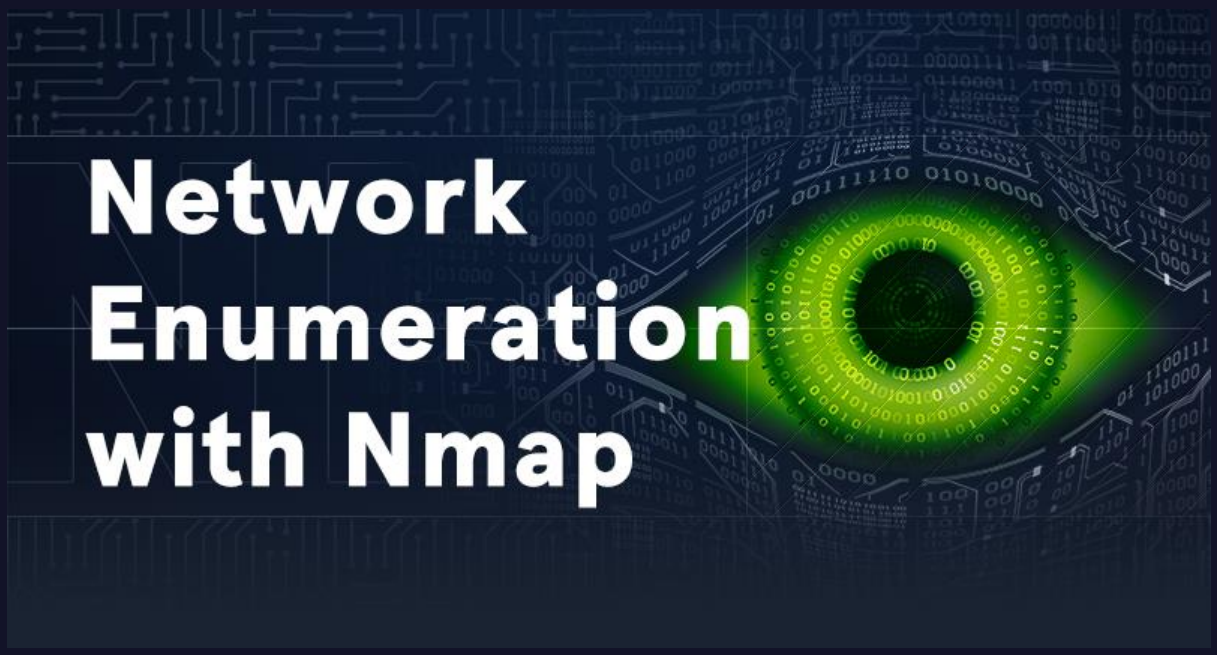
HACKTHEBOX



Tier I Easy Offensive

Nmap is one of the most used networking mapping and discovery tools because of its accurate results and efficiency. The tool is widely used by both offensive and defensive security practitioners. This module covers fundamentals that will be needed to use the Nmap tool for performing effective network enumeration.

By Saezel

Last Updated: 17 October 2024

Host Discovery

Based on the last result, find out which operating system it belongs to. Submit the name of the operating system as result.

Answer: windows

Host And Port Scanning

Find all TCP ports on your target. Submit the total number of found TCP ports as the answer.

Answer: 7

```
$ nmap -sS 10.129.112.20

    Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 00:42 EDT
    Nmap scan report for 10.129.112.20
    Host is up (0.53s latency).
    Not shown: 993 closed tcp ports (reset)

    PORT      STATE SERVICE
    22/tcp    open  ssh
    80/tcp    open  http
    110/tcp   open  pop3
    139/tcp   open  netbios-ssn
    143/tcp   open  imap
    445/tcp   open  microsoft-ds
    31337/tcp open  Elite

    Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
```

Enumerate the hostname of your target and submit it as the answer. (case-sensitive)

Answer: nix-nmap-default

Perform a full TCP port scan on your target and create an HTML report. Submit the number of the highest port as the answer.

Answer: 31337

Enumerate all ports and their services. One of the services contains the flag you have to submit as the answer.

Answer: HTB{pr0F7pDv3r510nb4nn3r}

```
$ nmap -sS -sV -sC -O --osscan-limit 10.129.112.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 00:50 EDT
Nmap scan report for 10.129.112.20
Host is up (0.50s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71:c1:89:90:7f:fd:4f:60:e0:54:f3:85:e6:35:6c:2b (RSA)
|   256 e1:8e:53:18:42:af:2a:de:c0:12:1e:2e:54:06:4f:70 (ECDSA)
|_  256 1a:cc:ac:d4:94:5c:d6:1d:71:e7:39:de:14:27:3c:3c (ED25519)
80/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
110/tcp  open  pop3        Dovecot pop3d
|_pop3-capabilities: UIDL RESP-CODES TOP CAPA AUTH-RESP-CODE SASL PIPELINING
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: LITERAL+ ID more post-login ENABLE have IDLE listed capabilities LOGINDISABLEDA0001 IMAP4rev1
LOGIN-REFERRALS Pre-login OK SASL-IR
445/tcp  open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
31337/tcp open  Elite?
| fingerprint-strings:
|   GetRequest, SIPOptions:
|_    220 HTB{pr0F7pDv3r510nb4nn3r}
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31337-TCP:V=7.94SVN%I=7%D=10/17%Time=671097B5%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,1F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n")%r(SIPOptions,1
SF:F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n");
Aggressive OS guesses: Linux 4.15 - 5.8 (95%), Linux 5.0 - 5.5 (95%), Linux 5.4 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux
5.3 - 5.4 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.32 (94%), HP P2000 G3 NAS device
(94%), ASUS RT-N56U WAP (Linux 3.4) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: NIX-NMAP-DEFAUL, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-10-17T04:54:46
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: nix-nmap-default
|   NetBIOS computer name: NIX-NMAP-DEFAULT\x00
|   Domain name: \x00
|   FQDN: nix-nmap-default
|_  System time: 2024-10-17T06:54:46+02:00
|_clock-skew: mean: -39m58s, deviation: 1h09m14s, median: 0s

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 278.62 seconds
```

NMap Scripting Engine

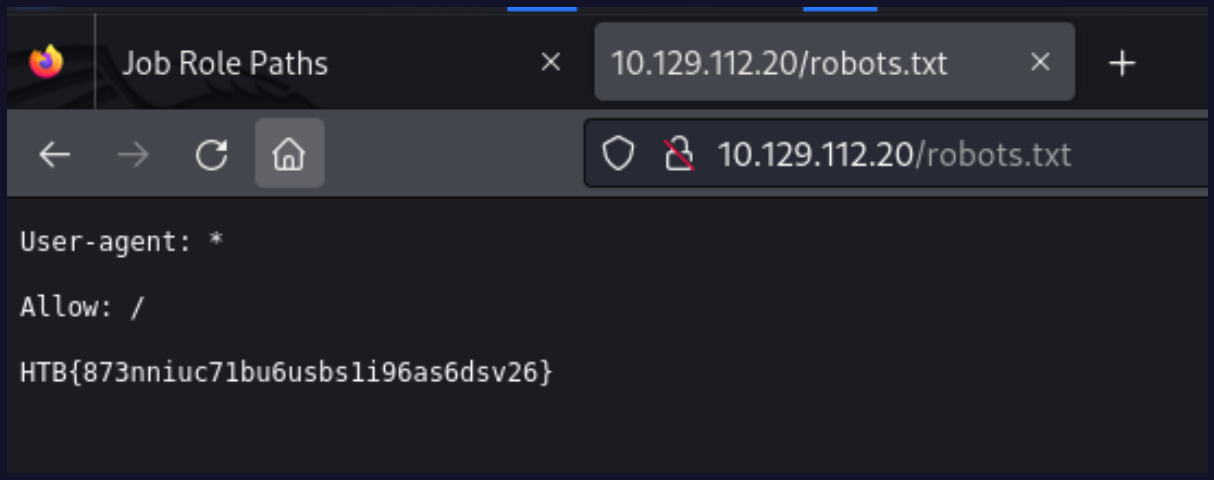
Use NSE and its scripts to find the flag that one of the services contain and submit it as the answer.

Answer: HTB{873nniuc71bu6usbs1i96as6dsv26}

```
$ sudo nmap 10.129.112.20 -p 80 --script=http-enum
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 01:29 EDT
        Nmap scan report for 10.129.112.20
        Host is up (1.7s latency).

        PORT   STATE SERVICE
        80/tcp open  http
        | http-enum:
        |_  /robots.txt: Robots file

        Nmap done: 1 IP address (1 host up) scanned in 108.61 seconds
```



Firewall and IDS/IPS Evasion - Easy Lab

Our client wants to know if we can identify which operating system their provided machine is running on. Submit the OS name as the answer.

Answer: Ubuntu

```
$ nmap -sS -A 10.129.70.133
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 01:49 EDT
        Nmap scan report for 10.129.70.133
        Host is up (0.34s latency).
        Not shown: 993 closed tcp ports (reset)
        PORT     STATE SERVICE     VERSION
        22/tcp   open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
        | ssh-hostkey:
        |   2048 71:c1:89:90:7f:fd:4f:60:e0:54:f3:85:e6:35:6c:2b (RSA)
        |   256 e1:8e:53:18:42:af:2a:de:c0:12:1e:2e:54:06:4f:70 (ECDSA)
        |_  256 1a:cc:ac:d4:94:5c:d6:1d:71:e7:39:de:14:27:3c:3c (ED25519)
        80/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
        |_http-title: Apache2 Ubuntu Default Page: It works
        |_http-server-header: Apache/2.4.29 (Ubuntu)
        110/tcp  open  pop3        Dovecot pop3d
        |_pop3-capabilities: UIDL CAPA TOP SASL RESP-CODES PIPELINING AUTH-RESP-CODE
        139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
        143/tcp  open  imap        Dovecot imapd (Ubuntu)
        |_imap-capabilities: IMAP4rev1 LITERAL+ more post-login have listed LOGINDISABLEDA0001 Pre-login OK IDLE LOGIN-
        REFERRALS ENABLE SASL-IR capabilities ID
        445/tcp  open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
        10001/tcp open  scp-config?
        Aggressive OS guesses: Linux 4.15 - 5.8 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1
        (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%),
        Linux 3.16 (93%), Linux 5.0 - 5.4 (93%)
        No exact OS matches for host (test conditions non-ideal).
        Network Distance: 2 hops
        Service Info: Host: NIX-NMAP-EASY; OS: Linux; CPE: cpe:/o:linux:linux_kernel

        Host script results:
        | smb2-time:
        |   date: 2024-10-17T05:52:46
        |_  start_date: N/A
        | smb-os-discovery:
        |   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
        |   Computer name: nix-nmap-easy
        |   NetBIOS computer name: NIX-NMAP-EASY\x00
        |   Domain name: \x00
        |   FQDN: nix-nmap-easy
        |_  System time: 2024-10-17T07:52:46+02:00
        | smb-security-mode:
        |   account_used: guest
        |   authentication_level: user
        |   challenge_response: supported
        |_  message_signing: disabled (dangerous, but default)
        |_clock-skew: mean: -39m58s, deviation: 1h09m14s, median: 0s
        |_nbstat: NetBIOS name: NIX-NMAP-EASY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
        | smb2-security-mode:
        |   3:1:1:
        |_    Message signing enabled but not required

        TRACEROUTE (using port 554/tcp)
        HOP RTT      ADDRESS
        1   245.17 ms 10.10.16.1
        2   497.92 ms 10.129.70.133
```

Firewall and IDS/IPS Evasion - Medium Lab

After the configurations are transferred to the system, our client wants to know if it is possible to find out our target's DNS server version. Submit the DNS server version of the target as the answer.

Answer: HTB{GoTtgUnyze9Psw4vGjcuMpHRp}

```
$ sudo nmap 10.129.69.230 -p53 -sUV
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 01:45 CDT
        Nmap scan report for 10.129.69.230
        Host is up (0.24s latency).

        PORT   STATE SERVICE VERSION
        53/udp open  domain  (unknown banner: HTB{GoTtgUnyze9Psw4vGjcuMpHRp})
```

Apparently, you won't get the answer on VPN

Pwnbox

```
┌[us-academy-6]-[10.10.14.91]-[htb-ac-1435902@htb-7zqwikvjel]-[~]
└─[★]$ sudo nmap 10.129.69.230 -p53 -sUV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 01:45 CDT
Nmap scan report for 10.129.69.230
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
53/udp open  domain  (unknown banner: HTB{G                              p})
1 service unrecognized despite returning data. If you know the service/ve
```

VPN

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.129.69.230 -p53 -sUV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 02:45 EDT
Nmap scan report for 10.129.69.230
Host is up (0.27s latency).

PORT   STATE SERVICE VERSION
53/udp open  domain  NLnet Labs NSD
```

Firewall and IDS/IPS Evasion - Hard Lab

Now our client wants to know if it is possible to find out the version of the running services. Identify the version of service our client was talking about and submit the flag as the answer

Answer: HTB{kjnsdf2n982n1827eh76238s98di1w6}

```
$sudo nmap -p- -sSV 10.129.69.193
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 02:57 EDT
        Stats: 0:12:50 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
        UDP Scan Timing: About 74.76% done; ETC: 03:14 (0:04:18 remaining)
        Nmap scan report for 10.129.69.193
        Host is up (0.71s latency).
        Not shown: 997 closed udp ports (port-unreach), 993 closed tcp ports (reset)

        PORT      STATE         SERVICE      VERSION
        22/tcp    open          ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
        80/tcp    open          http         Apache httpd 2.4.29 ((Ubuntu))
        110/tcp   open          pop3         Dovecot pop3d
        139/tcp   open          netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
        143/tcp   open          imap         Dovecot imapd (Ubuntu)
        445/tcp   open          netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
        50000/tcp filtered      ibm-db2
        Service Info: Host: NIX-NMAP-HARD; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 354.94 seconds
```

**Hint given practically tells us 50000 is the added port

```
$ sudo nmap -p50000 10.129.69.193 -sS -Pn -n --disable-arp-ping --source-port 53
        Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 03:47 EDT
        SENT (0.0333s) TCP 10.10.16.16:53 > 10.129.69.193:50000 S ttl=38 id=58758 iplen=44  seq=2966784027
        win=1024 <mss 1460>
        RCVD (0.2804s) TCP 10.129.69.193:50000 > 10.10.16.16:53 SA ttl=63 id=0 iplen=44  seq=1224368471
        win=64240 <mss 1338>
        Nmap scan report for 10.129.69.193
        Host is up (0.25s latency).

        PORT      STATE    SERVICE
        50000/tcp open     ibm-db2

        Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

**The firewall accepts TCP port 53

```
$ ncat -nv --source-port 53 10.129.69.193 50000
        Ncat: Version 7.94SVN ( https://nmap.org/ncat )
        Ncat: Connected to 10.129.69.193:50000.
        220 HTB{kjnsdf2n982n1827eh76238s98di1w6}
```