

# **N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network**

Submitted in partial fulfilment of the requirements for the award of  
Bachelor of Technology degree in  
Information Technology

By

**SRIRANGAPRASANTH V (Reg. No - 39120121)**  
**RAMANAN B (Reg. No - 39120091)**



**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**SCHOOL OF COMPUTING**

## **SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY**  
**(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE**  
**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,**  
**CHENNAI - 600119**

**MAY- 2023**



# SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)

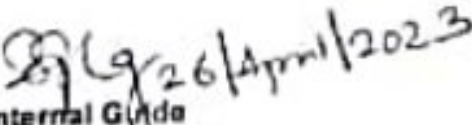
Accredited with Grade "A" by NAAC | ISO Status by UGC | Approved by AICTE

www.sathyabama.ac.in

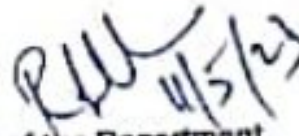
## DEPARTMENT OF INFORMATION TECHNOLOGY

### BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of Srirangaprasanth V (Reg. No - 39120121) and Ramanan B (Reg. No - 39120091) who carried out the Project work entitled "N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network" under my supervision from January 2023 to May 2023.

  
Internal Guide

Dr. G. Mathivanan M.E., Ph.D.,

  
Head of the Department

Dr. R. SUBHASHINI M.E., Ph.D.

Submitted for Viva voce Examination held on 11-05-2023

  
Internal Examiner

  
External Examiner

## DECLARATION

I, **Srirangaprasanth V** (Reg. No - 39120121), hereby declare that the Project work Report entitled "**N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network**" done by me under the guidance of **Dr. G. Mathivanan M.E., Ph.D.**, is submitted in partial fulfillment of the requirements for the award Bachelor of Technology degree in Information Technology.

DATE : 11-05-2023

PLACE : Chennai



SIGNATURE OF THE CANDIDATE



## ACKNOWLEDGEMENT

I am pleased to express my sincere thanks to the **Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph. D., Dean**, School of Computing and **Dr. R. SUBHASHINI M.E., Ph.D.**, Head of the Department, Department of Information Technology for providing me the necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. G. Mathivanan M.E., Ph.D.**, for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of this project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.



## ASTARCT

In the development of computer interconnection, computer networking is essential. It facilitated communication or data sharing between two or more devices over the same network (Intranet and Global Network) (Internet). However, due to a number of open protocols or ports, the lack of use of OS-based firewalls, weakened credentials for remote protocols, vulnerable services, service versions, etc., security is still a major concern in the network. A CLI (Command Line Interface) based network security testing tool, N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network was created using Python 3 and Bash. The Linux operating system in the Debian flavour is compatible with N3TU0N. When it comes to IP address, MAC address, route through, live host detection, port scanning, service version detection, OS detection, vulnerability detection, SOV (Service, OS, Vulnerability) script, firewall bypass, FTP login, and Telnet login, N3PTU0N is a tool that can be used by network security professionals. Ping, ARP, Nmap Scripting Engine (NSE), Mac-changer, Hgping3, Masscan, FTP, and TELNET are among the network utilities used by N3PTU0N. It makes it simple to create a report of the tested network and aids network security professionals in navigating fast. It also utilizes all of the stated tools' capabilities with a single comprehensive script.



| Chapter no | TITLE                                                                                     | Page No |
|------------|-------------------------------------------------------------------------------------------|---------|
|            | <b>ABSTRACT</b>                                                                           | v       |
|            | <b>LIST OF FIGURES</b>                                                                    | vii     |
|            | <b>LIST OF ABBREVIATIONS</b>                                                              | viii    |
| 1          | <b>INTRODUCTION</b>                                                                       | 1       |
|            | 1.1 Cyber Security                                                                        | 1       |
|            | 1.2 Network Enumeration                                                                   | 1       |
|            | 1.3 Penetration Testing                                                                   | 2       |
| 2          | <b>LITERATURE SURVEY</b>                                                                  | 3       |
|            | 2.1 Inferences from the literature survey                                                 | 3       |
| 3          | <b>REQUIREMENT ANALYSIS</b>                                                               | 6       |
|            | 3.1 Software requirements                                                                 | 6       |
|            | 3.2 VM Ware                                                                               | 6       |
|            | 3.3 Kali Linux                                                                            | 7       |
|            | 3.4 Metasploitable                                                                        | 7       |
|            | 3.5 Visual Studio Code                                                                    | 8       |
|            | 3.6 Python3                                                                               | 9       |
|            | 3.7 Bash                                                                                  | 9       |
| 4          | <b>DESCRIPTION OF THE PROPOSED SYSTEM</b>                                                 | 10      |
|            | 4.1 Selected Methodology or proposed model                                                | 10      |
|            | 4.2 System Architecture for the proposed system                                           | 13      |
|            | 4.3 Description of Software for Implementation and Testing<br>Plan of the Proposed System | 14      |
|            | 4.4 Project Implement plan                                                                | 14      |
| 5          | <b>IMPLEMENTATION</b>                                                                     | 15      |
|            | 5.1 Commands involved in the tool                                                         | 15      |
| 6          | <b>RESULT AND DISCUSSIONS</b>                                                             | 25      |
| 7          | <b>CONCLUSION</b>                                                                         | 26      |
|            | 7.1 Conclusion                                                                            | 26      |
|            | 7.2 Future Scope                                                                          | 26      |
|            | <b>REFERENCES</b>                                                                         | 27      |
|            | <b>APPENDIX</b>                                                                           | 28      |
|            | <b>A. SOURCE CODE</b>                                                                     | 28      |
|            | <b>B. SCREENSHOTS</b>                                                                     | 46      |
|            | <b>C. RESEARCH PAPER</b>                                                                  | 53      |



## LIST OF FIGURES

| FIGURENO | FIGURE NAME                      | Page No. |
|----------|----------------------------------|----------|
| 1.2      | Network Enumeration Nmap         | 2        |
| 1.3      | Penetration                      | 2        |
| 3.2      | VMware                           | 6        |
| 3.3      | Kali Linux                       | 7        |
| 3.4      | Metasploitable                   | 7        |
| 3.5      | Visual Studio Code               | 8        |
| 3.7      | Bash                             | 9        |
| 4.1      | Network Enumeration              | 10       |
| 4.2      | Port Scanning Nmap               | 11       |
| 5.1.1    | Ping                             | 15       |
| 5.1.2    | ARP(Address Resolution Protocol) | 16       |
| 5.1.3    | Live Host Detection              | 17       |
| 5.1.5    | MAC Changer                      | 18       |



## **LIST OF ABBREVIATION**

1. **N3PTU0N**-**N**etwork **E**numeration and **P**enetration **T**esting **U**nder an **O**rganized **N**etwork
2. **CLI** – **C**ommand **L**ine **I**nterface
3. **MAC**- **M**edia **A**ccess **C**ontrol
4. **IP**- **I**nternet **P**rotocol
5. **ARP**- **A**ddress **R**esolution **P**rotocol
6. **FTP**- **F**ile **T**ransfer **P**rotocol
7. **NSE**- **N**map **S**cripting **E**ngine
8. **OS**-**O**perating **S**ystem
9. **TELNET**-**T**eletype **N**etwork
10. **TCP**- **T**ransmission **C**ontrol **P**rotocol
11. **ICMP**- **I**nternet **C**ontrol **M**essage **P**rotocol



# CHAPTER 1

## INTRODUCTION

### 1.1 Cyber Security

Cyber Security is the practice of protecting critical systems and sensitive information from digital attacks. Also known as Information Technology Security, Ethical Hacking It is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. It is otherwise known as Computer Security or information Technology security. There are five stages in Cyber security. They are,

1. Information Gathering
2. Enumeration /Scanning
3. Vulnerability Assessment
4. Reporting.

The field of cyber security encompasses a wide range of technologies, practices, and policies aimed at safeguarding computer systems and networks against cyber-attacks, which may come in various forms such as viruses, malware, phishing, ransom ware, and social engineering attacks. Some common cyber security technologies and practices include firewalls, intrusion detection and prevention systems, antivirus software, encryption, access controls, incident response planning, and security awareness training for employees.

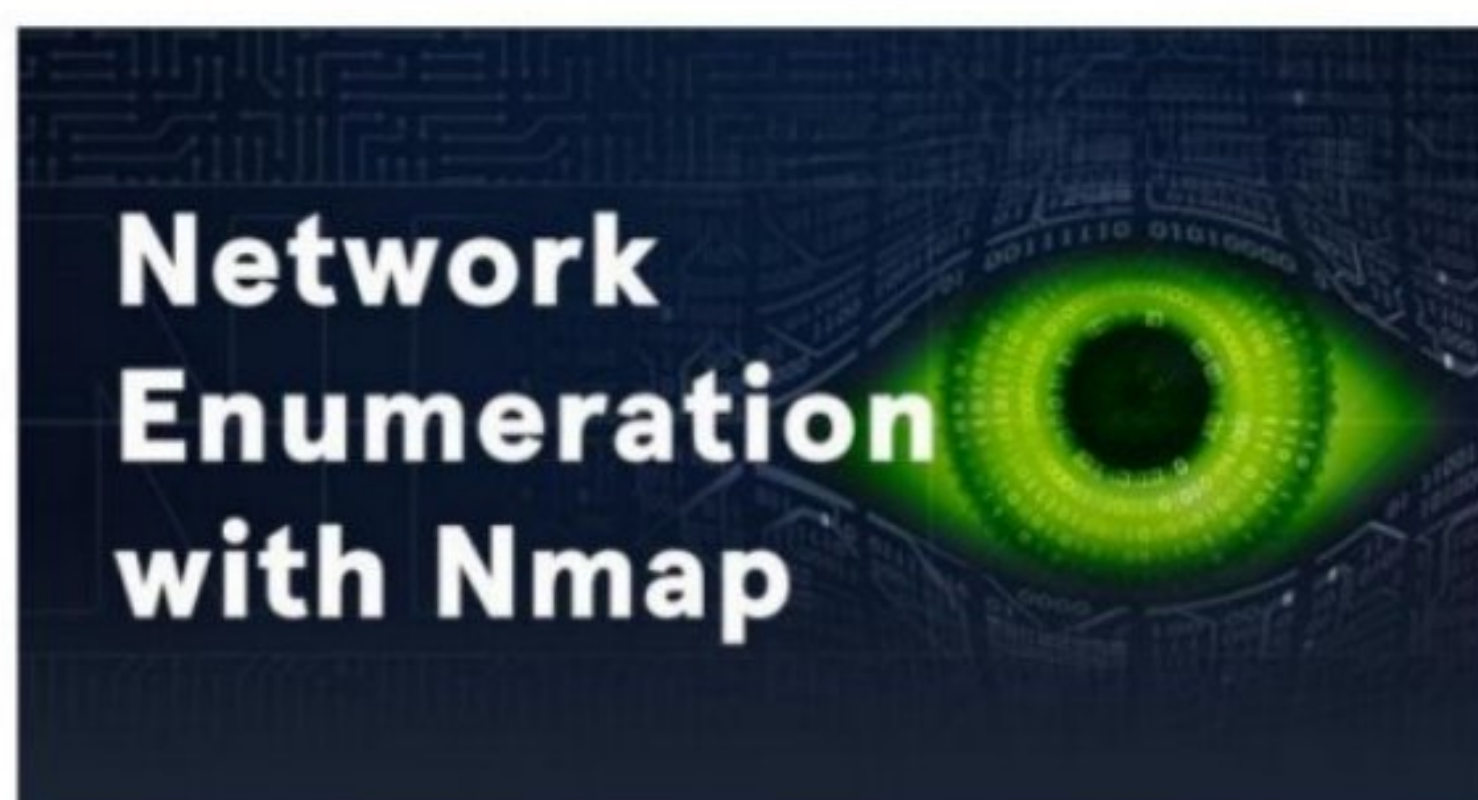
### 1.2 Network Enumeration

Network enumeration is the process of gathering information about a target network, with the goal of identifying potential vulnerabilities and weaknesses that can be exploited by attackers. This process typically involves scanning and probing the network, and collecting information such as IP addresses, open ports, operating systems, and applications running on the network.

Network enumeration is a critical first step in the process of conducting a security assessment or penetration testing, as it provides the attacker with a map of the



network, which can be used to identify potential targets and attack vectors. However, network enumeration can also be used by defenders to identify potential vulnerabilities and weaknesses in their own network, and to take steps to remediate them before they can be exploited by attackers.



***Fig.1.2 Network enumeration***

### **1.3 Penetration Testing**

Penetration testing (pen testing) is a type of security testing that involves evaluating the security of a system or network by simulating an attack from an external or internal threat actor. The objective of a penetration test is to identify potential vulnerabilities and weaknesses in the system, and to determine if unauthorized access, data disclosure, or other malicious activity can be achieved which involves a series of steps, including reconnaissance, scanning and enumeration, gaining access, and maintaining access. The results of a penetration test are typically presented in a report that includes a list of vulnerabilities discovered, their severity level, and recommendations for remediation. Penetration helps organizations identify and address vulnerabilities before they can be exploited by attackers



***Fig.1.3 Penetration Testing***



## CHAPTER 2

### LITERATURE SURVEY

#### 2.1 Inferences from the literature survey

In [1] 2021, G Jayasuryapal , P Meher Pranay has proposed A Survey on Network Penetration Testing which utilize on all the System along with information gathering to the post exploitation. Penetration testing operation follow specific rules and unity that both the gathering (client and pen testing team). By this testing, the organization's defects will be finding like open servers and open ports etc.

In [2] 2019, Pengfei Shi , Futong Qin has proposed The Penetration Testing Framework for Large-Scale Network Based on Network Fingerprint. The fundamentals and methodology of conventional penetration testing technology for big networks are examined, along with some of its practical limitations. A penetration testing framework for large-scale networks based on network fingerprint is 3tilizin by combining network fingerprinting with online search engine technologies.

In [3] 2017, Rodney R Rohrmann , Vincent J Ercolani has proposed Large scale port scanning through tor using parallel Nmap scans to scan large portions of the Ipv4 range. Though effective in assuming data-information during scanning, it is not expandable to the point of scanning the entire Ipv4 Address space on multiple ports, as scans take appreciably longer to execute through Tor. The benefit of a scanning method that shields researchers from targets who might potentially retaliate after being scanned is that it enables them to source their own scans.

In [4] 2015, Prerna Arote , Karam Veer Arya has proposed Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting . An IP network protocol called Internet Control Message Protocol (ICMP) is helpful for administering and controlling networks. A crucial component of IP implementations is ICMP. ARP was created for a more dependable world. The Data Link Layer is in charge of framing packets as they are processed and passed down the stack (DLL).

In [5] 2016, Enos LETSOALO , Sunday OJO has proposed Survey of Media Access



Control address spoofing attacks detection and prevention techniques in Wireless Networks. The Media Access Control addresses of the access point or other users can be extracted from packets intercepted by an attacker using packet sniffer software. In wireless networks, a client is connected to the access point using its MAC address. To disconnect 4tilizing4 users from the network and seize control of any already established TCP session, an attacker can fake the Media Access Control IP of the real access point.

In [6] 2017, Lerato Ramahlapane Moila , Mthulisi Velempini has proposed An Evaluation of the Effectiveness of Cognitive Radio Ad hoc Networks Routing Protocols . Real-time data quality of service needs is not guaranteed by the current protocols. Some of the issues preventing the development of routing protocols that are quality of service aware are caused by the dynamic environment of cognitive networks, which is also responsible for the mobility of nodes, the movement of the spectrum, and the nondeterministic availability of the spectrum.

In [7] 2017, Sathish A.P. Kumar , Brian Xu has proposed Vulnerability Assessment for Security in Aviation Cyber-Physical Systems. We have tested for vulnerabilities in data loaders and other aircraft systems in order to meet the standards for wireless network security set out by the aviation industry. Our efforts include increasing aircraft security and safety as well as identifying cyber vulnerabilities in these aviation systems 4tilizing vulnerability assessment and penetration testing tools like Metasploit Pro and BackTrack.

In [8] 2020, Mehr u Nisa , Kashif Kifayat has proposed Detection of Slow Port Scanning Attacks. In actuality, a scanning assault is a two-part process in which scanning is the first phase where the vulnerability of communication routes is discovered. The second step is the discovery of the targets, followed by the attack. In order to identify the system that can be abused, available open ports are therefore sought across the network during port scanning.

In [9] 2022, Sabah M. Morsy And Dalia Nashat has proposed D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. An ARP spoof-based MITM attack takes use of a flaw in the ARP protocol by associating the attacker's MAC address



with the IP address of the target legitimate host. ARP spoof based-MITM attacks have a variety of defence strategies, although these strategies are incomplete or have a limited effectiveness. Since they alter the basic ARP protocol, performance overhead.

In [10] 2020, Ron Andrews , Dalton A. Hahn has proposed Measuring the Prevalence of the Password Authentication Vulnerability in SSH. We suggest a novel technique for probing an SSH service to determine whether password authentication is permitted as part of our review, without being invasive or damaging to the host. We also show that some of these tools and services can be enhanced in order to assess the prevalence of password authentication in SSH particularly.

In [11] 2017, Debdeep Dey , Archisman Dinda has proposed Warezmater and Warezclicient : An Implementation of FTP Base R2L Attacks. The fact that all commands and data are transmitted using clear text indicates that the File Transfer Protocol (FTP) was not created with strict security measures in mind. Subsequent updates to the protocol have added security features, like upgrading the connection to Transport Layer Security (TLS) in FTPS.

In [12] 2016, Thierry Mbah Mbelli , Barry Dwolatzky has proposed Cyber Security, a Threat to Cyber Banking in South Africa. For South African businesses in particular as well as the nation as a whole, the rise of cybercrime is turning into a severe economic problem. The first section of this essay examines the numerous online hazards related to cyber banking. In addition, it suggests a boundary- and application-based approach to cyber-banking security.



## CHAPTER 3

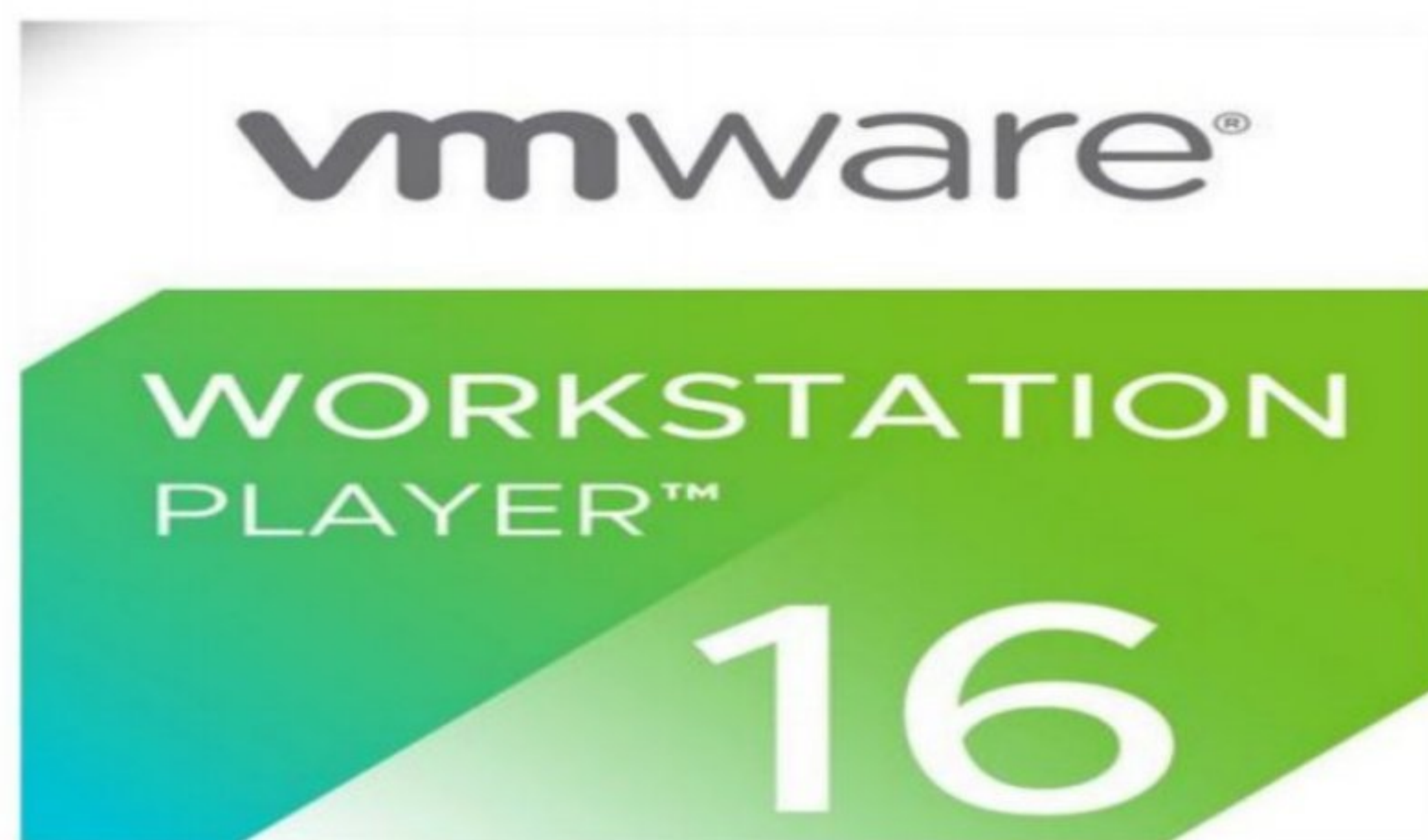
### REQUIREMENT ANALYSIS

#### 3.1 Software Requirements

- Vmware (Virtualization)
- Kali Linux (Main Operating System)
- Metasploitable (Vulnerable Machine)
- Visual Studio Code (Text Editor)
- Python3
- Bash

#### 3.2 VM Ware Workstation 16 Player

- Vmware is a software that enables users with virtualization
- It is a virtual machine software from VMWare.
- It enables multiple copies of the same operating system, or there can be several different operating systems that can run simultaneously on the same
- VMWare's virtualization technology one would be able to run another machine within another physical machine and perform all tasks.
- Hypervisor abstracts the software from PC's hardware and thus creates and manages the virtual machines.



**Fig. 3.2 VM Ware**



### 3.3 Kali Linux

- Kali Linux is a Debian-based Linux distribution.
- Kali Linux is a specially designed OS for network analysts, Penetration testers.
- It is completely free and open source. So you can use it for free and even contribute for its development.
- That is easily accessible and offered for free to information security experts and enthusiasts.
- Supported Platform of the Metasploitable a vulnerable machine for developing and executing security exploits.

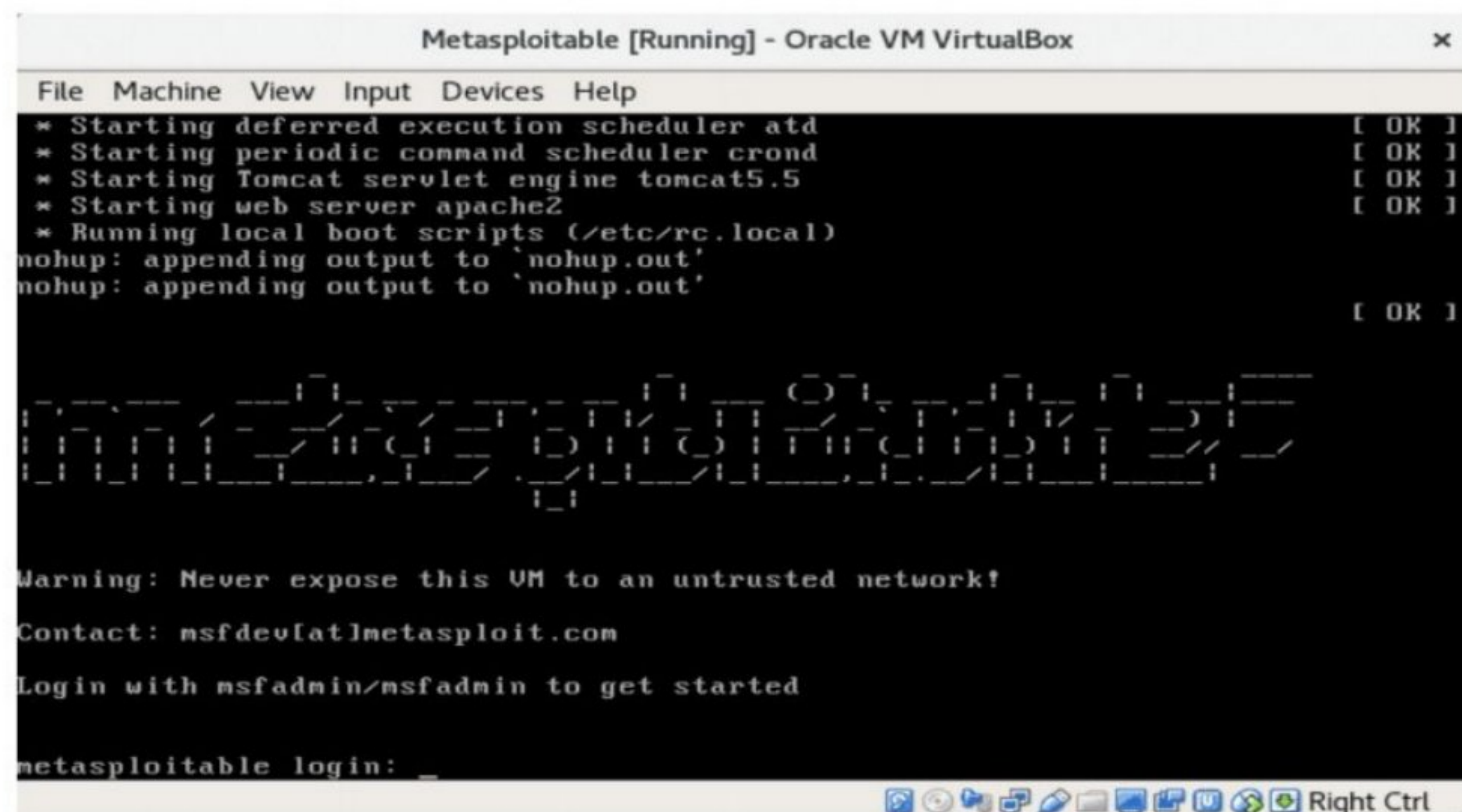


*Fig.3.3 Kali Linux*

### 3.4 Metasploitable

- Metasploitable is a Vulnerable Machine.
- It is an open-source penetration testing and development platform.
- It provides to exploitation of a variety of applications, operating systems, and platforms. The main components of Metasploits the module.
- It is easy to use Metasploit while conducting a large network penetration test. Metasploit conducts automated tests on all systems in order to exploit the vulnerability.
- Metasploit allows a clean exit from the target system it has compromised.

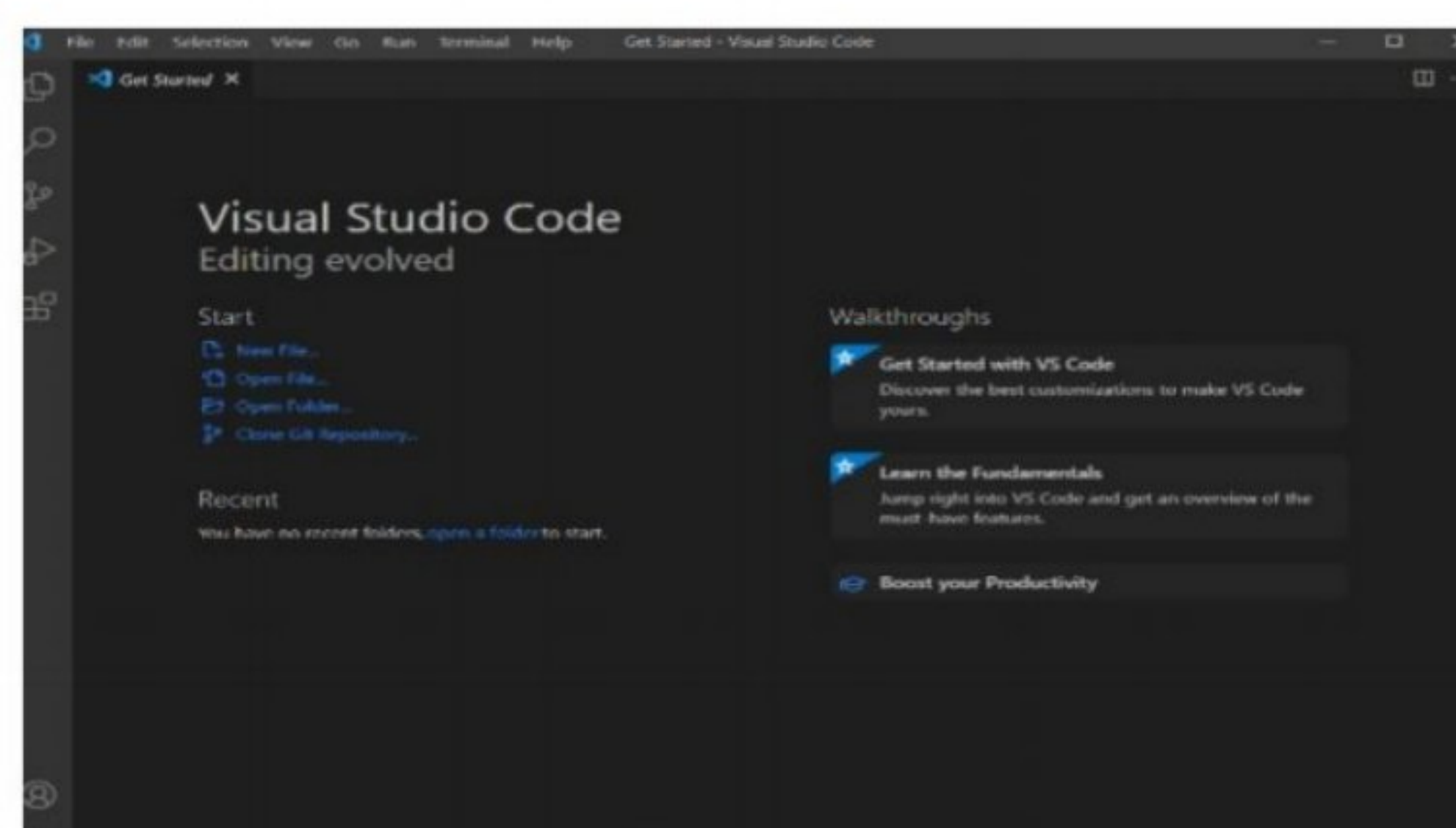




**Fig 3.4 Metasploitable**

### 3.5 Visual Studio Code

- Visual Studio Code, also commonly referred to as VS Code, is a source-code editor made by Microsoft with the Electron Framework, for Windows, Linux and mac OS.
- Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git.
- Users can change the theme, keyboard shortcuts, preferences, and install extensions that add additional functionality.
- In the Stack Overflow 2021 Developer Survey, Visual Studio Code was ranked the most popular developer environment tool among 82,000 respondents, with 70% reporting that they use it.



**Fig 3.5 Visual Studio Code**



### 3.6 Python3

- Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation.
- Python is dynamically-typed and garbage-collected.
- It supports multiple programming paradigms, including structured (particularly procedural), object-oriented and functional programming.
- It is often described as a “batteries included” language due to its comprehensive standard library.

### 3.7 Bash

- **BASH (BOURNE AGAIN SHELL)** is a shell program. SHELL is the command interpreter for the Operating System.
- It is a command line language for UNIX-based Operating Systems. It allows you to control the computer like a developer
- It is a command language that allows us to work with the file on the computer in a way that's more efficient and powerful than a **Graphical User Interface (GUI)**
- It provides functional improvements over Bourne Shell for both programming and interactive use
- To save the file with the extension of **.sh**



**Fig. 3.7 Bash**

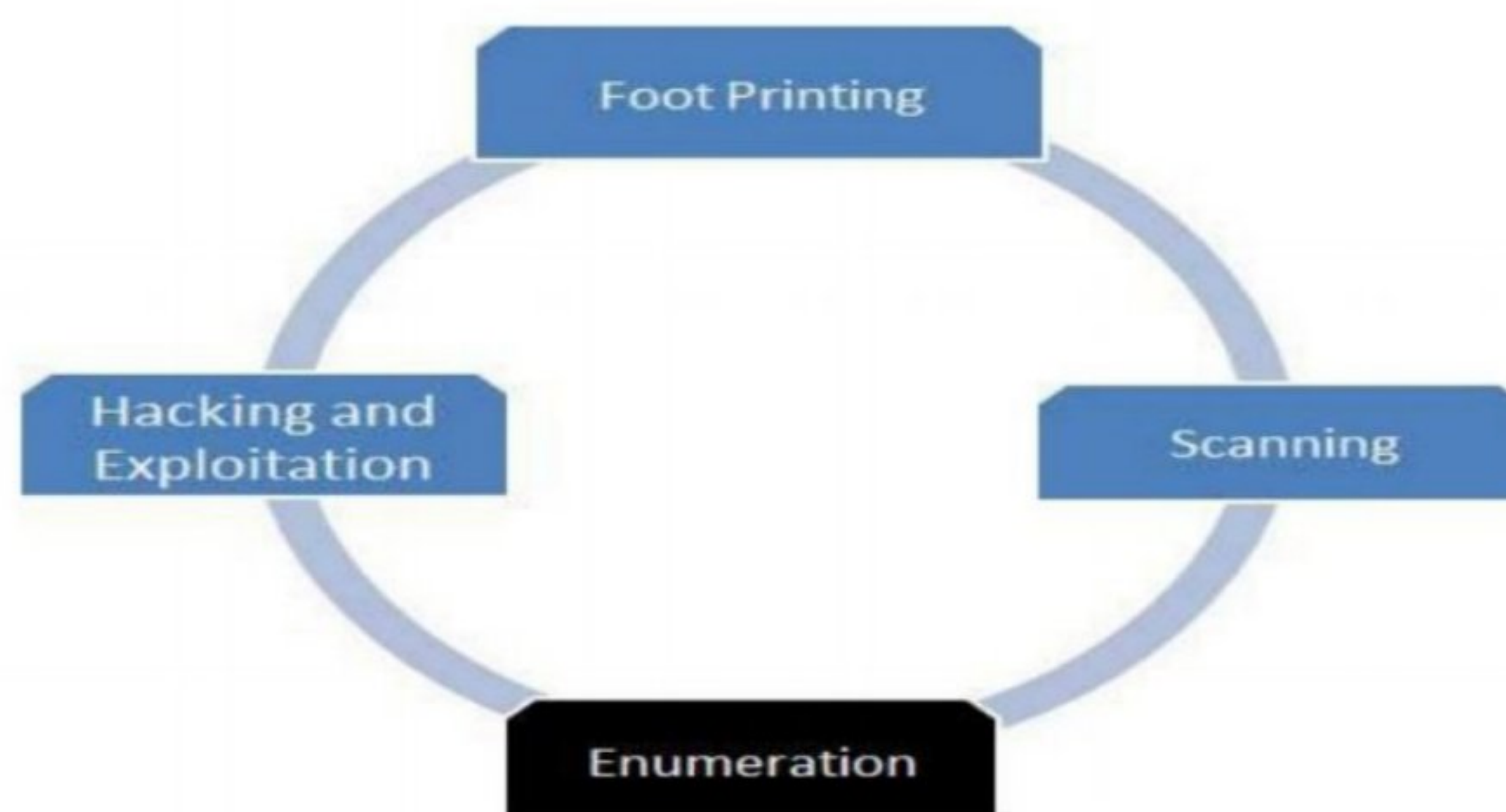


## CHAPTER 4

### DESCRIPTION OF THE PROPOSED SYSTEM

#### 4.1 Selected Methodology or proposed model

A component of “ethical hacking” for network security is networked scanning. Network enumeration may be carried out by certain penetration tests in an attempt to safeguard a software system. For network enumeration, choose any one tool, and then it asks you to type the IP address of the vulnerable machine. Once you completed typing of IP Address and then press enter it will give the result like the state of the port, vulnerability, operating system, services, how many ports are closed, and at last, it will display how long it takes for collecting that information.



**Fig. 4.1 Network Enumeration**

Nmap (Network Mapper) It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing. During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.



The NSE scripts can be categorized into several groups such as auth, broadcast, brute, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln. Each group contains a set of scripts that performs a specific task.

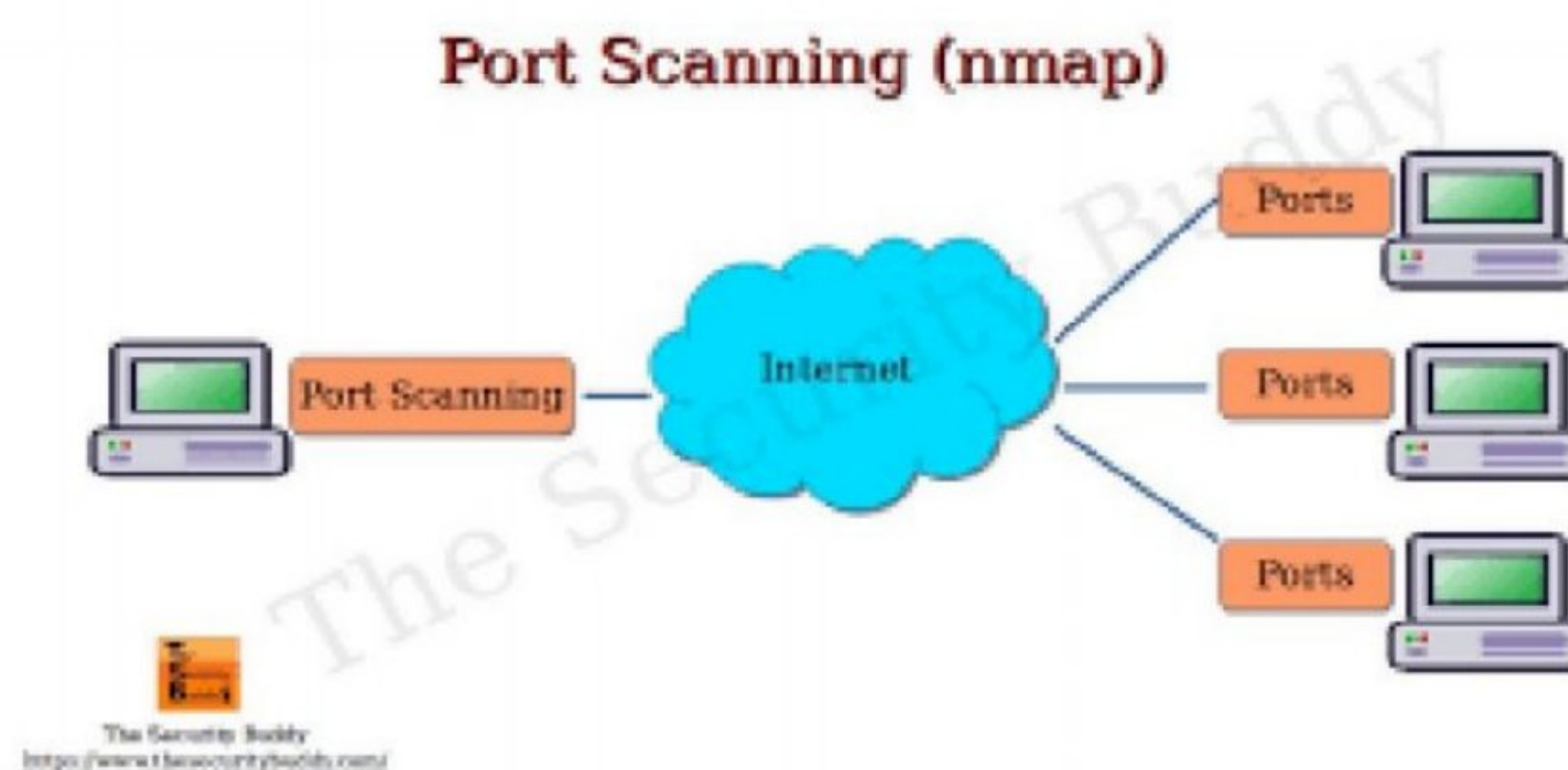
The Nmap Script Engine is a valuable tool for network administrators and security professionals who want to automate their network scanning and security testing tasks. It provides a flexible and extensible framework for developing custom scripts that can be used to detect and remediate security vulnerabilities in their networks.

## Advantages of NMAP

Nmap has a lot of advantages that make it different from other network scanning tools. Nmap is open-source and free to use.

Some other advantages are listed below.

- It is used for auditing network systems as it can detect new servers.
- It will search for subdomain and Domain Name System
- With the help of Nmap Scripting Engine (**NSE**), interaction can be made with the target host.
- It determines the nature of the service in the host and performs whether the host is a mail service or a web server.



**Fig. 4.2 Port Scanning nmap**

The **Nmap Scripting Engine (NSE)** is an incredibly powerful addition to Nmap, extending functionality quite considerably. NSE. It's the ability to let users write and share their own scripts, so you're not limited to relying on the Nmap default NSE



scripts. Nmap offers a variety of types of scans in order to scan a host for its open services. Used to identify services on a host, the operating system running on the host NSE scripts are great for drafting proof-of-concept code since the modules are written in Lua, a simple yet powerful language. NSE scripts must be coded in Lua language. It allows us to quickly program any task we have in mind with the help of the available NSE libraries. Its flexible syntax is easy to learn. API permits its Port scanning tool to take into account arguments specifying designate believable processes to be used during measurement. Browsers of the Command - line can write or distribute codes thanks to that too. it elevates Server well above typical fast and easy inspections into an even more automated, intricate one, including in space.

- Needed to handle specific tasks that cannot be done easily in Nmap in C++.
- Motivations for using Lua.
- NSE uses Lua to allow scripts to run against a host in parallel.
- Scripts use bindings to Nmap libraries for performance and access to networking facilities.
- It helps us to find the vulnerable, state, port, services, references, etc...

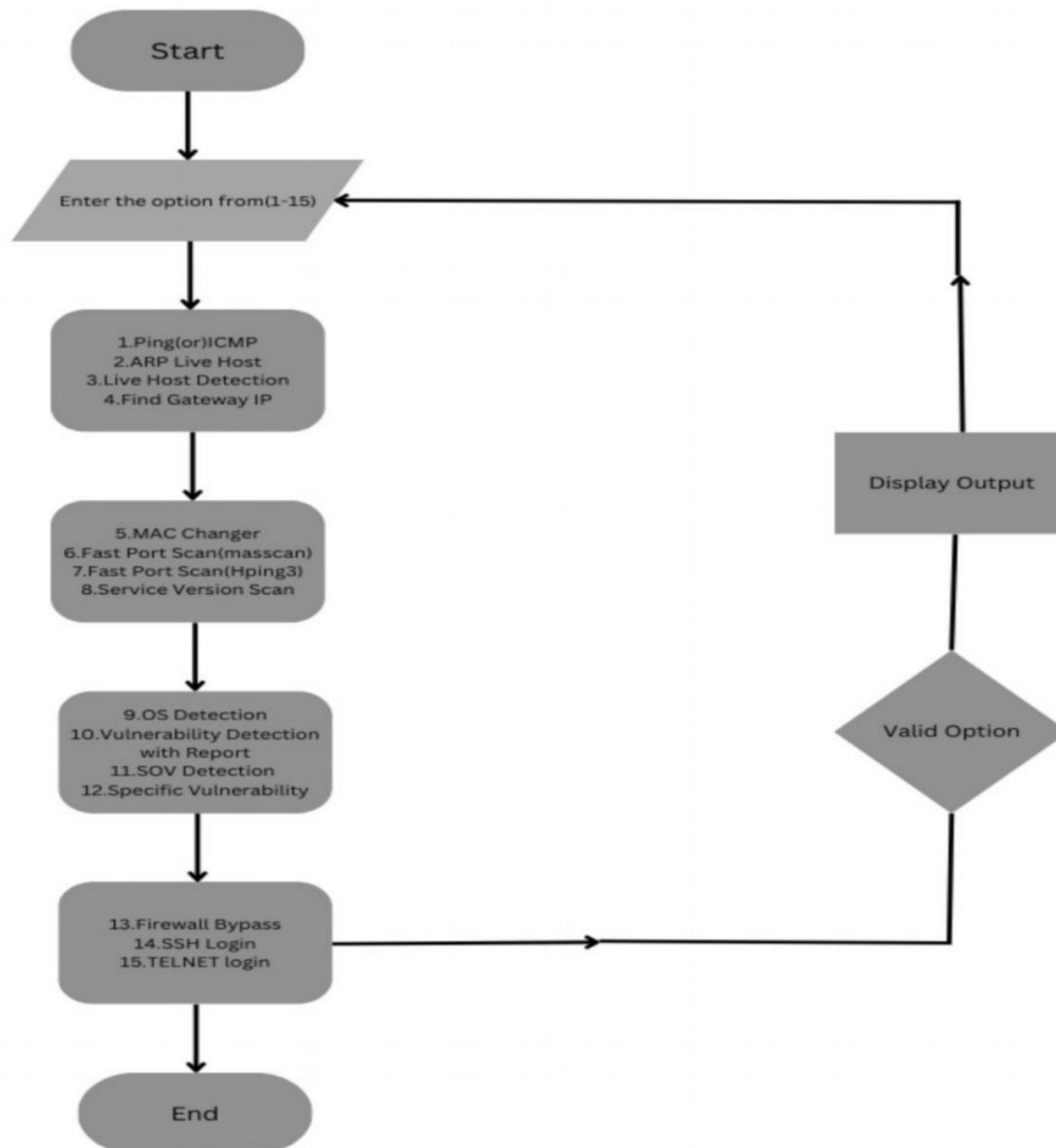
| NSE Script Rules              |                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Rule Name and Function Format | Description                                                                                                                        |
| prerule()                     | This rule is checked BEFORE nmap has started scanning any hosts. This is usually useful for discovery scripts.                     |
| hostrule(host)                | This rule is checked after each batch of hosts is scanned. This is useful if you have a script that only cares about hosts.        |
| portrule(host, port)          | This rule is checked after each batch of hosts is scanned.                                                                         |
| postrule()                    | This rule is checked after the scan has completed. This is useful if the script is looking to review the full results of the scan. |

To make life easier, the NSE library provides a helper called short port. This provides some simple helper functions that can make it easier to implement common rule checks and standardize these so we aren't constantly reinventing the wheel.



## 4.2 Architecture / Overall Design of Proposed System

N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network is a CLI (Command Line Interface) based Network Security Testing Tool, where It is Developed using Python3 & Bash. N3TU0N can work in Debian flavor of the Linux Operating System. N3PTU0N helps Network Security Professionals to enumerate Information about IP Address, MAC Address, Route through, Live Host Detection, Port Scanning, Service Version Detection, OS Detection, Vulnerability Detection, SOV (Service, OS, Vulnerability) Script, Firewall Bypass, FTP login, and Telnet login.





### 4.3 Description of software for implementation and testing plan of the proposed system

- Python3 is a computer programming language that is frequently used to create applications and websites, automate procedures, and analyze data.
- Python3 is not specialized for any particular issue and may be employed to develop a wide range of diverse programming.
- Python supports modules and packages, which encourages program modularity and code reuse.
- It is fully extensible as well as works well with other libraries and this language is perfectly suited to develop your tool.
- Its adaptability and complete novice-friendliness have elevated its position at the top of the list of languages for programming in practice nowadays.

### 4.4 PROJECT MANAGEMENT PLAN

Network Enumeration and Penetration Testing under an Organized Network contains fifteen tools there are:

- Ping
- ARP(Address Resolution Protocol)
- Live Host Detection
- Find Gateway's IP
- MAC Changer
- Fast Port Scan(masscan)
- Fast Port Scan(hping3)
- Service Version Scan
- OS Detection
- Vulnerability Detection with Report
- SOV Detection Scan
- Specific Vulnerability
- Firewall Bypass
- FTP Login
- TELNET Login



## CHAPTER 5

### IMPLEMENTATION

#### 5.1 Commands involved in the tool

##### 5.1.1 PING

Ping is a tool frequently used to detect a device's status on a network. ICMP is the basis of Ping. If the target device is available, it will respond with an ICMP echo when a Ping process command is given to it as an ICMP echo.



*Fig.5.1.1 Ping*

#### The Goal of Ping

Ping is used to send a test packet, also known as an echo packet, to a device in order to determine whether it can be reached and how long it takes for the packet to get there. There are two primary goals. Check the network latency between two devices and the network availability. Sending ICMP ping packets to the host is an easy approach to see if we have access to a specific host. However, this technique is only effective in networks that have ICMP and ping enabled. We are unable to receive a correct response if ICMP is deactivated.



### ***For example***

PING 192.168.133.129(192.168.133.129) 56(84) bytes of data.

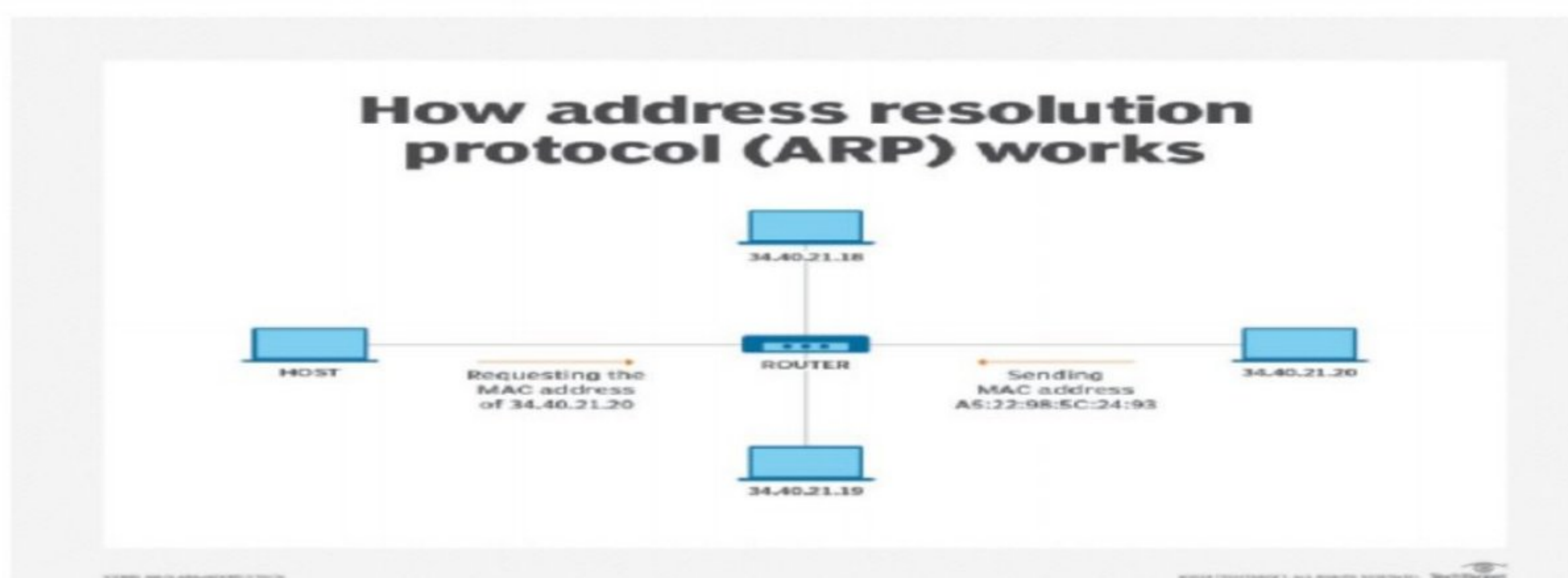
64 bytes from 192.168.133.129: icmp\_seq=1 ttl=64 time=1.21 ms

64 bytes from 192.168.133.129: icmp\_seq=2 ttl=64 time=0.781 ms

64 bytes from 192.168.133.129: icmp\_seq=3 ttl=64 time=0.858 ms

## **5.1.2 ARP (Address Resolution Protocol)**

Address Resolution Protocol, or ARP, is used to determine a device's MAC address from a known IP address. This indicates that the connect with the right already knows the IP location of the destination device but not its MAC address. You cannot interface with such a device in a local area network (Ethernet) without knowing its MAC address, hence the device's MAC address is necessary. Therefore, the Address Resolution Protocol aids in locating the destination device's MAC address.



***Fig.5.1.2 ARP***

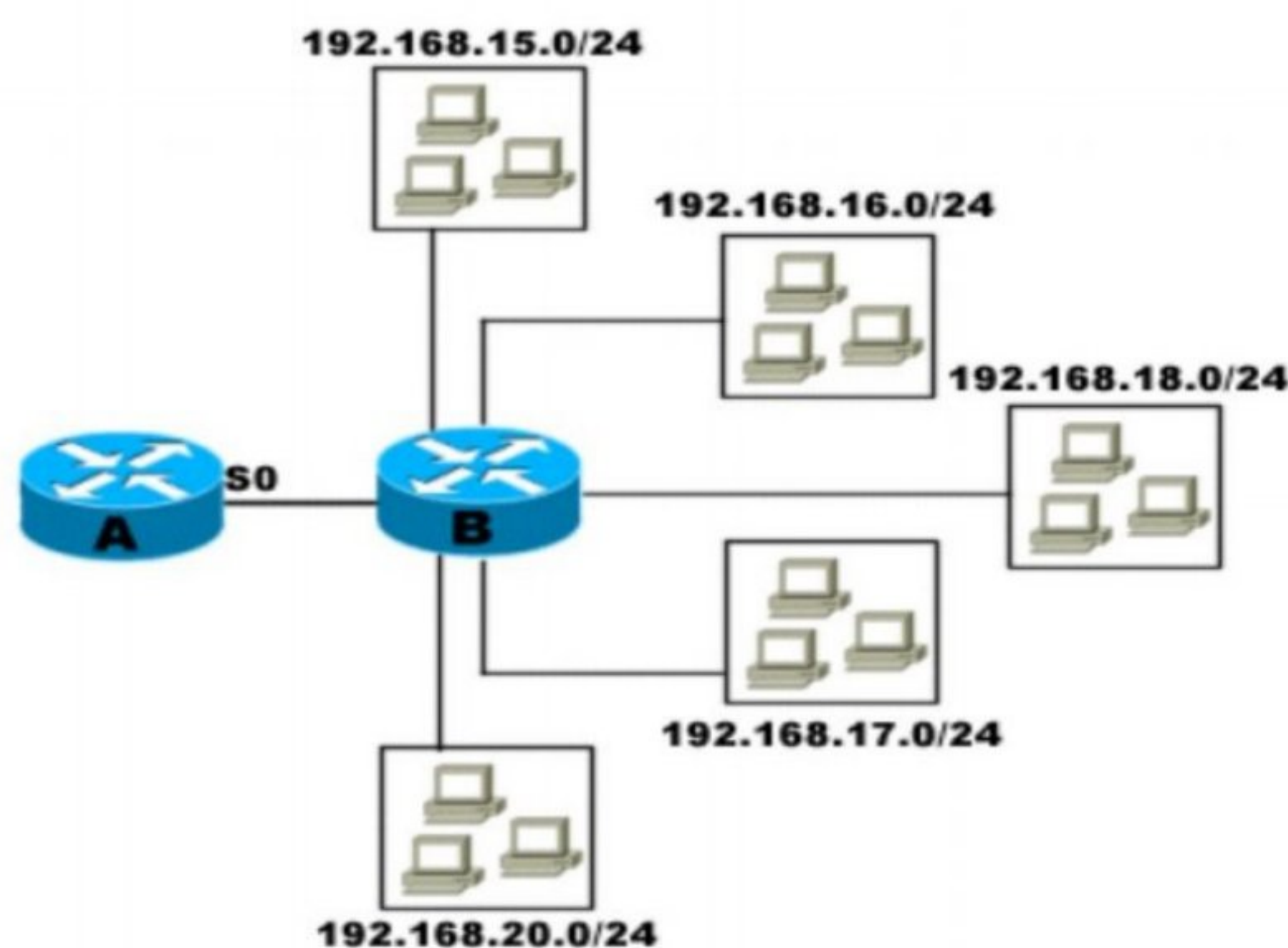
In an IPv4 Ethernet port, every operating system maintains an ARP cache. A host evaluates its ARP cache to check if the IP to MAC address translation already exists every time it requests a MAC address in order to send a packet to another computer in the LAN. A new ARP request is not required if it does. ARP is used in conjunction with the request for network addresses if the translation does not already exist. ARP transmits a request packet to every device on the LAN and queries whether any of them are utilising a specific IP address. When a device recognises the IP address as



being its own, it responds so that ARP can update the cache for later use and continue the communication. The Reverse ARP (RARP) protocol can be used by host machines to conduct discovery if they are unaware of their own IP address.

### 5.1.3 Live Host Detection

Live hosts detection is an essential tool for any ethical hacker or penetration tester. By using the `if config` command, you may specify the IP range to look for live hosts in. While penetration testers use live host discovery to find active targets in a network, system administrators commonly use it to count or monitor the number of active hosts. This recipe details how to find active hosts in a network using Nmap's ping scan. We will perform a ping scan on many probable live hosts in our network. Nmap will send a ping to every host in this radius to see if it is active. This tutorial will make use of `nmap`.



**Fig.5.1.3 Live Host Detection**

Finding the live hosts on the networks is our responsibility as network engineers or penetration testers. Today, we'll look at how to locate active hosts on the internet. To locate the active hosts on the network, we'll utilise the `nmap` utility. An open-source command-line programme for network research and security audits is called Nmap (network mapper). Using raw IP packets, Nmap is used to scan networks. To locate



active hosts on the network for this post, we will use the nmap tool.

### 5.1.4 Find Gateway's IP

A gateway is a network node that serves as an access point to another network, frequently including not just a change in addressing but also a different networking protocol. A router merely distributes packets between networks with different network prefixes, as it is more clearly described. A routing table, which is part of the networking software stack on each computer, lists which network router is in charge of forwarding traffic to a specific range of addresses and which interface is used for transmission. In the event that none of these forwarding rules work for a particular destination address, the default gateway is chosen as the router of last resort. Use the route command to specify the default gateway in order to configure the routing table and default route for the node.

- **Open a terminal and use the following command**

`ip route(command)`

- **You should see an output like this**

```
default via 192.168.133.2 dev eth0 proto dhcp src 192.168.133.128 metric
100
```

```
192.168.133.0/24 dev eth0 proto kernel scope link src 192.168.133.128
metric 100
```

```
0
```

Focus on the line that starts with default. This will give the default gateway IP.

- **Focus on the line that starts with default. This will give the default gateway IP.**

`Ip route | grep default`

**This will just give the default gateway IP in the output**

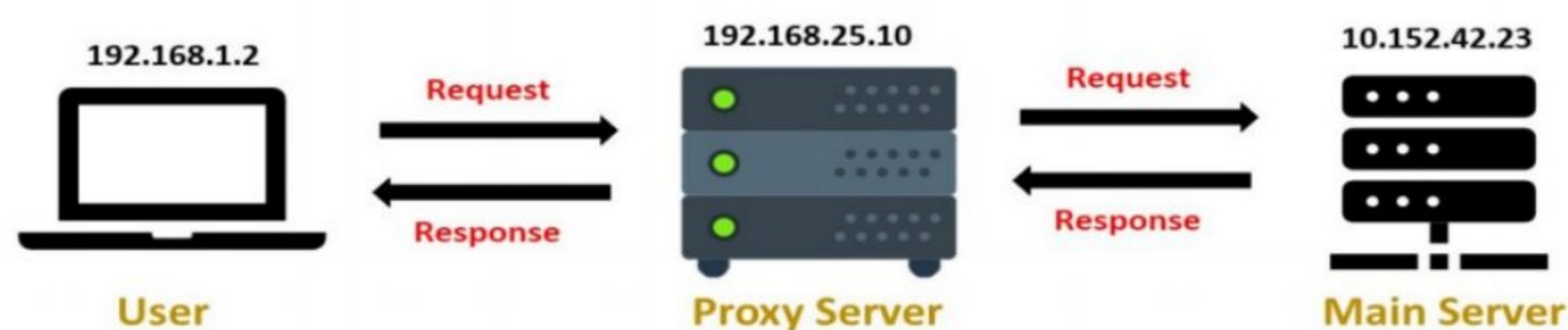
default via 192.168.133.2 dev wlp1s0 proto dhcp metric 100 And as you can see, 192.168.133.2 is the default gateway IP in my case.



### 5.1.5 MAC Changer

The manufacturer assigns a different MAC address to each device. When you are connected to the router, this MAC address is recorded in the router's table. Every device has a specific MAC address, which makes it possible to identify the system or device that the hacker used, thus revealing your identity.

You can momentarily alter your MAC address to prevent being recognized by it. Here is where ethical hacking using MacChanger is possible. Until the device is rebooted, an utility called MacChanger will alter the MAC address of that device to a false one.



*Fig.5.1.5 MAC Changer*

### The Goal of MAC Changer

- Detect a network device on the Internet.
- A physical network device's unique identification.
- Control access to shared network resources
- Supply a local area network routing address (LAN)

### 5.1.6 Fast Port Scan (masscan)

Masscan has been available for a while, and pentesters from around the world



already use it. It is a reconnaissance tool with a 10 million packets per second maximum rate of transmission. It makes use of a unique TCP/IP stack and asynchronous transmission. As a result, distinct threads are used for packet transmission and reception. Masscan can be utilised to speedily enumerate a huge number of hosts. The tool's creator even asserts that it can scan the entire internet in just six minutes. Due to its high rate of transmission, it can also be utilised for stress testing.

## Features

- Ultra-fast port scanning: capable of sending 10M packets per second (capable; NIC and PF RING drivers required)
- output in Nmap format
- Target settings and specifications in Nmap style
- grabbing a banner
- Fundamental Weakness Like Heart bleed scanning, custom TCP/IP stack

The most fundamental scanning procedure in masscan is this one. This allows you to scan any IPs. You can specify an IP range (192.168.133.129) like you would in nmap in place of the subnet value.

### 5.1.7 Fast Port Scan (hping3)

A network tool called hping3 may issue personalised TCP/IP packets and show target responses just like the ping software does with ICMP responses. Hping3 can be used to transfer files that are enclosed in supported protocols and can manage fragmentation, arbitrary packet body and size.

## Use of hping3 for UDP and TCP Packet Crafting

- Overview of Packet Crafting Packet crafting is a technique that allows you to find vulnerabilities or entry points into a target network.



- Basics of hping3 Open the Terminal after logging in to Kali Linux.
- UDP packet crafting To perform a UDP packet crafting in the target machine, type:
- Send TCP SYN Request Launch the Wireshark on Windows machine again and leave it running.

### 5.1.8 Service Version Scan

A type of network investigation known as a service version scan includes probing a target system or network to find the versions of services that are active on open ports. This can be helpful for a number of reasons, including determining possible vulnerabilities that might be present in out-of-date software versions and determining the system or network's overall security posture.

Service version scans can be carried out using a number of programs, including Nmap, Masscan, and Metasploit. To determine the version information of the services operating on a target system, these tools typically combine port scanning and banner grabbing methods.

If any current software versions have any known flaws, they can be identified by looking at the scan's results. Just keep in mind that you should only scan service versions on networks or computers where you have been granted permission to do so. Unauthorized scanning is possibly illegal and might result in severe consequences.

### 5.1.9 OS Detection

An essential component of internet security is OS detection. When carrying out security operations like vulnerability analyses, penetration testing, and breach detection, it can be useful to determine the operating system of the target system. For instance, a hacker needs to be aware that the target machine is running Windows in order to take advantage of a specific vulnerability in the Windows operating system. On the basis of the known vulnerabilities related to that operating system, a security analyst can use OS detection to ascertain whether the target system is susceptible to a particular assault.



In addition to this, OS detection can also help in identifying the type of network devices, such as routers and firewalls, which are running on a specific operating system. This information can be used to tailor specific attacks that target the vulnerabilities associated with that operating system, and thus improve the overall effectiveness of the attack. Overall, OS detection is an important tool in the arsenal of any cyber security professional, and it should be used to aid in the detection and prevention of potential security threats.

#### **5.1.10 Vulnerability Detection with Report**

An important component of cyber security is vulnerability detection, which entails locating flaws in applications, networks, and computer systems that might be exploited by hackers. It is a proactive strategy that enables organizations to find weaknesses before attackers take advantage of them.

It is crucial to notify the appropriate parties as soon as a weakness is discovered so that it can be fixed right away. The vulnerability's specifics, such as its seriousness, the affected systems, and the possible consequences if it is exploited, should be described in the report. Recommendations for mitigating the vulnerability, such as deploying a patch or updating software, should also be included in the report. The vulnerability report should be written in plain, simple English that both technical and non-technical stakeholders can understand. It should be accompanied by any supporting documentation that can help to verify the vulnerability, such as screenshots or log files.

It may be necessary to disclose vulnerabilities to external stakeholders, such as software vendors or government organizations, in addition to the appropriate individuals within the organization. This can make it more likely that the vulnerability will be addressed broadly and that the required precautions will be taken to defend against potential attacks.

#### **5.1.11 SOV Detection Scan (Share of Voice)**

A Share of Voice (SOV) Detection Scan is a valuable tool in cyber security to measure the visibility of a brand, product, or specific cyber security topic against competitors or related topics. To conduct a SOV Detection Scan, the first step is to



define the cyber security scope, followed by identifying competitors and collecting data on the number of mentions for the brand or topic and its competitors within a specified time frame. Once the data is collected, the SOV can be calculated, and the results can be analyzed to identify areas for improvement and develop strategies to increase visibility and awareness of the cyber security topic. In summary, the SOV Detection Scan is a crucial tool that enables cyber security professionals to gain insights into how their cyber security efforts are perceived and develop strategies to stay ahead of their competitors.

## **The Goal of SOV Detection Scan**

The primary objective of conducting a SOV Detection Scan is to identify and validate all the systems and assets that belong to an organization. The scan involves detecting all the network infrastructure, applications, servers, and devices that are currently in use within the organization. The main purpose of the scan is to ensure that the organization has an accurate record of its assets and systems and that no unauthorized or unaccounted-for devices or systems could potentially compromise the security of the organization. By performing a SOV Detection Scan, the organization can enhance its security posture and become more equipped to defend itself against cyber security threats.

### **5.1.12 Specific Vulnerability**

In the setting of cyber security, a weakness or flaw in a system, piece of software, or network that can be used by an attacker to compromise the security of the system is referred to as a specific vulnerability. Coding errors, setup issues, or design flaws can all lead to vulnerabilities. An attacker may be able to execute malicious code, get access to private data, or harm the system in other ways by exploiting a weakness. It's essential to locate and address vulnerabilities as soon as possible to thwart attacks and minimize potential harm.

Vulnerability management, which entails regularly scanning systems and networks for potential flaws, prioritizing them according to their severity, and implementing patches and other security measures to reduce the risks, is an essential part of cyber security. This makes it simpler to keep the safety and defense of systems and



networks against potential cyber-attacks.

### 5.1.13 Firewall Bypass

In cyber security, the term "bypassing a firewall" refers to getting through or getting beyond the security procedures that a firewall implements in order to gain unauthorized access to a network or system. This is typically seen as malicious behavior and is frequently connected to hacking or other online activities. Network security is not complete without firewalls, which help guard against viruses, illegal access, and other online dangers. The originating IP address, port number, or protocol are just a few examples of predefined rules that can be used to configure firewalls to block incoming and outgoing traffic.

There are many ways to get over firewalls, including:

1. Port scanning: The process of looking for open ports that the firewall has not blocked in order to establish a connection.
2. Tunneling: Forgoing a firewall by establishing an encrypted tunnel between two systems.
3. Application-layer attacks: gaining access to the network by taking advantage of flaws in apps that are permitted via the firewall.
4. DNS tunneling: Bypassing the firewall and smuggling data over DNS traffic.

Remember that trying to get past a firewall is against the law and can have serious repercussions. To defend against such attacks, organizations must put in place strong security measures and often update their firewall configurations.

### 5.1.14 FTP Login

The FTP (File transfer Protocol) protocol is frequently used to send files over the internet between servers and clients. However, if not correctly configured or secured, using FTP can also present security risks. The possibility for unauthorised access to sensitive data is one of the main security risks connected with FTP. If the FTP login



procedure is not properly secured, this is especially true.

Strong authentication procedures must be in place in order to reduce the dangers related to FTP login. This might entail using MFA (multi-factor authentication) or mandating the use of strong passwords that are updated regularly. Additionally, it is advised to switch from plain-text FTP to private FTP protocols like SFTP or FTPS (FTP over SSL/TLS).

The general configuration of the FTP server as well as the FTP login procedure may contain security vulnerabilities that can be found through routine security audits and vulnerability assessments.

### **5.1.15-TELNET Login**

TELNET is a protocol that connects two machines together over a network. Because TELNET transmits information in plain text, which can be intercepted and read by anyone with access to the network, using it for remote login can present a security risk. This means that your username and password will be transmitted in clear text if you use TELNET to log in to a remote system, making it simple for someone with malicious purpose to intercept your login information.

It is advised, in terms of cyber security, to steer clear of TELNET and instead use more safe protocols like SSH (safe Shell). Attackers will find it much harder to intercept and read confidential information like login credentials thanks to SSH's encryption of all data transmitted between the client and the server.

To reduce the chance of interception, it is advised to use a private network or VPN (Virtual Private Network) if you must use TELNET for remote login. Additionally, to help prevent unauthorized access to your networks, you should always use strong passwords and change them frequently.



## CHAPTER 6

### Result and Discussions

In general, the results of network enumeration and penetration testing can provide valuable insights into the security posture of a network. This information can be used to identify areas for improvement and strengthen the network's security controls. It is important to note that network enumeration and penetration testing should only be performed by trained professionals with the appropriate permissions and authorizations. Unauthorized or unprofessional testing can result in network disruptions, data breaches, and legal consequences.



## **CHAPTER 7**

### **CONCLUSION**

#### **7.1 Conclusion**

Everything is going online on the internet as a result of the ongoing digital revolution, and as we all know, the web is not an extremely secure protocol. As a result, precautions must be taken to protect the authenticity as well as the secrecy of the info. To expand reports of information security, cyber threats, as well as information leakage, researchers should ensure the security of our vital information. A vulnerability assessment is a complete and accurate method for detecting security vulnerabilities. This study provides crucial details about the stage as well as the significance of the testing process. System testing is divided into three stages: information gathering, scanning, and frailty evaluation. Each of the aforementioned phases can be done automatically utilizing Nmap and other tools.

#### **7.2 Future Scope**

In the future. According to a technical report, the open source intelligence (OSINT) market will develop at a significant rate between 2020 and 2026. The increase in the availability of open-source data, as well as rising cyber risks, is expected to assist future growth. Analysts predict that perhaps the huge amount of information dissemination will have a critical effect on the market performance from 2020 to 2026. During the forecast period, the market will be assisted by increased accessibility to public information and advancements in technology. Over the course of time. OSINT would be developed to take the entire details of an individual person which will gather utilizing extraneous APIs, Google Eavesdropping, phone books, and also web crawlers, collect appropriate data such as nation, quick response code, as well as transmission OSINT efficient process. Additionally, there have been a few merits of this system which are included below the prospective improvements.



## REFERENCE

- [1] Rodney Rohr Mann, Rd. Mark Patton, Rd. Hsinchun Chen, "Anonymous Port Scanning", in proceedings of IEEE conference, September 2016.
- [2] W. Lootah, W. Enck, and P. McDaniel, "TARP: Ticket-based Address Resolution Protocol," in IEEE Computer Society, vol. 51, no. 15, 2007, pp. 4322-4337.
- [3] S Jana and S Kasera, "On Fast and Accurate Detection of Unauthorised Wireless Access Points Using Clock Skews", IEEE Transactions on Mobile Computing, Vol. 9, No.3, March 2010.
- [4] S. Hijazi and M. S. Obaidat, "A new detection and prevention system for ARP attacks using static entry," IEEE Syst. J., vol. 13, no. 3, pp. 2732-2738, Sep. 2019.
- [5] D. Springall, Z. Durumeric, J. Halderman, 'FTP: The Forgotten Cloud', 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 1-3, 2016.
- [6] Plummer: An Ethernet addresses resolution protocol. RFC 826 (1982).
- [7] <https://nmap.org/book/man-briefoptions.htm>.
- [8] <https://www.linkedin.com/learning/paths/prepare-for-comptia-network-plus-n10-007-certification>.
- [9] Gordon Lyon, "Nmap Network Scanning" Sunnyvale, CA: Insecure.com, LLC, 2002 p.129
- [10] Huitema, C. (1997), IPv6, The new Internet Protocol.
- [11] Unknown Author, "Kali Linux Tutorial: Setting Up Proxy Chains + Tor For Anonymity , Security" <http://www.picateshackz.com/2015/05/kali-linux-tutorial-setting-up-html>.
- [12] Nmap cheats sheet see-security hacking defined experts by Nativ.y, 2015.
- [13] Lyon Gordon NMAP-the Network Mapper-free security lancer, 2017.
- [14] Ethical hacking and penetration guide by Baloch R, 2017.
- [15] A guide to penetration testing by Tang A., Network security, 2014.



## APPENDIX

### A. SOURCE CODE

#### LOGO

```
1 #N3PTU0N
2 #Color
3 grey = "\033[1;37m"
4 red = "\033[1;31m"
5 green = "\033[1;32m"
6 yellow = "\033[1;33m"
7 cyan = "\033[2;96m"
8 purple = "\033[3;35m"
9
10
11 def main_menu():
12
13     print("""
14
15     """)
16     print(grey + " ;0000. xk0d          l000000ko. k000000000 0000 d000," + cyan + " .,;;,. " + grey + "x000x 'k00," )
17     print(grey + " lMMMMM MMMO          xMMMMMMMMMc MMMMMMMMMMM MMW OMW:" + cyan + " .:c::;;,. " + grey + "KMMMM: :MMW;" )
18     print(grey + " cMMMMM: MMWk" + cyan + " .:ll, " + grey + " xMMMXOMMMMM.MMMMMMMMMMM MMW OMW:" + cyan + " .oolcc::;'.. " + grey
19     + "KMMMM ;MM," )
20     print(grey + " cMMMMMM MMWx" + cyan + " .XMMMMMM' " + grey + " dMMWl .MMW; KMMW MMW OMW;" + cyan + " clollllcc::;'.. " + grey
21     + "OMMMMMd ;MM," )
22     print(grey + " :MMMMMMo MMWx" + cyan + " .MMMMMMX " + grey + " oMMMc MMW; OMW MMW kMM;" + cyan + " 'lcccc::;;;' " + grey
23     + "OMMMMMM ;MM," )
24     print(grey + " :MMMMMM.MMMd" + cyan + " 0x:OMMMW " + grey + " oMMMc ;MMW. OMW MMW kMM," + cyan + " :cc::;'..... " + grey
25     + "OMMMMMM,MM," )
26     print(grey + " ;MM'MMMMMMMo" + cyan + " .lMMMd " + grey + " lMMMXOMMMd OMW MMW xMM," + cyan + " 'lllllc::;' " + grey
27     + "OMMlMMMMMM." )
28     print(grey + " ,MM dMMMMMMo" + cyan + " oMMWx " + grey + " lMMMMMMMd OMW MMW xMM," + cyan + " :lllcc:ccc::;' " + grey + "kMMO
29     xMMMMMM." )
30     print(grey + " ,MM XMMMMMo" + cyan + " dMMMMW: " + grey + " lMMOxd:. OMW MMW OMW'" + cyan + " .cc::;'...'.. " + grey
31     + "kMMO ,MMMMM." )
32     print(grey + " ;MM. ;MMMMMd" + cyan + " ,odMMW " + grey + " lMMW: OMW MMWxkKMMW " + cyan + " clcccc::;'.... " + grey + "OMWk
33     OMMMMM." )
34     print(grey + " cMMW. OMMMWx" + cyan + " . .MMW " + grey + " dMMMc KMMW :MMMMMMMMMc " + cyan + " ;::;::;' " + grey
35     + "OMWx .MMMMM'" )
36     print(grey + " cWWW. .WWWx" + cyan + " 'MMMMMMO " + grey + " dMMWc XMMW ,OMMMWd, " + cyan + " .,,'..... " + grey + "KMMX
37     lWWW'" )
38     print(grey + " " + cyan + " .MMMMMM " + grey + " ... " + cyan + " .... " )
39     print(grey + " " + cyan + " oxkxl' " )
40
41     print("*****")
42     print("""
43     Created By : RAMANAN B , SRIRANGAPRASATH V
44     Register No : 39120091 , 39120121
45     Email ID : ramanantssr3032@gmail.com
46                srirangaprasath@gmail.com
47     Purpose : Network Enumeration and Penetration Testing Under an Organized Network
48     """)
49
50     print("\033[1;31m
51     [**] Available Scripts""")
52
53     print("\033[2;34m
54     [1] Ping
55     [2] ARP (ARP Live Host)
56     [3] Live Host detection
57     [4] Find Gateway IP
58     """)
```



```

49 [5] MAC Changer
50 [6] Fast Port Scan (masscan)
51 [7] Fast Port Scan (hping3)
52 [8] Service Version Scan
53 [9] OS Detection
54 [10] Vulnerability Detection with Report
55 [11] SOV Detection Scan
56 [12] Specific vulnerability
57 [13] Firewall Bypass
58 [14] FTP Login
59 [15] TELNET Login
60 """)
61
62 n3ptu0n()
63
64 def n3ptu0n():
65
66     from Ping import ping
67     from ARP import arp
68     from LiveHostDetect import fping
69     from GatewayIP import iproute
70     from MacChanger import macchanger
71     from FastPortMasscan import fastportmasscan
72     from FastPortHping3 import fastporthping3
73     from OSDetection import osdetection
74     from ServiceVersionDetection import ServiceversionDetection
75     from VulnerabilityDetection import VulnerabilityDetection
76     from SOVDetection import SOVDetect
77     from SpecificvulnerabilityDetection import SpecificvulnerabilityDetection
78     from FirewallBypass import Firewallbypass

```

```

79     from FTPLogin import ftplogin
80     from Telnetlogin import telnetlogin
81
82
83     inp = (input(green + " [+] Enter The Option from [1-15] OR [x] to Exit → "))
84     if (inp == '1'):
85         ping()
86
87     elif (inp == '2'):
88         arp()
89
90     elif (inp == '3'):
91         fping()
92
93     elif (inp == '4'):
94         iproute()
95
96     elif (inp == '5'):
97         macchanger()
98
99     elif (inp == '6'):
100         fastportmasscan()
101
102     elif (inp == '7'):
103         fastporthping3()
104
105     elif (inp == '8'):
106         ServiceversionDetection()
107
108     elif (inp == '9'):

```



```

109     osdetection()
110
111     elif (inp == '10'):
112         VulnerabilityDetection()
113
114     elif (inp == '11'):
115         SOVDetect()
116
117     elif (inp == '12'):
118         SpecificvulnerabilityDetection()
119
120     elif (inp == '13'):
121         Firewallbypass()
122
123     elif (inp == '14'):
124         ftplogin()
125
126     elif (inp == '15'):
127         telnetlogin()
128
129
130
131
132
133
134     elif (inp == 'x'):
135         exit()
136
137     elif (inp == 'ls'):
138         print(green + ""

```

```

140
141         [1] Ping
142         [2] ARP (ARP Live Host)
143         [3] Live Host detection
144         [4] Find Gateway's IP
145         [5] MAC Changer
146         [6] Fast Port Scan (masscan)
147         [7] Fast Port Scan (hgping3)
148         [8] Service Version Scan
149         [9] OS Detection
150         [10] Vulnerability Detection with Report
151         [11] SOV Detection Scan
152         [12] Specific vulnerability
153         [13] Firewall Bypass
154         [14] FTP Login
155         [15] TELNET Login
156
157         """)
158     else:
159         print(red + "Enter an valid option")
160
161     while True:
162         n3ptu0n()
163
164
165
166 if name == " main ":

```



## Ping

```
#Ping
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"

def ping():

ip = input("\033[2;35m [+] IP >> ")
print(os.system("sudo ping "+ip))

if __name__=="__main__":
ping()
```

## ARP Live Host:

```
#ARP
Import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"

def arp():

print(os.system("sudo arp "))

if __name__=="__main__":
arp()
```

## Live Host Detection:

```
#FPing
import os

#Color
```



```

grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"

def fping():

ipcidr = input("\033[2;35m [+] Enter IP/CIDR ~> ")
print(os.system("sudo fping -a -g "+ ipcidr +"> Live.txt"))
print(os.system("clear"))
print(os.system("cat Live.txt"))

if __name__=="__main__":
    fping()

```

### Find Gateway IP:

```

#iproute
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"

def iproute():

print(os.system("sudo ip route"))

if __name__=="__main__":
    iproute()

```

### MAC Changer:

```

#MacChanger
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"

```



```
cyan= "\033[0;96m"
purple= "\033[0;35m"
```

```
def macchanger():
```

```
    mac = input(green+" [+] Enter MAC Address ~> ")
    interface = input(green+" [+] Enter the Interface ~> ")
    print(os.system("sudo ifconfig "+ interface +" down"))
    print(os.system("sudo macchanger -m "+ mac +" "+ interface))
    print(os.system("sudo ifconfig "+ interface +" up"))
```

```
if __name__=="__main__":
    macchanger()
```

### **Fast Port Scan (masscan):**

```
#Massscan
import os
```

```
#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple= "\033[0;35m"
```

```
def fastportmasscan():
```

```
    ip = input("\033[2;35m [+] Enter IP ~> ")
    print(os.system("sudo masscan "+ip+" -p0-65535 --max-rate 100000"))
```

```
if __name__=="__main__":
    fastportmasscan()
```

### **Fast Port Scan (hping3):**

```
#Hping3
import os
```

```
#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple= "\033[0;35m"
```



```
def fastporthping3():
```

```
    ip = input("\033[2;35m [+] Enter IP ~> ")
    print(os.system("sudo hping3 --scan 0-65535 -S "+ ip))
```

```
if __name__=="__main__":
    fastporthping3()
```

### **Service Version Scan:**

```
#ServiceversionDetection
import os
```

```
#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"
```

```
def ServiceversionDetection():
```

```
    ip = input("\033[2;35m [+] Enter IP ~> ")
    print(os.system("sudo nmap -sV -Pn --min-rate 300 "+ ip))
```

```
if __name__=="__main__":
    ServiceversionDetection()
```

### **OS Detection:**

```
#Os detection
import os
```

```
#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"
```

```
def osdetection():
```

```
    ip = input("\033[2;35m [+] Enter IP ~> ")
```



```
print(os.system("sudo nmap -O -T 5 "+ip ))
```

```
if __name__=="__main__":  
    osdetection()
```

### **Vulnerability Detection with Report:**

```
#vulnDetect  
import os  
  
#Color  
grey = "\033[1;37m"  
red = "\033[1;31m"  
green = "\033[1;32m"  
yellow = "\033[1;33m"  
cyan= "\033[0;96m"  
purple="\033[0;35m"  
  
def VulnerabilityDetection():  
  
    ip = input("\033[2;35m [+] Enter IP ~> ")  
    print(os.system("sudo nmap --script=vuln "+ ip))  
  
if __name__=="__main__":  
    VulnerabilityDetection()
```

### **SOV Dectection Scan:**

```
#SOVDetect  
import os  
  
#Color  
grey = "\033[1;37m"  
red = "\033[1;31m"  
green = "\033[1;32m"  
yellow = "\033[1;33m"  
cyan= "\033[0;96m"  
purple="\033[0;35m"  
  
def SOVDetect():  
  
    ip = input("\033[2;35m [+] Enter IP ~> ")  
    print(os.system("sudo nmap -sV -n -v -Pn -p- -T4 "+ip+" -A --open"))  
  
if __name__=="__main__":  
    SOVDetect()
```



### Specific Vulnerability:

```
#Specific vulnerability
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"

def SpecificvulnerabilityDetection():

    ip = input("\033[2;35m [+] Enter IP ~> ")
    script = input("\033[2;35m [+] Enter Script ~> ")
    print(os.system("sudo nmap --script="+script+" "+ ip))

if __name__=="__main__":
    SpecificvulnerabilityDetection()
```

### Firewall Bypass:

```
#Firewallbypass
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan= "\033[0;96m"
purple="\033[0;35m"

def Firewallbypass():

    ip = input("\033[2;35m [+] Enter IP ~> ")
    print(os.system("sudo nmap -sF -p1-65535 -T4 "+ ip))

if __name__=="__main__":
    Firewallbypass()
```



## FTP Login:

```
#FTPLOGIN
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan = "\033[0;96m"
purple = "\033[0;35m"

def ftplogin():

    ip = input("\033[2;35m [+] Enter IP ~> ")
    user = input("\033[2;35m [+] Enter USER ~> ")
    print(os.system("sudo ftp "+user+"@"+ ip))

if __name__=="__main__":
    ftplogin()
```

## TELNET Login:

```
#telnetLOGIN
import os

#Color
grey = "\033[1;37m"
red = "\033[1;31m"
green = "\033[1;32m"
yellow = "\033[1;33m"
cyan = "\033[0;96m"
purple = "\033[0;35m"
def telnetlogin():

    ip = input("\033[2;35m [+] Enter IP ~> ")
    print(os.system("sudo telnet "+ ip))

if __name__=="__main__":
    telnetlogin
```



## B. SCREENSHOTS

### 1. PING

```
[+] Enter The Option from [1-16] OR [x] to Exit → 1
[+] IP >> 192.168.133.129
PING 192.168.133.129 (192.168.133.129) 56(84) bytes of data.
64 bytes from 192.168.133.129: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.168.133.129: icmp_seq=2 ttl=64 time=0.781 ms
64 bytes from 192.168.133.129: icmp_seq=3 ttl=64 time=0.858 ms
64 bytes from 192.168.133.129: icmp_seq=4 ttl=64 time=0.810 ms
64 bytes from 192.168.133.129: icmp_seq=5 ttl=64 time=0.848 ms
64 bytes from 192.168.133.129: icmp_seq=6 ttl=64 time=0.885 ms
64 bytes from 192.168.133.129: icmp_seq=7 ttl=64 time=0.992 ms
64 bytes from 192.168.133.129: icmp_seq=8 ttl=64 time=0.718 ms
64 bytes from 192.168.133.129: icmp_seq=9 ttl=64 time=0.859 ms
64 bytes from 192.168.133.129: icmp_seq=10 ttl=64 time=0.868 ms
64 bytes from 192.168.133.129: icmp_seq=11 ttl=64 time=0.912 ms
64 bytes from 192.168.133.129: icmp_seq=12 ttl=64 time=0.649 ms
^C
— 192.168.133.129 ping statistics —
12 packets transmitted, 12 received, 0% packet loss, time 11024ms
rtt min/avg/max/mdev = 0.649/0.865/1.209/0.134 ms
0
[+] Enter The Option from [1-16] OR [x] to Exit → █
```

### 2. ARP(Address Resolution Protocol)

```
[+] Enter The Option from [1-16] OR [x] to Exit → 2
Address           HWtype  HWaddress      Flags Mask    Iface
192.168.133.254    ether   00:50:56:e8:74:88  C             eth0
192.168.133.129    ether   00:0c:29:80:81:71  C             eth0
192.168.133.2      ether   00:50:56:ec:85:19  C             eth0
0
[+] Enter The Option from [1-16] OR [x] to Exit → █
```

### 3. Live Host Detection

```
0
192.168.133.2
192.168.133.128
192.168.133.129
0
[+] Enter The Option from [1-16] OR [x] to Exit → █
```



## 4. Find Gateway's IP

```
[+] Enter The Option from [1-16] OR [x] to Exit → 4
default via 192.168.133.2 dev eth0 proto dhcp src 192.168.133.128 metric 100
192.168.133.0/24 dev eth0 proto kernel scope link src 192.168.133.128 metric 100
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```

## 5. MAC Changer

```
[+] Enter The Option from [1-15] OR [x] to Exit → 5
[+] Enter MAC Address → 00:0c:29:63:a6:95
[+] Enter the Interface → lo
0
Current MAC: 00:00:00:00:00:00 (XEROX CORPORATION)
Permanent MAC: 00:00:00:00:00:00 (XEROX CORPORATION)
New MAC: 00:0c:29:63:a6:95 (VMware, Inc.)
0
0
[+] Enter The Option from [1-15] OR [x] to Exit →

(kali@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:0c:29:63:a6:95 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
        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 00:0c:29:63:a6:95 brd ff:ff:ff:ff:ff:ff
    inet 192.168.133.128/24 brd 192.168.133.255 scope global dynamic noprefixroute eth0
        valid_lft 1668sec preferred_lft 1668sec
    inet6 fe80::96ec:6d95:1982:f467/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

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

## 6. Fast Port Scan (masscan)

```
[+] Enter The Option from [1-16] OR [x] to Exit → 6
[+] Enter IP → 192.168.133.129
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-31 09:31:25 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 139/tcp on 192.168.133.129
Discovered open port 22/tcp on 192.168.133.129
Discovered open port 514/tcp on 192.168.133.129
Discovered open port 21/tcp on 192.168.133.129
Discovered open port 6697/tcp on 192.168.133.129
Discovered open port 8009/tcp on 192.168.133.129
Discovered open port 5432/tcp on 192.168.133.129
Discovered open port 111/tcp on 192.168.133.129
Discovered open port 2121/tcp on 192.168.133.129
Discovered open port 8180/tcp on 192.168.133.129
Discovered open port 3632/tcp on 192.168.133.129
Discovered open port 3306/tcp on 192.168.133.129
Discovered open port 25/tcp on 192.168.133.129
Discovered open port 5900/tcp on 192.168.133.129
Discovered open port 6667/tcp on 192.168.133.129
Discovered open port 512/tcp on 192.168.133.129
Discovered open port 38773/tcp on 192.168.133.129
Discovered open port 513/tcp on 192.168.133.129
Discovered open port 39562/tcp on 192.168.133.129
Discovered open port 41689/tcp on 192.168.133.129
Discovered open port 53/tcp on 192.168.133.129
Discovered open port 2049/tcp on 192.168.133.129
Discovered open port 8787/tcp on 192.168.133.129
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```



## 7. Fast Port Scan (hping3)

```
[+] Enter The Option from [1-16] OR [x] to Exit → 7
[+] Enter IP → 192.168.133.129
Scanning 192.168.133.129 (192.168.133.129), port 0-65535
65536 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+-----+-----+
|port| serv name | flags | ttl | id | win | len |
+-----+-----+-----+-----+-----+-----+
111 sunrpc : .S..A... 64 0 5840 46
139 netbios-ssn: .S..A... 64 0 5840 46
445 microsoft-d: .S..A... 64 0 5840 46
512 exec : .S..A... 64 0 5840 46
513 login : .S..A... 64 0 5840 46
514 shell : .S..A... 64 0 5840 46
1099 rmiregistry: .S..A... 64 0 5840 46
1524 ingreslock : .S..A... 64 0 5840 46
2049 nfs : .S..A... 64 0 5840 46
2121 iprop : .S..A... 64 0 5840 46
3306 mysql : .S..A... 64 0 5840 46
3632 distcc : .S..A... 64 0 5840 46
5432 postgresql : .S..A... 64 0 5840 46
5900 : .S..A... 64 0 5840 46
6000 x11 : .S..A... 64 0 5840 46
6667 ircd : .S..A... 64 0 5840 46
6697 ircs-u : .S..A... 64 0 5840 46
8009 : .S..A... 64 0 5840 46
8180 : .S..A... 64 0 5840 46
8787 : .S..A... 64 0 5840 46
38773 : .S..A... 64 0 5840 46
39562 : .S..A... 64 0 5840 46
41689 : .S..A... 64 0 5840 46
49592 : .S..A... 64 0 5840 46
22 ssh : .S..A... 64 0 5840 46
21 ftp : .S..A... 64 0 5840 46
80 http : .S..A... 64 0 5840 46
All replies received. Done.
Not responding ports:
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```

## 8. Service Version Scan

```
[+] Enter The Option from [1-16] OR [x] to Exit → 9
[+] Enter IP → 192.168.133.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 07:24 EST
Nmap scan report for 192.168.133.129
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:80:81:71 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 12.68 seconds
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```



## 9. OS Detection

```
[+] Enter The Option from [1-15] OR [x] to Exit → 9
[+] Enter IP → 192.168.133.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:40 EDT
Nmap scan report for 192.168.133.129
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:80:81:71 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 2.19 seconds
0
[+] Enter The Option from [1-15] OR [x] to Exit →
```

## 10. Vulnerability Detection with Report

```
[+] Enter The Option from [1-10] OR [x] to Exit → 10
[+] Enter IP → 192.168.133.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 13:07 EST
Nmap scan report for 192.168.133.129
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://www.securityfocus.com/bid/48539
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|   Transport Layer Security (TLS) services that use anonymous
|   Diffie-Hellman key exchange only provide protection against passive
|   eavesdropping, and are vulnerable to active man-in-the-middle attacks
|   which could completely compromise the confidentiality and integrity
|   of any data exchanged over the resulting session.
|   Check results:
|   ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: Unknown/Custom-generated
|   Modulus Length: 512
|   Generator Length: 8
|   Public Key Length: 512
|   References:
|   https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|   State: VULNERABLE
|   IDs: CVE-2015-4000 BID:74733
|   The Transport Layer Security (TLS) protocol contains a flaw that is
|   triggered when handling Diffie-Hellman key exchanges defined with
|   the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|   to downgrade the security of a TLS session to 512-bit export-grade
|   cryptography, which is significantly weaker, allowing the attacker
|   to more easily break the encryption and monitor or tamper with
```



## 11. SOV Detection Scan (Share of Voice)

```
[+] Enter The Option from [1-15] OR [x] to Exit → 11
[+] Enter IP → 192.168.133.129
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-20 12:36 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:36
Completed NSE at 12:36, 0.00s elapsed
Initiating NSE at 12:36
Completed NSE at 12:36, 0.00s elapsed
Initiating NSE at 12:36
Completed NSE at 12:36, 0.00s elapsed
Initiating ARP Ping Scan at 12:36
Scanning 192.168.133.129 [1 port]
Completed ARP Ping Scan at 12:36, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:36
Scanning 192.168.133.129 [65535 ports]
Discovered open port 3306/tcp on 192.168.133.129
Discovered open port 5900/tcp on 192.168.133.129
Discovered open port 25/tcp on 192.168.133.129
Discovered open port 111/tcp on 192.168.133.129
Discovered open port 53/tcp on 192.168.133.129
Discovered open port 139/tcp on 192.168.133.129
Discovered open port 21/tcp on 192.168.133.129
Discovered open port 80/tcp on 192.168.133.129
Discovered open port 23/tcp on 192.168.133.129
Discovered open port 22/tcp on 192.168.133.129
Discovered open port 445/tcp on 192.168.133.129
Discovered open port 55206/tcp on 192.168.133.129
Discovered open port 6697/tcp on 192.168.133.129
Discovered open port 3632/tcp on 192.168.133.129
Discovered open port 8180/tcp on 192.168.133.129
Discovered open port 512/tcp on 192.168.133.129
```

```
Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|_ clock-skew: mean: -2h57m58s, deviation: 2h30m00s, median: -4h12m59s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-01-31T09:21:03-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 1.00 ms 192.168.133.129

NSE: Script Post-scanning.
Initiating NSE at 13:34
Completed NSE at 13:34, 0.00s elapsed
Initiating NSE at 13:34
Completed NSE at 13:34, 0.00s elapsed
Initiating NSE at 13:34
Completed NSE at 13:34, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
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 146.77 seconds
Raw packets sent: 65555 (2.885MB) | Rcvd: 65551 (2.623MB)
0
[+] Enter The Option from [1-16] OR [x] to Exit → █
```



## 12. Specific Vulnerability

```
[+] Enter The Option from [1-16] OR [x] to Exit → 12
[+] Enter IP → 192.168.133.129
[+] Enter Script → smb-enum-shares.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 14:11 EST
Nmap scan report for 192.168.133.129
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:80:81:71 (VMware)
```

```
Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.133.129\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.133.129\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.133.129\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.133.129\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\192.168.133.129\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|_   Anonymous access: READ/WRITE
Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```







## C. RESEARCH PAPER

### N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network

**Ramanan B**

UG Scholar

Department of IT

Sathyabama Institute of Science and  
Technology Chennai ,India

ramananbtssr3032@gmail.com

**Srirangaprasanth V**

UG Scholar

Department of IT

Sathyabama Institute of Science and  
Technology Chennai ,India

srirangaprasanth@gmail.com

**Mathivana G**

Associate Professor

Department of IT

Sathyabama Institute of Science and  
Technology Chennai ,India

Mathivanan.it@sathyabama.ac.in

#### ABSTRACT

In the development of computer interconnection, computer networking is essential. It facilitated communication or data sharing between two or more devices over the same network (Intranet and Global Network) (Internet). However, due to a number of open protocols or ports, the lack of use of OS-based firewalls, weakened credentials for remote protocols, vulnerable services, service versions, etc., security is still a major concern in the network. A CLI (Command Line Interface) based network security testing tool, N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network was created using Python 3 and Bash. The Linux operating system in the Debian flavour is compatible with N3PTU0N. N3PTU0N is a tool that network security experts can use when it comes to IP address, MAC address, route through, live host detection, port scanning, service version detection, OS detection, vulnerability detection, SOV (Service, OS, Vulnerability) script, firewall bypass, FTP login, and Telnet login. Ping, ARP, Nmap Scripting Engine (NSE), Mac-changer, Hgping3, Masscan, FTP, and TELNET are among the network utilities used by N3PTU0N. It makes it simple to create a report of the tested network and aids network security professionals in navigating fast. It also utilises all of the stated tools' capabilities with a single comprehensive script.

**Keywords:-** *Command Line Interface(CLI) – OS Detection – Vulnerability Services – Network Enumeration – Penetration Testing.*

#### 1. INTRODUCTION

Since "network security" is a broad concept, it encompasses a variety of techniques, tools, and procedures. It can be described as a

collection of policies and settings intended to safeguard the reliability, usability, and security of computer networks and data utilising both software and hardware technologies. Every organisation needs some type of network security solutions in place, regardless of its size, industry, or architecture, to safeguard it against the wide range of cyber threats that are now present in the wild. Today's network architecture is sophisticated in addition to dealing with a dynamic threat environment and attackers who are always searching for and attempting to exploit flaws.

A crucial first step in performing a security assessment or penetration test is network enumeration since it gives the attacker a network map that they can use to locate prospective targets and attack routes. However, defenders can also utilise network enumeration to spot potential flaws and weaknesses in their own network and take action to fix them before attackers can exploit them.

A security assessment known as a penetration test, also known as a pen test or ethical hacking, simulates cyber-attacks on a computer system. It is used to evaluate how strong (or weak) the system's security is. Penetration testing enables a thorough risk assessment because it searches for both potential weaknesses and strengths in a system's security. All firms should regularly conduct penetration testing, which is a crucial and beneficial task. This is so that the results of pen testing can be utilised to strengthen and reinforce existing security procedures inside an organisation in order to counteract emerging cyber threats.

Professional programmers who practise ethical hacking frequently have doctorates and pen testing certifications. The best ethical hackers, though, frequently pick things up on their own. Some hackers are actually former criminals who have atoned for their misdeeds and are now helping to fix security weaknesses. The ideal pen test candidate can vary significantly depending on the target company and the sort of pen test being used.



## 2. RELATED WORK

In 2021, G Jayasuryapal and P Meher Pranay conducted a survey on network penetration testing, which covers all aspects of the testing process, from information gathering to post-exploitation. Penetration testing operations follow specific rules and require cooperation between the client and the testing team. Through this testing, organizations can identify vulnerabilities such as open servers and ports.

In 2019, Pengfei Shi and Futong Qin proposed a penetration testing framework for large-scale networks based on network fingerprinting. They examined the principles and methodology of conventional penetration testing technology for large networks, along with its practical limitations. By integrating network fingerprinting with internet search engine technologies, they developed a framework for penetration testing that is based on network fingerprinting and is suitable for large-scale networks.

In 2017, Rodney R Rohrmann and Vincent J Ercolani suggested using parallel Nmap scans through Tor to conduct large-scale port scanning on parts of the IPv4 range. While this method is useful for gathering data during scanning, it is not feasible to use it to scan the entire IPv4 Address space on multiple ports as it takes significantly longer to run through Tor. One advantage of this scanning method is that it protects researchers from potential retaliation from targets who may not appreciate being scanned and allows them to conduct their own scans.

In 2015, Prerna Arote and Karam Veer Arya proposed a method for detecting and preventing ARP poisoning attacks using a modified ICMP and voting system. The Internet Control Message Protocol (ICMP) is an IP network protocol that is useful for managing and controlling networks. ICMP is an essential component of IP implementations. ARP was created to increase the reliability of networks. The Data Link Layer (DLL) is responsible for framing packets as they are processed and passed down the stack.

In 2016, Enos LETSOALO and Sunday OJO proposed a survey on detecting and preventing Media Access Control (MAC) address spoofing attacks in wireless networks. Attackers can use packet sniffer software to intercept packets and extract the MAC addresses of access points or other users. By spoofing the MAC address of a legitimate access point, an attacker can disconnect authorized users and take control of established TCP sessions.

In 2017, Lerato Ramahlapane Moila and Mthulisi Velempini conducted an evaluation of the effectiveness of routing protocols in cognitive radio ad hoc networks. Existing protocols do not provide sufficient assurances for real-time data quality of service, and the dynamic nature of cognitive networks, including node mobility and spectrum availability, poses challenges in developing QoS-aware routing protocols.

Also in 2017, Sathish A.P. Kumar and Brian Xu proposed a vulnerability assessment for security in aviation cyber-physical systems. The goal was to identify vulnerabilities in aircraft equipment, such as data loaders, and improve aircraft security and safety by using penetration testing tools like Metasploit Pro and BackTrack to detect cyber weaknesses in critical aviation systems.

Detection of Slow Port Scanning Attacks was proposed by Kashif Kifayat and Mehr u Nisa in 2020. A scanning attack is a two-stage process, with scanning being the first stage, during which communication routes' vulnerabilities are identified. The second stage is finding the targets, which is then followed by the attack. During port scanning, open ports are sought across the network in order to locate the system that can be exploited.

In 2022, Sabah M. Morsy and Dalia Nashat proposed D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. An ARP spoof-based MITM attack exploits a flaw in the ARP protocol by associating the attacker's MAC address with the IP address of the target legitimate host. ARP spoof-based MITM attacks have various defence strategies, but these strategies are incomplete or have limited effectiveness. Performance overhead is also a concern due to the fundamental ARP protocol change.

Measuring the Prevalence of the Password Authentication Vulnerability in SSH was proposed by Ron Andrews and Dalton A. Hahn in 2020. They proposed a novel technique for probing an SSH service to determine whether password authentication is permitted without being invasive or damaging to the host. They also showed that some of these tools and services can be enhanced to assess the prevalence of password authentication in SSH.

In 2017, Debdeep Dey and Archisman Dinda proposed Warezmaster and Warezclient: An Implementation of FTP Base R2L Attacks. The File Transfer Protocol (FTP) was not designed with stringent security precautions in mind, as all commands and data are sent in clear text. The protocol has since received modifications that have

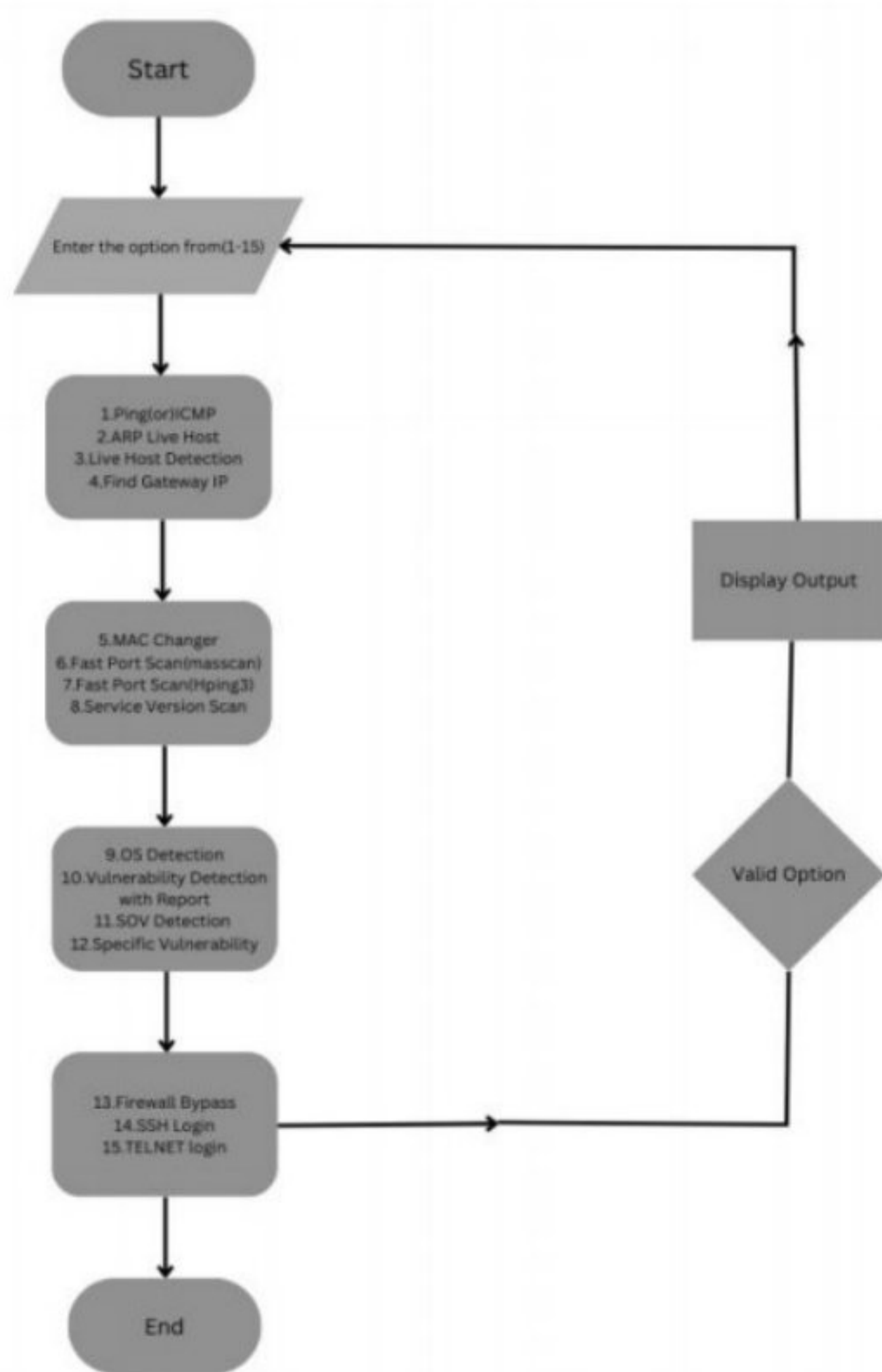


introduced security capabilities, such as the ability to upgrade an FTPS connection to Transport Layer Security (TLS).

Cyber Security, a Threat to Cyber Banking in South Africa was proposed by Barry Dwolatzky and Thierry Mbah Mbelli in 2016. The rise of cybercrime is becoming a serious economic issue for South African enterprises, as well as the country as a whole. The essay's first section examines the various internet risks associated with online banking. A boundary- and application-based approach to cyber-banking security is also proposed

3.1 PROPOSED WORK

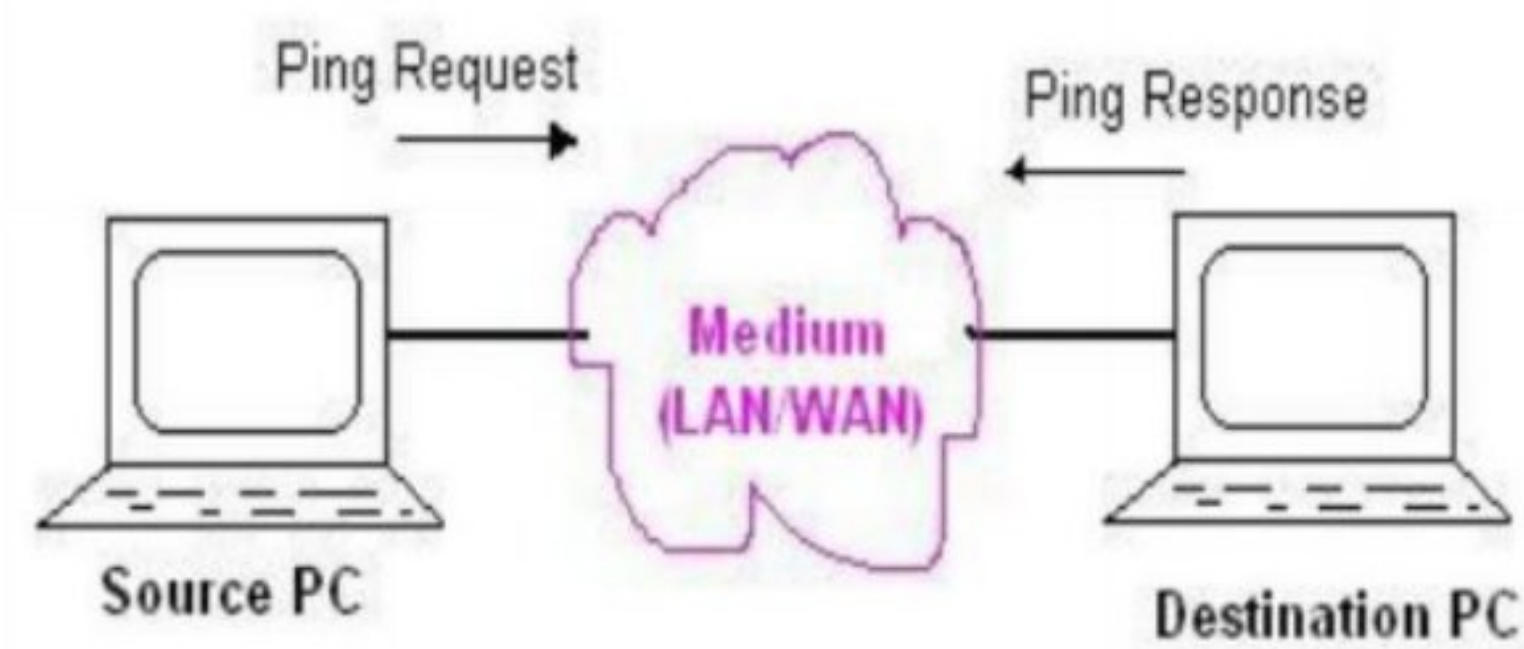
N3PTU0N | Network Enumeration and Penetration Testing Under an Organized Network is a CLI (Command Line Interface) based Network Security Testing Tool, where It is Developed using Python3 & Bash. N3TU0N can work in Debian flavor of the Linux Operating System. N3PTU0N helps Network Security Professionals to enumerate Information about IP Address, MAC Address, Route through, Live Host Detection, Port Scanning, Service Version Detection, OS Detection, Vulnerability Detection, SOV (Service, OS, Vulnerability) Script, Firewall Bypass, FTP login, and Telnet login.



3.1.1 PING

Ping is a tool frequently used to detect a device's status on a network. ICMP is the basis of Ping. If the target device is available, it will

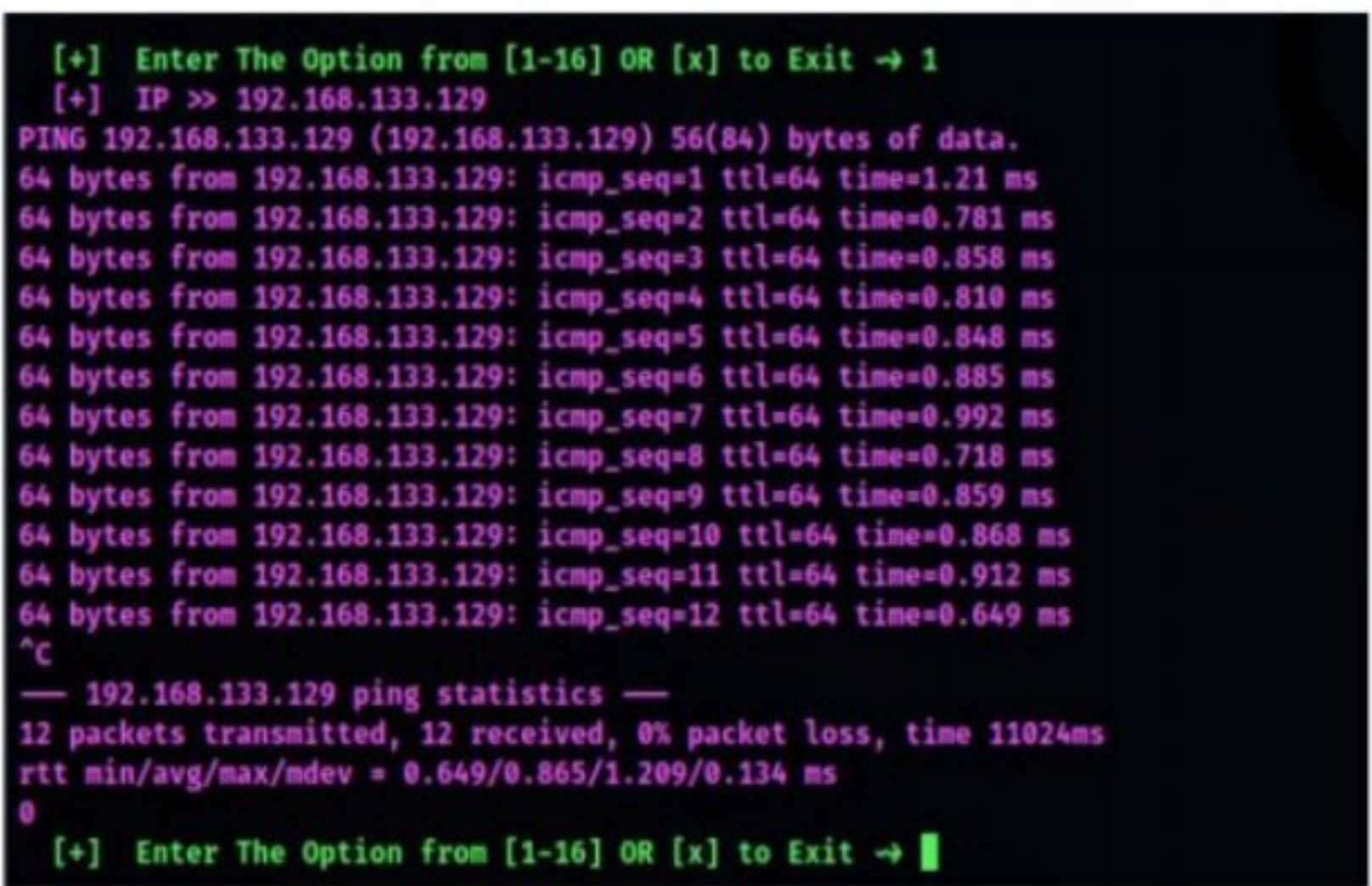
respond with an ICMP echo when a Ping process command is given to it as an ICMP echo.



The Goal of Ping

Ping is used to send a test packet, also known as an echo packet, to a device in order to determine whether it can be reached and how long it takes for the packet to get there. There are two primary goals. Test the network availability and latency between two devices. It is simple to check if we have access to a particular host by sending ICMP ping packets to it. However, this technique is only effective in networks that have ICMP and ping enabled. We are unable to receive a correct response if ICMP is deactivated.

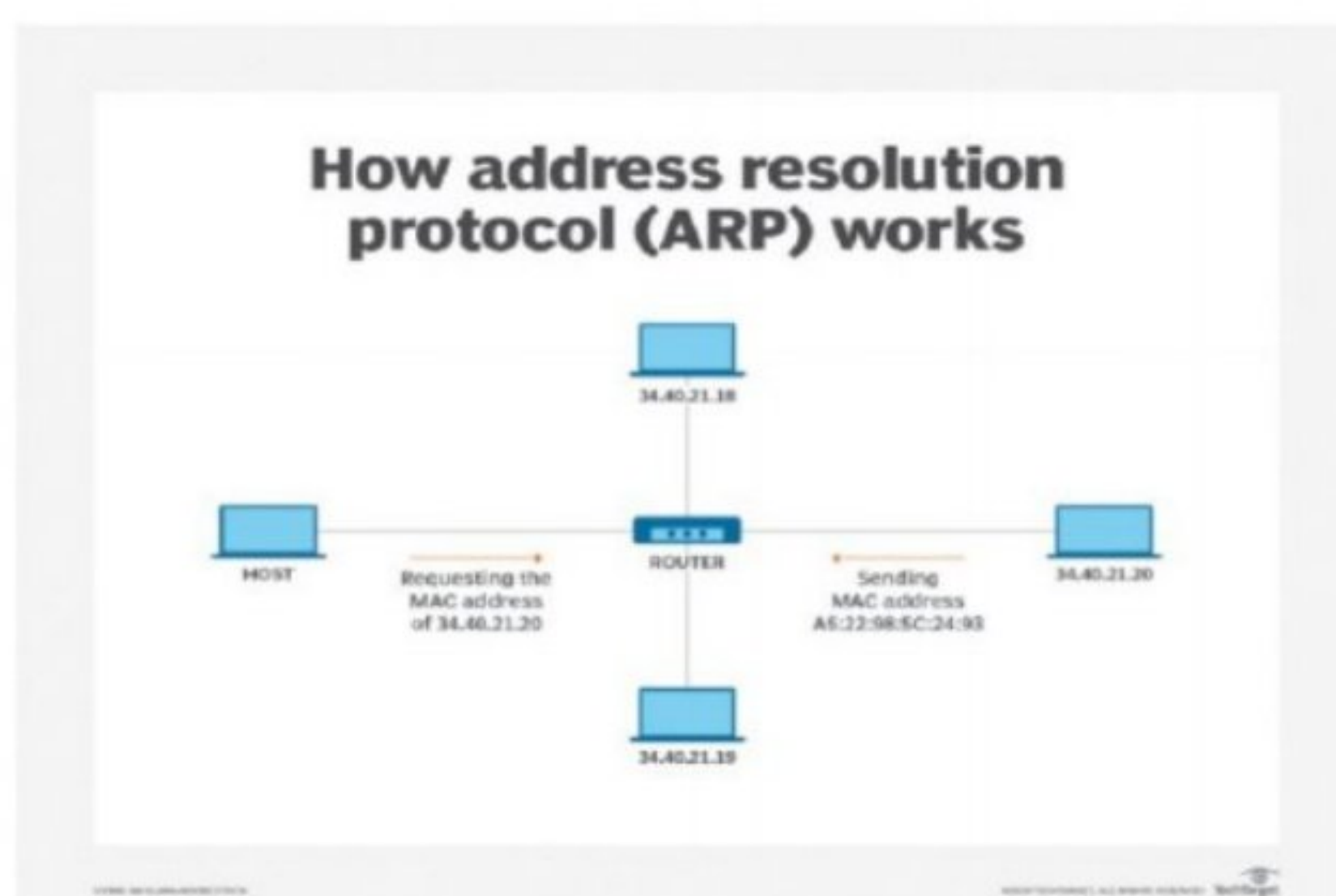
For example:  
PING 192.168.133.129(192.168.133.129) 56(84) bytes of data.  
64 bytes from 192.168.133.129: icmp\_seq=1 ttl=64 time=1.21 ms  
64 bytes from 192.168.133.129: icmp\_seq=2 ttl=64 time=0.781 ms  
64 bytes from 192.168.133.129: icmp\_seq=3 ttl=64 time=0.858 ms



3.1.2 ARP(Address Resolution Protocol)

ARP is a protocol used to find the MAC address of a device from a known IP address. When communicating with a device in a local area network (Ethernet), the sender needs to know the MAC address of the recipient, which is not known beforehand. ARP helps to locate the MAC address of the destination device by mapping it to its IP address.





An ARP cache is kept by every operating system in an IPv4 Ethernet link. A host checks its ARP cache to determine if the IP to MAC address translation already exists each time it requires a MAC address to send a packet to another computer in the local area network. If it does, there is no need to make a new ARP request. ARP is combined with the network address request if the translation does not already exist. ARP sends a request packet to every LAN device and asks if any of them are using a particular IP address. In order for ARP to update the cache for later usage and continue the conversation, a device must respond when it identifies the IP address as being its own. If a host system doesn't know its own IP address, it can do discovery via the Reverse ARP (RARP) protocol.

```
[+] Enter The Option from [1-16] OR [x] to Exit -> 2
Address      Hwtype  Hwaddress  Flags Mask  Iface
192.168.133.254 ether  00:50:56:e8:74:88 C          eth0
192.168.133.129 ether  00:0c:29:80:81:71 C          eth0
192.168.133.2 ether   00:50:56:ec:85:19 C          eth0
0
[+] Enter The Option from [1-16] OR [x] to Exit -> 0
```

The Address Resolution Protocol (ARP) is responsible for mapping a device's IP address to its Media Access Control (MAC) address, which is the unique hardware address. ARP uses the device's IP address to determine its corresponding MAC address.

### 3.1.3 Live Host Detection

Any ethical hacker or penetration tester must have access to live hosts detection. You can specify the IP range to search in by using the if config command. While penetration testers use live host discovery to find active targets in a network, system administrators commonly use it to count or monitor the number of active hosts. This recipe details how to find active hosts in a network using Nmap's ping scan. We will perform a ping scan arranged many probable live hosts in our network. Nmap will send a ping to every host in this radius to see if it is active. This tutorial will make use of nmap.



Finding the live hosts on the networks is our responsibility as network engineers or penetration tester. Today, we'll look at how to locate active the internet's hosts. To locate the active hosts on the network, we'll utilise the nmap utility. An open-source command-line programme for network research and security audits is called Nmap (network mapper). Using raw IP packets, Nmap is used to scan networks. To locate active hosts on the network for this post, we will use the nmap tool.

```
0
192.168.133.2
192.168.133.128
192.168.133.129
0
[+] Enter The Option from [1-16] OR [x] to Exit -> 0
```

### 3.1.4 Find Gateway's IP

An access point to another network that frequently involves not only a change in addressing but also a different networking protocol is provided by a gateway, which is a network node. A router merely distributes packets between networks with different network prefixes, as it is more clearly described. A routing table, which is part of the networking software stack on each computer, lists which network router is in charge of forwarding traffic to a specific range of addresses and which interface is used for transmission. In the event that none of these forwarding rules work for a particular destination address, the default gateway is chosen as the router of last resort. To set up the routing table and default route for the node, use the route command to specify the default gateway.

- **Open a terminal and use the following command**

```
ip route(command)
```

- **You should see an output like this**

```
default via 192.168.133.2 dev eth0
proto dhcp src 192.168.133.128
metric 100
192.168.133.0/24 dev eth0 proto
kernel scope link src
192.168.133.128 metric 100
```



0

Focus on the line that starts with default. This will give the default gateway IP.

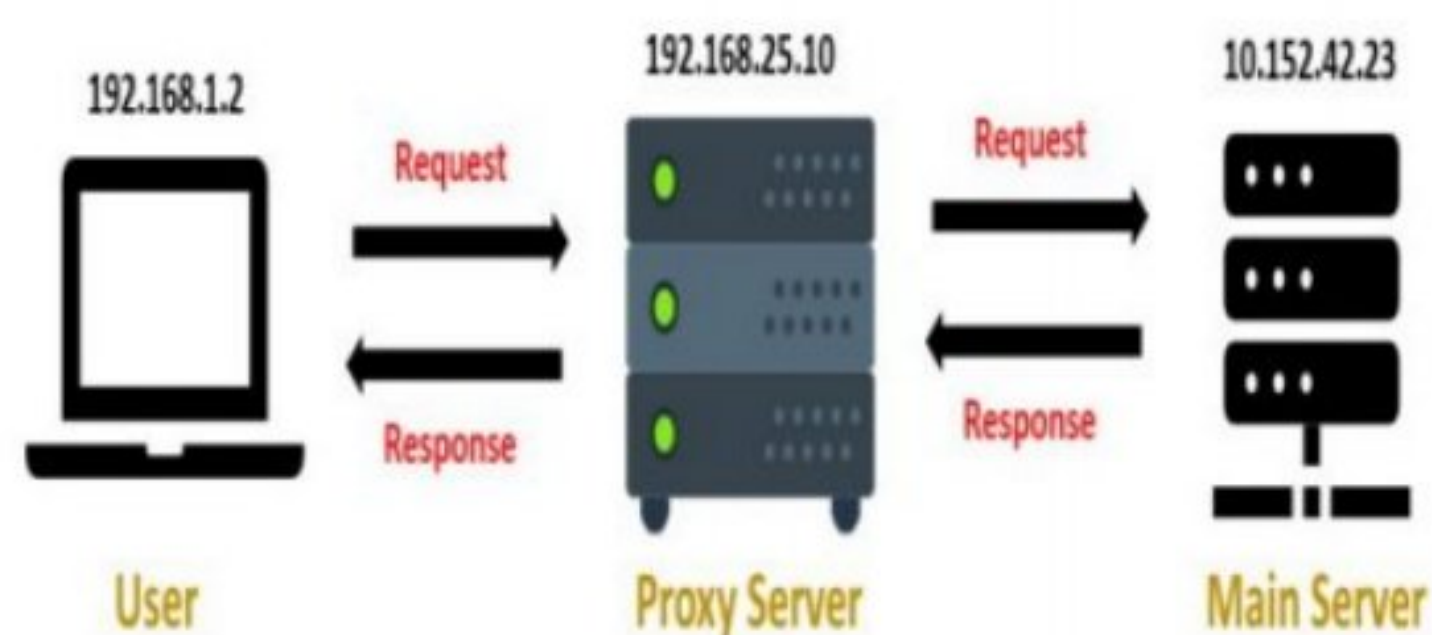
```
[+] Enter The Option from [1-16] OR [x] to Exit → 4
default via 192.168.133.2 dev eth0 proto dhcp src 192.168.133.128 metric 100
192.168.133.0/24 dev eth0 proto kernel scope link src 192.168.133.128 metric 100
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```

- Focus on the line that starts with default. This will give the default gateway IP.  
ip route | grep default
- This will just give the default gateway IP in the output:  
default via 192.168.133.2 dev wlp1s0 proto dhcp metric 100  
And as you can see, 192.168.133.2 is the default gateway IP in my case.

### 3.1.5 MAC Changer

The manufacturer assigns a different MAC address to each device. When you are connected to the router, this MAC address is recorded in the router's table. Every device has a specific MAC address, which makes it possible to identify the system or device that the hacker used, thus revealing your identity.

You can temporarily change your MAC address so that it won't recognise you. Here is where ethical hacking using MacChanger is possible. Until the device is rebooted, a utility called MacChanger will alter the MAC address of that device to a false one.



#### The Goal of MAC Changer

- Detect a network device on the Internet.
- The specific identity of a physical network device.

- control access to shared network resources
- supply a local area network routing address (LAN)

```
[+] Enter The Option from [1-16] OR [x] to Exit → 4
default via 192.168.133.2 dev eth0 proto dhcp src 192.168.133.128 metric 100
192.168.133.0/24 dev eth0 proto kernel scope link src 192.168.133.128 metric 100
0
[+] Enter The Option from [1-16] OR [x] to Exit → 5
[+] Enter MAC Address → 00:0c:29:63:a6:95
[+] Enter the Interface → lo
0
Current MAC: 00:00:00:00:00:00 (XEROX CORPORATION)
Permanent MAC: 00:00:00:00:00:00 (XEROX CORPORATION)
New MAC: 00:0c:29:63:a6:95 (VMware, Inc.)
0
0
```

### 3.1.6 Fast Port Scan (masscan)

Masscan has been available for a while, and pentesters from around the world already use it. It is a reconnaissance tool with a 10 million packets per second maximum rate of transmission. It makes use of a unique TCP/IP stack and asynchronous transmission. As a result, distinct threads are used for packet transmission and reception. Masscan can be utilised to speedily enumerate a huge number of hosts. The tool's creator even asserts that it can scan the entire internet in just six minutes. Due to its high rate of transmission, it can also be utilised for stress testing.

#### Features

- Ultra-fast port scanning: capable of sending 10M packets per second (capable; NIC and PF RING drivers required)
- output in Nmap format
- Target settings and specifications in Nmap style
- grabbing a banner
- Fundamental Weakness Like Heart bleed scanning, custom TCP/IP stack

```
[+] Enter The Option from [1-16] OR [x] to Exit → 6
[+] Enter IP → 192.168.133.129
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-31 09:31:25 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
Discovered open port 139/tcp on 192.168.133.129
Discovered open port 22/tcp on 192.168.133.129
Discovered open port 514/tcp on 192.168.133.129
Discovered open port 21/tcp on 192.168.133.129
Discovered open port 6697/tcp on 192.168.133.129
Discovered open port 8009/tcp on 192.168.133.129
Discovered open port 5432/tcp on 192.168.133.129
Discovered open port 111/tcp on 192.168.133.129
Discovered open port 2121/tcp on 192.168.133.129
Discovered open port 8180/tcp on 192.168.133.129
Discovered open port 3632/tcp on 192.168.133.129
Discovered open port 3306/tcp on 192.168.133.129
Discovered open port 25/tcp on 192.168.133.129
Discovered open port 5900/tcp on 192.168.133.129
Discovered open port 6667/tcp on 192.168.133.129
Discovered open port 512/tcp on 192.168.133.129
Discovered open port 38773/tcp on 192.168.133.129
Discovered open port 513/tcp on 192.168.133.129
Discovered open port 39562/tcp on 192.168.133.129
Discovered open port 41689/tcp on 192.168.133.129
Discovered open port 53/tcp on 192.168.133.129
Discovered open port 2049/tcp on 192.168.133.129
Discovered open port 8787/tcp on 192.168.133.129
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```



The most fundamental scanning procedure in masscan is this one. This allows you to scan any IPs. You can specify an IP range (192.168.133.129) like you would in nmap in place of the subnet value.

Now, using the IPs we scanned, we try to capture banners. For this, there can be a problem. The OS might reject the packet because masscan utilises a custom stack. The tool's home page provides a clear explanation of this. Therefore, we must specify a different IP address in the same subnet for the time being.

### 3.1.7 Fast Port Scan (hping3)

Hping3 is a network tool that can send custom TCP/IP packets and display the responses from the target, much like how the ping program displays ICMP responses. It can handle fragmentation, packet body customization, and size when transferring files wrapped in supported protocols.

**You can execute at least the following tasks using hping3**

Test firewall settings - Scanners for advanced ports utilize various protocols, packet sizes, types of services, and fragmentation to test the performance of the network. Transferring files between even the most fascist firewall regulations.

#### Use of hping3 for UDP and TCP Packet Crafting

- Overview of Packet Crafting  
Packet crafting is a technique that allows you to find vulnerabilities or entry points into a target network.
- Fundamentals of hping3 Open the Terminal after logging in to Kali Linux.
- UDP packet crafting To perform a UDP packet crafting in the target machine, type:
- Send TCP SYN Request Launch the Wire shark on Windows machine again and leave it running.

```
[+] Enter The Option from [1-16] OR [x] to Exit → 7
[+] Enter IP → 192.168.133.129
Scanning 192.168.133.129 (192.168.133.129), port 0-65535
65536 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+-----+
|port|serv name|flags|ttl|id|win|len|
+-----+-----+-----+-----+-----+-----+
111 sunrpc : .S..A... 64 0 5840 46
139 netbios-ssn: .S..A... 64 0 5840 46
445 microsoft-d: .S..A... 64 0 5840 46
512 exec : .S..A... 64 0 5840 46
513 login : .S..A... 64 0 5840 46
514 shell : .S..A... 64 0 5840 46
1099 rmiregistry: .S..A... 64 0 5840 46
1524 ingreslock : .S..A... 64 0 5840 46
2049 nfs : .S..A... 64 0 5840 46
2121 iprop : .S..A... 64 0 5840 46
3306 mysql : .S..A... 64 0 5840 46
3632 distcc : .S..A... 64 0 5840 46
5432 postgresql : .S..A... 64 0 5840 46
5900 : .S..A... 64 0 5840 46
6000 x11 : .S..A... 64 0 5840 46
6667 ircd : .S..A... 64 0 5840 46
6697 ircs-u : .S..A... 64 0 5840 46
8009 : .S..A... 64 0 5840 46
8180 : .S..A... 64 0 5840 46
8787 : .S..A... 64 0 5840 46
38773 : .S..A... 64 0 5840 46
39562 : .S..A... 64 0 5840 46
41689 : .S..A... 64 0 5840 46
49592 : .S..A... 64 0 5840 46
22 ssh : .S..A... 64 0 5840 46
21 ftp : .S..A... 64 0 5840 46
80 http : .S..A... 64 0 5840 46
All replies received. Done.
Not responding ports:
0
[+] Enter The Option from [1-16] OR [x] to Exit →
```

### 3.1.8 Service Version Scan

A type of network investigation known as a service version scan includes probing a target system or network to find the versions of services that are active on open ports. This can be helpful for a number of reasons, including determining possible vulnerabilities that might be present in out-of-date software versions and determining the system or network's overall security posture.

Service version scans can be carried out using a number of programs, including Nmap, Masscan, and Metasploit. To determine the version information of the services operating on a target system, these tools typically combine port scanning and banner grabbing methods.

```
[+] Enter The Option from [1-16] OR [x] to Exit → 4
[+] Enter IP → 192.168.133.129
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-31 07:24 EST
Nmap scan report for 192.168.133.129
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 6ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login        OpenSSH or Sshd
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath gnuiregistry
1524/tcp  open  ingreslock   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100000)
2121/tcp  open  iprop        ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-MariaDB
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
NAC Address: 00:0C:29:00:01:71 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.lan; OS: Unix, 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 12.60 seconds
[+] Enter The Option from [1-16] OR [x] to Exit →
```

If any current software versions have any known flaws, they can be identified by looking at the scan's results. Just keep in mind that you should only scan service versions on networks or



computers where you have been granted permission to do so. Unauthorized scanning is possibly illegal and might result in severe consequences.

### 3.1.9 OS Detection

An essential component of internet security is OS detection. When carrying out security operations like vulnerability analyses, penetration testing, and breach detection, it can be useful to determine the operating system of the target system.

To exploit a vulnerability in a specific operating system, the attacker must first identify the OS running on the target machine. OS detection can help a security analyst determine if a system is vulnerable to a particular attack by identifying the known vulnerabilities associated with the operating system in question.

```
[*] Enter The Option from [1-15] OR [x] to Exit -> 9
[*] Enter IP -> 192.168.133.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 00:40 EDT
Nmap scan report for 192.168.133.129
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:80:81:71 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 2.19 seconds
[*] Enter The Option from [1-15] OR [x] to Exit -> 0
```

In addition to this, OS detection can also help in identifying the type of network devices, such as routers and firewalls, which are running on a specific operating system. This information can be used to tailor specific attacks that target the vulnerabilities associated with that operating system, and thus improve the overall effectiveness of the attack. Overall, OS detection is an important tool in the arsenal of any cyber security professional, and it should be used to aid in the detection and prevention of potential security threats.

### 3.1.10 Vulnerability Detection with Report

An important component of cyber security is vulnerability detection, which entails locating flaws in applications, networks, and computer systems that might be exploited by hackers. It is a proactive strategy that enables organisations to find weaknesses before attackers take advantage of them.

It is crucial to notify the appropriate parties as soon as a weakness is discovered so that

it can be fixed right away. The vulnerability's specifics, such as its seriousness, the affected systems, and the possible consequences if it is exploited, should be described in the report. Recommendations for mitigating the vulnerability, such as deploying a patch or updating software, should also be included in the report. The vulnerability report should be written in plain, simple English that both technical and non-technical stakeholders can understand. It should be accompanied by any supporting documentation that can help to verify the vulnerability, such as screenshots or log files.

It may be necessary to disclose vulnerabilities to external stakeholders, such as software vendors or government organizations, in addition to the appropriate individuals within the organisation. This can make it more likely that the vulnerability will be addressed broadly and that the required precautions will be taken to defend against potential attacks.

```
[*] Enter The Option from [1-15] OR [x] to Exit -> 10
[*] Enter IP -> 192.168.133.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 13:07 EDT
Nmap scan report for 192.168.133.129
Host is up (0.0031s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsf2pd-backdoor:
|_  VULNERABLE:
|_  vsFTPd version 2.3.4 backdoor
|_  State: VULNERABLE (Exploitable)
|_  ID: CVE-2011-2523 BID-48529
|_  vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-06.
|_  Disclosure date: 2011-07-06
|_  Exploit results:
|_  Shell command: id
|_  Results: uid=0(root) gid=0(root)
|_  References:
|_  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_  https://www.securityfocus.com/bid/48529
|_  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_  https://github.com/rupid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsf2pd_234_backdoor.rb
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
25/tcp    open  smtp
|_  exl-08-param:
|_  VULNERABLE:
|_  Anonymous Diffie-Hellman Key Exchange MITM Vulnerability
|_  State: VULNERABLE
|_  Transport Layer Security (TLS) services that use anonymous
|_  Diffie-Hellman key exchange only provide protection against passive
|_  eavesdropping, and are vulnerable to active man-in-the-middle attacks
|_  which could completely compromise the confidentiality and integrity
|_  of any data exchanged over the resulting session.
|_  Check results:
|_  ANONYMOUS DH GROUP 1
|_  Cipher Suite: TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
|_  Module Type: Safe prime
|_  Module Source: Unknown/Custom-generated
|_  Module Length: 512
|_  Generator Length: 0
|_  Public Key Length: 512
|_  References:
|_  https://www.ietf.org/rfc/rfc2246.txt
|_  Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MITM (Logjam)
|_  State: VULNERABLE
|_  ID: CVE-2015-4000 BID-74723
|_  The Transport Layer Security (TLS) protocol contains a flaw that is
|_  triggered when handling Diffie-Hellman key exchanges defined with
|_  the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|_  to downgrade the security of a TLS session to 512-bit export-grade
|_  cryptography, which is significantly weaker, allowing the attacker
|_  to more easily break the encryption and monitor or tamper with
```

In general, vulnerability detection and reporting are crucial components of cyber security that can assist organisations in identifying and reducing possible risks before attackers take advantage of them. It is essential to approach vulnerability identification and reporting with a proactive mind set and collaborates with all relevant stakeholders in order to fix vulnerabilities in a timely and effective manner.

### 3.1.11 SOV Detection Scan (Share Of Voice)

A Share of Voice (SOV) Detection Scan is a valuable tool in cyber security to measure the visibility of a brand, product, or specific cybersecurity topic against competitors or related topics. To conduct a SOV Detection Scan, the first step is to define the cybersecurity scope, followed by identifying competitors and collecting data on the number of mentions for the brand or topic and its competitors within a specified time frame. Once



the data is collected, by calculating the Security Operations Visibility (SOV), it is possible to analyze the findings and identify opportunities for improvement and create plans to enhance awareness and visibility regarding cybersecurity. In summary, the SOV Detection Scan is a crucial tool that enables cybersecurity professionals to gain insights into how their cybersecurity efforts are perceived and develop strategies to stay ahead of their competitors.

```
Host script results:
| nbtstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
| METASPLOITABLE<00> Flags: <unique><active>
| METASPLOITABLE<03> Flags: <unique><active>
| METASPLOITABLE<20> Flags: <unique><active>
| \x01\x02_\MSR0NSE_\x02<01> Flags: <group><active>
| WORKGROUP<00> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
| _clock-skew: mean: -2h57m58s, deviation: 2h30m00s, median: -4h12m59s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| System time: 2023-01-31T09:21:03-05:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 1.00 ms 192.168.133.129

NSE: Script Post-scanning.
Initiating NSE at 13:34
Completed NSE at 13:34, 0.00s elapsed
Initiating NSE at 13:34
Completed NSE at 13:34, 0.00s elapsed
Initiating NSE at 13:34
Completed NSE at 13:34, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
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 146.77 seconds
Raw packets sent: 65535 (2.805MB) | Rcvd: 65531 (2.623MB)

[+] Enter The Option from [1-16] OR [x] to Exit -> 11
```

## The Goal of SOV Detection Scan

The primary objective of conducting a SOV Detection Scan is to identify and validate all the systems and assets that belong to an organization. The scan involves detecting all the network infrastructure, applications, servers, and devices that are currently in use within the organization. The main purpose of the scan is to ensure that the organization has an accurate record of its assets and systems and that no unauthorized or unaccounted-for devices or systems could potentially compromise the security of the organization. By performing a SOV Detection Scan, the organization can enhance its security posture and become more equipped to defend itself against cyber security threats.

### 3.1.12 Specific Vulnerability

In the realm of cyber security, a specific vulnerability refers to a weakness or defect in a system, software, or network that can be exploited by attackers to compromise its security. These vulnerabilities can result from coding errors, configuration problems, or flaws in the system's

design.

An attacker may be able to execute malicious code, get access to private data, or harm the system in other ways by exploiting a weakness. It's essential to locate and address vulnerabilities as soon as possible to thwart attacks and minimise potential harm.

```
[+] Enter The Option from [1-16] OR [x] to Exit -> 12
[+] Enter IP -> 192.168.133.129
[+] Enter Script -> smb-enumerate.shares.nse
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 14:11 EST
Nmap scan report for 192.168.133.129
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2221/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:00:01:71 (VMware)

Host script results:
| smb-enumerate-shares:
| account_used: <blank>
| \\192.168.133.129\ADMIN$:
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\192.168.133.129\IPC$:
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\192.168.133.129\opt:
| Type: STYPE_DIRECTORY
| Comment:
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\192.168.133.129\print$:
| Type: STYPE_DIRECTORY
| Comment: Printer Drivers
| Users: 1
| Max Users: <unlimited>
| Path: C:\usr\lib\samba\printers
| Anonymous access: <none>
| \\192.168.133.129\tmp:
| Type: STYPE_DIRECTORY
| Comment: oh noes!
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
[+] Enter The Option from [1-16] OR [x] to Exit -> 11
```

Vulnerability management, which entails regularly scanning systems and networks for potential flaws, prioritising them according to their severity, and implementing patches and other security measures to reduce the risks, is an essential part of cyber security. This makes it simpler to keep the safety and defence of systems and networks against potential cyber-attacks.

### 3.1.13 Firewall Bypass

In cyber security, the term "bypassing a firewall" refers to getting through or getting beyond the security procedures that a firewall implements in order to gain unauthorised access to a network or system. This is typically seen as malicious behaviour and is frequently connected to hacking or other online activities.

Network security is not complete without firewalls, which help guard against viruses, illegal access, and other online dangers. The originating IP address, port number, or protocol are just a few examples of predefined rules that can be used to configure firewalls to block incoming and outgoing traffic.



There are many ways to get over firewalls, including:

- Port scanning: The process of looking for open ports that the firewall has not blocked in order to establish a connection.
- Tunneling: Forgoing a firewall by establishing an encrypted tunnel between two systems.
- Application-layer attacks: gaining access to the network by taking advantage of flaws in apps that are permitted via the firewall.
- DNS tunneling: Bypassing the firewall and smuggling data over DNS traffic.

```
[+] Enter The Option from [1-16] OR [x] to Exit → 13
[+] Enter IP → 192.168.133.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-31 23:10 EST
Nmap scan report for 192.168.133.129
Host is up (0.0039s latency).
All 65535 scanned ports on 192.168.133.129 are in ignored states.
Not shown: 65505 closed tcp ports (reset), 30 open/filtered tcp ports (no-response)
MAC Address: 00:0C:29:80:81:71 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.00 seconds
0
```

Remember that trying to get past a firewall is against the law and can have serious repercussions. To defend against such attacks, organisations must put in place strong security measures and often update their firewall configurations.

### 3.1.14 FTP Login

The FTP (File transfer Protocol) protocol is frequently used to send files over the internet between servers and clients. However, if not correctly configured or secured, using FTP can also present security risks. The possibility for unauthorised access to sensitive data is one of the main security risks connected with FTP. If the FTP login procedure is not properly secured, this is especially true.

Strong authentication procedures must be in place in order to reduce the dangers related to FTP login. This might entail using MFA (multi-factor authentication) or mandating the use of strong passwords that are updated regularly. Additionally, it is advised to switch from plain-text FTP to private FTP protocols like SFTP or FTPS (FTP over SSL/TLS).

```
[+] Enter The Option from [1-15] OR [x] to Exit → 14
[+] Enter IP → 192.168.133.129
[+] Enter USER → msfadmin
Connected to 192.168.133.129.
220 (vsFTPD 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Permissions for users and groups should be correctly defined, and access to the FTP server should be restricted. For instance, it is advisable to deactivate anonymous FTP access when sending sensitive data.

The general configuration of the FTP server as well as the FTP login procedure may contain security vulnerabilities that can be found through routine security audits and vulnerability assessments.

### 3.1.15 TELNET Login

TELNET is a protocol that connects two machines together over a network. Because TELNET sends data in plain text, making it possible for anyone with network access to intercept and read it, using it for remote login can present a security risk. This means that your username and password will be transmitted in clear text if you use TELNET to access a distant system, making it simple for someone with malicious purpose to intercept your login information.

It is advised, in terms of cyber security, to steer clear of TELNET and instead use more safe protocols like SSH (safe Shell). Attackers will find it much harder to intercept and read confidential information like login credentials, please to SSH's encryption of all data transmitted between the client and the server.

```
[+] Enter The Option from [1-15] OR [x] to Exit → 15
[+] Enter IP → 192.168.133.129
Trying 192.168.133.129 ...
Connected to 192.168.133.129.
Escape character is '^['.

metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Mar 28 13:00:55 EDT 2023 on tty1
linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ █
```

To reduce the chance of interception, it is advised to use a private network or VPN (Virtual Private Network) if you must use TELNET for remote login. Additionally, to help prevent unauthorised access to your networks, you should always use strong passwords and change them frequently.



## 4. Result and Discussion

The results of network enumeration and penetration testing carried out within a structured network can vary depending on the precise testing objectives and the level of security systems in place. If conducted by a trained professional and with the express approval of the company, penetration testing can provide significant insights into the network's security posture. The results could include recommendations for tightening security measures as well as an in-depth analysis of the vulnerabilities and weaknesses found during testing.

## 5. Conclusion

To summarize, network enumeration and penetration testing are essential steps in cyber security for detecting possible vulnerabilities and weaknesses in a target network. Network enumeration is the process of collecting information about a network to comprehend its topology, operating systems, applications, and users. In contrast, penetration testing aims to exploit these vulnerabilities to gain unauthorized access. By performing network enumeration and penetration testing, organizations can proactively evaluate their current security measures and identify areas for enhancement. But it's crucial that these procedures are carried out by knowledgeable professionals who abide by moral standards and best practises, with the express consent of the organisation being tested. Regular network enumeration and penetration testing can aid organizations in enhancing their overall security posture and avoiding potential cyber threats. By recognizing and fixing vulnerabilities before they can be exploited by malicious actors, organizations can minimize the risk of financial loss, data breaches, and harm to their reputation.

## 6. Reference

[1] Rodney Rohr Mann, Rd. Mark Patton, Rd. Hsinchun Chen, "Anonymous Port Scanning", in proceedings of IEEE conference, September 2016.

[2] W. Lootah, W. Enck, and P. McDaniel, "TARP: Ticket-based Address Resolution Protocol," in IEEE Computer Society, vol. 51, no. 15, 2007, pp. 4322-4337.

[3] S. Jana and S. Kasera, "On Fast and Accurate Detection of Unauthorised Wireless Access Points Using Clock Skews", IEEE Transactions on Mobile Computing, Vol. 9, No.3, March 2010.

[4] S. Hijazi and M. S. Obaidat, "A new detection and prevention system for ARP attacks using static entry," IEEE Syst. J., vol. 13, no. 3, pp. 2732-2738, Sep. 2019.

[5] D. Springall, Z. Durumeric, J. Halderman, "FTP: The Forgotten Cloud", 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 1-3, 2016.

[6] Plummer: An Ethernet addresses resolution protocol. RFC 826 (1982).

[7] <https://nmap.org/book/man-briefoptions.htm>.

[8] <https://www.linkedin.com/learning/paths/prepare-for-comptia-network-plus-n10-007-certification>.

[9] Gordon Lyon, "Nmap Network Scanning" Sunnyvale, CA: Insecure.com, LLC, 2002 p.129

[10] Huitema, C. (1997), IPv6, The new Internet Protocol.

[11] Unknown Author, "Kali Linux Tutorial: Setting Up Proxy Chains + Tor For Anonymity , Security" <http://www.picateshackz.com/2015/05/kali-linux-tutorial-setting-up-html>.

[12] Nmap cheats sheet see-security hacking defined experts by Nativ.y, 2015.

[13] Lyon Gordon NMAP-the Network Mapper-free security lancer, 2017.

[14] Ethical hacking and penetration guide by Baloch R, 2017.

[15] A guide to penetration testing by Tang A., Network security, 2014.