Blog Alpha Rhob

February 15, 2023 ▪ Cyber Security / EC-Council (CEH) / English / Notes

CEH Practical – Engagement I Flag Hunting (1 – 20)

Posted by Roberto Alfaro

Those are the steps that I took to complete the flag-hunting session in the engagement module of the CEH Practical Laboratory

Flag 1

Perform vulnerability scanning for the webserver hosting movies.cehorg.com using OpenVAS and identify the severity level of RPC vulnerability.

Pentesting > Vulnerability Analysis > Openvas – Greenbone > Start Greenbone Vulnerability

Search

Search

Recent Posts

Writeups of HackTheBox's Machines {Irked}

Writeups of HackTheBox's Machines {Lame}

Solutions To HackTheBox's Machines {Bashed}

Solutions To HackTheBox's Machines {Magic}

Manager Service

Vulnerability	Severity	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	192.168.0.51	movies.cehorg.com	general/tcp	Tue, Jan 10, 2023 7:53 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.0.51	movies.cehorg.com	135/tcp	Tue, Jan 10, 2023 8:01 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.0.51	movies.cehorg.com	80/tcp	Tue, Jan 10, 2023 8:01 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.0.51	movies.cehorg.com	3389/tcp	Tue, Jan 10, 2023 8:01 PM UTC
Traceroute	0.0 (Log)	80 %	192.168.0.51	movies.cehorg.com	general/tcp	Tue, Jan 10, 2023 7:53 PM UTC
Services	0.0 (Log)	80 %	192.168.0.51	movies.cehorg.com	3389/tcp	Tue, Jan 10, 2023 7:53 PM UTC
Services	0.0 (Log)	80 %	192.168.0.51	movies.cehorg.com	47001/tcp	Tue, Jan 10, 2023 7:53 PM UTC
SMB/CIFS Server Detection	0.0 (Log)	80 %	192.168.0.51	movies.cehorg.com	139/tcp	Tue, Jan 10, 2023 7:56 PM UTC
Services	0.0 (Log)	80 %	192.168.0.51	movies.cehorg.com	25/tcp	Tue, Jan 10, 2023 7:53 PM UTC
SMB/CIFS Server Detection	0.0 (Log)	80 %	192.168.0.51	movies.cehorg.com	445/tcp	Tue, Jan 10, 2023 7:56 PM UTC

Greenbone's output

You can see that the RPC vulnerability has a score of 5

A: 5

Flag 2

Perform vulnerability scanning for the Linux host in the 172.16.0.0/24 network using OpenVAS and find the number of vulnerabilities with severity level as medium.

Linux IP: 172.16.0.11

Check for Chargen Service (TCP)	5.0 (Medium)	80 %	172.16.0.12	19/tcp	Tue, Jan 10, 2023 3:34 PM UTC
echo Service Reporting (TCP + UDP)	5.0 (Medium)	80 %	172.16.0.12	7/tcp	Tue, Jan 10, 2023 3:34 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.0.12	135/tcp	Tue, Jan 10, 2023 3:34 PM UTC
Check for Quote of the Day (qotd) Service (TCP)	5.0 (Medium)	80 %	172.16.0.12	17/tcp	Tue, Jan 10, 2023 3:34 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	172.16.0.2	80/tcp	Tue, Jan 10, 2023 3:31 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	172.16.0.12	21/tcp	Tue, Jan 10, 2023 3:31 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.0.12	3389/tcp	Tue, Jan 10, 2023 3:34 PM UTC

A: 0

Flag 3

Solutions To HackTheBox's Machines {Forgot}

Recent Comments

Aditya Jevlikar on CEH Practical – Scanning Network Flag Hunting (1 – 15)

Roberto Alfaro on CEH Practical – Scanning Network Flag Hunting (1 – 15)

Aditya Jevlikar on CEH Practical – Scanning Network Flag Hunting (1 – 15)

Roberto Alfaro on CEH Practical – Vulnerability Analysis Flag Hunting (1 – 14)

Nichole on CEH Practical – Vulnerability Analysis Flag Hunting (1 – 14)

Archives

You are performing reconnaissance for CEHORG and has been assigned a task to find out the physical location of one of their webservers hosting www.certifiedhacker.com. What are the GEO Coordinates of the webserver? Note: Provide answer as Latitude, Longitude.

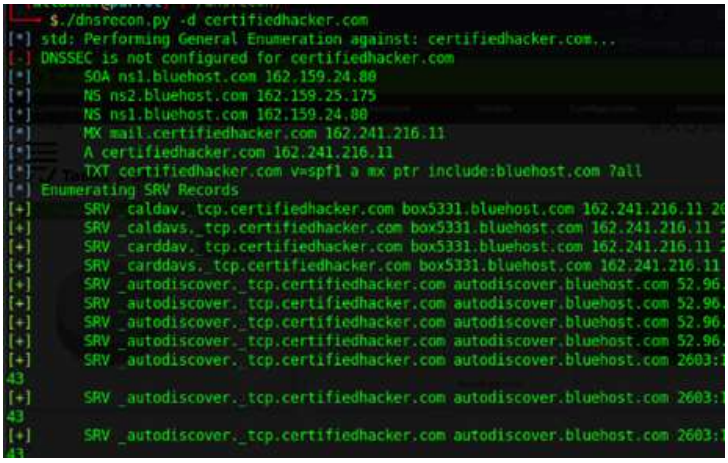
Go to: https://tools.keycdn.com/geo?host=162.241.216.11

A: 37.751, -97.822

Flag 4

Identify if the website www.certifiedhacker.com allows DNS zone transfer. (Yes/No)

- Term: cd dnsrecon
- Term: chmod +x ./dnsrecon.py
- Term: ./dnsrecon.py -d <target>
-



From module 02, Lab 7, Task 2. dnsrecon.py

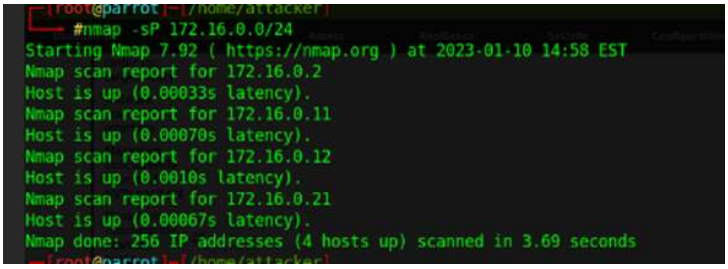
Categories

A: No

Flag 5

Identify the number of live machines in 172.16.0.0/24 subnet.

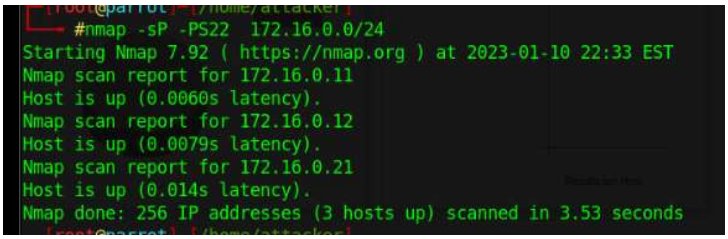
Try: nmap -sP 172.16.0.0/24



nmap's output

Here you are scanning even nodes, so to avoid "additional hosts" let's try another scan option.

Try: nmap -sP -PS22 172.16.0.0/24



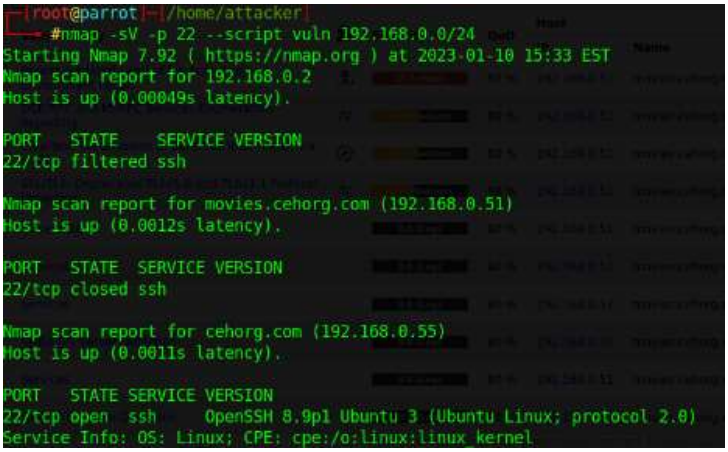
Try: nmap -PU 172.16.0.0/24

A: 3

Flag 6

While performing a security assessment against the CEHORG network, you came to know that one machine in the network is running OpenSSH and is vulnerable. Identify the version of the OpenSSH running on the machine. Note: Target network 192.168.0.0/24.

Try: nmap -sV -p 22 –script vuln 192.168.0.0/24



You can add **–open** at the end of the command

A: 8.9p1

Flag 7

During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database.

Try: nmap -T4 -A cehorg.com

```
#nmap -T4 -A cehorg.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 00:14 EST
Nmap scan report for cehorg.com (192.168.0.55)
Host is up (0.0061s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 28:52:84:53:60:ec:72:72:ce:80:ba:db:35:74:b5:55 (ECDSA)
|_  256 9a:1e:e9:21:07:9f:7c:25:95:c9:6a:b6:5e:fe:e4:51 (ED25519)
80/tcp open  http    Apache httpd 2.4.52
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/11%OT=22%CT=1%CU=32420%PV=Y%DS=2%DC=T%G=Y%TM=63BE45F
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=105%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Port 22 shows the detail, you can use -O too

A: Ubuntu

Flag 8

Find the IP address of the Domain Controller machine.

INFO: Domain controllers will show port 389 running the Microsoft Windows AD LDAP service

Try: nmap -T4 -A movies.cehorg.com

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 00:06 EST
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0024s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Microsoft ESMTP 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.10], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
 TURN ETRN BDAT VRFY
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Login - Movies
```

```
TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   7.17 ms 10.10.1.2
2   3.12 ms movies.cehorg.com (192.168.0.51)
```

Just to get some information, now let's scan another batch of IPs

Try: nmap -p389 -sV 10.10.10.0/24 –open

```
└──╼ #nmap -p389 -sV 10.10.10.0/24 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-12 23:10 EST
Nmap scan report for 10.10.10.25
Host is up (0.0015s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    Microsoft Windows Active Directory LDAP (Domain: CEHORG.co
m0., Site: Default-First-Site-Name)
Service Info: Host: ADMINDEPT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 10.90 seconds
```

A 10.10.10.25

Flag 9

Perform a host discovery scanning and identify the NetBIOS name of the host at 10.10.10.25.

Try: nmap -sV –script nbstat.nse 10.10.10.25

Try: nmap -T4 -A 10.10.10.25

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
|   Computer name: AdminDept
|   NetBIOS computer name: ADMINDEPT\x00
|   Domain name: CEHORG.com
|   Forest name: CEHORG.com
|   FQDN: AdminDept.CEHORG.com
|   System time: 2023-01-10T20:17:41-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled and required
| smb2-time:
|   date: 2023-01-11T04:17:40
|   start_date: N/A
|_clock-skew: mean: 8h36m01s, deviation: 3h34m42s, median: 7h00m00s
```

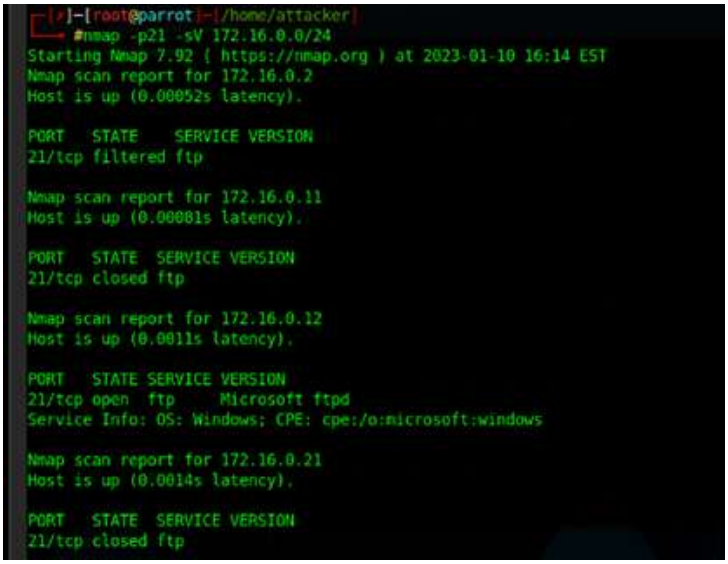
nmap's scan output

A: ADMINDEPT

Flag 10

Find the IP address of the machine which has port 21 open. Note: Target network 172.16.0.0/24

Try: nmap -p21 -sV 172.16.0.0/24



Previous command's output

You can try: **nmap -p21 -sV 172.16.0.0/24 –open**

A: 172.16.0.12

Flag 11

Perform an intense scan on 10.10.10.25 and find out the FQDN of the machine in the network.

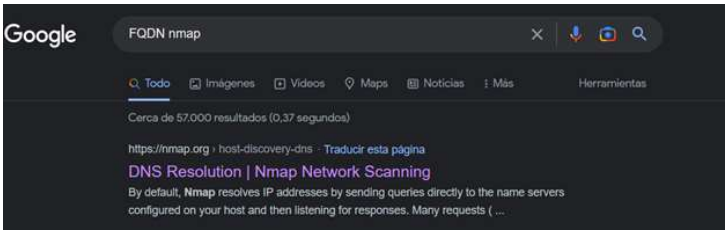
Try: nmap -T4 -A 10.10.10.25

```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
|   Computer name: AdminDept
|   NetBIOS computer name: ADMINDEPT\x00
|   Domain name: CEHORG.com
|   Forest name: CEHORG.com
|   FQDN: AdminDept.CEHORG.com
|_  System time: 2023-01-10T20:17:41-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
```

A: AdminDept.CEHORG.com

Flag 12

What is the DNS Computer Name of the Domain Controller?



Google search, are the same

A: AdminDept.CEHORG.com

Flag 13

Perform LDAP enumeration on the target network and find out how many user accounts are associated with the domain.

For LDAP Enumeration I suggest to use ldapsearch, is a lot more comfortable than the

search through nmap or the python script suggested by the documentation.

Try: nmap -p 389 –script ldap-brute –script-args ldap.base='"cn=AdminDept,dc=CEHORG,dc=com"' 10.10.10.25

```
└──╼ #nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=AdminDept,dc=
CEHORG,dc=com"' 10.10.10.25
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 23:13 EST
Nmap scan report for 10.10.10.25
Host is up (0.0012s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-brute:
|   cn=root,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=admin,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=administrator,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=webadmin,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=sysadmin,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=netadmin,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=guest,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=user,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|   cn=web,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials
|_  cn=test,cn=AdminDept,dc=CEHORG,dc=com:<empty> => Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

nmap's output, cn=user exist!

Try: ldapsearch -x -h 10.10.10.25 -b "dc=CEHORG,dc=com" "objectclass=user"

```
# search reference
ref: ldap://DomainDnsZones.CEHORG.com/DC=DomainDnsZones,DC=CEHORG,DC=com

# search reference
ref: ldap://ForestDnsZones.CEHORG.com/DC=ForestDnsZones,DC=CEHORG,DC=com

# search reference
ref: ldap://CEHORG.com/CN=Configuration,DC=CEHORG,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 13
# numEntries: 9
# numReferences: 3
┌──[root@parrot]─[/home/attacker]
└──╼ #
```

ldapsearch's output, does not show users

Try: ldapsearch -x -h 10.10.10.25 -b "dc=CEHORG,dc=com" "objectclass=user" cn=user

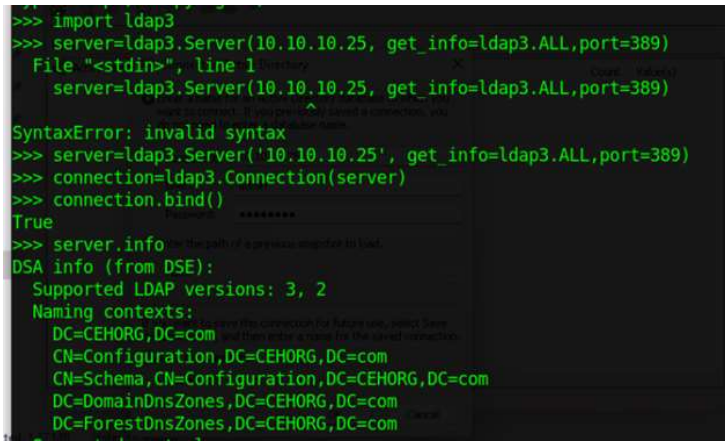
A: 8

Flag 14

Perform an LDAP Search on the Domain Controller machine and find out the version of the LDAP protocol.

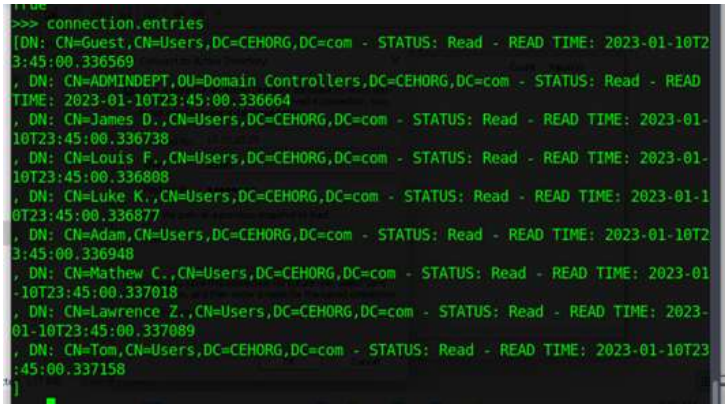
The following command **ldapsearch -x -h 10.10.10.25 -b "dc=CEHORG,dc=com" "objectclass=user"** shows the LDAP's protocol version too, but in this flag I will shows the step by using the Python Script

- Try: python3
- Py import ldap3
- Py server=ldap3.Server('10.10.10.25', get_info=ldap3.ALL,port=389)
- Py connection=ldap3.Connection(server)
- Py connection.bind()
- Py server.info



server.info's output, always use the highest supported version

- Py connection.search(search_base='DC=CEHORG,DC=com',search_filter='(&(objectclass=*))',search_scope='SUBTREE', attributes='*')
- Py connection.entries
- Py connection.search(search_base='DC=CEHORG,DC=com',search_filter='(&(objectclass=person))',search_scope='SUBTREE', attributes='userpassword')
- Py connection.entries



Final output

A: LDAPv3

Flag 15

What is the IP address of the machine that has NFS service enabled? Note: Target network 192.168.0.0/24.

Remember: NFS Service port = 2049

- Try: nmap -p 2049 192.168.0.0/24

```
#nmap -p 2049 192.168.0.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 23:47 EST
Nmap scan report for 192.168.0.2
Host is up (0.00046s latency).

PORT     STATE    SERVICE
2049/tcp filtered nfs

Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0013s latency).

PORT     STATE SERVICE
2049/tcp open  nfs

Nmap scan report for cehorg.com (192.168.0.55)
Host is up (0.0011s latency).

PORT     STATE  SERVICE
2049/tcp closed nfs
```

command's output, it is noisy

- Try: nmap -p 2049 192.168.0.0/24 –open

```
#nmap -p 2049 192.168.0.0/24 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 23:48 EST
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0013s latency).

PORT     STATE SERVICE
2049/tcp open  nfs

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.11 seconds
```

nmap output with –open

A: 192.168.0.51

Flag 16

Perform a DNS enumeration on www.certifiedhacker.com and find out the name servers used by the domain.

- Try: nmap –script=broadcast-dns-service-discovery www.certifiedhacker.com

```
└──╼ #nmap --script=broadcast-dns-service-discovery www.certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 23:50 EST
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.10s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 984 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
5432/tcp open  postgresql
```

First I tried to use nmap, but it was now precise and did not shows the answer, so I decided to use another command.

- Try: dig ns www.certifiedhacker.com

```
└──╼ #dig ns www.certifiedhacker.com

; <<>> DiG 9.16.22-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40438
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.     21600  IN      NS      ns1.bluehost.com.
certifiedhacker.com.     21600  IN      NS      ns2.bluehost.com.

;; Query time: 128 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jan 10 23:55:11 EST 2023
;; MSG SIZE  rcvd: 111
```

dig ns's output, check on ANSWER SECTION

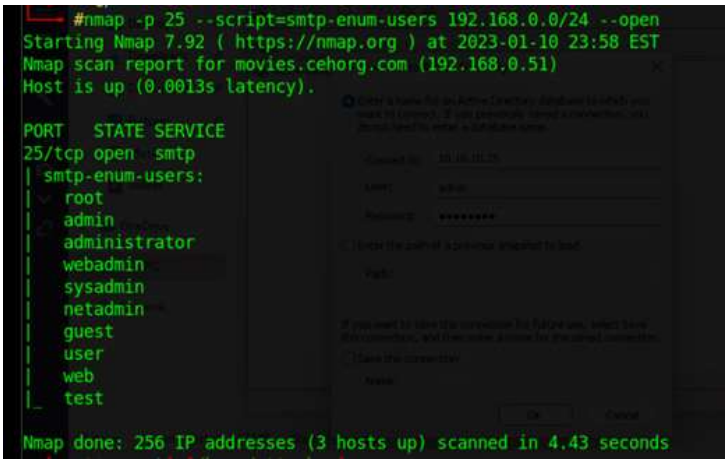
A: ns1.bluehost.com, ns2.bluehost.com

Flag 17

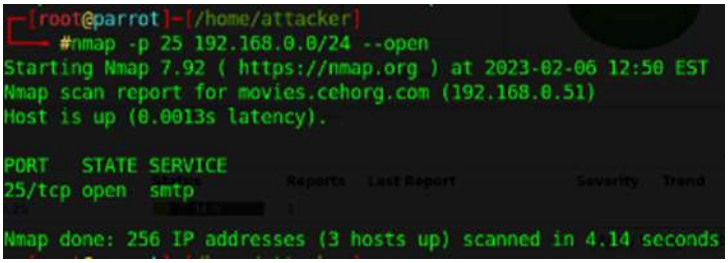
Find the IP address of the machine running SMTP service on the 192.168.0.0/24 network.

Remember: SMTP Service port is 25

- Try: nmap -p 25 –script=smtp-enum-users 192.168.0.0/24 –open



- Try: nmap -p 25 192.168.0.0/24 –open



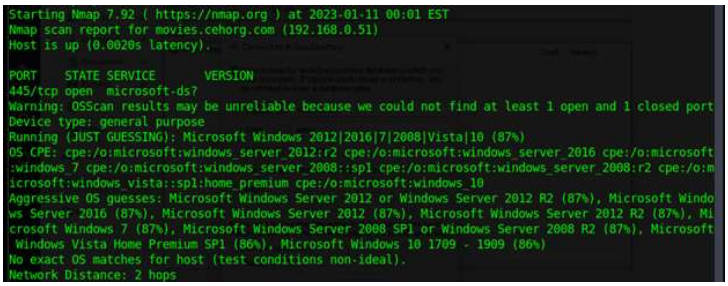
A: 192.168.0.51

Flag 18

Perform an SMB Enumeration on 192.168.0.51 and check whether the Message signing feature is enabled or disabled. Give your response as Yes/No.

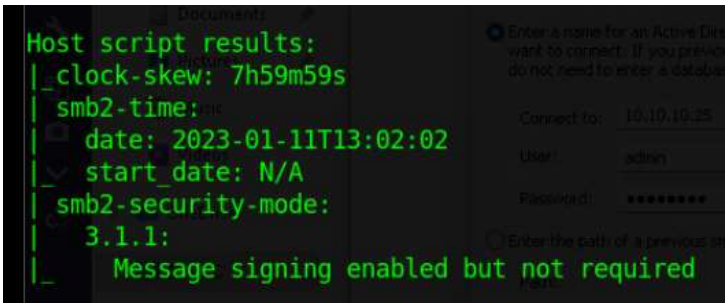
SMB Port: 445

- Try: nmap -p 445 -A 192.168.0.51



```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 00:01 EST
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0020s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016|7|2008|Vista|10 (87%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft
:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_vista::sp1:home_premium cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (87%), Microsoft Windo
ws Server 2016 (87%), Microsoft Windows Server 2012 (87%), Microsoft Windows Server 2012 R2 (87%), Mi
crosoft Windows 7 (87%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (87%), Microsoft
 Windows Vista Home Premium SP1 (86%), Microsoft Windows 10 1709 - 1909 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```



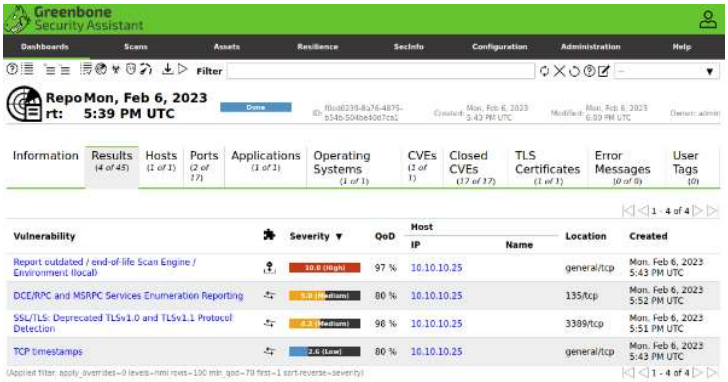
```
Host script results:
|_clock-skew: 7h59m59s
| smb2-time:
|   date: 2023-01-11T13:02:02
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
```

A: Yes

Flag 19

Perform vulnerability scanning for the domain controller using OpenVAS and identify the number of vulnerabilities with severity level as “medium”.

Using Greenbone, scan the IP 10.10.10.25 and watch the result



A: 2

Flag 20

Perform a vulnerability research on CVE-2022-30171 and find out the base score and impact of the vulnerability.

Google: CVE-2022-30171

https://nvd.nist.gov/vuln/detail/cve-2022-30171

A: 5.5 Medium

« Previous Post
CEH Practical – Vulnerability Analysis Flag Hunting (1 – 14)

Next Post »
Solutions to HackTheBox's Machines {Jarvis}

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

WordPress Theme: Maxwell by ThemeZee.