Lab 3: Perform OS Discovery

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the open ports and services running on the target range of IP addresses is to perform OS discovery. Identifying the OS used on the target system allows you to assess the system’s vulnerabilities and the exploits that might work on the system to perform additional attacks.

Lab Objectives

- Perform OS discovery using Nmap Script Engine (NSE)

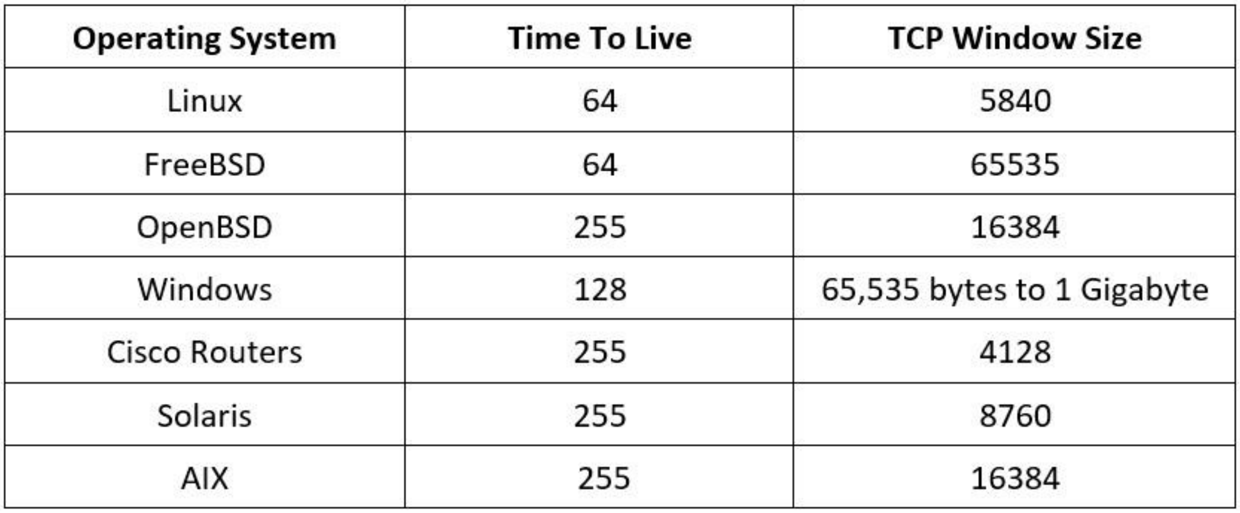
Overview of OS Discovery/ Banner Grabbing

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

There are two types of OS discovery or banner grabbing techniques:

- **Active Banner Grabbing** Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.
- **Passive Banner Grabbing** This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.



Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Task 1: Perform OS Discovery using Nmap Script Engine (NSE)

Nmap, along with Nmap Script Engine (NSE), can extract considerable valuable information from the target system. In addition to Nmap commands, NSE provides scripts that reveal all sorts of useful information from the target system. Using NSE, you may obtain information such as OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, system time of a target system, etc.

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

1. Click Parrot Security to switch to the **Parrot Security** machine and Login with **attacker**/**toor**.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

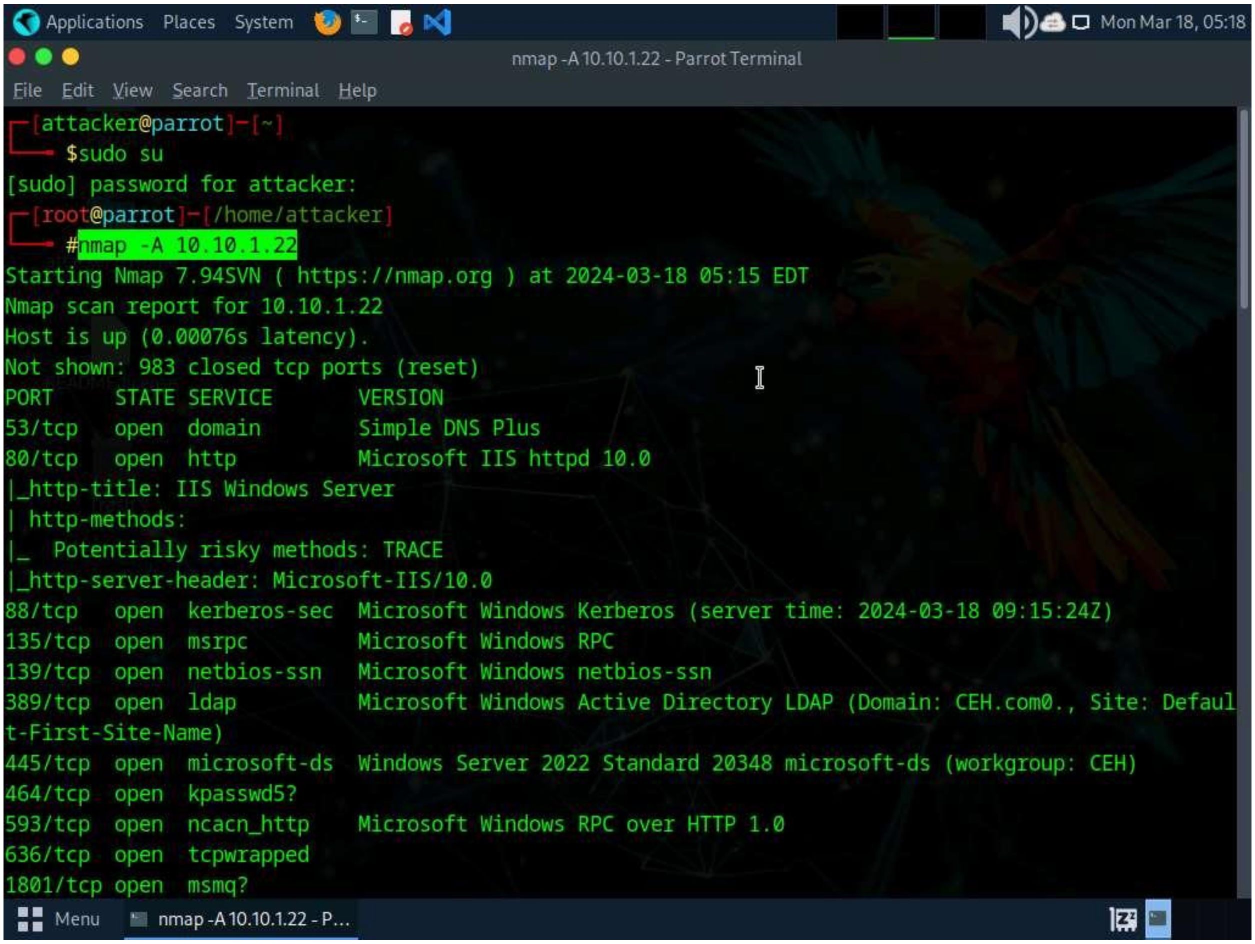
2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

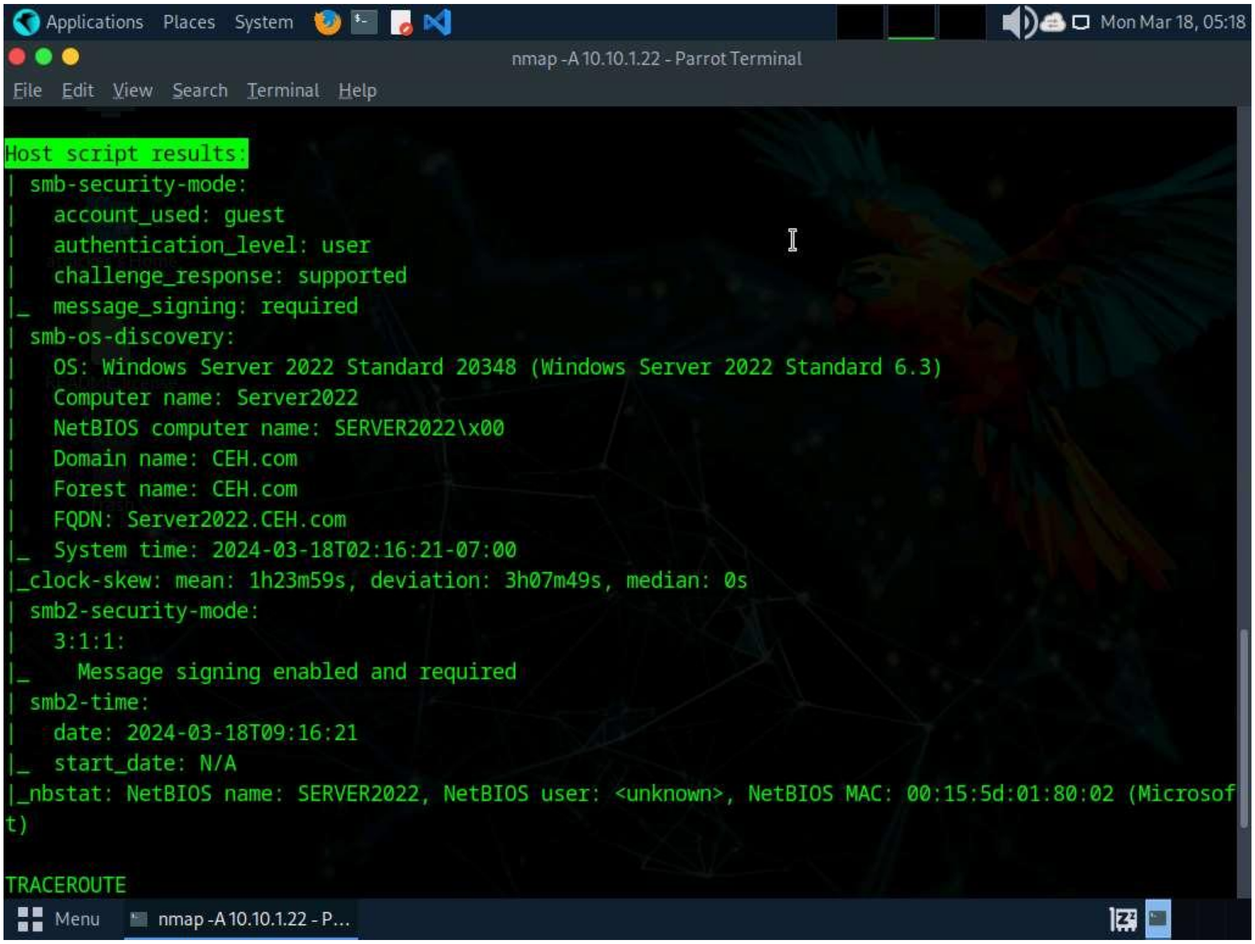
3. In the terminal window, run **nmap -A [Target IP Address]** command (here, the target machine is **Windows Server 2022** [**10.10.1.22**]). The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the **Host script results** section.

-A: to perform an aggressive scan.

The scan takes approximately 10 minutes to complete.



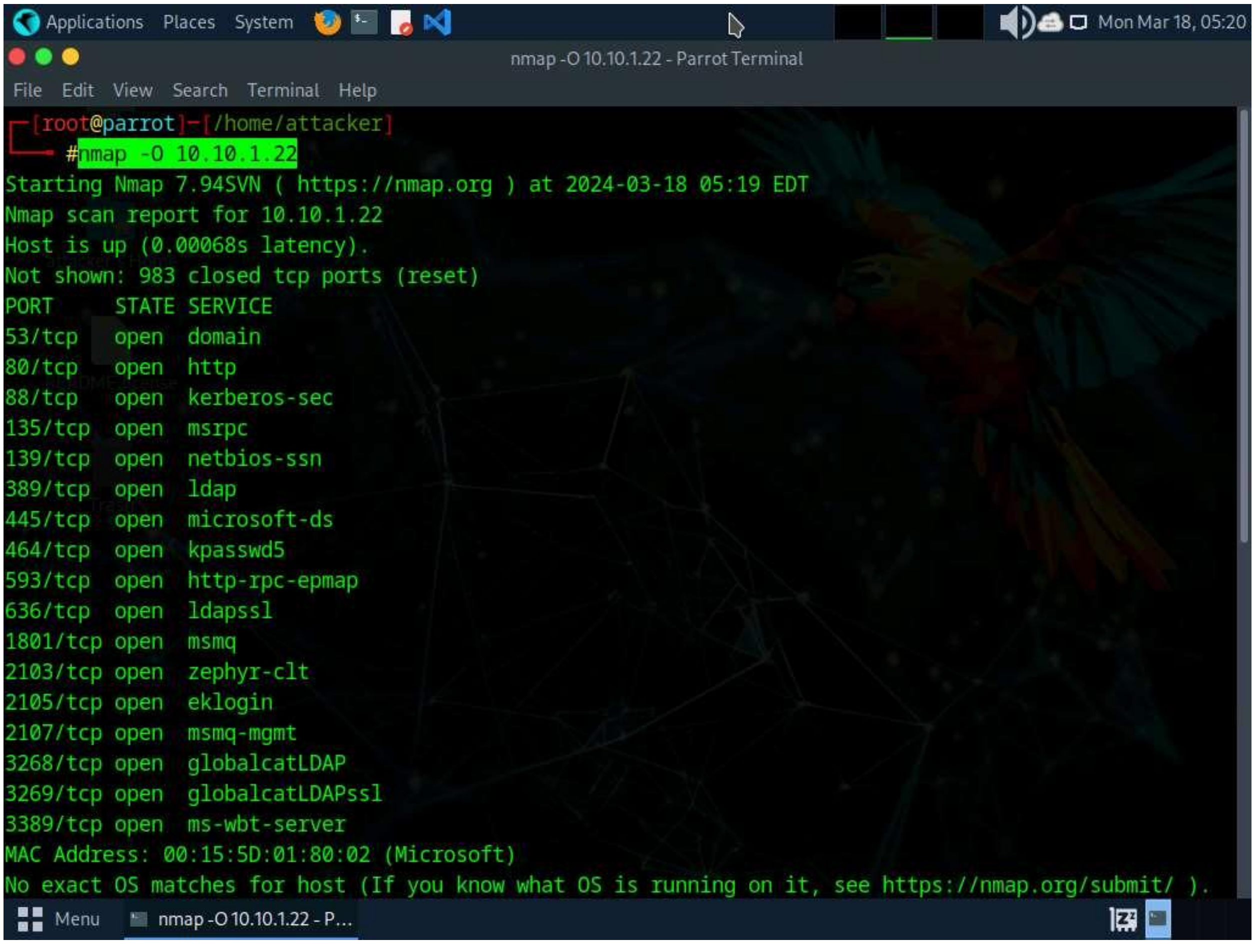
```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -A 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 05:15 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00076s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-03-18 09:15:24Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Defaul
t-First-Site-Name)
445/tcp  open  microsoft-ds  Windows Server 2022 Standard 20348 microsoft-ds (workgroup: CEH)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1801/tcp open  msmq?
```



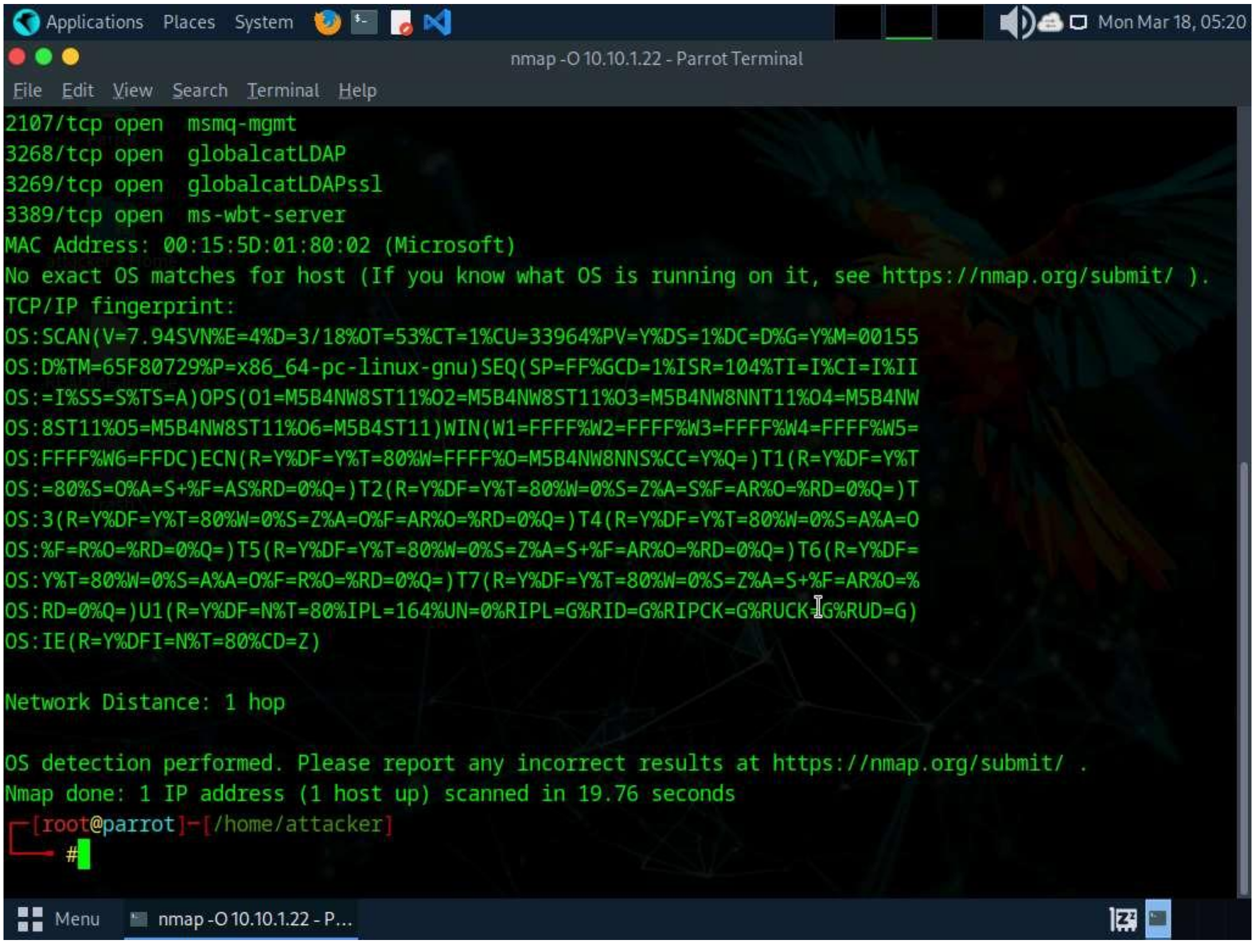
```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
|   Computer name: Server2022
|   NetBIOS computer name: SERVER2022\x00
|   Domain name: CEH.com
|   Forest name: CEH.com
|   FQDN: Server2022.CEH.com
|_  System time: 2024-03-18T02:16:21-07:00
|_clock-skew: mean: 1h23m59s, deviation: 3h07m49s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-03-18T09:16:21
|_  start_date: N/A
|_nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:02 (Microsof
t)

TRACEROUTE
```

4. In the terminal window, run **nmap -O [Target IP Address]** command (here, the target machine is **Windows Server 2022** [**10.10.1.22**]). The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.

-O: performs the OS discovery.



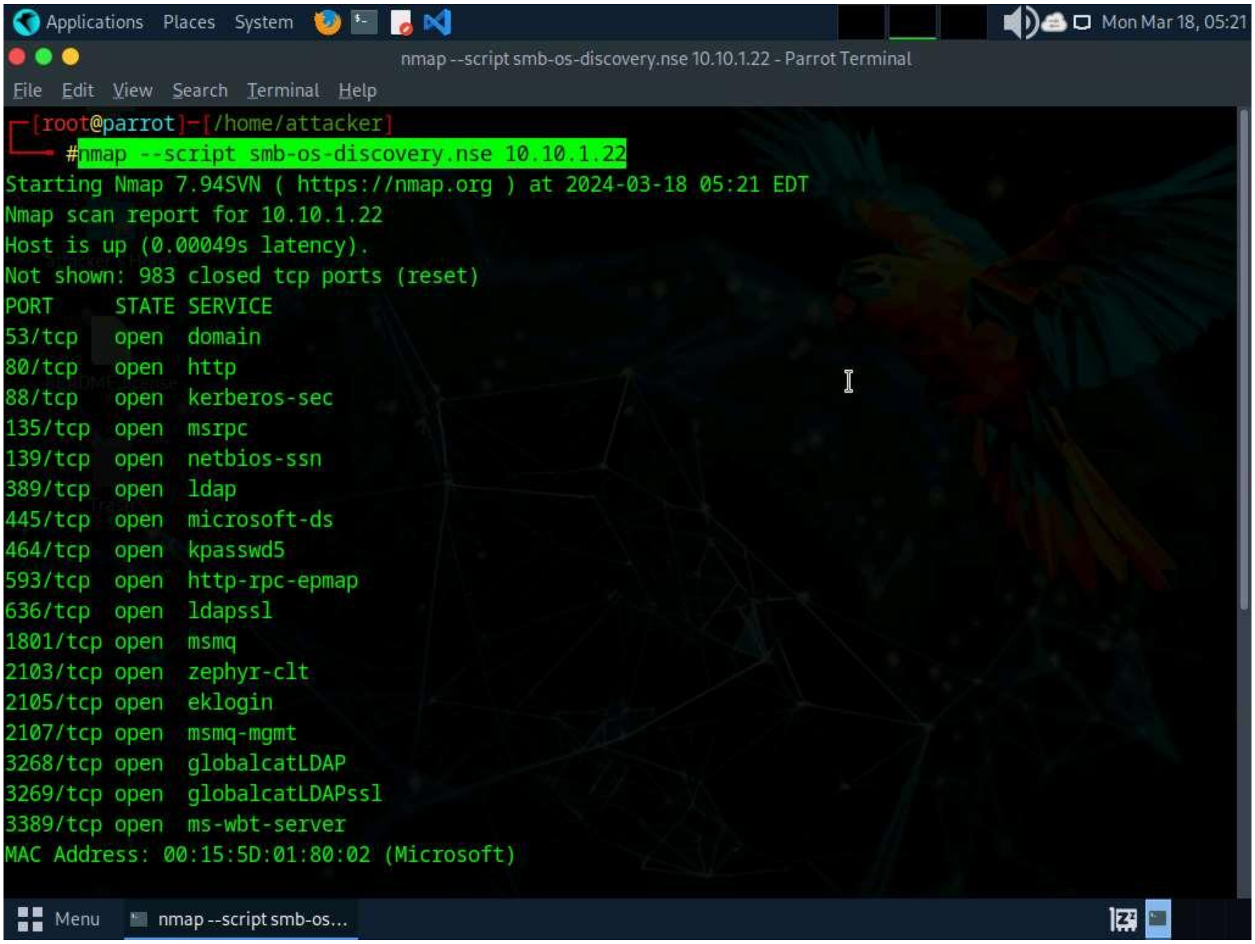
```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -O 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 05:19 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00068s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



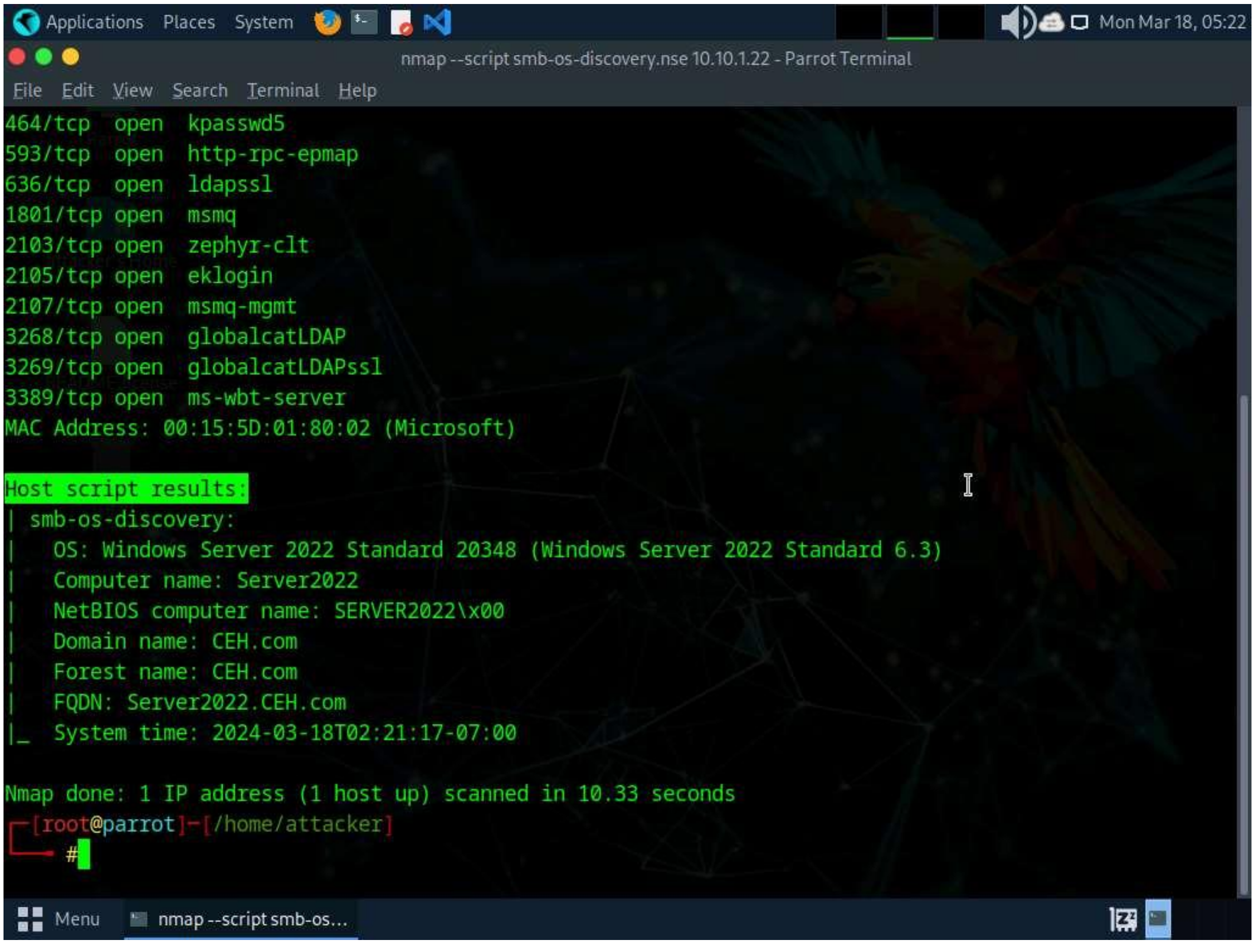
```
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/18%OT=53%CT=1%CU=33964%PV=Y%DS=1%DC=D%G=Y%M=00155
OS:D%TM=65F80729%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=104%TI=I%CI=I%II
OS:=I%SS=S%TS=A)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW
OS:8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=
OS:FFFF%W6=FFDC)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.76 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

5. In the terminal window, run **nmap --script smb-os-discovery.nse [Target IP Address]** command (here, the target machine is **Windows Server 2022** [**10.10.1.22**]). The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.

--script: specifies the customized script and **smb-os-discovery.nse**: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).


Applications Places System
Mon Mar 18, 05:21
nmap --script smb-os-discovery.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
Menu
nmap --script smb-os...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap --script smb-os-discovery.nse 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 05:21 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00049s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
```



Applications Places System
Mon Mar 18, 05:22
nmap --script smb-os-discovery.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
Menu
nmap --script smb-os...

```
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
|   Computer name: Server2022
|   NetBIOS computer name: SERVER2022\x00
|   Domain name: CEH.com
|   Forest name: CEH.com
|   FQDN: Server2022.CEH.com
|_  System time: 2024-03-18T02:21:17-07:00

Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

6. This concludes the demonstration of discovering the OS running on the target system using Nmap.

7. Close all open windows and document all the acquired information.

Question 3.3.1.1

Use Nmap Scripting Engine (NSE) to perform OS discovery and find the OS on the machine at the IP address 10.10.1.22.