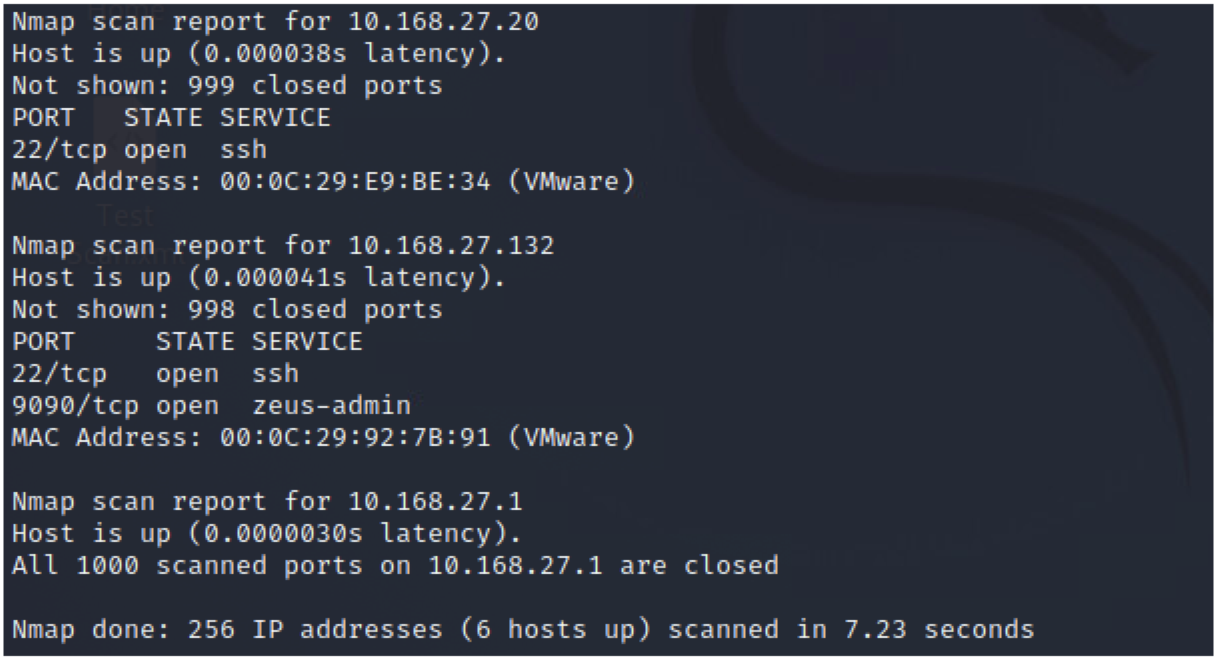
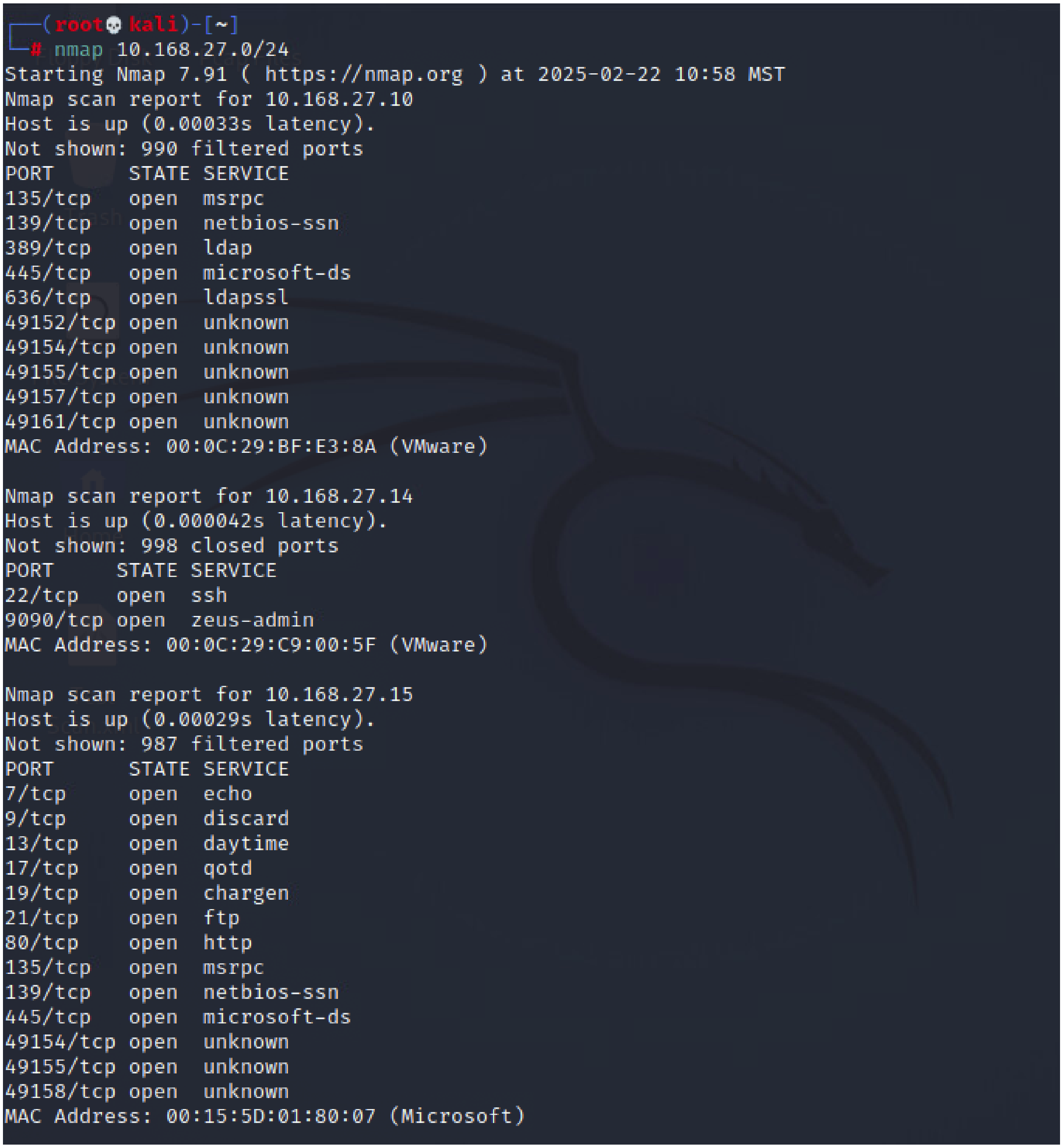
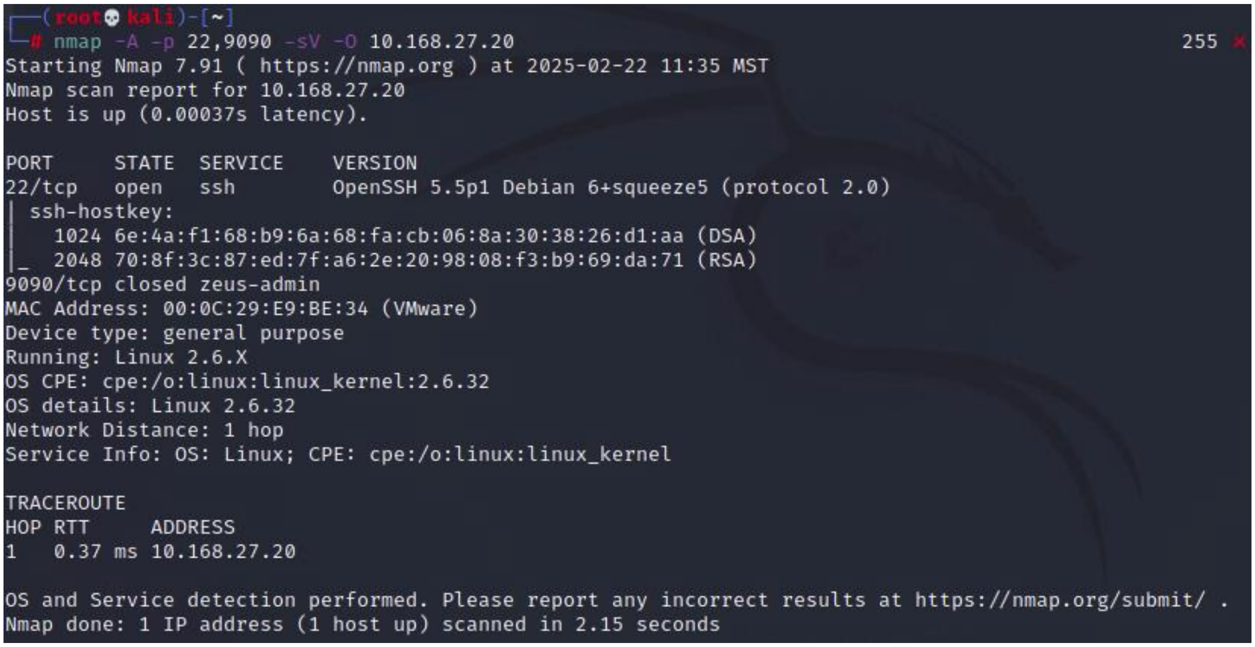
NMAP Lab Session Pictures



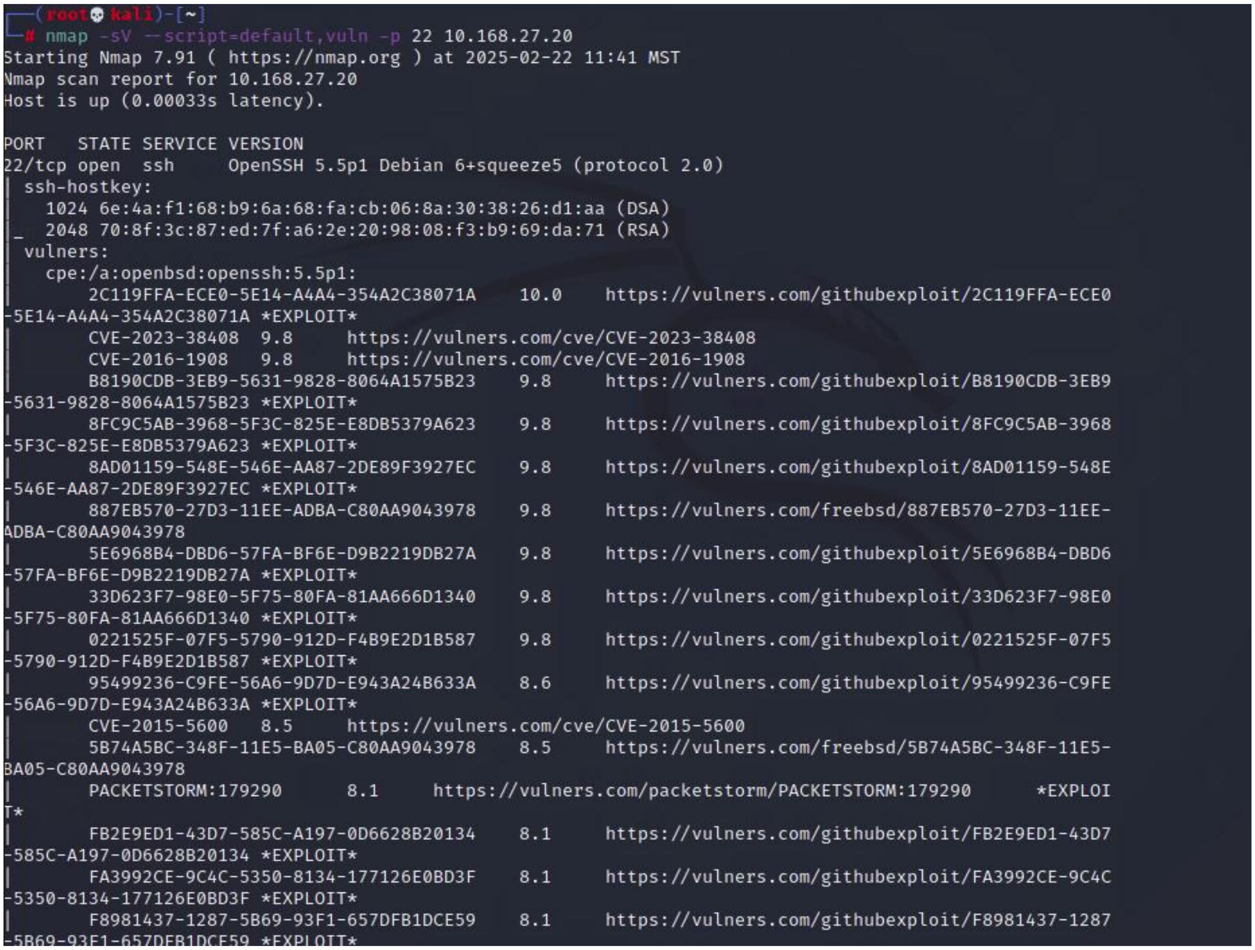
```
Nmap scan report for 10.168.27.20
Host is up (0.000038s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:E9:BE:34 (VMware)

Nmap scan report for 10.168.27.132
Host is up (0.000041s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9090/tcp open  zeus-admin
MAC Address: 00:0C:29:92:7B:91 (VMware)

Nmap scan report for 10.168.27.1
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.168.27.1 are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 7.23 seconds
```



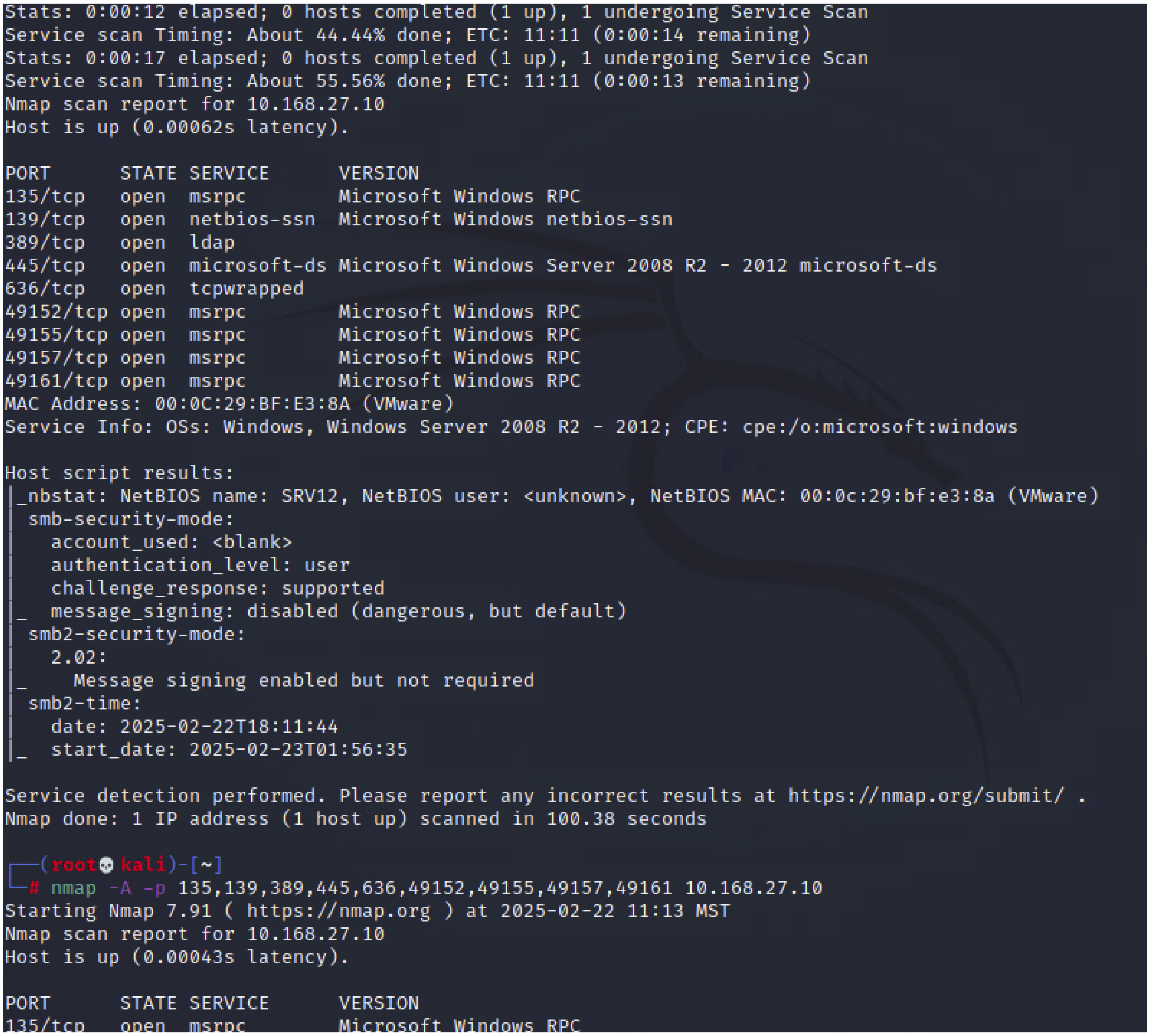
```
┌──(root💀kali)-[~]
└─# nmap 10.168.27.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 10:58 MST
Nmap scan report for 10.168.27.10
Host is up (0.00033s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
636/tcp   open  ldapssl
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49161/tcp open  unknown
MAC Address: 00:0C:29:BF:E3:8A (VMware)

Nmap scan report for 10.168.27.14
Host is up (0.000042s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9090/tcp open  zeus-admin
MAC Address: 00:0C:29:C9:00:5F (VMware)

Nmap scan report for 10.168.27.15
Host is up (0.00029s latency).
Not shown: 987 filtered ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:15:5D:01:80:07 (Microsoft)
```



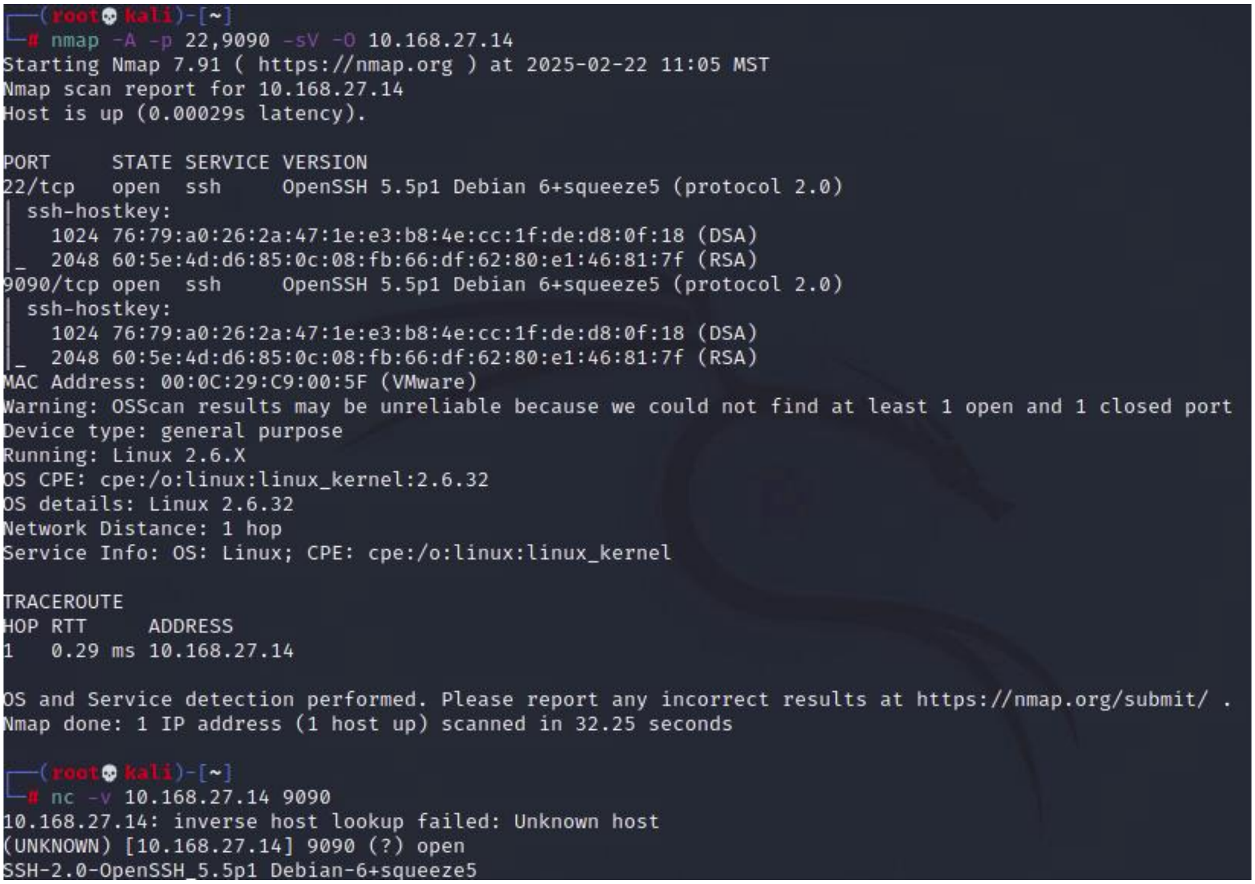
```
┌──(root💀kali)-[~]
└─# nmap -A -p 22,9090 -sV -O 10.168.27.20                                                       255 ✕
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:35 MST
Nmap scan report for 10.168.27.20
Host is up (0.00037s latency).

PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey: 
|   1024 6e:4a:f1:68:b9:6a:68:fa:cb:06:8a:30:38:26:d1:aa (DSA)
|_  2048 70:8f:3c:87:ed:7f:a6:2e:20:98:08:f3:b9:69:da:71 (RSA)
9090/tcp closed zeus-admin
MAC Address: 00:0C:29:E9:BE:34 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 10.168.27.20

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
```



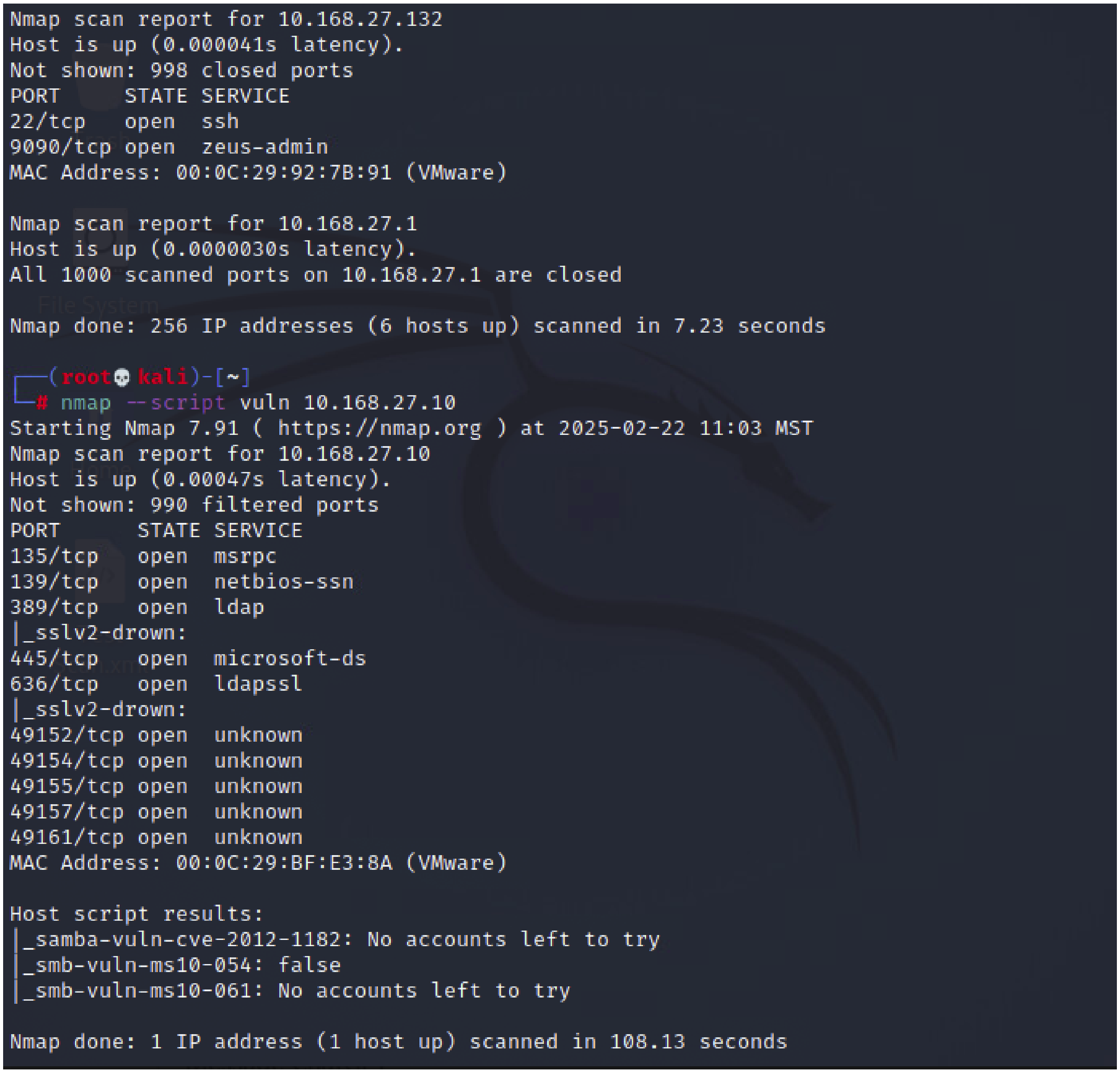
```
┌──(root💀kali)-[~]
└─# nmap -sV --script=default,vuln -p 22 10.168.27.20
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:41 MST
Nmap scan report for 10.168.27.20
Host is up (0.00033s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 6e:4a:f1:68:b9:6a:68:fa:cb:06:8a:30:38:26:d1:aa (DSA)
|_  2048 70:8f:3c:87:ed:7f:a6:2e:20:98:08:f3:b9:69:da:71 (RSA)
| vulners:
|   cpe:/a:openbsd:openssh:5.5p1:
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0
-5E14-A4A4-354A2C38071A *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9
-5631-9828-8064A1575B23 *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968
-5F3C-825E-E8DB5379A623 *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E
-546E-AA87-2DE89F3927EC *EXPLOIT*
|       887EB570-27D3-11EE-ADBA-C80AA9043978    9.8     https://vulners.com/freebsd/887EB570-27D3-11EE-
ADBA-C80AA9043978
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6
-57FA-BF6E-D9B2219DB27A *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0
-5F75-80FA-81AA666D1340 *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5
-5790-912D-F4B9E2D1B587 *EXPLOIT*
|       95499236-C9FE-56A6-9D7D-E943A24B633A    8.6     https://vulners.com/githubexploit/95499236-C9FE
-56A6-9D7D-E943A24B633A *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       5B74A5BC-348F-11E5-BA05-C80AA9043978    8.5     https://vulners.com/freebsd/5B74A5BC-348F-11E5-
BA05-C80AA9043978
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOI
T*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7
-585C-A197-0D6628B20134 *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C
-5350-8134-177126E0BD3F *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287
-5B69-93F1-657DFB1DCE59 *EXPLOIT*
```



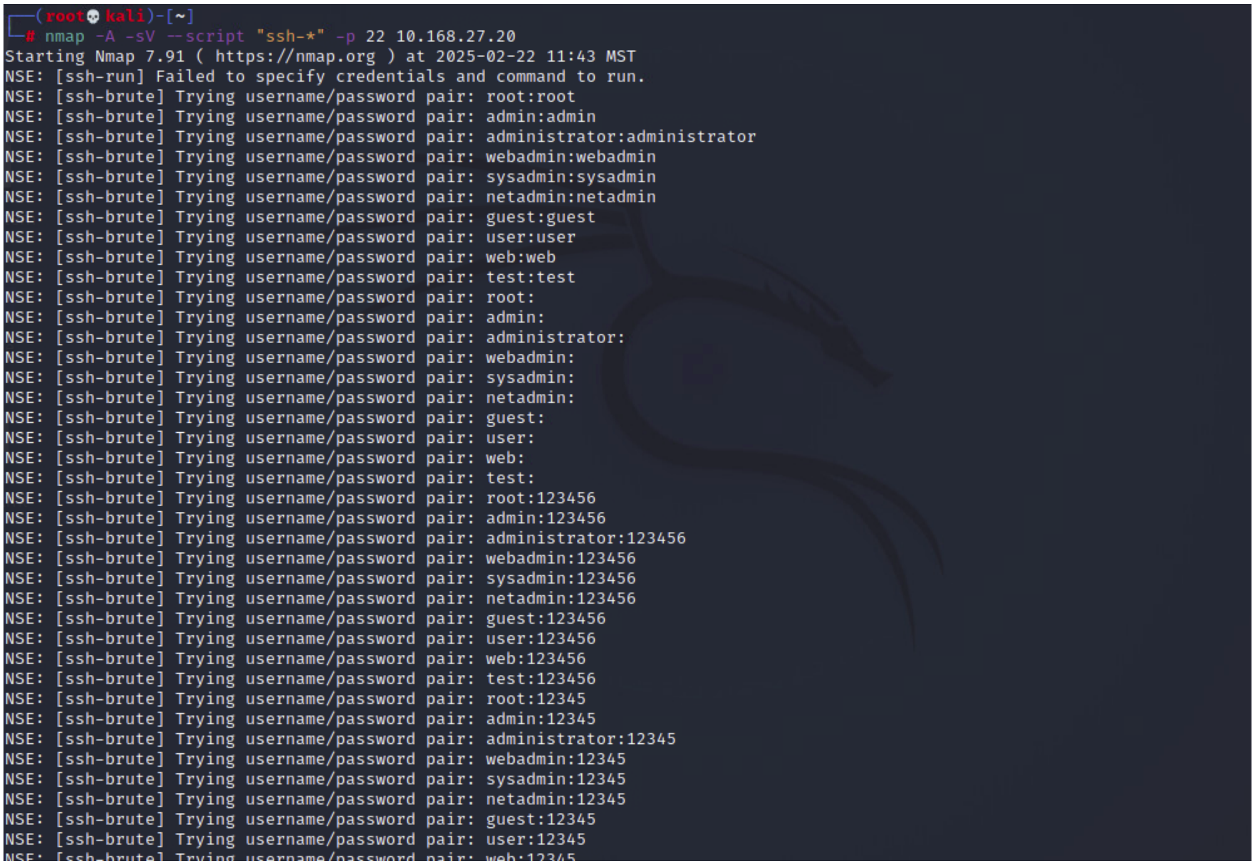
```
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 44.44% done; ETC: 11:11 (0:00:14 remaining)
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 55.56% done; ETC: 11:11 (0:00:13 remaining)
Nmap scan report for 10.168.27.10
Host is up (0.00062s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
636/tcp   open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:BF:E3:8A (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: SRV12, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:bf:e3:8a (VMware)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-02-22T18:11:44
|_  start_date: 2025-02-23T01:56:35

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.38 seconds

┌──(root💀kali)-[~]
└─# nmap -A -p 135,139,389,445,636,49152,49155,49157,49161 10.168.27.10
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:13 MST
Nmap scan report for 10.168.27.10
Host is up (0.00043s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
```



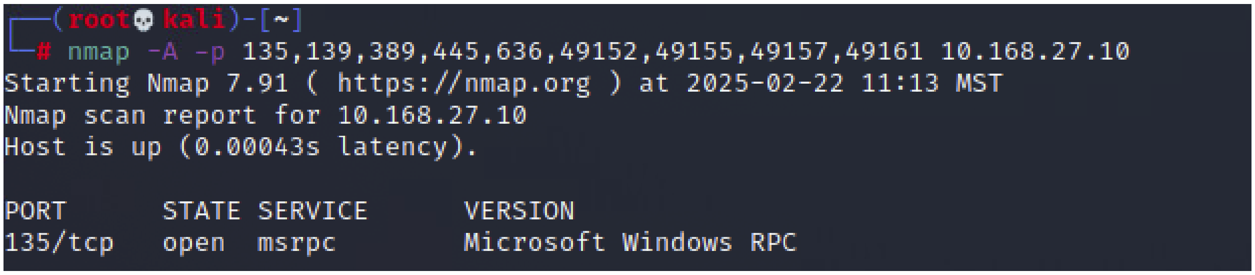
```
┌──(root💀kali)-[~]
└─# nmap -A -p 22,9090 -sV -O 10.168.27.14
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:05 MST
Nmap scan report for 10.168.27.14
Host is up (0.00029s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 76:79:a0:26:2a:47:1e:e3:b8:4e:cc:1f:de:d8:0f:18 (DSA)
|_  2048 60:5e:4d:d6:85:0c:08:fb:66:df:62:80:e1:46:81:7f (RSA)
9090/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
| ssh-hostkey:
|   1024 76:79:a0:26:2a:47:1e:e3:b8:4e:cc:1f:de:d8:0f:18 (DSA)
|_  2048 60:5e:4d:d6:85:0c:08:fb:66:df:62:80:e1:46:81:7f (RSA)
MAC Address: 00:0C:29:C9:00:5F (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 10.168.27.14

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.25 seconds

┌──(root💀kali)-[~]
└─# nc -v 10.168.27.14 9090
10.168.27.14: inverse host lookup failed: Unknown host
(UNKNOWN) [10.168.27.14] 9090 (?) open
SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze5
```



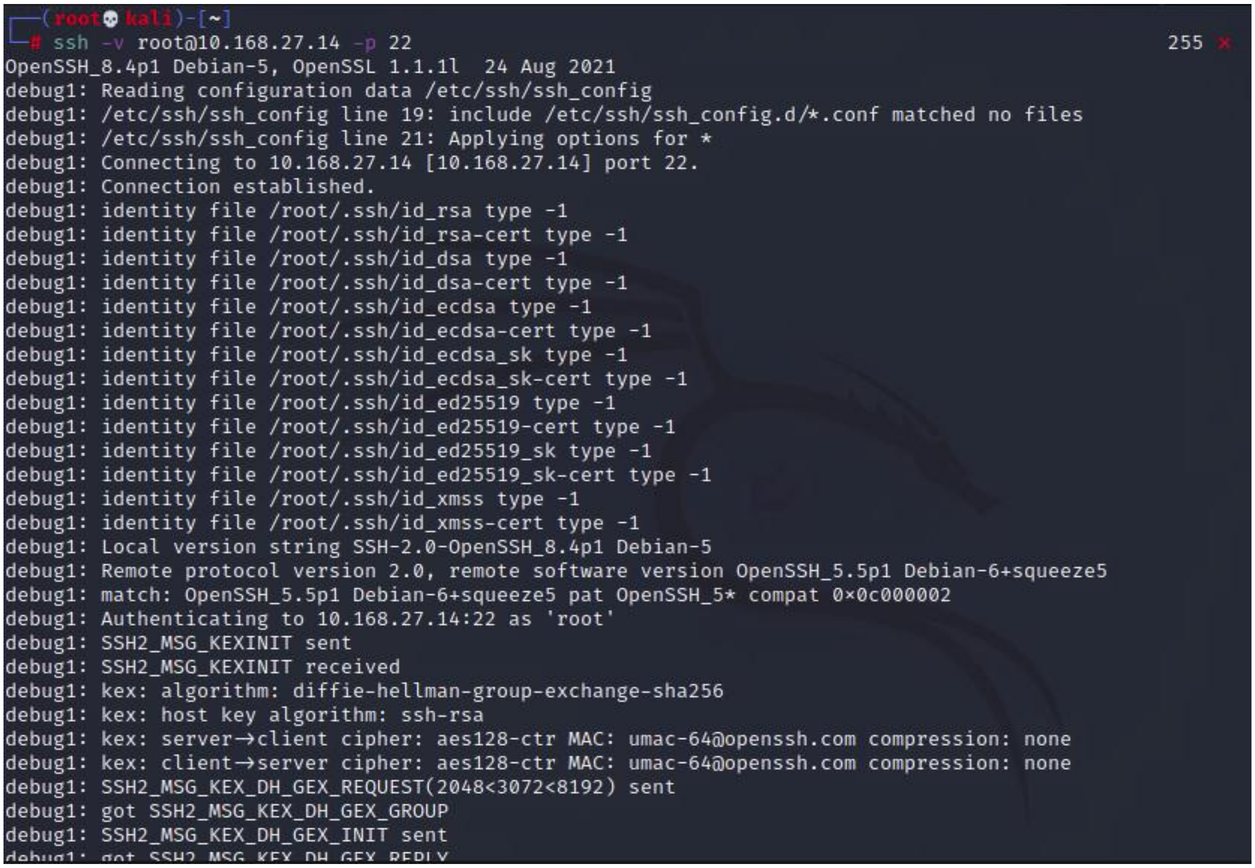
```
Nmap scan report for 10.168.27.132
Host is up (0.000041s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9090/tcp open  zeus-admin
MAC Address: 00:0C:29:92:7B:91 (VMware)

Nmap scan report for 10.168.27.1
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.168.27.1 are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 7.23 seconds

┌──(root💀kali)-[~]
└─# nmap --script vuln 10.168.27.10
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:03 MST
Nmap scan report for 10.168.27.10
Host is up (0.00047s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
|_sslv2-drown:
445/tcp   open  microsoft-ds
636/tcp   open  ldapssl
|_sslv2-drown:
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49161/tcp open  unknown
MAC Address: 00:0C:29:BF:E3:8A (VMware)

Host script results:
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: No accounts left to try

Nmap done: 1 IP address (1 host up) scanned in 108.13 seconds
```



```
┌──(root💀kali)-[~]
└─# nmap -A -sV --script "ssh-*" -p 22 10.168.27.20
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:43 MST
NSE: [ssh-run] Failed to specify credentials and command to run.
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
NSE: [ssh-brute] Trying username/password pair: root:123456
NSE: [ssh-brute] Trying username/password pair: admin:123456
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: webadmin:123456
NSE: [ssh-brute] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute] Trying username/password pair: netadmin:123456
NSE: [ssh-brute] Trying username/password pair: guest:123456
NSE: [ssh-brute] Trying username/password pair: user:123456
NSE: [ssh-brute] Trying username/password pair: web:123456
NSE: [ssh-brute] Trying username/password pair: test:123456
NSE: [ssh-brute] Trying username/password pair: root:12345
NSE: [ssh-brute] Trying username/password pair: admin:12345
NSE: [ssh-brute] Trying username/password pair: administrator:12345
NSE: [ssh-brute] Trying username/password pair: webadmin:12345
NSE: [ssh-brute] Trying username/password pair: sysadmin:12345
NSE: [ssh-brute] Trying username/password pair: netadmin:12345
NSE: [ssh-brute] Trying username/password pair: guest:12345
NSE: [ssh-brute] Trying username/password pair: user:12345
NSE: [ssh-brute] Trying username/password pair: web:12345
```



```
┌──(root💀kali)-[~]
└─# nmap -A -p 135,139,389,445,636,49152,49155,49157,49161 10.168.27.10
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-22 11:13 MST
Nmap scan report for 10.168.27.10
Host is up (0.00043s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
```



```
┌──(root💀kali)-[~]
└─# ssh -v root@10.168.27.14 -p 22                                                                    255 ×
OpenSSH_8.4p1 Debian-5, OpenSSL 1.1.1l  24 Aug 2021
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 10.168.27.14 [10.168.27.14] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: identity file /root/.ssh/id_dsa type -1
debug1: identity file /root/.ssh/id_dsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa type -1
debug1: identity file /root/.ssh/id_ecdsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa_sk type -1
debug1: identity file /root/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /root/.ssh/id_ed25519 type -1
debug1: identity file /root/.ssh/id_ed25519-cert type -1
debug1: identity file /root/.ssh/id_ed25519_sk type -1
debug1: identity file /root/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /root/.ssh/id_xmss type -1
debug1: identity file /root/.ssh/id_xmss-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.4p1 Debian-5
debug1: Remote protocol version 2.0, remote software version OpenSSH_5.5p1 Debian-6+squeeze5
debug1: match: OpenSSH_5.5p1 Debian-6+squeeze5 pat OpenSSH_5* compat 0×0c000002
debug1: Authenticating to 10.168.27.14:22 as 'root'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: diffie-hellman-group-exchange-sha256
debug1: kex: host key algorithm: ssh-rsa
debug1: kex: server→client cipher: aes128-ctr MAC: umac-64@openssh.com compression: none
debug1: kex: client→server cipher: aes128-ctr MAC: umac-64@openssh.com compression: none
debug1: SSH2_MSG_KEX_DH_GEX_REQUEST(2048<3072<8192) sent
debug1: got SSH2_MSG_KEX_DH_GEX_GROUP
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: got SSH2_MSG_KEX_DH_GEX_REPLY
```