VOCATIONAL COURSE

PROJECT
OF
ETHICAL HACKING COURSE

VOCATIONAL COURSE

Project Title: Footprinting and Network Scanning using Nmap

Software Used: Kali Linux, Nmap, WHOIS, Google Dorking

ABSTRACT

This project focuses on foot printing and network scanning, key techniques in ethical hacking. Using WHOIS and Google Dorking, passive reconnaissance was performed to gather publicly available domain and website information. Active scanning was conducted with Nmap to identify live hosts, open ports, services, and operating systems. All tasks were executed in a safe, educational environment with ethical intent. The project builds foundational skills in information gathering, network analysis, and tool usage, while emphasizing responsible cybersecurity practices. It also highlights the importance of documenting findings clearly and understanding how attackers exploit exposed data to plan further intrusions.

INTRODUCTION

In the domain of cybersecurity, the ability to gather information about a target system is a critical skill for both ethical hackers and malicious attackers. This process begins with foot printing, which involves collecting publicly available data to understand the structure, ownership, and potential vulnerabilities of a network or website. It is followed by network scanning, where tools are used to actively probe systems for open ports, running services, and operating system details.

This project explores both passive and active reconnaissance techniques using widely available tools. WHOIS is used to extract domain registration details, such as the owner's name, contact information, and server data. Google Dorking helps uncover exposed directories, login pages, and sensitive files through advanced search queries. For active scanning, Nmap is employed to identify live hosts, detect open ports, and analyse services and OS fingerprints.

All activities were conducted in a controlled, educational environment with strict adherence to ethical guidelines. The goal is to build practical skills in information gathering, network analysis, and tool usage, while understanding how attackers exploit exposed data. By documenting each step and interpreting the results, this project emphasizes the importance of ethical hacking practices and responsible cybersecurity awareness.

This topic was chosen to align with academic requirements while deepening hands-on understanding of real-world security tools. It also supports my long-term goal of building a strong foundation in ethical hacking and network defence.

PROJECT OVERVIEW

The project titled "Footprinting and Network Scanning using Nmap" focuses on the initial stages of ethical hacking, specifically the techniques used to gather information about a target system before any exploitation occurs. These stages are critical for understanding how attackers identify vulnerabilities and how defenders can proactively secure systems.

The project is divided into two core phases:

- **Footprinting (Passive Reconnaissance):** This phase involves collecting publicly available information without interacting directly with the target system. Tools such as WHOIS were used to extract domain registration data, including registrar details, contact information, and server locations. Google Dorking was employed to uncover exposed directories, login portals, and sensitive files using advanced search operators.
- **Network Scanning (Active Reconnaissance):** In this phase, Nmap was used to perform detailed scans of target IP addresses. The scans revealed live hosts, open ports, running services, and operating system fingerprints. Techniques such as TCP SYN scans, OS detection, and service version enumeration were applied to understand the network's structure and potential vulnerabilities.

Key Features of the Project: -

- Tool Integration: The project utilizes a combination of passive and active tools—WHOIS, Google Dorking, and Nmap—to simulate real-world reconnaissance workflows.
- Protocol-Level Analysis: Nmap scans provided insights into network protocols (e.g., TCP, UDP), port states (open, closed, filtered), and service banners, enabling deeper understanding of system exposure.
- Ethical Execution: All scanning and data collection were performed in a controlled lab environment, ensuring compliance with ethical hacking standards and avoiding unauthorized access.
- Structured Documentation: Each step of the process was documented with tool outputs, command syntax, and observations. Screenshots and result interpretations were included to support analysis.

FOOTPRINTING (PASSIVE RECONNAISSANCE)

Footprinting is the initial phase of ethical hacking, where information about a target system or organization is gathered without directly interacting with it. This passive reconnaissance helps attackers and security professionals understand the target's digital footprint, including domain details, exposed files, and infrastructure components. The goal is to collect as much relevant data as possible while remaining undetected.

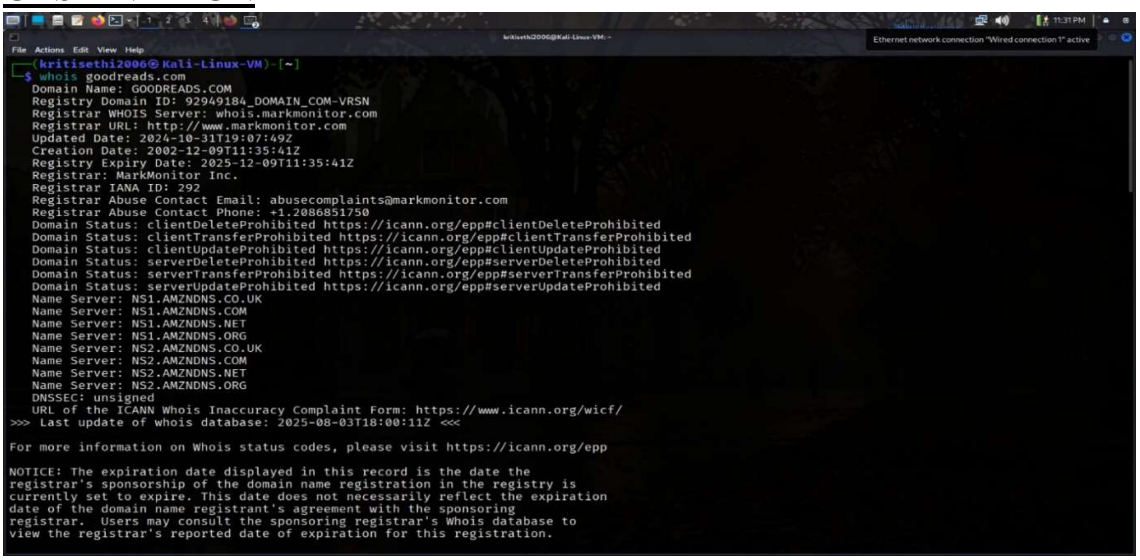
❖ WHOIS Lookup on Goodreads.com:

The WHOIS tool was used to extract domain registration details for the website Goodreads.com. The lookup revealed:

- Domain Registered On: 9th December 2002
- Expiry Date: 9th December 2025
- Registrar: MarkMonitor Inc.
- Registrant Organization: Goodreads LLC (United States)
- Name Servers: Hosted via Amazon DNS (e.g., ns1.amzndns.com, ns2.amzndns.net)
- Status Flags: Domain is protected against unauthorized deletion, transfer, and updates

This data helps identify the hosting provider and potential entry points for social engineering or technical attacks.

OBSERVATION



```
(kritisethi2006㉿Kali-Linux-VM)-[~]
└─$ whois goodreads.com
   Domain Name: GOODREADS.COM
   Registry Domain ID: 92949184_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-10-31T19:07:49Z
   Creation Date: 2002-12-09T11:35:41Z
   Registry Expiry Date: 2025-12-09T11:35:41Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.AMZNDNS.CO.UK
   Name Server: NS1.AMZNDNS.COM
   Name Server: NS1.AMZNDNS.NET
   Name Server: NS1.AMZNDNS.ORG
   Name Server: NS2.AMZNDNS.CO.UK
   Name Server: NS2.AMZNDNS.COM
   Name Server: NS2.AMZNDNS.NET
   Name Server: NS2.AMZNDNS.ORG
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-08-03T18:00:11Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: goodreads.com
Registry Domain ID: 92949184_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-10-31T19:07:49+0000
Creation Date: 2002-12-09T11:35:41+0000
Registrar Registration Expiration Date: 2025-12-09T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Goodreads LLC
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/goodreads.com
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/goodreads.com
Name Server: ns2.amzndns.net
Name Server: ns2.amzndns.co.uk
Name Server: ns2.amzndns.org
Name Server: ns1.amzndns.org
Name Server: ns1.amzndns.co.uk
Name Server: ns1.amzndns.com
Name Server: ns2.amzndns.com
Name Server: ns1.amzndns.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-08-03T18:00:37+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant or Technical
```

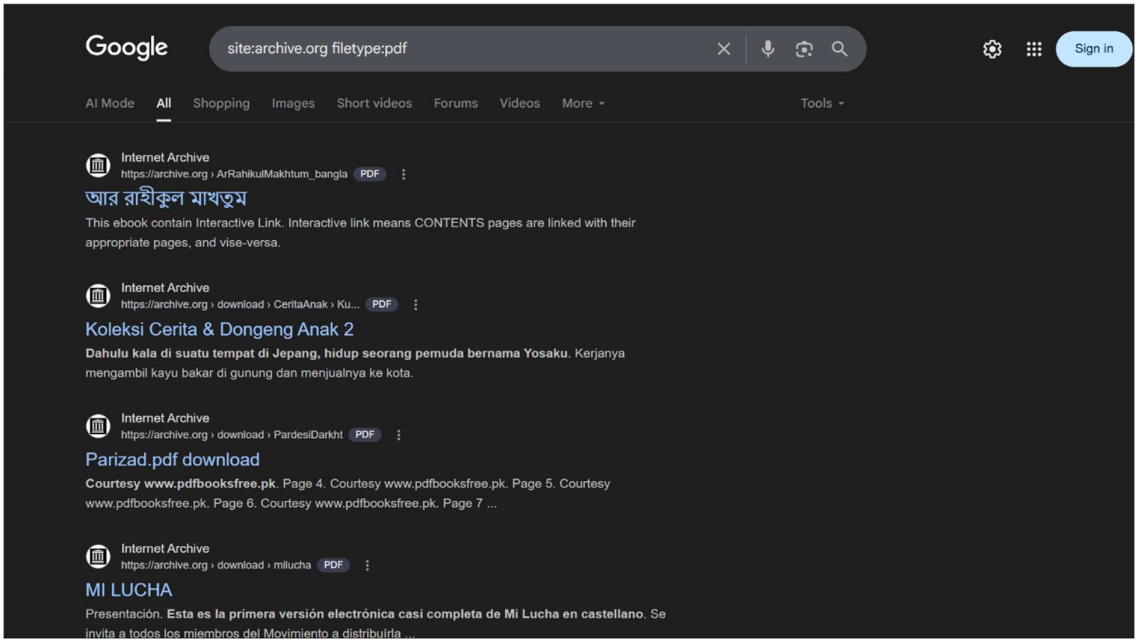
❖ Google Dorking:

Google Dorking was performed on archive.org using advanced search operators to identify publicly exposed resources. Queries such as:

- site:archive.org filetype:pdf
- inurl:login site:archive.org
- intitle:"index of" site:archive.org

These queries were used to locate downloadable documents, login interfaces, and open directories. The results revealed multiple publicly accessible files and metadata, demonstrating how misconfigured or unprotected content can be discovered through search engines.

OBSERVATION



Google

site:archive.org inurl:login

Sign in

AI Mode | All | Images | Videos | Shopping | Short videos | News | More | Tools

Internet Archive
https://archive.org › account › login

Log in

Search the history of over __WB_PAGES_ARCHIVED__ web pages on the Internet. Search the Wayback Machine. An illustration of a magnifying glass.

Internet Archive
https://archive.org › details › login-april-1986

LOGiN Magazine (ログイン) - April 1986 (600DPI) : ASCII

16 Aug 2023 — **LOGiN Magazine** (ログイン) - April 1986 scanned in at 600DPI with a Fujitsu fi-7460. PDF was OCR'd with Searchable Text in Adobe Acrobat.

Internet Archive
https://archive.org › details › login-may-1982

LOGiN Magazine (ログイン) - May 1982 (600DPI) : ASCII

29 Sept 2022 — **LOGiN Magazine** (ログイン) - May 1982 scanned in at 600DPI with a Fujitsu fi-7460. PDF was OCR'd with Searchable Text in Adobe Acrobat.

Internet Archive
https://archive.org › details › login-january-1987

LOGiN Magazine (ログイン) - January 1987 (600DPI) : ASCII

8 Sept 2022 — **LOGiN Magazine** (ログイン) - January 1987 scanned in at 600DPI with a Fujitsu fi-7460.PDF was OCR'd with Searchable Text in Adobe Acrobat.

Google

intitle:"index of" site:archive.org

Sign in

AI Mode | All | Images | Shopping | Videos | Short videos | News | More | Tools

Internet Archive
https://ia903403.us.archive.org › items › data15

Index of /23/items/data15/

Index of /23/items/data15/ ../ data15.thumbs/ 06-Apr-2021 18:26 - The Pursuit Of Happyness (2006).mkv 06-Apr-2021 16:28 1611927213 The Pursuit Of Happyness ...

archive.org
https://purl.archive.org › documents › dcmi-point

Index of /documents/dcmi-point

Index of /documents/dcmi-point. Parent Directory · index.shtml/

Internet Archive
https://archive.org › details › dli.ernet.211980

Index Of Spectra : Watts, Marshall. W

11 Oct 2020 — Index Of Spectra ; Language: English ; Item Size: 90.0M ; Addeddate: 2020-10-11 08:38:31 ; Identifier: dli.ernet.211980 ; Identifier-ark: ark:/13960/ ...

Internet Archive
https://ia803102.us.archive.org › items › CharlesDuhig...

Index of /35/items/CharlesDuhigg.ThePowerOfHabit_201808/

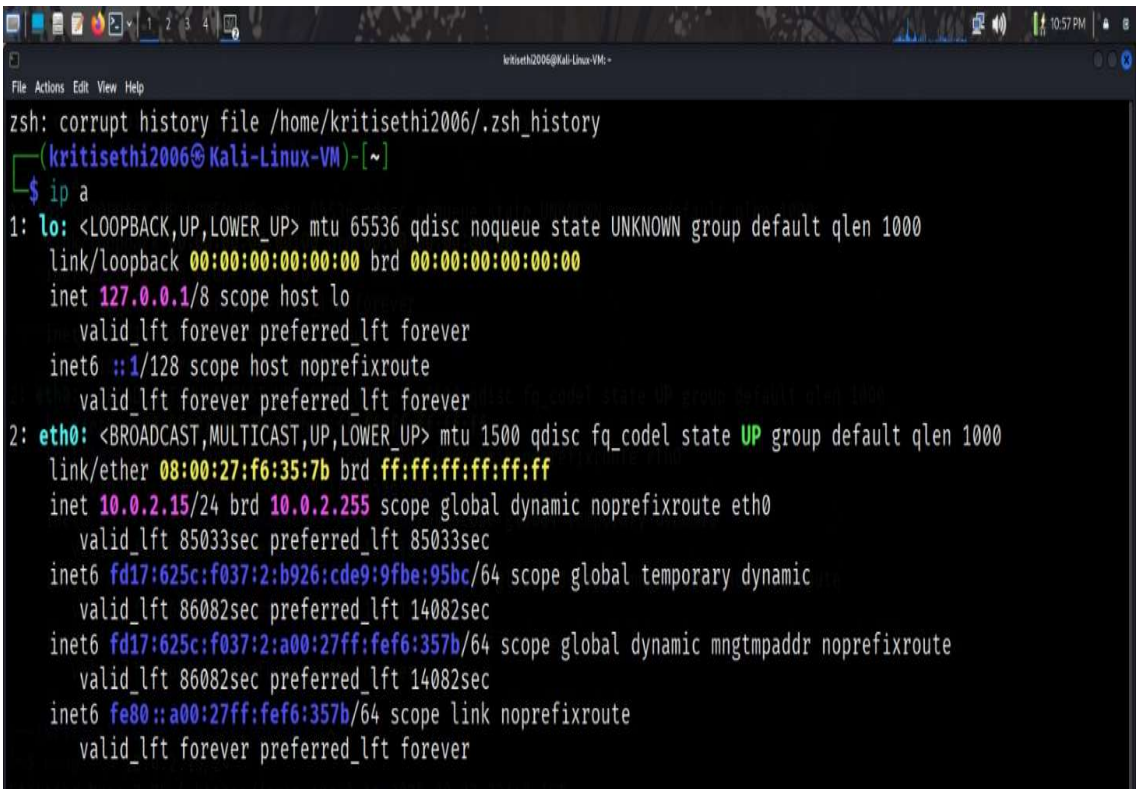
Charles-Duhigg.The-Power-of-Habit.epub 08-Nov-2023 02:43 1153763 Charles-Duhigg.The-Power-of-Habit.pdf 30-Aug-2018

NETWORK SCANNING (ACTIVE RECONNAISSANCE)

Active reconnaissance is a critical phase in ethical hacking where the tester directly interacts with the target system to gather technical information. Unlike passive methods, active scanning involves sending packets to the target and analysing the responses. This approach helps identify live hosts, open ports, running services, and operating system details—essential for understanding the network's structure and potential vulnerabilities.

- **<u>IP Address Finding:</u>** To identify the IP address of a system in Kali Linux, the '*ip a*' command is used. This command lists all active network interfaces along with their assigned IP addresses.

<u>OBSERVATION</u>



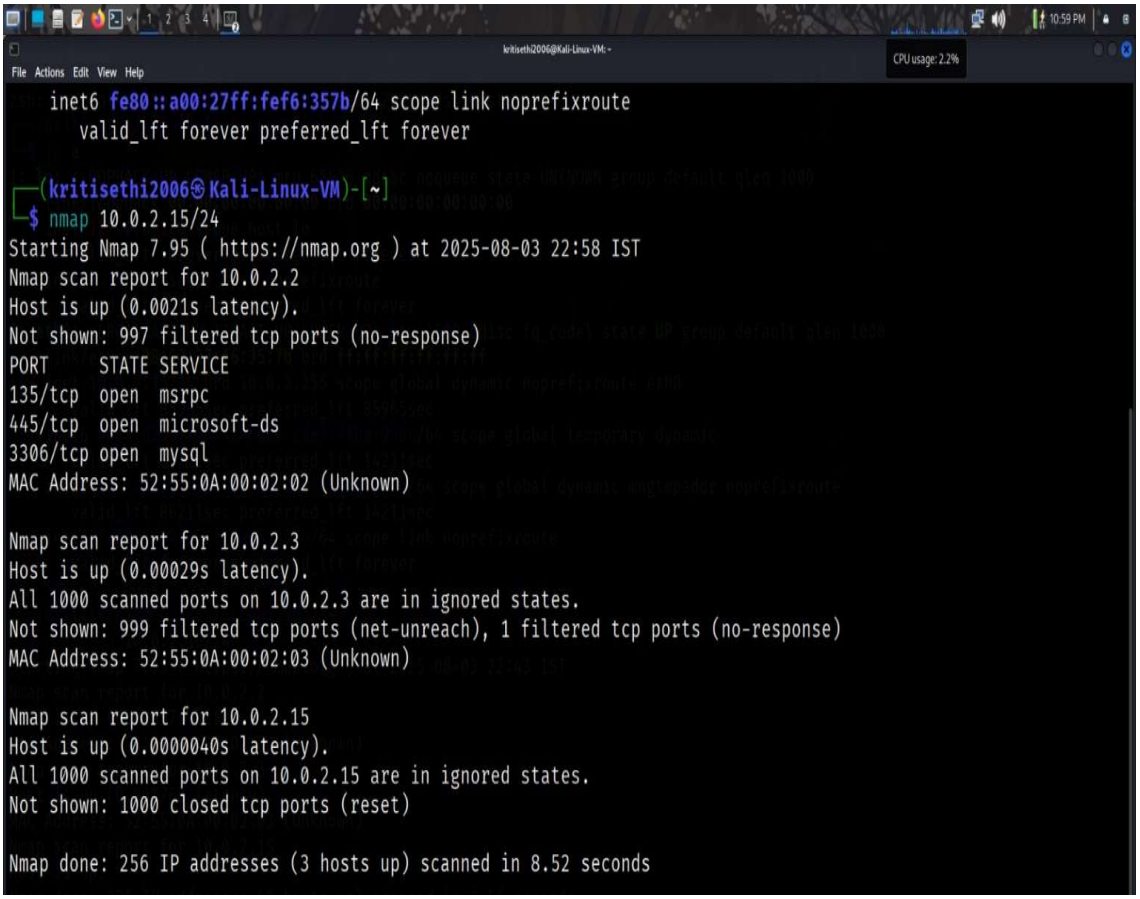
```
zsh: corrupt history file /home/kritisethi2006/.zsh_history
┌──(kritisethi2006㉿Kali-Linux-VM)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f6:35:7b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85033sec preferred_lft 85033sec
    inet6 fd17:625c:f037:2:b926:cde9:9fbe:95bc/64 scope global temporary dynamic
       valid_lft 86082sec preferred_lft 14082sec
    inet6 fd17:625c:f037:2:a00:27ff:fef6:357b/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86082sec preferred_lft 14082sec
    inet6 fe80::a00:27ff:fef6:357b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Key Interfaces: -

- **lo (Loopback Interface):**
  - **IPv4:** 127.0.0.1 (used for internal testing)
  - **IPv6:** ::1
- **eth0 (Ethernet Interface):**
  - **IPv4:** 10.0.2.15 (local IP assigned to the system)
  - **IPv6:** Multiple addresses including fe80::... (link-local)

❖ **<u>Port Scan:</u>** Port scanning helps identify which services are running on target systems by probing their network ports. In this scan, the subnet 10.0.2.0/24 was scanned using Nmap to detect open ports and active hosts.

<u>OBSERVATION</u>



```
inet6 fe80::a00:27ff:fef6:357b/64 scope link noprefixroute
    valid_lft forever preferred_lft forever

┌──(kritisethi2006㉿Kali-Linux-VM)-[~]
└─$ nmap 10.0.2.15/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 22:58 IST
Nmap scan report for 10.0.2.2
Host is up (0.0021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00029s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.52 seconds
```

➢ **10.0.2.2**:

- **Open ports:**
  - 135/tcp – Microsoft RPC
  - 445/tcp – Microsoft-DS (file sharing)
  - 3306/tcp – MySQL (database service)
- Indicates a system running Windows services and a database.

➢ **10.0.2.3**:

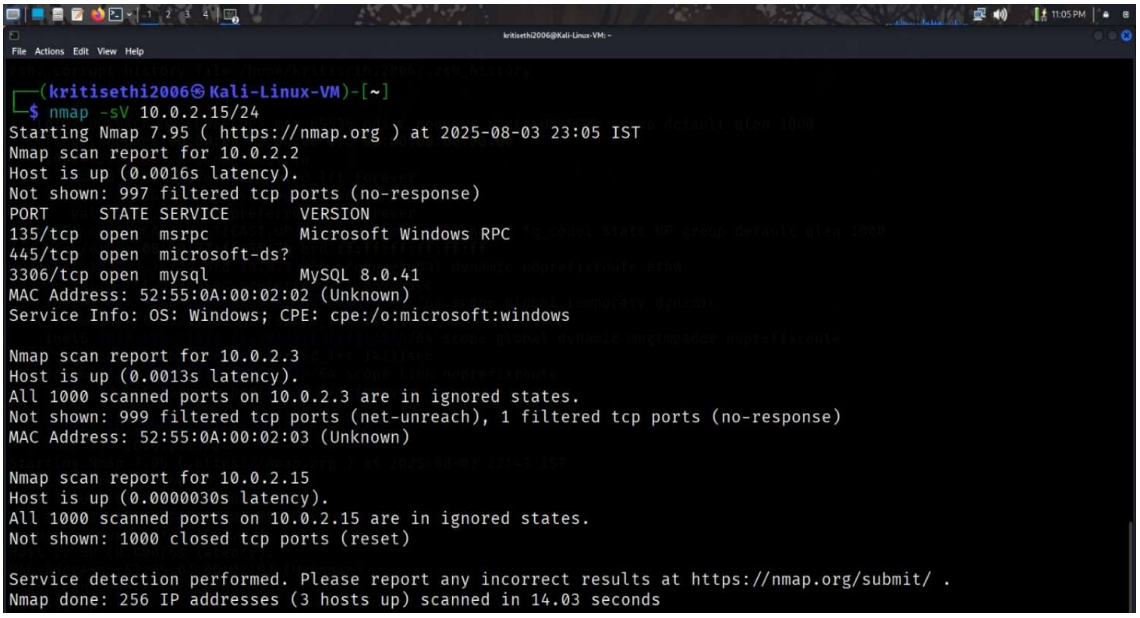
- All ports filtered or unreachable.
- May be protected by a firewall or not running any services.

➢ **10.0.2.15**:

- All ports closed (reset response).
- Indicates a system that is reachable but not offering any services on common ports.

❖ **<u>Service Version Detection:</u>** Service version detection helps identify not just which ports are open, but which services are running on those ports and their specific versions. This is useful for pinpointing exact software (e.g., MySQL 8.0.41), matching services with known vulnerabilities and understanding the role of each host in the network

OBSERVATION



```
┌──(kritisethi2006㉿Kali-Linux-VM)-[~]
└─$ nmap -sV 10.0.2.15/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 23:05 IST
Nmap scan report for 10.0.2.2
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL 8.0.41
MAC Address: 52:55:0A:00:02:02 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.3
Host is up (0.0013s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 14.03 seconds
```

➢ **Host: 10.0.2.2**

- **Detected Services:**
  - 135/tcp – Microsoft RPC *(version not specified)*
  - 445/tcp – Microsoft-DS *(version not specified)*
  - 3306/tcp – MySQL version 8.0.41
- **Service Info:**
  - OS fingerprinting suggests Windows operating system
  - **CPE string:** cpe:/o:microsoft:windows confirm Windows environment
- **MAC Address:** 52:55:0A:00:02:02

➢ **Host: 10.0.2.3**

- **Service Detection Result:**
  - All ports are filtered — no service banners or version info retrieved.
- **MAC Address:** 52:55:0A:00:02:03

➢ **Host: 10.0.2.15**

- **Service Detection Result:**
  - All ports are closed — Nmap received reset responses.
- **MAC Address:** 52:55:0A:00:02:15

❖ **<u>Operating System Detection:</u>** Operating system detection was performed using Nmap's -O flag, which uses TCP/IP stack fingerprinting to estimate the OS running on target hosts. The scan was conducted on the subnet 10.0.2.0/24 to identify host types, OS families, and network characteristics.

OBSERVATION

```
┌──(kritisethi2006㉿Kali-Linux-VM)-[~]
└─$ sudo nmap -O 10.0.2.15/24
[sudo] password for kritisethi2006:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 23:06 IST
Nmap scan report for 10.0.2.2
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 52:55:0A:00:02:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|general purpose|bridge
Running (JUST GUESSING): AT&T embedded (99%), QEMU (95%), Oracle Virtualbox (94%), Slirp (94%)
OS CPE: cpe:/a:qemu:qemu cpe:/a:oracle:vm_virtualbox cpe:/a:danny_gasparovski:slirp
Aggressive OS guesses: AT&T BGW210 voice gateway (99%), QEMU user mode network gateway (95%), Oracle Virtualbox
 Slirp NAT bridge (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.0.2.3
Host is up (0.00088s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: QEMU
OS CPE: cpe:/a:qemu:qemu
OS CPE: cpe:/a:qemu:qemu cpe:/a:oracle:vm_virtualbox cpe:/a:danny_gasparovski:slirp
Aggressive OS guesses: AT&T BGW210 voice gateway (99%), QEMU user mode network gateway (95%), Oracle Virtualbox
 Slirp NAT bridge (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.0.2.3
Host is up (0.00088s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: QEMU
OS CPE: cpe:/a:qemu:qemu
OS details: QEMU user mode network gateway
Network Distance: 1 hop

Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 14.22 seconds
```

- **Host: 10.0.2.2**
  - **Open Ports:** 135/tcp (msrpc), 445/tcp (microsoft-ds), 3306/tcp (mysql)
  - **MAC Address:** 52:55:0A:00:02:02
  - **OS Detection Result:**
    - **Device type:** VoIP adapter General purpose Bridge
    - **OS guesses:**
      - AT&T BGW210 voice gateway (99%)
      - QEMU user-mode gateway (95%)
      - Oracle VirtualBox (94%)
      - Slirp NAT bridge (94%)
    - **OS CPEs:**
      - cpe:/a:qemu:qemu
      - cpe:/a:oracle:vm_virtualbox
      - cpe:/a:danny_gasparovski:slirp
- **Host: 10.0.2.3**
  - **All Ports:** Filtered or unreachable
  - **MAC Address:** 52:55:0A:00:02:03
  - **OS Detection Result:**
    - **Device type:** General purpose
    - **OS guess:** QEMU
    - **OS CPE:** cpe:/a:qemu:qemu
- **Host: 10.0.2.15**
  - No OS fingerprinting data available in the scan output.
  - Likely all ports were closed or filtered, preventing OS analysis.

❖ **<u>Aggressive Scan:</u>** An aggressive scan was conducted using the command sudo nmap -A 10.0.2.15/24 to gather comprehensive information about live hosts, open ports, service versions, operating systems, and SSL configurations. The scan targeted the subnet 10.0.2.0/24.

OBSERVATION

```
┌──(kritisethi2006㉿Kali-Linux-VM)-[~]
└─$ sudo nmap -A 10.0.2.15/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 23:07 IST
Nmap scan report for 10.0.2.2
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL 8.0.41
| ssl-cert: Subject: commonName=MySQL_Server_8.0.41_Auto_Generated_Server_Certificate
| Not valid before: 2025-02-18T18:25:23
|_Not valid after:  2035-02-16T18:25:23
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.41
|   Thread ID: 37
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, IgnoreSigpipes, Speaks41ProtocolOld, FoundRows, SwitchToSSLAfterHandshake
, InteractiveClient, LongPassword, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew, DontAllowData
baseTableColumn, SupportsLoadDataLocal, ODBCClient, LongColumnFlag, IgnoreSpaceBeforeParenthesis, SupportsTrans
actions, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x02&\x06> e\x12j5\x7F]i9p#\x1E\x04\x04+:
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 52:55:0A:00:02:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|general purpose|bridge
Running (JUST GUESSING): AT&T embedded (99%), QEMU (95%), Oracle Virtualbox (94%), Slirp (94%)
```


```
|   Some Capabilities: Support41Auth, IgnoreSigpipes, Speaks41ProtocolOld, FoundRows, SwitchToSSLAfterHandshake
, InteractiveClient, LongPassword, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew, DontAllowData
baseTableColumn, SupportsLoadDataLocal, ODBCClient, LongColumnFlag, IgnoreSpaceBeforeParenthesis, SupportsTrans
actions, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x02&\x06> e\x12j5\x7F]i9p#\x1E\x04\x04+:
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 52:55:0A:00:02:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|general purpose|bridge
Running (JUST GUESSING): AT&T embedded (99%), QEMU (95%), Oracle Virtualbox (94%), Slirp (94%)
```


```
OS CPE: cpe:/a:qemu:qemu cpe:/a:oracle:vm_virtualbox cpe:/a:danny_gasparovski:slirp
Aggressive OS guesses: AT&T BGW210 voice gateway (99%), QEMU user mode network gateway (95%), Oracle Virtualbox
 Slirp NAT bridge (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 1s
| smb2-time:
|   date: 2025-08-03T17:38:03
|_  start_date: N/A
TRACEROUTE
HOP RTT     ADDRESS
1   1.31 ms 10.0.2.2

Nmap scan report for 10.0.2.3
Host is up (0.00056s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 999 filtered tcp ports (net-unreach), 1 filtered tcp ports (no-response)
MAC Address: 52:55:0A:00:02:03 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: QEMU
OS CPE: cpe:/a:qemu:qemu
OS details: QEMU user mode network gateway
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms 10.0.2.3

Nmap scan report for 10.0.2.15
Host is up (0.000095s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.22 seconds
```

- **Host: 10.0.2.2**
  - **Status:** Host is up (latency: 0.0013s)
  - **Open Ports & Services:**
    - 135/tcp – Open Service: msrpc Version: *Microsoft Windows RPC*
    - 445/tcp – Open Service: microsoft-ds Version: *Not detected*
    - 3306/tcp – Open Service: MySQL Version: *MySQL 8.0.41*
  - **MySQL SSL Certificate:**
    - **Subject:** CN=MySQL_Server_8.0.41_Auto_Generated_Server_Certificate
    - **Validity:** 2025-02-18 to 2035-02-16
    - **TLS randomness:** Does not represent time
  - **MySQL Server Details:**
    - **Protocol:** 10 Thread ID: 37 Status: Autocommit
    - **Auth Plugin:** caching_sha2_password
    - **Capabilities:** Includes support for transactions, compression, multiple results/statements, and SSL
  - **MAC Address:** 52:55:0A:00:02:02 (Vendor: Unknown)
  - **OS Detection:**
    - **Device type:** VoIP adapter General purpose Bridge
    - **OS guesses:**
      - AT&T embedded gateway (99%)
      - QEMU (95%)
      - Oracle VirtualBox (94%)
      - Slirp NAT bridge (94%)
  - Warning: OSScan results may be unreliable due to missing closed ports
  - **SMB2 Security Mode:**
    - Message signing is enabled but not required, indicating moderate protection against man-in-the-middle attacks.
  - **Clock Skew:**
    - **Detected skew: 1 second**, suggesting minimal time drift between scanner and target.
  - **SMB2 Time:**
    - **Server Date:** 2025-08-03T17:38:03
    - **Start Date:** Not available
  - **Traceroute**
    - **Network Distance:** 1 hop

    - **Hop RTT:** 1.31 ms
    - **Hop Address:** 10.0.2.2
    - The host is directly reachable with minimal latency, confirming its presence on the local subnet.
- **Service Info**
    - **Operating System:** Windows
    - **CPE Identifier:** cpe:/o:microsoft:windows
    - **MAC Address:** 52:55:0A:00:02:02 (Vendor: Unknown)
- **OS Detection Reliability**
    - Nmap reports no exact OS matches due to non-ideal test conditions (e.g., insufficient closed ports).
    - **Aggressive guesses still point to:**
        - AT&T BGW210 voice gateway (99%)
        - QEMU user-mode gateway (95%)
        - Oracle VirtualBox (94%)
        - Slirp NAT bridge (94%)

➢ **Host: 10.0.2.3**

- **Status:** Host is up (latency: 0.00056s)
- **Port Scan Result:**
    - All 1000 scanned ports are in ignored states
    - 999 ports: filtered (net-unreachable)
    - 1 port: filtered (no-response)
- **MAC Address:** 52:55:0A:00:02:03 (Vendor: Unknown)
- **OS Detection:**
    - **Device type:** General purpose
    - **OS:** QEMU user-mode network gateway
    - **OS CPE:** cpe:/a:qemu:qemu
    - Warning: OSScan results may be unreliable due to absence of open/closed ports
- **Traceroute:**
    - Network Distance: 1 hop
    - RTT: 0.56 ms
- Host is likely a virtual machine with strict firewall rules or limited network exposure.
- OS detection is approximate, and port filtering prevents deeper analysis.

➢ **Host: 10.0.2.15**

- **Status:** Host is up (latency: 0.000095s)

- **Port Scan Result:**
  - All 1000 scanned ports are in ignored states
  - 1000 ports: closed (reset)
- **OS Detection:**
  - Too many fingerprints matched; no specific OS identified
- **Traceroute:**
  - Network Distance: 0 hops

LEARNING OUTCOMES

1. Understanding Reconnaissance Techniques:
   - Gained a clear distinction between passive and active reconnaissance methods, including how attackers and defenders use them to assess network exposure.
2. Tool Proficiency:
   - Acquired hands-on experience with industry-standard tools such as WHOIS, Google Dorking, and Nmap, including advanced scan types like service version detection, OS fingerprinting, and aggressive scanning.
3. Network Awareness:
   - Learned how to identify live hosts, open ports, running services, and operating systems within a subnet, and how these elements contribute to a network's attack surface.
4. Ethical Hacking Practices:
   - Developed an understanding of ethical boundaries in cybersecurity, ensuring all scans and data collection were performed in a controlled, non-intrusive environment.
5. Technical Documentation Skills:
   - Practiced structured reporting by documenting scan commands, outputs, observations, and interpretations in a formal academic format suitable for evaluation.
6. Security Insight:
   - Recognized how misconfigured services, exposed directories, and outdated software versions can be exploited, reinforcing the importance of proactive defence strategies.
7. Virtualization Awareness:
   - Interpreted scan results from virtualized environments (e.g., QEMU, VirtualBox), understanding how virtualization affects OS detection and network behaviour.

CONCLUSION

This project provided a comprehensive exploration of reconnaissance techniques and network scanning methodologies essential to ethical hacking. Through the use of tools such as WHOIS, Google Dorking, and Nmap, both passive and active information gathering strategies were successfully implemented and analyzed.

The practical execution of various Nmap scans—including ping sweeps, port scanning, service version detection, and OS fingerprinting—enabled a deeper understanding of how network vulnerabilities can be identified and documented. Observations from virtualized environments highlighted the nuances of scan interpretation, especially in cases where OS detection yielded generic or ambiguous results.

Importantly, the project reinforced the ethical responsibilities associated with cybersecurity practices. All activities were conducted within a controlled, permission-based environment, emphasizing the importance of legal compliance and responsible disclosure.

Overall, this exercise not only strengthened technical proficiency but also enhanced academic documentation skills, preparing the groundwork for more advanced cybersecurity research and professional engagement in the field.

REFRENCES

[1] Skoudis, E., & Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.

[2] Lyon, G. F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.

[3] EC-Council. (2020). *Ethical Hacking and Countermeasures: Reconnaissance*. EC-Council Press.

[4] Kumar, R. (2021). *Cybersecurity Essentials*. Wiley India.

[5] Nmap.org. (n.d.). Nmap Reference Guide

[6] ARIN WHOIS Database. (n.d.). https://www.arin.net

[7] Google Advanced Search Operators. (n.d.). https://support.google.com/websearch/answer/2466433