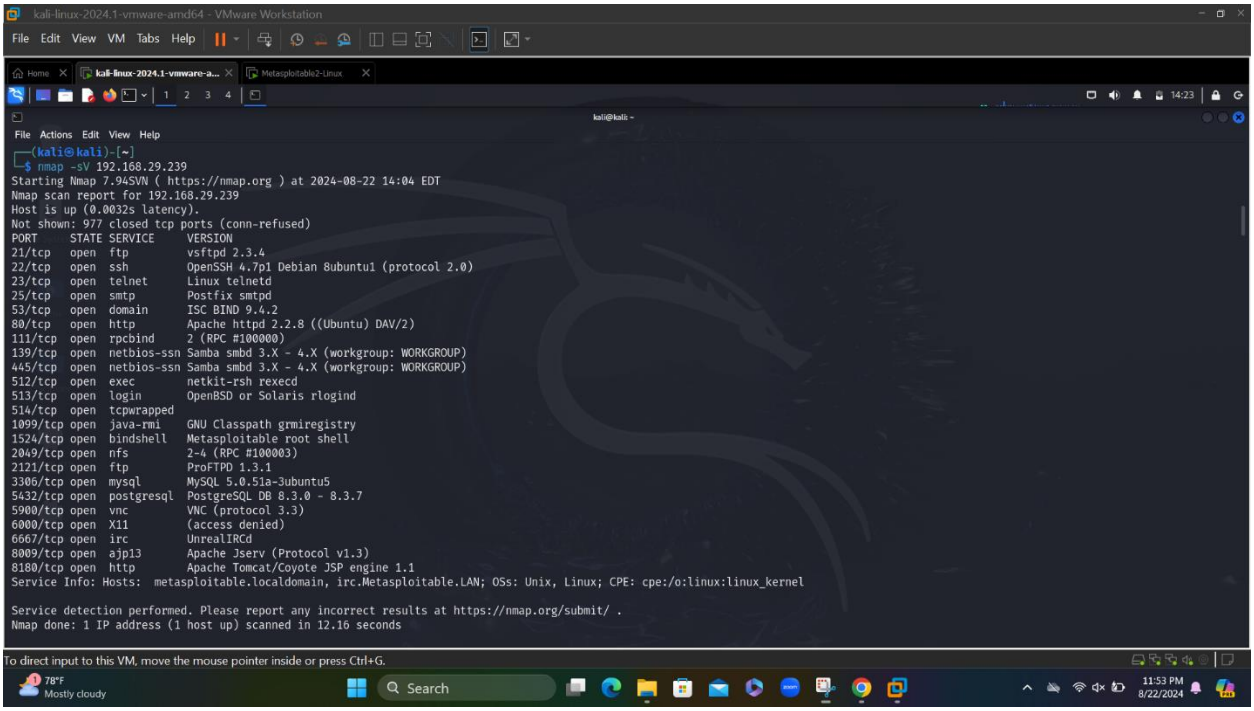
Executive Post Graduate Certification in Cyber Security and Ethical Hacking

project

NMAP SCAN



Scan Date: 2024-08-22

Scan Tool: Nmap 7.94SVN

Target IP: 192.168.29.239

Summary of Findings

The Nmap scan identified the following open ports and services on the target host:

Port	State	Service	Version
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	OpenBSD or Solaris rlogind
514/tcp	open	tcpwrapped	
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell

2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Potential Targets for Further Enumeration

1. **FTP Services**
    - **Port 21 (vsftpd 2.3.4)** and **Port 2121 (ProFTPD 1.3.1)**:
        - Both FTP services might be configured with weak credentials or allow anonymous access. They are prime candidates for further testing for weak passwords or insecure configurations.
2. **SSH Service**
    - **Port 22 (OpenSSH 4.7p1)**:
        - Older version of OpenSSH may have known vulnerabilities. Consider further testing for default or weak credentials and any potential exploits for the specific version.
3. **Telnet Service**
    - **Port 23 (Linux telnetd)**:
        - Telnet is generally insecure. Test for default or weak credentials and consider exploiting its inherent insecurity if sensitive information is transmitted.

4. **SMTP Service**
    - **Port 25 (Postfix smtpd)**:
        - This service can be tested for open relay configurations and potential vulnerabilities in the version.
5. **Web Services**
    - **Port 80 (Apache httpd 2.2.8)** and **Port 8180 (Apache Tomcat/Coyote JSP engine 1.1)**:
        - Both web servers might have vulnerabilities associated with their versions. Testing for common web application vulnerabilities (e.g., XSS, SQL injection) and configuration issues is recommended.

6. **Database Services**
    - **Port 3306 (MySQL 5.0.51a-3ubuntu5)** and **Port 5432 (PostgreSQL DB 8.3.0 - 8.3.7)**:
        - Test for default credentials, unpatched vulnerabilities, and unauthorized access possibilities.

7. **Network Services**
    - **Port 111 (rpcbind)**, **Port 2049 (NFS)**, **Port 1099 (Java RMI)**:
        - These services could be vulnerable to unauthorized access or misconfigurations. Further enumeration to assess permissions and vulnerabilities is advised.

8. **Other Services**
    - **Port 1524 (Metasploitable root shell)**:
        - This port is specifically noted for having a root shell associated with Metasploitable. It is a high-risk target and should be thoroughly examined.

- **Port 5900 (VNC)**:
    - Check for weak or default credentials, as VNC is often misconfigured.
- **Port 6667 (UnrealIRCd)**:
    - This IRC service could have specific vulnerabilities or misconfigurations that need to be explored.

Recommendations

- **Verify and Enumerate Services:** Focus on verifying the versions and configurations of the services running. Check for known vulnerabilities and security misconfigurations associated with these services.
- **Exploit Potential Vulnerabilities:** Using tools and techniques appropriate to each service, attempt to exploit any discovered vulnerabilities to assess potential risks.
- **Secure Weak Points:** Implement strong access controls, update services to their latest versions, and disable unnecessary services to reduce the attack surface.

Employ smbclient to establish connections with SMB shares

```
Nmap done: 1 IP address (1 host up) scanned in 12.16 seconds

┌──(kali㉿kali)-[~]
└─$ smbclient
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr]
        [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING]
        [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet] [-B|--browse]
        [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value]
        [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER]
        [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME]
        [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP] [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]]
        [-N|--no-pass] [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE] [-P|--machine-pass]
        [--simple-bind-dn=DN] [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE] [--use-winbind-ccache]
        [--client-protection=sign|encrypt|off] [-k|--kerberos] [-V|--version] [OPTIONS] service <password>
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 192.168.29.239
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\192.168.29.239\\IPC$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> exit

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\192.168.29.239\\ADMIN$
Password for [WORKGROUP\kali]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient \\\\192.168.29.239\\IPC$
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
```

```
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> exit
```

List of Shares on the Target (192.168.29.239)

- print$: Disk share for printer drivers

- tmp: Disk share, labeled "oh noes!"

- opt: Disk share with no comment

- IPC$: Inter-process communication share

- ADMIN$: Administrative share

Access Attempts

- IPC$: Connection successful but directory listing failed (`NT_STATUS_NETWORK_ACCESS_DENIED`).

- ADMIN$: Connection attempted but failed with `NT_STATUS_ACCESS_DENIED`.

Next Steps

- **Brute Force or Dictionary Attack:**

  If you need to access `IPC$` or `ADMIN$` and are authorized to do so, consider using a password brute-force or dictionary attack tool if you suspect weak or default passwords.

- **Examine Permissions and Security Settings:**

  The error `NT_STATUS_NETWORK_ACCESS_DENIED` suggests there may be permissions issues. Investigate if there are specific security settings or ACLs that need adjusting or bypassing.

- **Use Additional Tools:**

  Tools like `enum4linux`, `smbmap`, or `crackmapexec` can provide more in-depth enumeration and may help identify additional shares or configuration details:

  bash

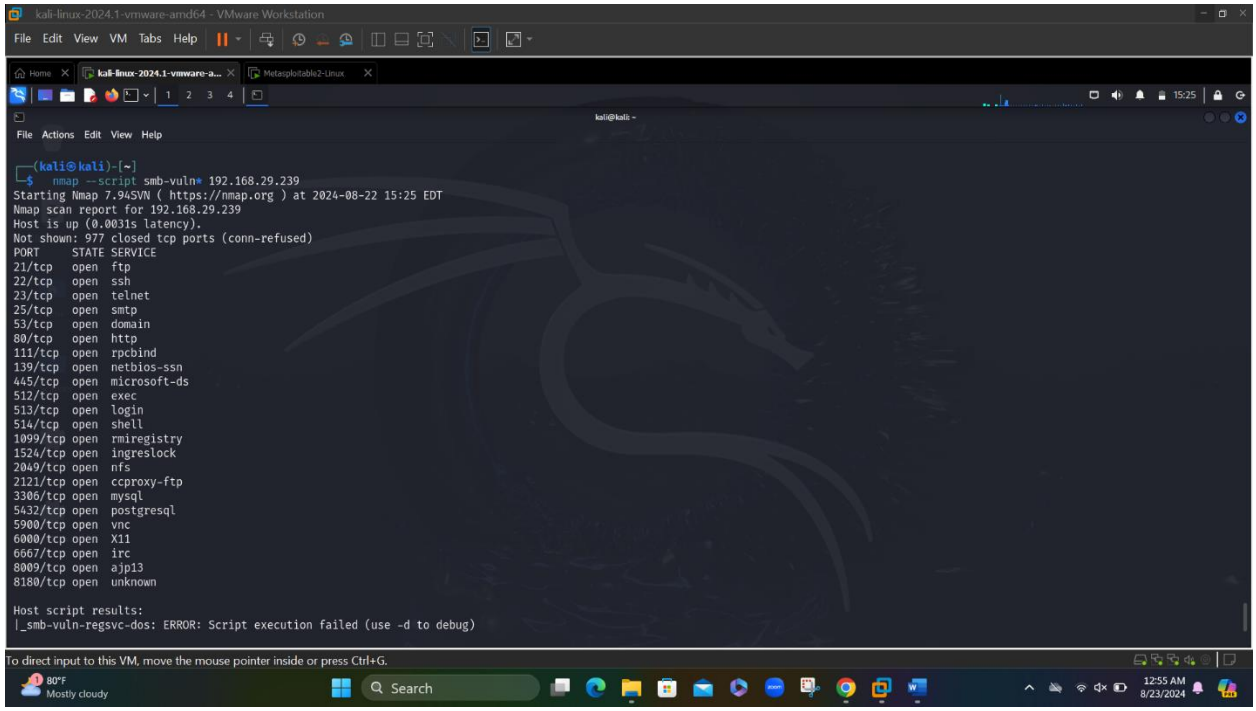
  ```
  enum4linux -a 192.168.29.239
  ```

🔹 Check for SMB Vulnerabilities:

Given this is a Metasploitable machine, it might be worth running some automated vulnerability scanners or exploits against SMB to find known issues:

bash

```
nmap --script smb-vuln* 192.168.29.239
```



ENUM4LINUX scan

```
┌──(kali㉿kali)-[~]
└─$ enum4linux 192.168.29.239
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Aug 22 14:18:06 2024

 ========================== ( Target Information ) ==========================

Target ........... 192.168.29.239
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============ ( Enumerating Workgroup/Domain on 192.168.29.239 ) ============


[+] Got domain/workgroup name: WORKGROUP


 ============ ( Nbtstat Information for 192.168.29.239 ) ============

Looking up status of 192.168.29.239
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ============ ( Session Check on 192.168.29.239 ) ============
```

```
        MAC Address = 00-00-00-00-00-00

 ============ ( Session Check on 192.168.29.239 ) ============


[+] Server 192.168.29.239 allows sessions using username '', password ''


 ============ ( Getting domain SID for 192.168.29.239 ) ============

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ============ ( OS information on 192.168.29.239 ) ============


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.29.239 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03


 ============ ( Users on 192.168.29.239 ) ============
```

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.1-vmware-a... | Metasploitable2-Linux

kali@kali: ~

File Actions Edit View Help

```
=================================( Users on 192.168.29.239 )=================================

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games    Name: games      Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody   Name: nobody     Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind     Name: (null)     Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy    Name: proxy      Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog   Name: (null)     Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data   Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root       Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news       Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,,       Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin      Name: bin        Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail     Name: mail       Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd  Name: (null)     Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd  Name: (null)     Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp     Name: (null)     Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon  Name: daemon     Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd    Name: (null)     Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man     Name: man        Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp      Name: lp         Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql   Name: MySQL Server,,,   Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats   Name: Gnats Bug-Reporting System (admin)       Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null)     Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup  Name: backup     Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin      Name: msfadmin,,,      Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null)     Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys     Name: sys        Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog    Name: (null)     Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null)     Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,,        Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list    Name: Mailing List Manager      Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc     Name: ircd       Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp     Name: (null)     Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55      Name: (null)     Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync    Name: sync       Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp    Name: uucp       Desc: (null)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

78°F Mostly cloudy | Search | 11:58 PM 8/22/2024

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.1-vmware-a... | Metasploitable2-Linux

kali@kali: ~

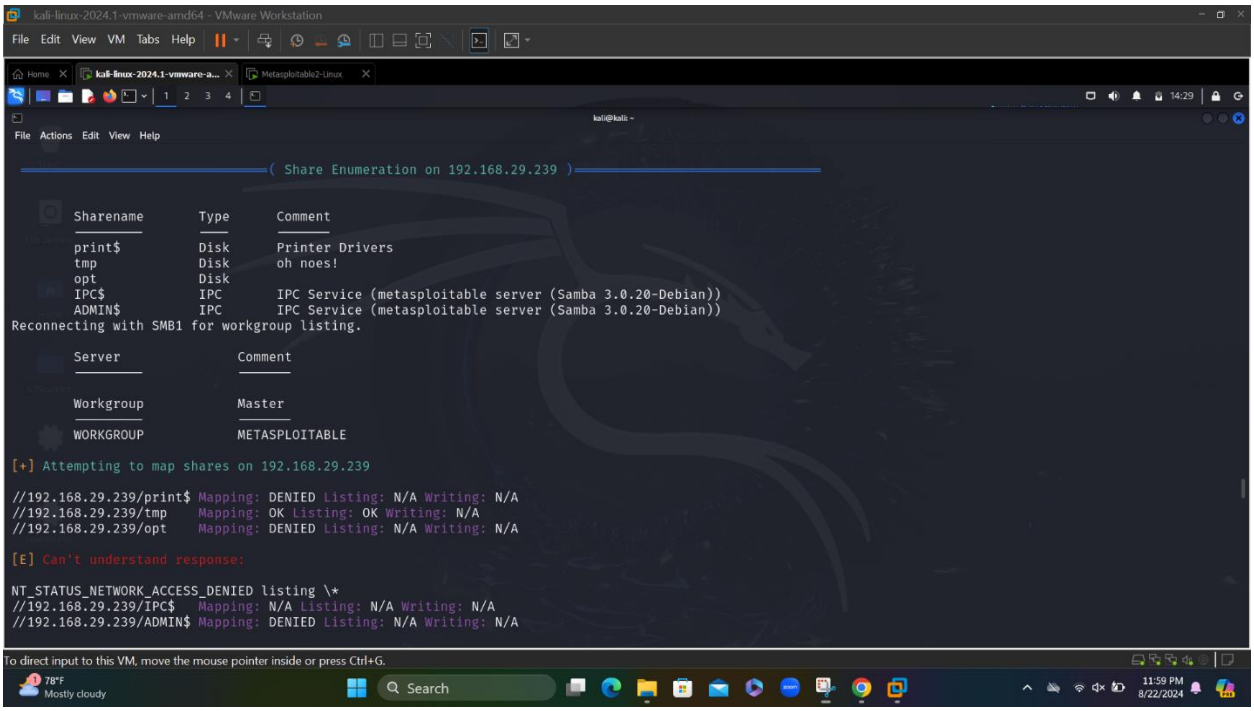
File Actions Edit View Help

```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]

=================================( Share Enumeration on 192.168.29.239 )=================================
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

78°F Mostly cloudy | Search | 11:58 PM 8/22/2024



- **enum4linux` Enumeration results**

submitted by

sairaj mothukuri

sairajmothukuri28@gmail.com

.