

## Introduction

This report presents an overview of Network Enumeration using Nmap, a critical tool in network security. It details Nmap's functionality in discovering and auditing network vulnerabilities, emphasizing its role in host discovery, service enumeration, and evasion tactics against firewalls and IDS/IPS. The report highlights Nmap's diverse scanning techniques, scriptable capabilities via the Nmap Scripting Engine, and practical applications in real-world security scenarios.

<https://academy.hackthebox.com/achievement/949661/19>

## 1. Enumeration

Enumeration is a critical phase in network security, focusing on collecting as much information as possible about target systems. It involves interacting with services to understand their behavior and potential vulnerabilities. The goal is to find attack vectors through detailed information gathering.

### Key Concepts

- Tools are aids, but knowledge and attention to detail are crucial.
- Understanding service syntax and protocols is essential.
- Manual enumeration is vital as tools can't always bypass security measures.

## 2. Introduction to Nmap

Nmap, or Network Mapper, is a versatile tool used for network discovery and security auditing. It's capable of identifying hosts, services, operating systems, and vulnerabilities in a network.

### Use Cases

- Security auditing
- Penetration testing
- Network mapping

### Key Features

- Various scanning techniques, including host discovery, port scanning, and OS detection.
- Scriptable interactions using the Nmap Scripting Engine.

## 3. Host Discovery

Determining which systems are online within a network is crucial for internal penetration tests. Nmap provides several methods for host discovery.

### Techniques

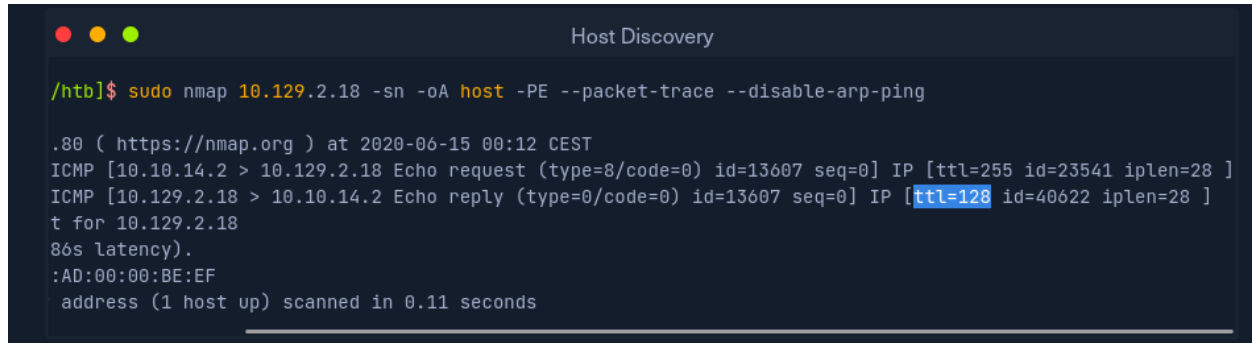
- ICMP echo requests
- Scanning network ranges and IP lists

- Options for stealth and evasion

Question:

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

**A: WINDOWS**



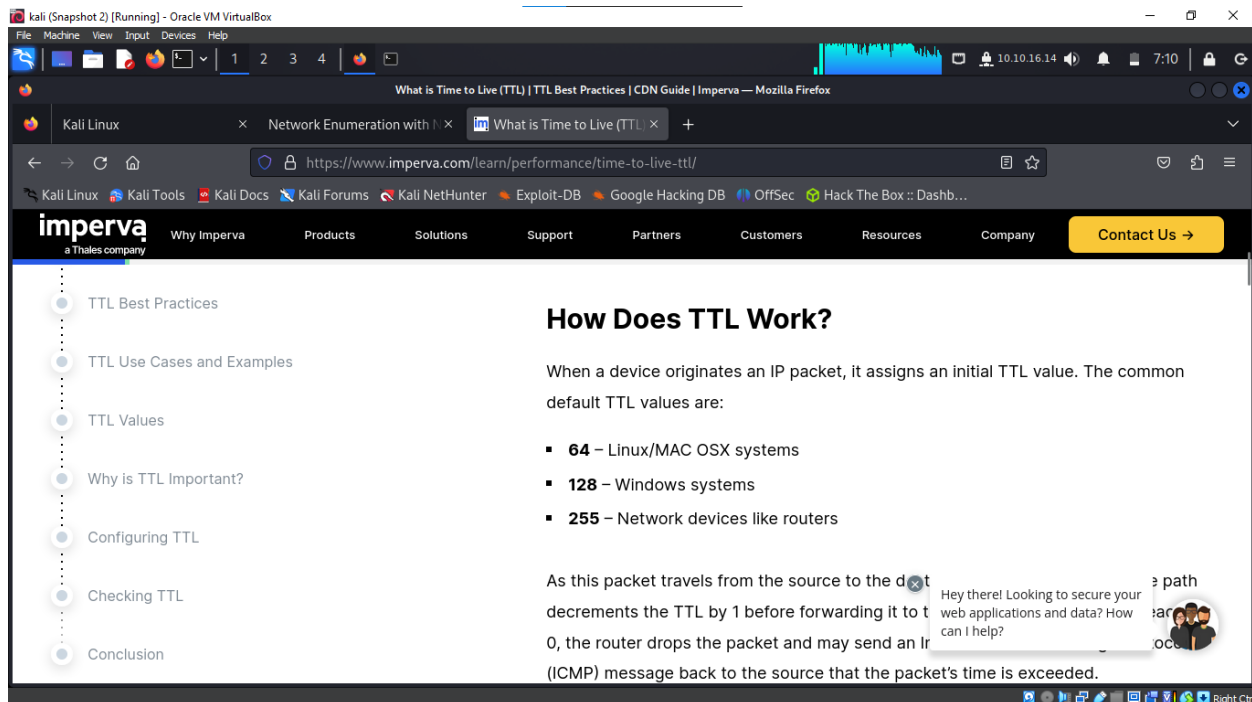
```

Host Discovery

/htb]$ sudo nmap 10.129.2.18 -sn -oA host -PE --packet-trace --disable-arp-ping

.80 ( https://nmap.org ) at 2020-06-15 00:12 CEST
ICMP [10.10.14.2 > 10.129.2.18 Echo request (type=8/code=0) id=13607 seq=0] IP [ttl=255 id=23541 iplen=28 ]
ICMP [10.129.2.18 > 10.10.14.2 Echo reply (type=0/code=0) id=13607 seq=0] IP [ttl=128 id=40622 iplen=28 ]
t for 10.129.2.18
86s latency).
:AD:00:00:BE:EF
address (1 host up) scanned in 0.11 seconds
  
```

Windows operating system have a TTL of 128



## 4. Host and Port Scanning

Host and Port Scanning with Nmap is crucial for gaining a deeper understanding of a target system's network interface. This process involves identifying open ports and the services running on them, their versions, and the operating system of the target.

### Key Aspects

- Nmap can detect six different states of a scanned port: open, closed, filtered, unfiltered, open|filtered, and closed|filtered.
- Default scans typically involve the top 1000 TCP ports using SYN scan (-sS).
- TCP Connect Scan (-sT) and UDP scans (-sU) are used for more detailed analysis.

- Version scans (-sV) provide information on service versions.

## Techniques and Tools

- Packet tracing to understand the interaction between Nmap and the target.
- Analyzing different TCP flags and responses to deduce port states.
- Utilizing Nmap's scripting capabilities for more detailed service information.

## Practical Implications

- Understanding the state of network ports helps in assessing the security posture of a target system.
- Detecting service versions allows for a targeted approach in vulnerability exploitation.

## Additional Resources

- Nmap's official documentation offers extensive information on port scanning techniques: [Nmap Port Scanning Techniques](https://nmap.org/docs/nmap-port-scanning-techniques/)

## Questions:

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

A: 7

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
(kali@kali)~$ sudo nmap -sS 10.129.111.253
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 07:34 EAT
Nmap scan report for 10.129.111.253
Host is up (0.22s 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 26.08 seconds
(kali@kali)~$ sudo nmap -sS 10.129.111.253 | wc
  14   63  419
(kali@kali)~$

```

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

A: NIX-NMAP-DEFAULT

```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
143/tcp open imap
445/tcp open microsoft-ds
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 26.08 seconds
(kali@kali)-[~]
$ sudo nmap -sS 10.129.111.253 | wc
  14    63    419
(kali@kali)-[~]
$ sudo nmap -sS -sV 10.129.111.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 07:40 EAT
Nmap scan report for 10.129.111.253
Host is up (0.24s 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)
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)
31337/tcp open  Elite?
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=2/4%Time=65BF1547XP=x86_64-pc-linux-gnu%r
SF:(GetRequest,1F,"220\x20HTB[pr0F7pDv3r510nb4nn3r]\r\n");
Service Info: Host: NIX-NMAP-DEFAULT; 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 186.60 seconds
(kali@kali)-[~]
$
```

## 5. Saving the Results

Nmap can save scan results in multiple formats for later analysis and comparison.

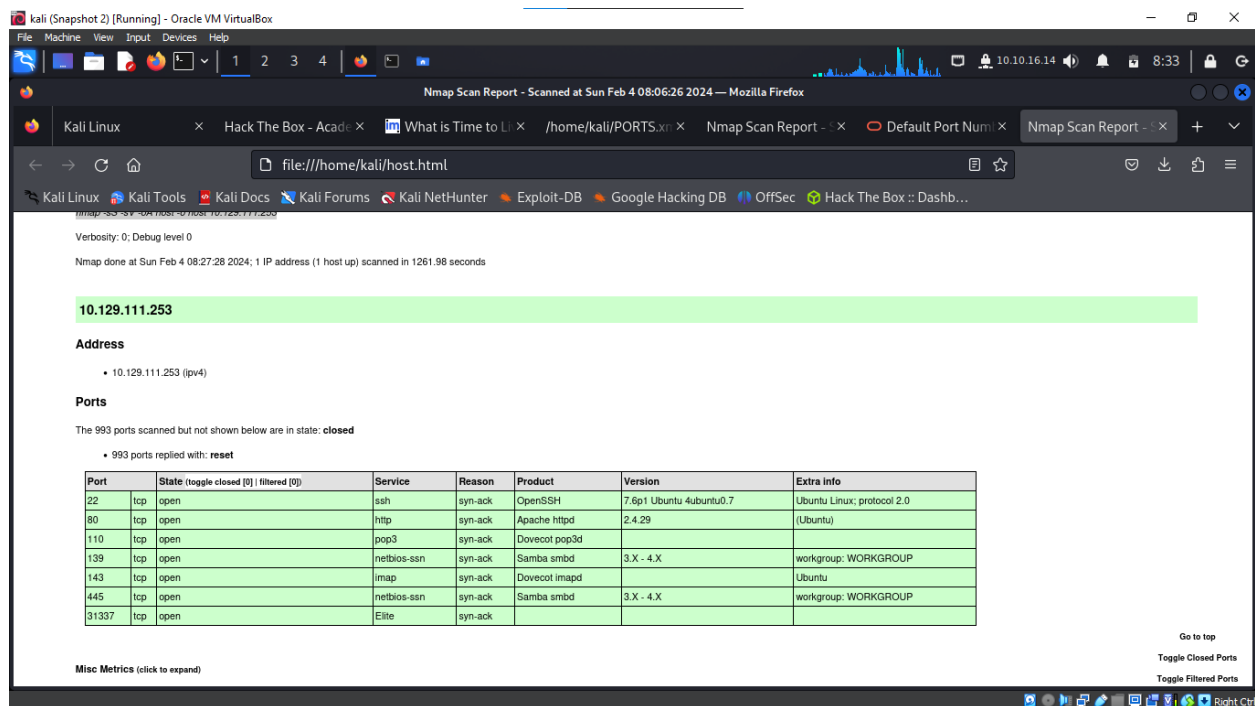
Formats

- Normal output (.Nmap)
- Grepable output (.gnmap)
- XML output (.xml)
- Conversion to HTML for easy reading

### Questions:

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

A: 31337



## 6. Service Enumeration

Identifying the exact service and its version on a target machine helps in finding precise exploits and vulnerabilities.

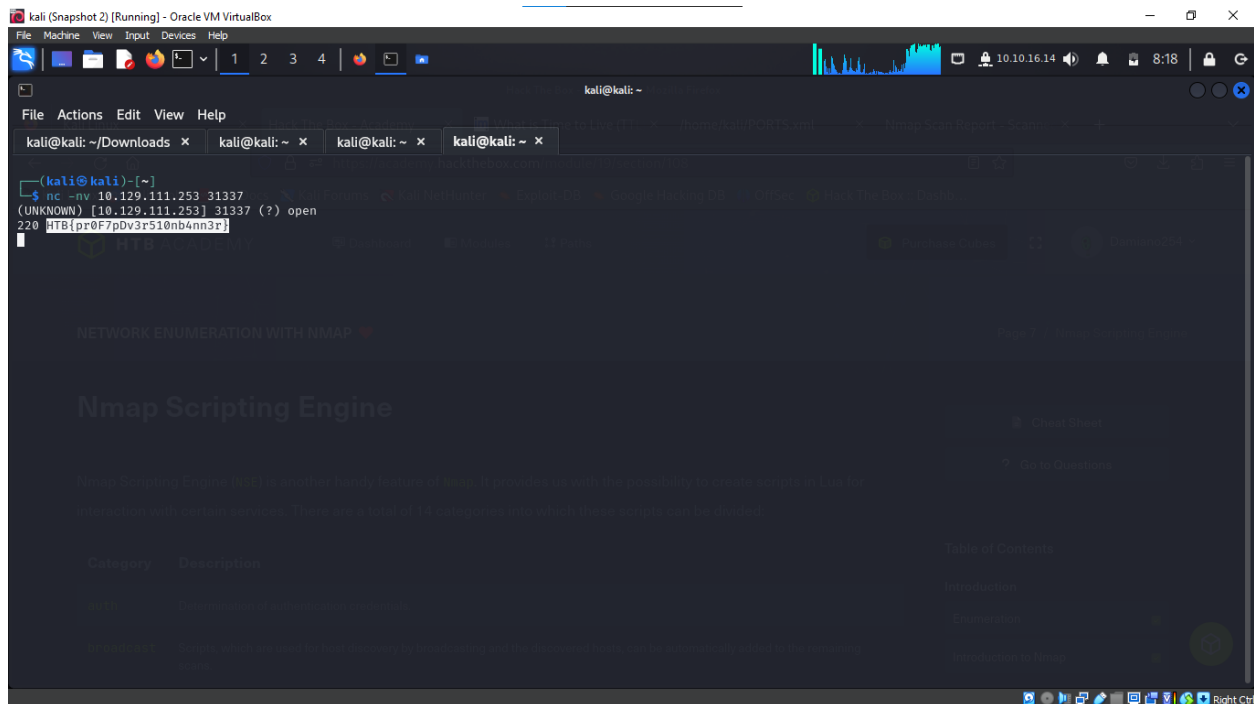
Techniques

- Quick port scans for an overview
- Service version detection
- Banner grabbing for additional information

## Questions

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

A: HTB{pr0F7pDv3r510nb4nn3r}



## 7. Nmap Scripting Engine (NSE)

NSE allows for more advanced and targeted scanning using scripts.

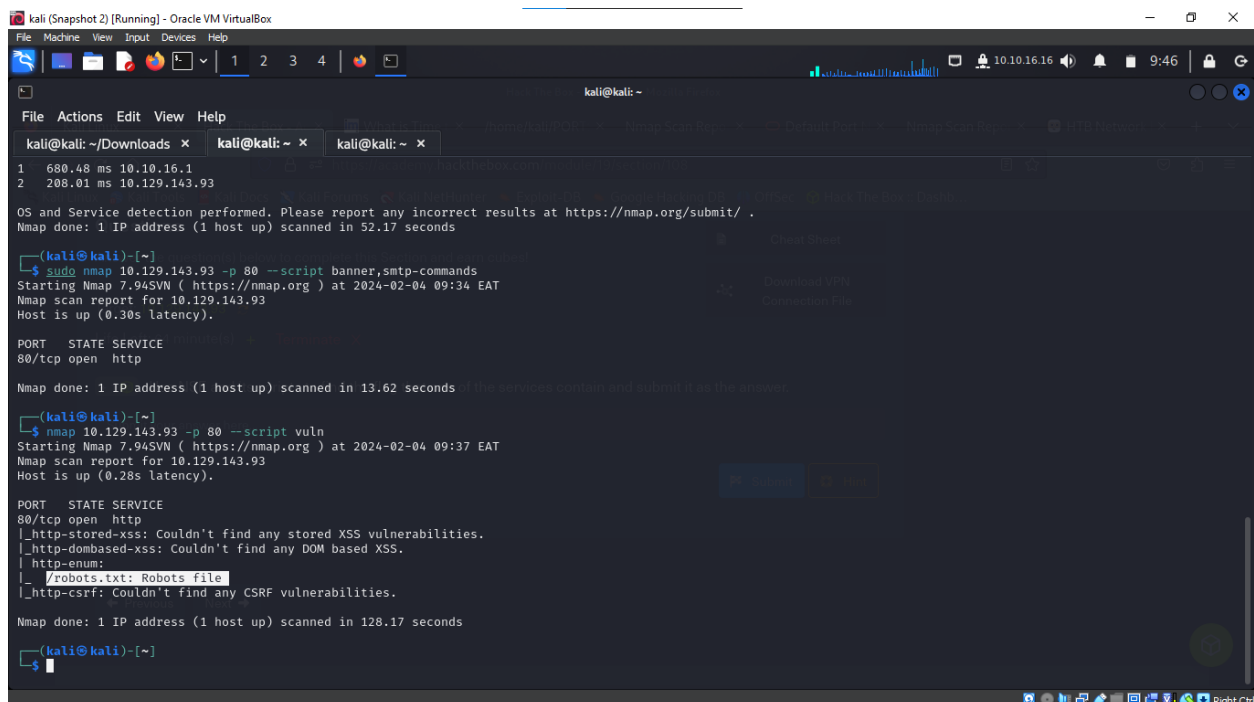
Categories

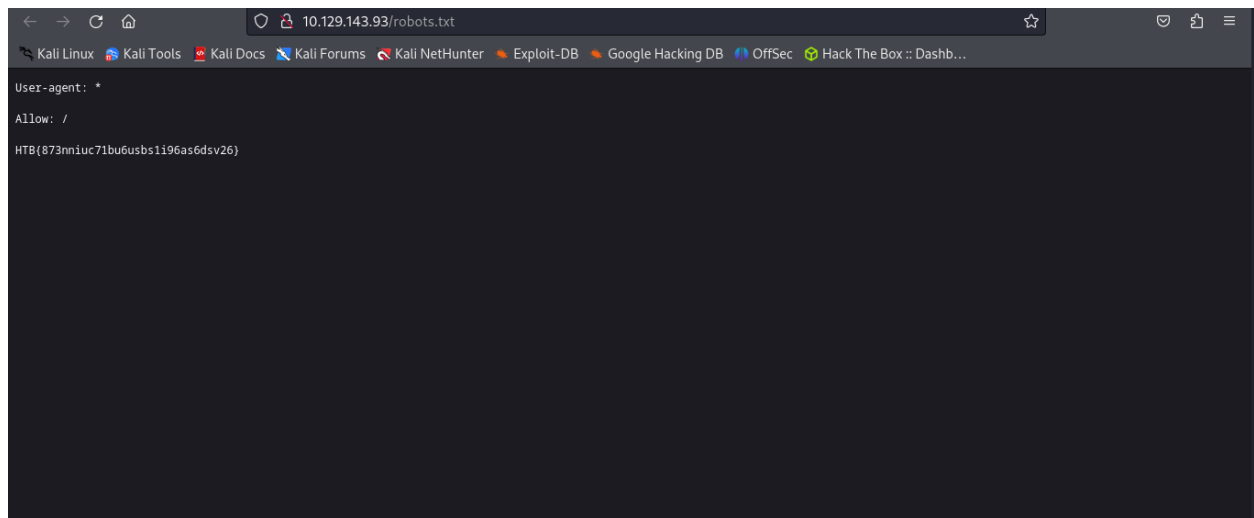
- Includes auth, broadcast, brute, discovery, and more.
- Specific scripts can be chosen for targeted scanning.

Questions

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

A: HTB{873nniuc71bu6usbs1i96as6dsv26}





## 8. Performance

Optimizing scanning performance is essential, especially for extensive networks or when dealing with bandwidth constraints.

### Techniques

- Adjusting timeouts, retries, and packet rates
- Using Nmap's timing templates for efficient scanning

## 9. Firewall and IDS/IPS Evasion

Nmap offers methods to bypass firewall rules and IDS/IPS systems, such as packet fragmentation and decoy use.

### Techniques

- Understanding firewall and IDS/IPS functioning
- Using ACK scans, decoys, and source IP manipulation
- DNS proxying for evasion

## 10. Firewall and IDS/IPS Evasion Labs

### Practical Labs

Three lab scenarios (Easy, Medium, Hard) provide hands-on experience in bypassing firewall and IDS/IPS systems.

### Objectives

- Identifying the operating system, DNS server version, and service versions under various security configurations.

## Questions and Answers

1. OS Identification (Easy Lab): Ubuntu

```
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ nmap --script smb-os-discovery 10.129.219.56
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 10:08 EAT
Nmap scan report for 10.129.219.56
Host is up (0.82s latency).
Not shown: 993 closed tcp ports (conn-refused)
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
10001/tcp open  scp-config

Host script results:
| 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: 2024-02-04T08:09:46+01:00

Nmap done: 1 IP address (1 host up) scanned in 97.88 seconds
```

## 2. DNS Server Version (Medium Lab): HTB{GoTtgUnyze9Psw4vGjcuMpHRp}

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-academy-1]-[10.10.14.161]-[htb-ac-949661@htb-bhx7pg52aq]-[~]
[*]$ sudo nmap -sSU -p 53 --script dns-nsid 10.129.190.31
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-04 08:10 GMT
Nmap scan report for 10.129.190.31
Host is up (0.0094s latency).
h b-ac-949661's
PORT      STATE SERVICE
53/tcp    filtered domain
53/udp    open  domain
| dns-nsid:
|_ bind.version: HTB{GoTtgUnyze9Psw4vGjcuMpHRp}
m
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
[eu-academy-1]-[10.10.14.161]-[htb-ac-949661@htb-bhx7pg52aq]-[~]
[*]$
```

## 3. Service Version (Hard Lab): HTB{kjnsdf2n982n1827eh76238s98di1w6}



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
$ sudo nmap -p- -sS -T4 --min-rate=1000 --max-retries=1 10.129.206.106
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 04:51 EAT
Warning: 10.129.206.106 giving up on port because retransmission cap hit (1).
Nmap scan report for 10.129.206.106
Host is up (0.21s latency).
Not shown: 50609 filtered tcp ports (no-response), 14924 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 119.33 seconds

(kali@kali)-[~]
$ sudo nmap -p- -sS -T4 -Pn --min-rate=1000 --max-retries=1 -g 10.129.206.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 04:57 EAT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds

(kali@kali)-[~]
$ sudo nmap -p- -sS -T4 -Pn --min-rate=1000 --max-retries=1 -g 53 10.129.206.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 04:57 EAT
Warning: 10.129.206.106 giving up on port because retransmission cap hit (1).
Nmap scan report for 10.129.206.106
Host is up (0.24s latency).
Not shown: 60674 closed tcp ports (reset), 4858 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
50000/tcp open  ibm-db2
Nmap done: 1 IP address (1 host up) scanned in 83.80 seconds

(kali@kali)-[~]
$
```

```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
Nmap done: 1 IP address (1 host up) scanned in 119.33 seconds

(kali@kali)-[~]
$ sudo nmap -p- -sS -T4 -Pn --min-rate=1000 --max-retries=1 -g 10.129.206.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 04:57 EAT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds

(kali@kali)-[~]
$ sudo nmap -p- -sS -T4 -Pn --min-rate=1000 --max-retries=1 -g 53 10.129.206.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 04:57 EAT
Warning: 10.129.206.106 giving up on port because retransmission cap hit (1).
Nmap scan report for 10.129.206.106
Host is up (0.24s latency).
Not shown: 60674 closed tcp ports (reset), 4858 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
50000/tcp open  ibm-db2
Nmap done: 1 IP address (1 host up) scanned in 83.80 seconds

(kali@kali)-[~]
$ sudo nc -nv -p 53 10.129.206.106 50000
(UNKNOWN) [10.129.206.106] 50000 (?) open

(kali@kali)-[~]
$ sudo nc -nv -p 53 10.129.206.106 50000
(UNKNOWN) [10.129.206.106] 50000 (?) open
220 HTB[kjnsdf2n982n1827eh76238s98di1w6]
```

## Conclusion

Nmap's comprehensive exploration in this report demonstrates its essential role in network security. It showcases the tool's adaptability across various functionalities, from simple network mapping to advanced intrusion detection. The practical labs underscore Nmap's effectiveness in real-world network defence strategies, making it a vital asset for network security professionals in identifying vulnerabilities and enhancing network resilience.



# HTB ACADEMY

## Network Enumeration with Nmap



Congratulations **Damiano254**, you have completed this module!

Module: **Network Enumeration with Nmap**

Difficulty: **Easy**

Exercises Completed: **9 / 9**

Completed at: 04 Feb 2024