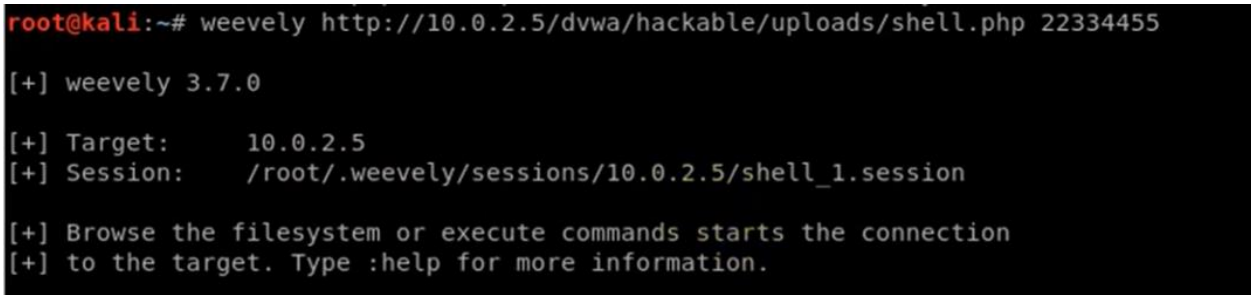
Tcpdump: Tcpdump is a command-line network packet analyzer for Unix-like systems. It captures and displays network traffic in real-time, allowing users to monitor and analyze data on a network interface. Tcpdump is valuable for diagnosing network issues, troubleshooting, and security analysis, helping professionals inspect and understand network communications.



```
┌──(root㉿kali)-[~]
└─# tcpdump -i eth0 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:43:50.742124 IP (tos 0×0, ttl 64, id 14513, offset 0, flags [DF], proto UDP (17), length 349)
    local.airtelfiber.com.38319 > 192.168.1.255.9995: UDP, length 321
20:43:50.862143 IP (tos 0×0, ttl 64, id 42549, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.1.6.56916 > local.airtelfiber.com.domain: 26488+ PTR? 255.1.168.192.in-addr.arpa. (44)
20:43:50.946281 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.6 tell local.airtelfiber.com, length
 46
20:43:50.946300 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.6 is-at 08:00:27:41:07:33 (oui Unknown), lengt
h 28
20:43:50.947983 IP (tos 0×0, ttl 64, id 5402, offset 0, flags [DF], proto UDP (17), length 149)
    local.airtelfiber.com.domain > 192.168.1.6.56916: 26488 NXDomain 0/1/0 (121)
20:43:50.948243 IP (tos 0×0, ttl 64, id 17938, offset 0, flags [DF], proto UDP (17), length 70)
    192.168.1.6.51086 > local.airtelfiber.com.domain: 52375+ PTR? 1.1.168.192.in-addr.arpa. (42)
20:43:50.951946 IP (tos 0×0, ttl 64, id 5406, offset 0, flags [DF], proto UDP (17), length 105)
    local.airtelfiber.com.domain > 192.168.1.6.51086: 52375* 1/0/0 1.1.168.192.in-addr.arpa. PTR local.airtelfiber.
com. (77)
20:43:50.952542 IP (tos 0×0, ttl 64, id 4004, offset 0, flags [DF], proto UDP (17), length 70)
    192.168.1.6.37682 > local.airtelfiber.com.domain: 60404+ PTR? 6.1.168.192.in-addr.arpa. (42)
20:43:50.977680 IP (tos 0×0, ttl 64, id 5408, offset 0, flags [DF], proto UDP (17), length 147)
    local.airtelfiber.com.domain > 192.168.1.6.37682: 60404 NXDomain 0/1/0 (119)
20:43:56.037325 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has local.airtelfiber.com tell 192.168.1.6, length
 28
20:43:56.039420 ARP, Ethernet (len 6), IPv4 (len 4), Reply local.airtelfiber.com is-at b4:a7:c6:35:ff:30 (oui Unkno
wn), length 46
20:43:57.811342 IP (tos 0×0, ttl 64, id 14895, offset 0, flags [DF], proto UDP (17), length 349)
    local.airtelfiber.com.38319 > 192.168.1.255.9995: UDP, length 321
20:44:05.187912 IP (tos 0×0, ttl 64, id 15591, offset 0, flags [DF], proto UDP (17), length 349)
    local.airtelfiber.com.38319 > 192.168.1.255.9995: UDP, length 321
20:44:05.818591 ARP, Ethernet (len 6), IPv4 (len 4), Reply local.airtelfiber.com is-at b4:a7:c6:35:ff:30 (oui Unkno
```

10 Post Exploration:

Weevely: Weevely is a web shell tool designed for penetration testing and ethical hacking. It provides a stealthy way to maintain remote access to web servers, execute commands, and upload/download files through a PHP backdoor. Security professionals use Weevely to assess web application security and test server defenses against unauthorized access and control.



```
root@kali:~# weevely http://10.0.2.5/dvwa/hackable/uploads/shell.php 22334455

[+] weevely 3.7.0

[+] Target:     10.0.2.5
[+] Session:    /root/.weevely/sessions/10.0.2.5/shell_1.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.
```