ASSIGNMENT – 2

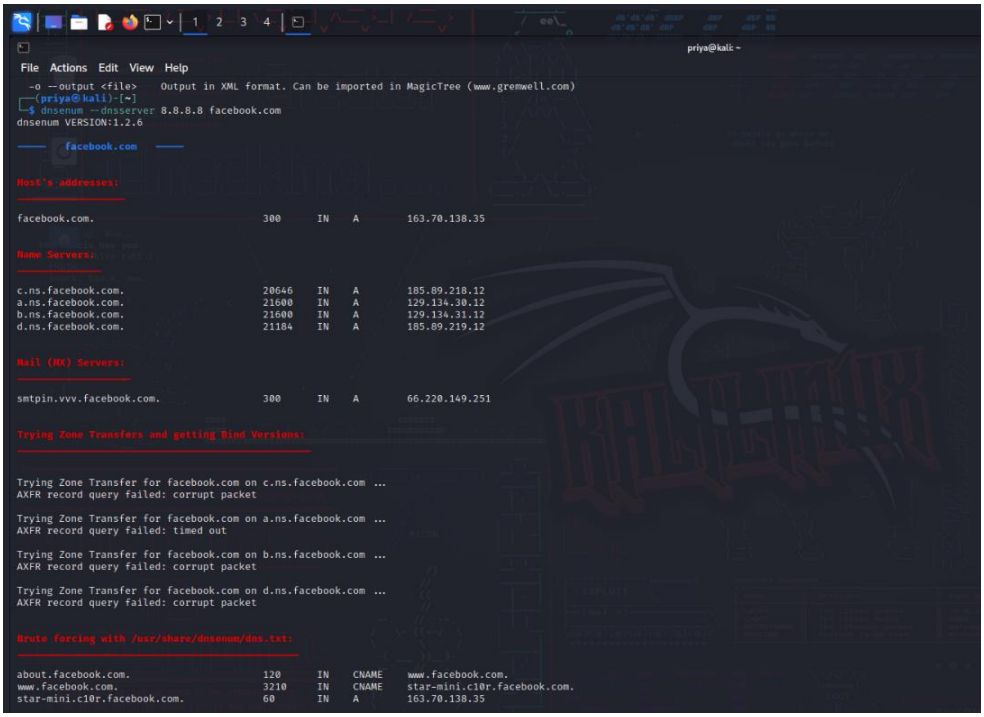
NAME: RAMAR PRIYA MAHA LAKSHMI

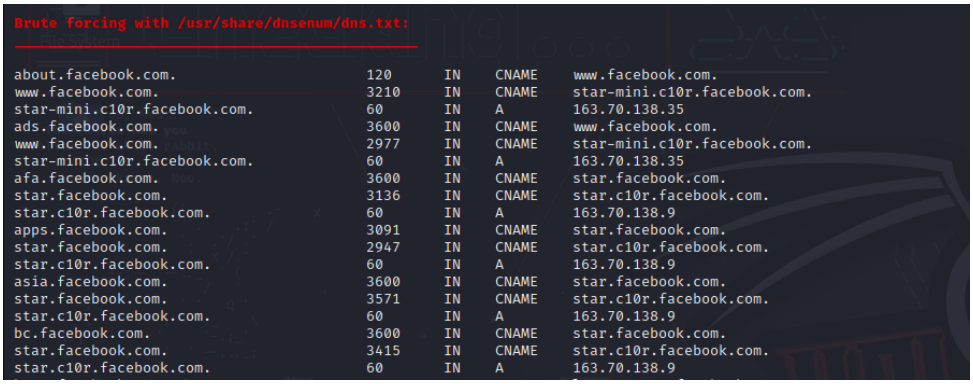
REGNO: 21BCE7521

1. **Exploring tools in Kali Linux.**

01 – Information Gathering.

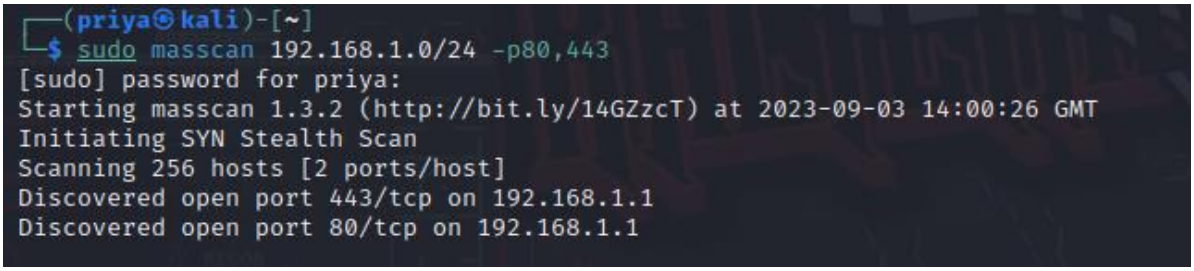
Dnsenum: DNSenum is a command-line network reconnaissance tool designed for domain analysis and reconnaissance. It assists in gathering critical information about a target domain's DNS infrastructure. It helps in subdomain enumeration, brute-force subdomain discovery, and DNS zone transfer attempts. 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.





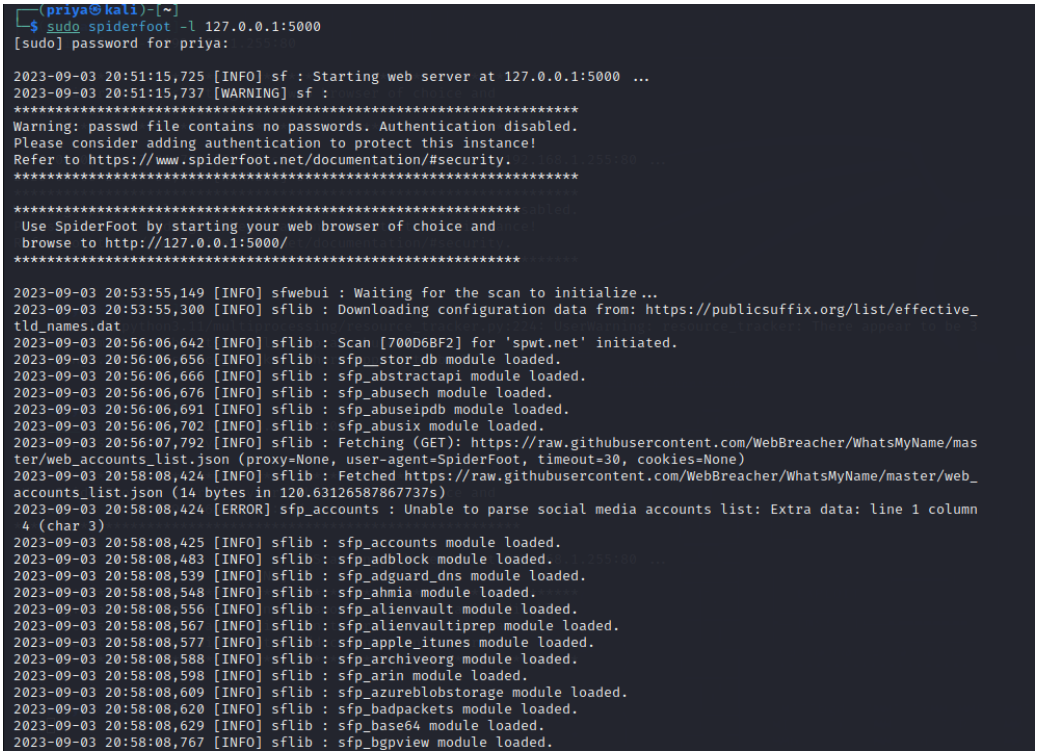
Wafw00f: Wafw00f is a security tool used to identify and profile web application firewalls (WAFs). By sending HTTP requests to a target website and analyzing the responses, it can detect if a WAF is actively protecting the web application. This information is invaluable as it helps in understanding the 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.

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.



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.

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.



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
```

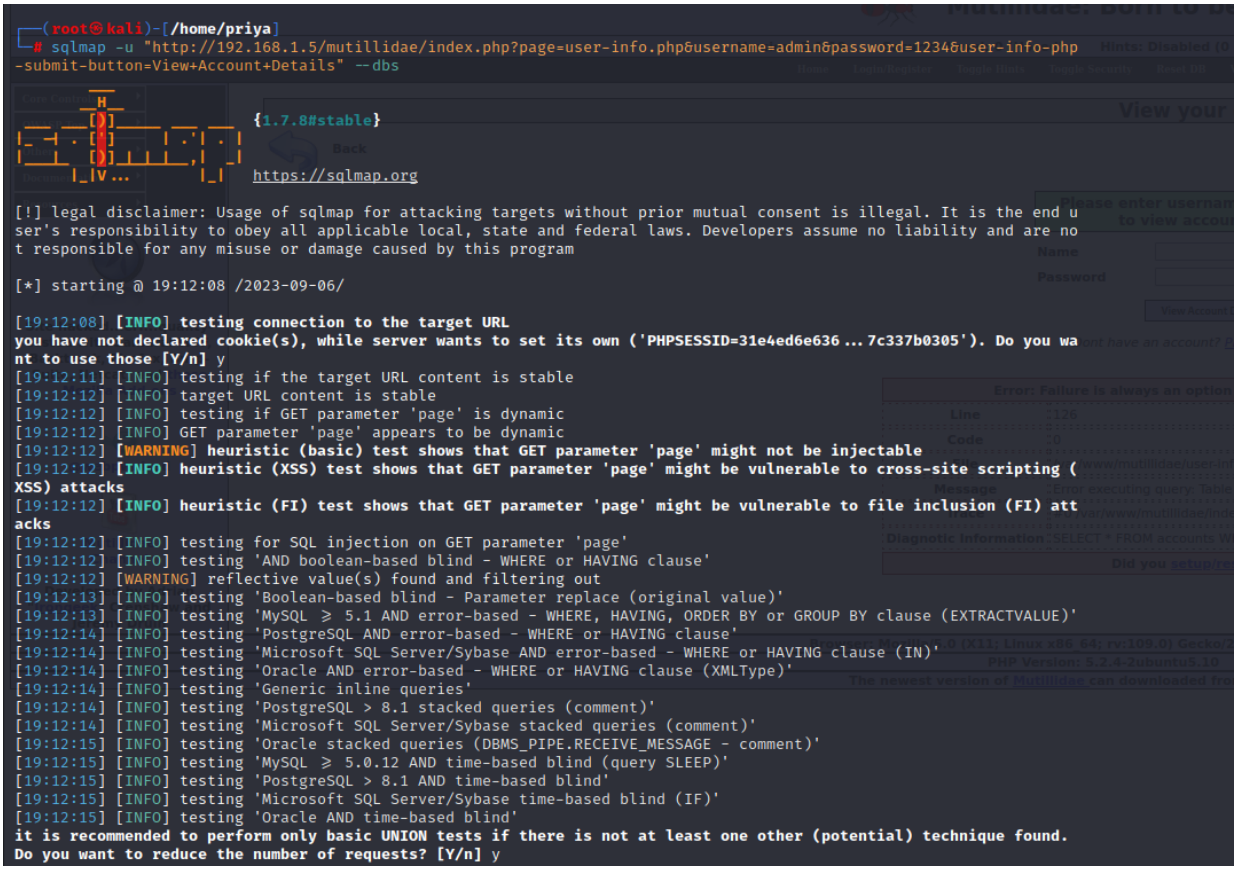
03 Web Application Analysis:

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
/\ \__//\ \/\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \ \/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_/\_\ 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'.
```

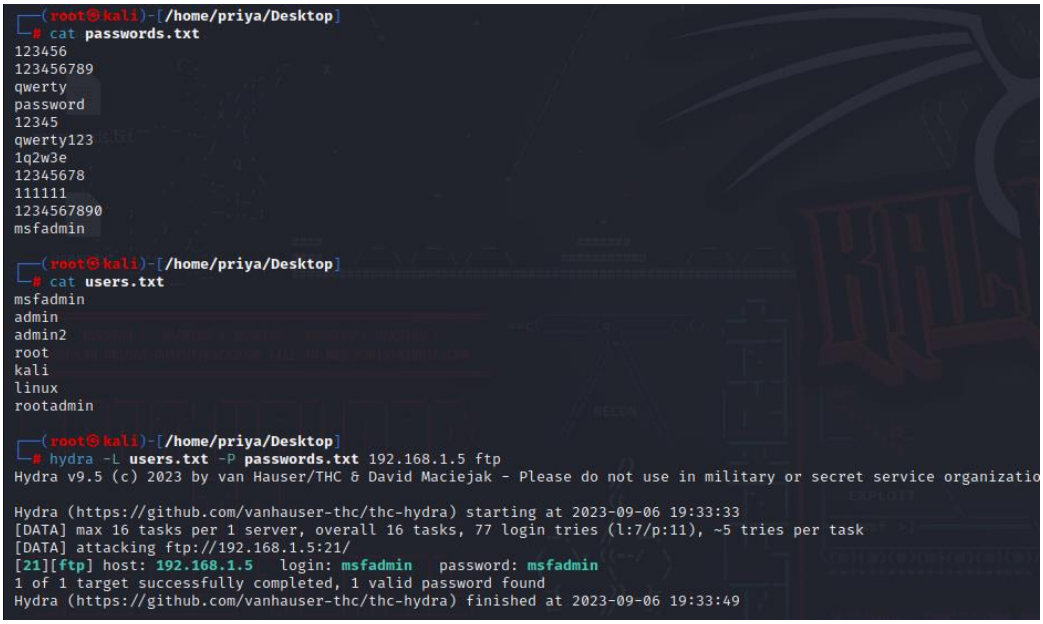
04 Database Assessment:

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.



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.



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.

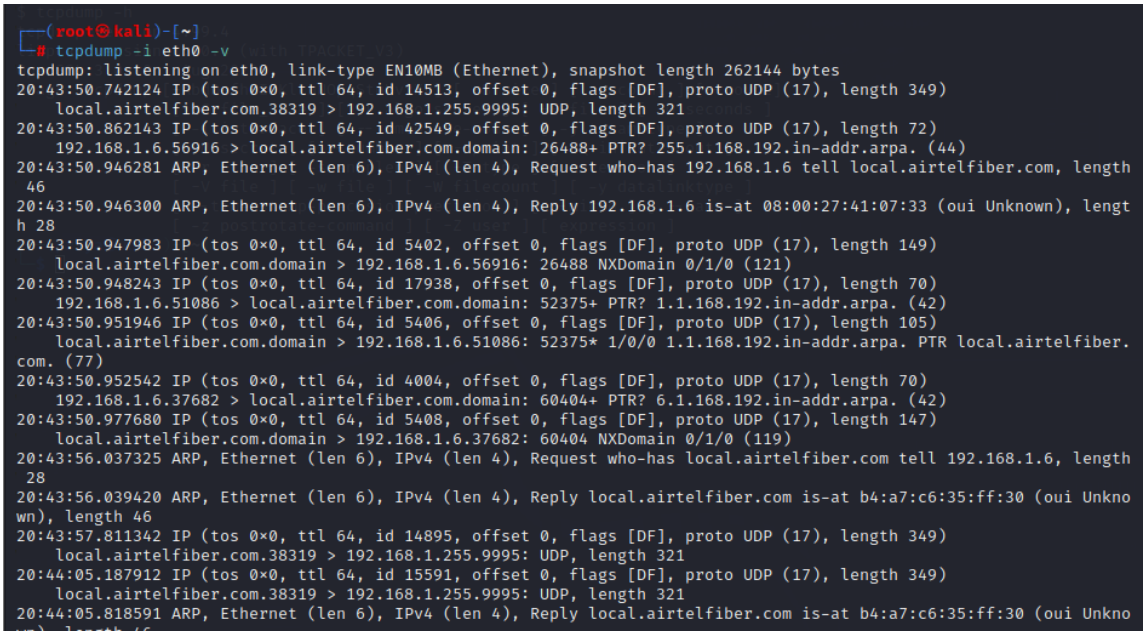
08 Exploitation Tools:

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.

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.



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.