

PROFESSIONAL TRAINING REPORT
AT
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Technology in Information Technology

BY
J. ANUBAMA
REG. NUMBER: - 39120010



DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU



**SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**
Accredited with Grade “A” by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI
CHENNAI– 600119
www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **J.ANUBAMA (39120010)** who carried out the project entitled “**NETWORK ENUMERATION**” under my supervision November 2021.

Internal Guide

Dr. SENDURU. SRINIVASULU

Head of the Department

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

Submitted for Viva voce Examination held on

Internal Examiner

External Examiner

DECLARATION

I, **J. ANUBAMA** hereby declare that the project report entitled **NETWORK ENUMERATION** done by me under the guidance of **Dr. SENDURU. SRINIVASULU** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in **INFORMATION TECHNOLOGY**

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D., Dean, School of Computing, Dr. S. Vignesh Wari, M.E., Ph.D. and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department of INFORMATION TECHNOLOGY** for providing me 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. SENDURU. SRINIVASULU** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my 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.

TRAINING CERTIFICATE



CERTIFICATE OF COMPLETION

CSW-I-21-081121 is given to

ANUBAMA J

For completing the Cyber Security training that includes basics of Cyber Security, Pentesting, Networking, and WebApp.

Aaron V Sandeen

AARON SANDEEN
CEO - CSW

N. Vengatesh

VENGATESH NAGARAJAN
MENTOR



ABSTRACT

- **Network Enumeration** is a process that involves gathering information about a network such as the hosts, connected devices, along with usernames, group information and related data.
- A Host system is used to **Identify and Exploit vulnerabilities in the Operating System**, installed applications, and other programs.
- A Port scan is a method for determining which **ports on a network are open**.

LIST OF FIGURES

LIST OF FIGURES	PAGE NO
Screenshot	12
Screenshot	13
Screenshot	14

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	i
	LIST OF FIGURES	iii
1	INTRODUCTION	1
	1.1 Cyber Security	1
	1.2 Enumeration	3
	1.3 Network Enumeration	4
	1.4 Live Host Scanner	7
	1.5 Port Scanner	7
2	EXPERIMENTAL OR MATERIALS AND METHODS, ALGORITHMS USED	8
	2.1 Virtual Box	8
	2.2 Kali Linux	8
	2.3 Metasploitable	9
	2.4 python3	9
	2.5 Visual Studio Code	9
3	SUMMARY	10
	3.1 RESULTS	10
	3.2 CONCLUSIONS	11
4	REFERENCES	11
5	APPENDIX	11
	5.1 SCREENSHOTS	12
	2.2 SOURCE CODE	15

1 INTRODUCTION

1.1 Cyber Security

Cyber security is the **application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks.**

It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies.

How do cyber security works?

Cyber security is the **practice of defending your electronic systems, networks, computers, mobile devices, programs and data from malicious digital attacks.**

This type of security uses hardware and software to protect any data that's sent through your computer and other devices to the network.

Cyber Security Example

1. Examples of Network Security includes **Antivirus and Antispyware programs,**
2. Firewall that blocks unauthorized access to a network and VPNs (Virtual Private Networks)
3. used for secure remote access.

Advantages and Disadvantages of Cyber Security

Advantages:

- 1) Protects system against viruses, worms, spyware and other unwanted programs.
- 2) Protection against data from theft.
- 3) Protects the computer from being hacked.
- 4) Minimizes computer freezing and crashes.
- 5) Gives privacy to users

Disadvantages:

- 1) Firewalls can be difficult to configure correctly.
- 2) Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
- 3) Makes the system slower than before.
- 4) Need to keep updating the new software in order to keep security up to date.
- 5) Could be costly for average user.

1.2 Enumeration

Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.

Significance of enumeration

Enumeration is often considered as a critical phase in penetration testing, as the outcome of enumeration can be used directly for exploiting the system.

What are the goals of the Enumeration?

Goal 1 – To map the end-to-end details that we need to check after the enumeration step

Goal 2 - The ways to execute the attacks in the upcoming phases

Goal 3 – Identify all the information we need to do the execution in future testing

Goal 4 – Compile a list of devices with configuration for testing

Goal 5 – Complete the network map to finalize the steps for testing

Goal 6 – Compile the list of people who support the testing

Goal 7 – Collect even irrelevant information that might still be significant in the future

1.3 NETWORK ENUMERATION

Network enumeration is a process that involves gathering information about a network such as the hosts, connected devices, along with usernames, group information and related data. Using protocols like ICMP and SNMP, network enumeration offers a better view of the network for either protection or hacking purposes.

Network enumeration tools scan ports to gather information. They may also fingerprint the operating system. All of these are done for the purpose of looking more closely at how a network is set up and how data traffic is handled.

Some IT specialists refer to network enumeration as part of “ethical hacking” for security work. Some vulnerability scanners may perform network enumeration to try to protect a computer system. The idea is that, with network enumeration, vulnerabilities can be discovered, which can then be used by network/system administrators to fix the system or by hackers to attack the same.

Most vulnerability Scanners will also perform network enumeration task and a whole lot more, if you are looking for vulnerability scanners go to **Network Mapping Tools**.

USE OF NETWORK ENUMERATION

Network Enumeration is used by an attacker to establishes an active connection with the

victim and try to discover as much data by which a hacker (or cracker) can gain access to a

computer or network server in order to deliver a payload or malicious outcome which can be

used to exploit the systems further.

Network Enumeration can be used to Gain information on

- ✓ Usernames, Group name
- ✓ Hostnames
- ✓ Network shares and services
- ✓ IP tables and routing tables
- ✓ Service settings and Audit configurations
- ✓ Application and banners
- ✓ SNMP and DNS Details

List of network enumerators

- Metasploit Project.
- Nmap.
- Nessus.
- OpenVAS.
- SAINT (software)
- Security Administrator Tool for Analysing Networks.
- Map (software)

1.4 LIVE HOST SCANNER

A common method to accessing host systems is **by identifying and exploiting vulnerabilities in the operating system**, installed applications, and other programs. Tools such as Nessus are automated methods to evaluate systems for known vulnerabilities.

1.5 PORT SCANNER

A Port scan is **a method for determining which ports on a network are open.**

A port scanner is a computer program that checks network ports for one of three possible (statuses – open, closed, or filtered).

Port scanners are valuable tools in diagnosing network and connectivity issues. However, attackers use port scanners to detect possible access points for infiltration and to identify what kinds of devices you are running on the network, like firewalls, proxy servers or VPN servers. Here, we'll take you through the ins and outs of a port scanner

PORT SCANNING BASICS

A port scanner sends a TCP or UDP network packet and asks the port about their current

status. The three types of responses are below:

- **Open, Accepted:** The computer responds and asks if there is anything it can do for you.
- **Closed, Not Listening:** The computer responds that “This port is currently in use and unavailable at this time.”
- **Filtered, Dropped, Blocked:** The computer doesn’t even bother to respond.

2 EXPERIMENTAL OR MATERIALS AND METHODS, REQUIREMENTS USED

2.1 VIRTUAL BOX

Oracle **VM VirtualBox** is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation. **IT is a virtualization software.**

Operating system: Windows, macOS (only Intel-based Macs), Linux and Solaris.

USES OF VIRTUAL BOX

Oracle VM VirtualBox is cross-platform virtualization software. It **allows users to extend their existing computer to run multiple operating systems** including Microsoft Windows, MacOS X, Linux, and Oracle Solaris, at the same time.

2.2 KALI LINUX

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

USES OF KALI LINUX

Kali Linux is mainly used for **advanced Penetration Testing and Security Auditing**. Kali contains several hundred tools which are geared towards various information security tasks such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

2.3 METASPLOITABLE

Metasploitable is a **vulnerable system** that can be used as a target for attacks and security testing.

USE OF METASPOITABLE

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to **conduct security training, test security tools, and practice common penetration testing techniques**.

2.4 python3

Python is an interpreted high-level general-purpose programming language. Its design philosophy emphasizes code readability with its use of significant indentation. Its language constructs as well as its object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects.

2.5 Visual Studio Code

Visual Studio Code is a source-code editor made by Microsoft for Windows, Linux and macOS. 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

SYSTEM REQUIREMENTS

- ✓ 1TB HDD
- ✓ 8 GB RAM

TOOLS USED

- Install Virtual Box (Virtualization)
- Install Kali Linux (Main Operating System)
- Install Metasploitable (Vulnerable Machine)
- Install Visual Studio Code (Text Editor)
- Install python3
- `sudo python3 filename`

Result

- ✓ NETWORK ENUMERATION is the important stage in Cyber Security.
- ✓ By using this tool, we can save the Time.
- ✓ So, I want to automate. & This tool is Reliable.

CONCLUSION

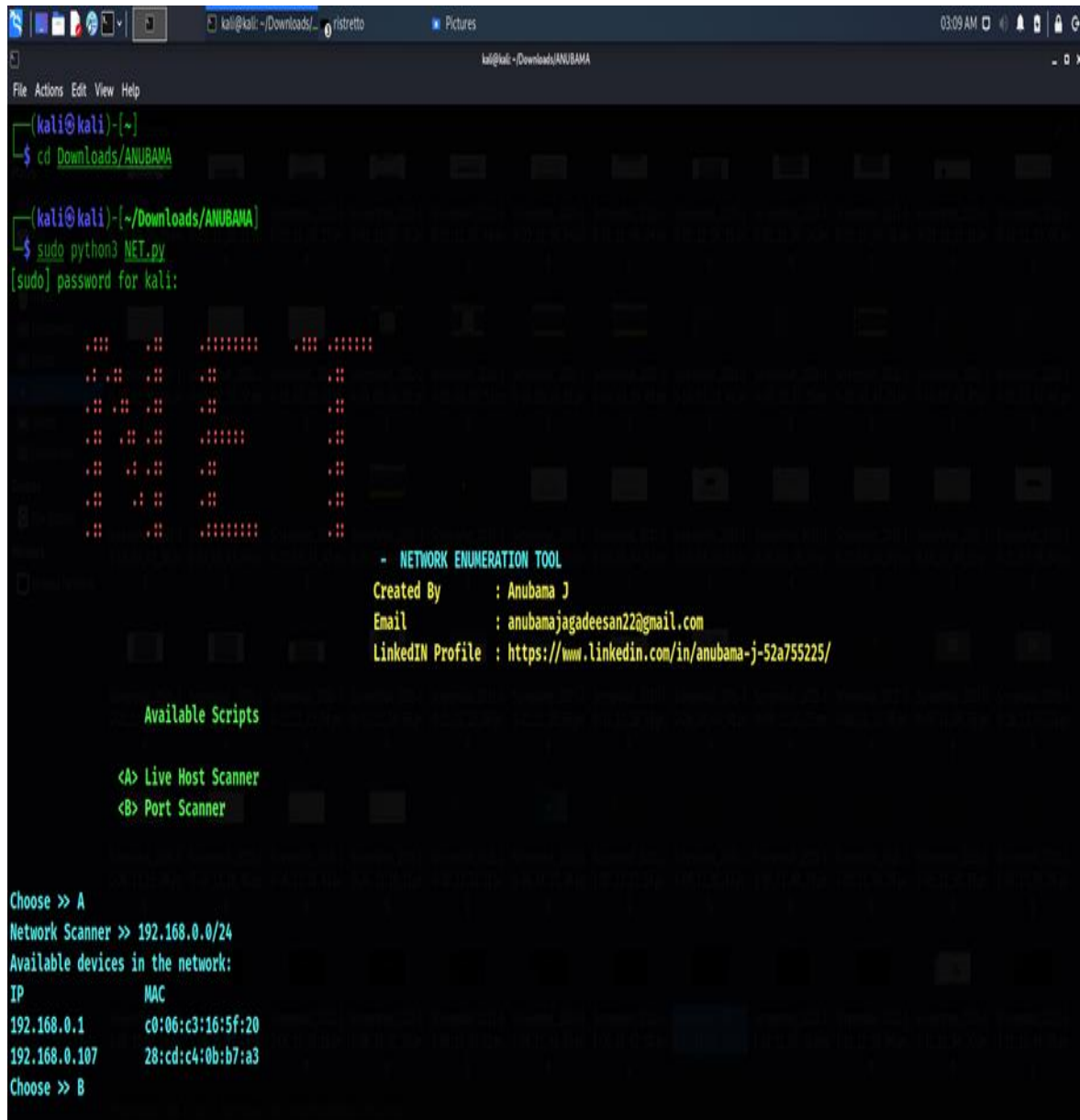
- ▶ **THUS, the tool I have been implemented has been executed success fully.**

REFERENCES

- **Red Team Field Manual (BOOK)**
- **Black Hat Python second edition (BOOK)**
- **Github.com**
- **Google.com**

APPENDIX

SCREENSHOTS OF OUTPUT



```
kali@kali: ~/Downloads/
File Actions Edit View Help
192.168.0.107      28:cd:c4:0b:b7:a3
Choose >> B
IP Address >> 192.168.0.102
Scanning target 192.168.0.102
Time started: 2021-11-13 03:28:39.740075
Port 21 is open
Port 22 is open
Port 23 is open
Port 25 is open
Port 80 is open
Port 111 is open
Port 139 is open
Port 445 is open
Port 512 is open
Port 513 is open
Port 514 is open
Port 1099 is open
Port 1524 is open
Port 2049 is open
Port 2121 is open
Port 3306 is open
Port 3632 is open
Port 5432 is open
Port 5900 is open
Port 6000 is open
Port 6667 is open
Port 6697 is open
Port 8009 is open
Port 8180 is open
```

```
kali@kali: ~/Downloads/... 03:29 AM
kali@kali: ~/Downloads/ANUBAMA
File Actions Edit View Help
Port 23 is open
Port 25 is open
Port 80 is open
Port 111 is open
Port 139 is open
Port 445 is open
Port 512 is open
Port 513 is open
Port 514 is open
Port 1099 is open
Port 1524 is open
Port 2049 is open
Port 2121 is open
Port 3306 is open
Port 3632 is open
Port 5432 is open
Port 5900 is open
Port 6000 is open
Port 6667 is open
Port 6697 is open
Port 8009 is open
Port 8180 is open
Port 8787 is open
Port 34098 is open
Port 41764 is open
Port 42674 is open
Port 49473 is open
Choose >> exit

(kali@kali) - [~/Downloads/ANUBAMA]
$
```

SOURCE CODE

LiveHost.py

```
from scapy.all import ARP, Ether, srp

def livehost():

    target_ip = input("Network Scanner >> ")

    arp = ARP(pdst=target_ip)

    ether = Ether(dst="ff:ff:ff:ff:ff:ff")

    packet = ether/arp

    result = srp(packet, timeout=3, verbose=0)[0]

    clients = []

    for sent, received in result:

        clients.append({'ip': received.psrc, 'mac': received.hwsrc})

    print("Available devices in the network:")

    print("IP" + " " * 18 + "MAC")

    for client in clients:

        print("{:16} {}".format(client['ip'], client['mac']))

if __name__ == "__main__":

    livehost()
```

PortScanner

```
#!/usr/bin/env python

import sys

import socket

from datetime import datetime

def PortScanner():

    target = input("IP Address >> ")

    print("-" * 50)

    print("Scanning target "+target)

    print("Time started: "+str(datetime.now()))

    print("-" * 50)

    try:

        for port in range(1,65535):

            s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

            socket.setdefaulttimeout(1)

            result = s.connect_ex((target,port))

            # print("Checking port {}".format(port))
```

```

if result == 0:

    print("Port {} is open ".format(port))

    s.close()

except KeyboardInterrupt:

    print("\nExiting program. ")

    sys.exit()

except socket.gaierror:

    print("Hostname could not be resolved. ")

    sys.exit()

except socket.error:

    print("Couldn't connect to server. ")

    sys.exit()

if __name__=="__main__":

    PortScanner()

```

NET.py

```

from LiveHost import livehost

from PortScanner import PortScanner

R = '\033[1;31;20m'

```

G = '\033[1;32;20m'

C = '\033[1;36;20m'

Y = '\033[1;33;20m'

B = '\033[1;37;20m'

print("")

print(R+" .:. .: .:.:.:. .:. .:. ")

print(R+" .: .: .: .: .: ")

print(R+" .:. .: .: .: .: ")

print(R+" .: .: .: .:.:. .: ")

print(R+" .: .: .: .: .: ")

print(R+" .: .: .: .: .: ")

print(R+" .: .: .:.:. .: ")

print(C+" - NETWORK ENUMERATION
TOOL")

print(Y+" Created By : Anubama J
")

print(Y+" Email :
anubamajagadeesan22@gmail.com ")

print(Y+" LinkedIn Profile :
<https://www.linkedin.com/in/anubama-j-52a755225/> ")

```
print(G+"""
```

Available Scripts

<A> Live Host Scanner

** Port Scanner**

```
""")
```

```
def net():
```

```
inp=(input(C+"Choose >> "))
```

```
if(inp == 'A'):
```

```
livehost()
```

```
elif (inp=='B'):
```

```
PortScanner()
```

```
elif(inp=='exit'):
```

```
exit()
```

```
elif(inp=='ls'):
```

```
print(G+""""Tools available
```

<A> Live Host Scanner

** Port Scanner**

usage:type exit to stop

```
""")
```

else:

print(R+"Enter an valid option")

while True:

net()

if __name__=="__main__":

net()