

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 Degree in

Information Technology

By

Aishwaryalakshmi.k
(Reg. No. 39120005)



DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING

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

(Established under Section 3 of UGC Act, 1956)
Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600119
www.sathyabamauniversity.ac.in



APRIL 2022



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 INFORMATION TECHNOLOGY

BONA FIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **Aishwaryalakshmi.k** (Reg. No: 39120005) who carried out the project entitled “**Perform OS discovery and scan beyond IDS and Firewall**” under my supervision from March 2022 to April 2022.

Internal Guide

Dr. V.Maria Anu M.E., Ph.D.,

Head of the Department

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

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I, **Aishwaryalakshmi.k** (Reg. No. 39120005) hereby declare that the Project report entitled "**Perform OS discovery and scan beyond IDS and Firewall**" done by me under the guidance of **Dr. V.Maria Anu M.E., Ph.D.**, is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology 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 INSTITUTE OF SCIENCE AND TECHNOLOGY** 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** and **Dr. R SUBHASHINI, M.E., Ph.D., Head 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.V.Maria Anu M.E., Ph.D.,** for her 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



ABSTRACT

Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology (OT) security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries. Use of the term “cybersecurity” as a key challenge and a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines. Recommendation for security leaders is that they should use the term “cybersecurity” to designate only security practices related to the defensive actions involving or relying upon information technology and/or OT environments and systems. Within this paper, we are aiming to explain “cybersecurity” and describe the relationships among cybersecurity, information security, OT security, IT security, and other related disciplines and practices, e.g. cyber defence, related to their implementation aligned with the planned or existing cybersecurity strategy at the national level. In the case study given example of The National Cybersecurity Strategy of the Republic of Croatia and Action plan is presented and elaborated. The Strategy's primary objective is to recognize organizational problems in its implementation and broaden the understanding of the importance of this issue in the society. In this we see OS discovery and scan beyond IDS and firewall. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on aa organization's previously established security policies. As its most basic, a firewall is essentially the barrier that sites between a private internal network and the public internet.

TABLE OF CONTENTS

Chapter No.	TITLE	Page No.
	ABSTRACT	i
	LIST OF ABBREVIATIONS	ii
1.	INTRODUCTION	1
1.1	WHAT IS OS DISCOVERY?	1
1.2	WHAT IS IDS AND FIREWALL?	1
1.3	REQUIREMENTS FOR SCANNING	2
2.	PERFORM OS DISCOVERY	
2.1	AIM	3
2.3	VIRTUAL BOX	3
2.4	EXECUTION: SCANNING BEYOND IDS AND FIREWALL	4
3.	SUMMARY AND CONCLUSIONS	8
	REFERENCE	9
	APPENDIX	18
	A. SOURCE CODE	10
	B. SCREENSHOTS	14

LIST OF ABBREVIATIONS

IDS	-	Intrusion Detection System
App	-	Application
Chars	-	Characters
IPS	-	Intrusion Prevention System
Acc	-	According
OS	-	Operating System
aspx	-	Active server pages
IIS	-	Internet Information System

CHAPTER 1

INTRODUCTION

1.1 What is OS DISCOVERY?

Banner grabbing or OS fingerprinting is the method used to determine the operating system running on a remote target system. There are two types of banner grabbing there are active and passive. Identifying the OS used on the target host allows an attacker to figure out the vulnerabilities possessed by the system and the exploits that might work on a system to further carry out additional attacks.

In active banner grabbing specify crafted packets are sent to the remote OS and the responses are noted. The responses are then compared with a database determine the OS. Responses from different uses vary due to differences in the TCP/IP stack implementation

In passive banner grabbing there are three methods. Firstly, banner grabbing from error messages provide information such as the type of server, type of OS and SSL tool used by the remote target remote system. Secondly, In sniffing the network traffic they capture and analyze packets from the targets enables an attacker to determine the OS used by the remote system .Lastly, and banner grabbing from page extensions they capture and analyzing packets from the target enables an attacker to determine the OS used by the remote target system.Eg.aspx => IIS server and windows platform.

1.2 WHAT IS IDS AND FIREWALL?

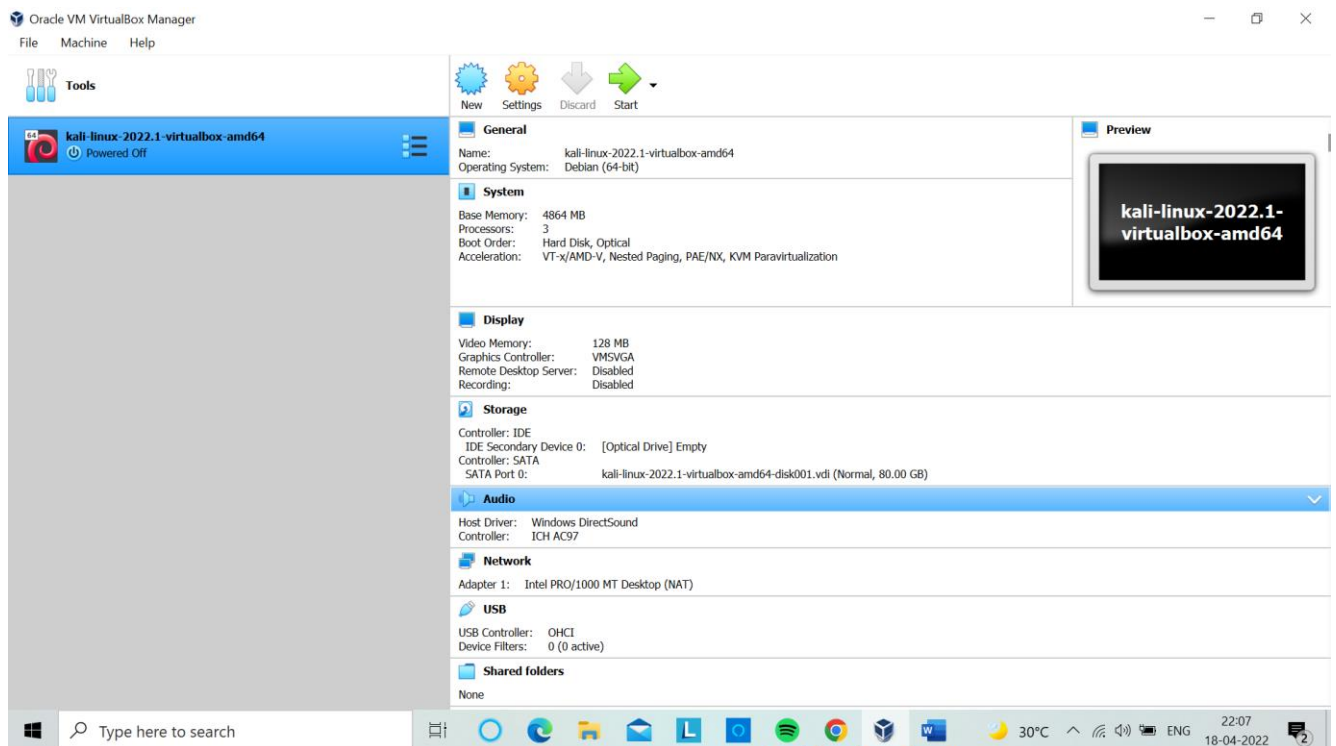
Through firewalls and IDSs can prevent malicious traffic(packets) from entering a network , attackers can manage to send intended packets to the target by evading and IDS or firewall through the following techniques:-

- Packet Fragmentation
- Source Routing
- Source Port Manipulation
- IP Address Decoy
- IP Address Spoofing
- Creating Custom Packet
- Randomizing Host Order
- Sending Bad Checksums

- Anonymizers

1.3 REQUIREMENTS FOR STARVATION:

- Install Kali linux
- Install Virtual Box
- Install Metasploitable
- Launch the terminal stimulation



(2)

CHAPTER 2

AIM AND SCOPE OF THE PRESENT INVESTIGATION

2.1 Aim:

This project aims to do Perform OS discovery and scan beyond IDS and Firewall in kali linux.

2.2 Functional Requirements:

To execute this attack , some major tools are being used. The tools used in this attack are listed below:

❖ Kali linux:

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

The advantages of the kali linux is more than 600 penetration tools included. Adherence of file system hierarchy standard open development tree. Multiple language support. completely customizable free(as in beer) and always will be wide ranging wireless device support.

2.3 Virtual box:

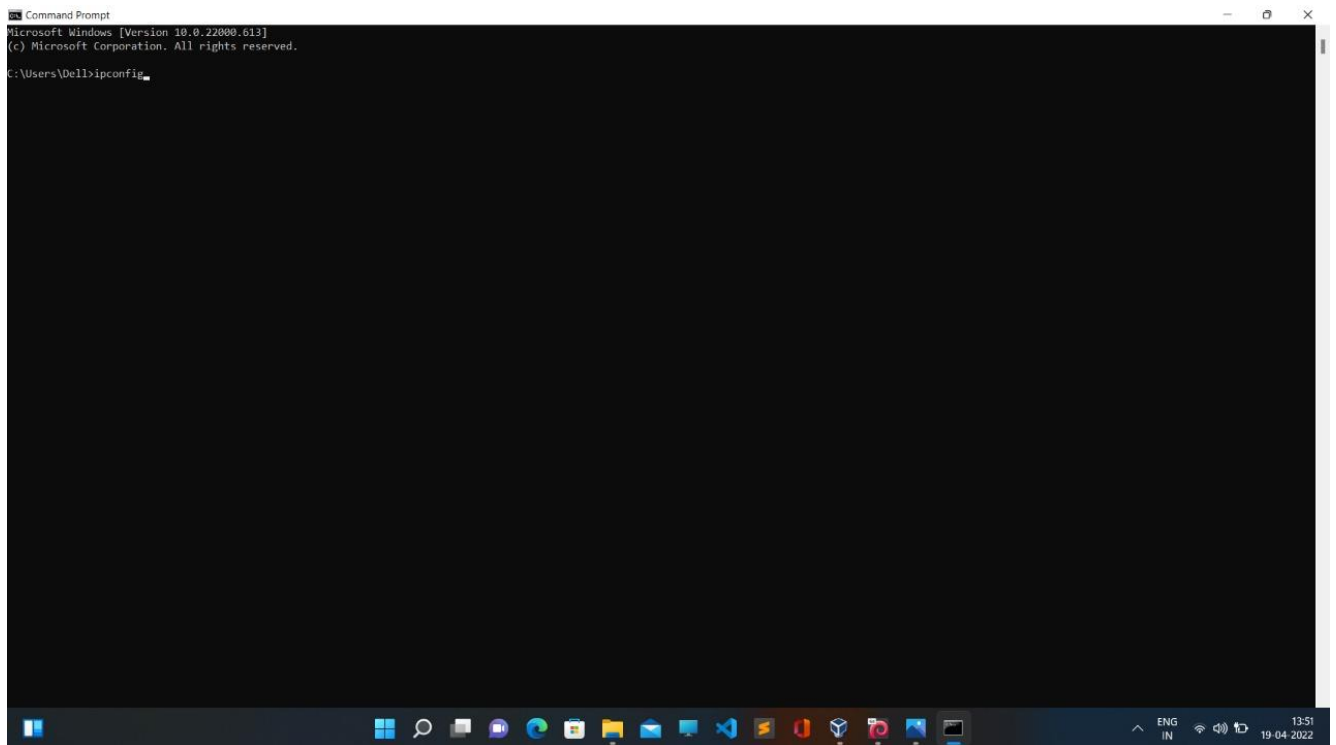
Oracle VM VirtualBox is cross-platform virtualization software. It allows users to extend their existing computer to run multiple operating systems including Microsoft Windows, Mac OS X, Linux, and Oracle Solaris, at the same time.

VirtualBox is designed to run virtual machines on your physical machine without reinstalling your OS that is running on a physical machine. One more VirtualBox advantage is that this product can be installed for free. A virtual machine (VM) works much like a physical o

PERFORM OS DISCOVERY AND SCAN BEYOND IDS AND FIREWALL

In this we can see the firewalls and IDSs can prevent malicious traffic(packets) from entering a network, attackers can manage to send intended packets to the target by evading and IDSs or firewall through the several techniques.

1. Discover the IP Address



```
Command Prompt
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Dell>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bda8:6e5f:9aa3:67fb%8
    Autoconfiguration IPv4 Address. . : 169.254.103.251
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

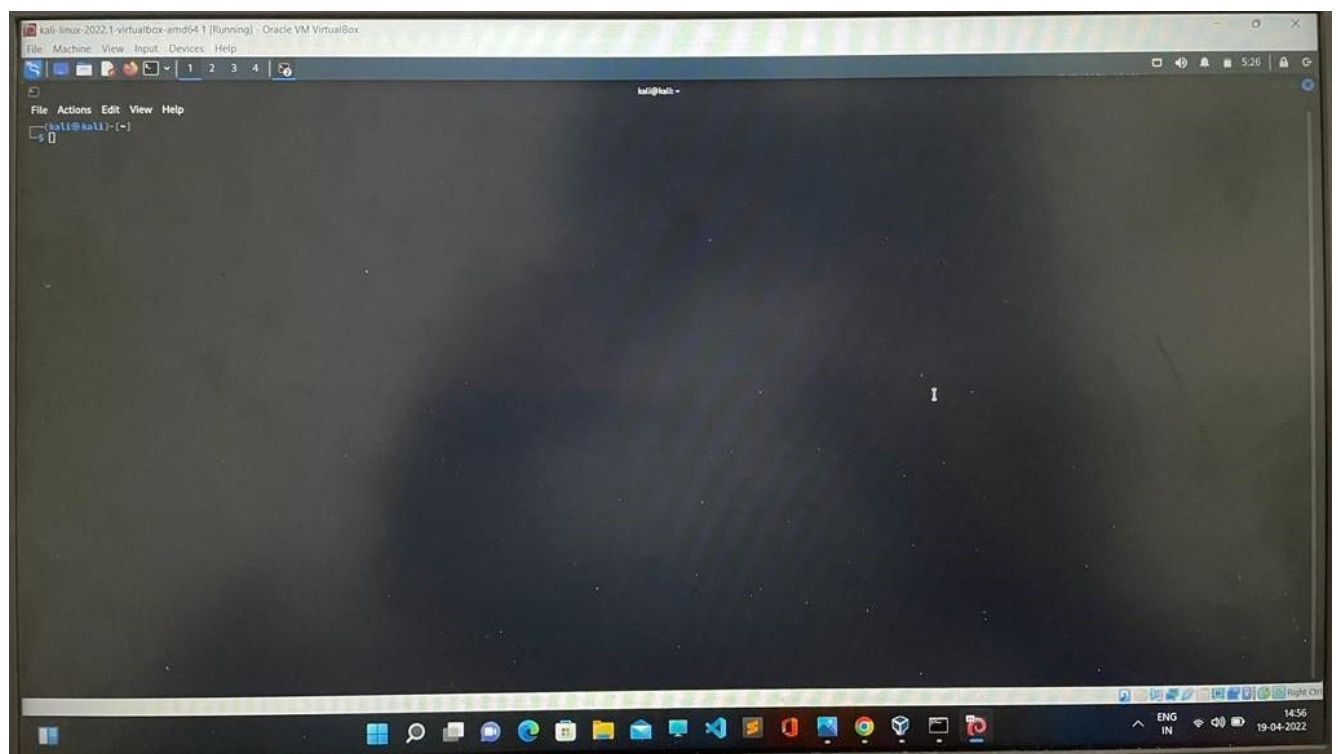
Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

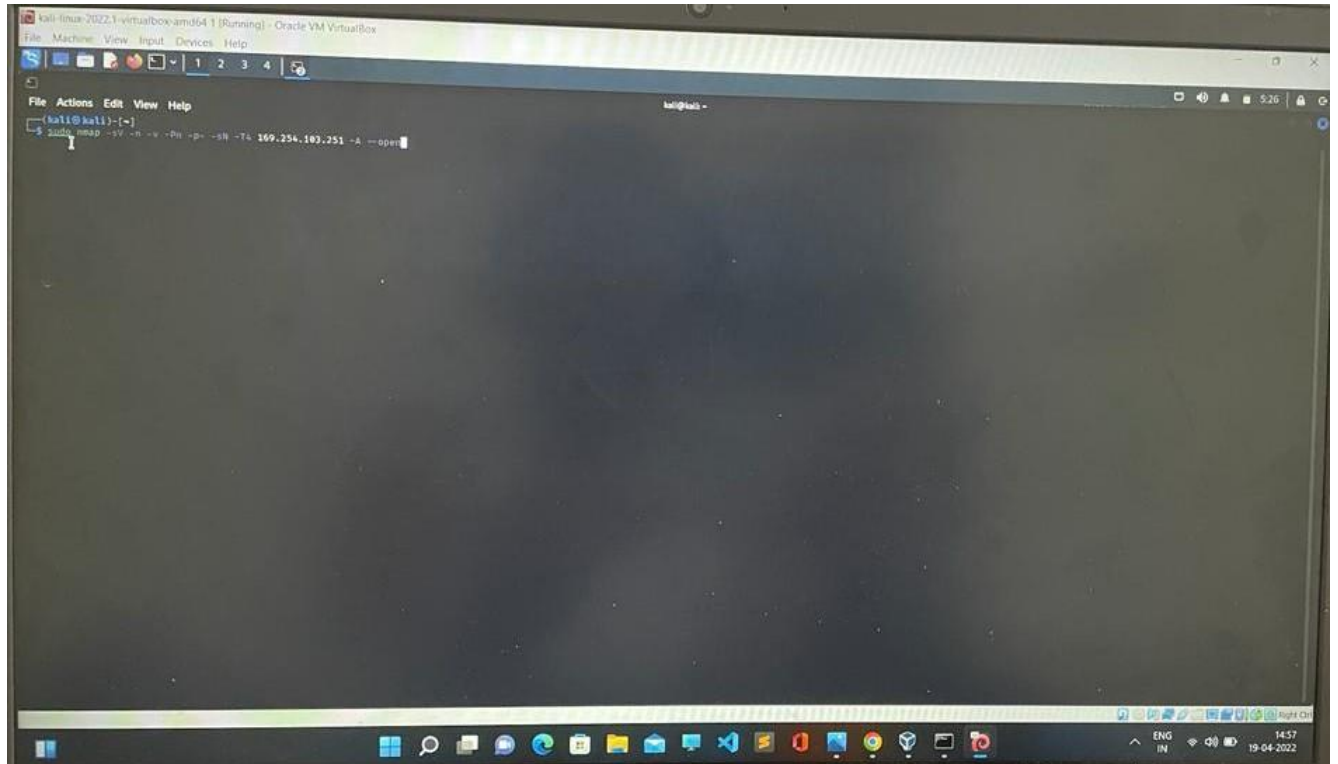
    Connection-specific DNS Suffix  . : domain.name
    Link-local IPv6 Address . . . . . : fe80::f4a0:b18e:4118:43ef%17
    IPv4 Address. . . . . : 192.168.100.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::12be:f5ff:fe7b:6b23%17
    . . . . . : 192.168.100.1

C:\Users\Dell>
```



(5)

Terminal emulator of linux.



```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```

Warning: Never expose this VM to an untrusted network!

```

C:\Windows\system32\cmd.exe
U=Certification Services Division, O="thawte, Inc.", C=US" added to store.
virtualbox-iso: CertUtil: -addstore command completed successfully.
virtualbox-iso:
virtualbox-iso: C:\Users\vagrant>cmd /c certutil -addstore -f "Root" A:\utn-userfirst.cer
==> virtualbox-iso: Gracefully halting virtual machine...
virtualbox-iso: Removing floppy drive...
==> virtualbox-iso: Preparing to export machine...
virtualbox-iso: Deleting forwarded port mapping for the communicator (SSH, WinRM, etc) (host port 3487)
==> virtualbox-iso: Exporting virtual machine...
virtualbox-iso: Executing: export packer-virtualbox-iso-1497355880 --output output-virtualbox-iso\packer-virtualbox-iso-1497355880.ovf

==> virtualbox-iso: Unregistering and deleting virtual machine...
==> virtualbox-iso: Running post-processor: vagrant
==> virtualbox-iso (vagrant): Creating Vagrant box for 'virtualbox' provider
virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\packer-virtualbox-iso-1497355880-disk001.vmdk

virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\packer-virtualbox-iso-1497355880.ovf
virtualbox-iso (vagrant): Renaming the OVF to box.ovf...
virtualbox-iso (vagrant): Using custom Vagrantfile: vagrantfile-windows_2008_r2.template
virtualbox-iso (vagrant): Compressing: Vagrantfile
virtualbox-iso (vagrant): Compressing: box.ovf
virtualbox-iso (vagrant): Compressing: metadata.json
virtualbox-iso (vagrant): Compressing: packer-virtualbox-iso-1497355880-disk001.vmdk
Build 'virtualbox-iso' finished.

==> Builds finished. The artifacts of successful builds are:
--> virtualbox-iso: 'virtualbox' provider box: windows_2008_r2_virtualbox.box

C:\Users\admin\Desktop\metasploitable3-master\metasploitable3-master>

```

CHAPTER 3

SUMMARY AND CONCLUSIONS

- **SUMMARY:**

IDS will stop working if the target host keeps the session active for long time.

The principle of this attack is very simple:

All traffic from outside to inside vice-versa passes through the firewall

Only authorized traffic, as defined by local security policy, will be allowed to pass

The objective is achieved by installing kali linux.

The firewall itself is immune to penetration.

- **CONCLUSION:**

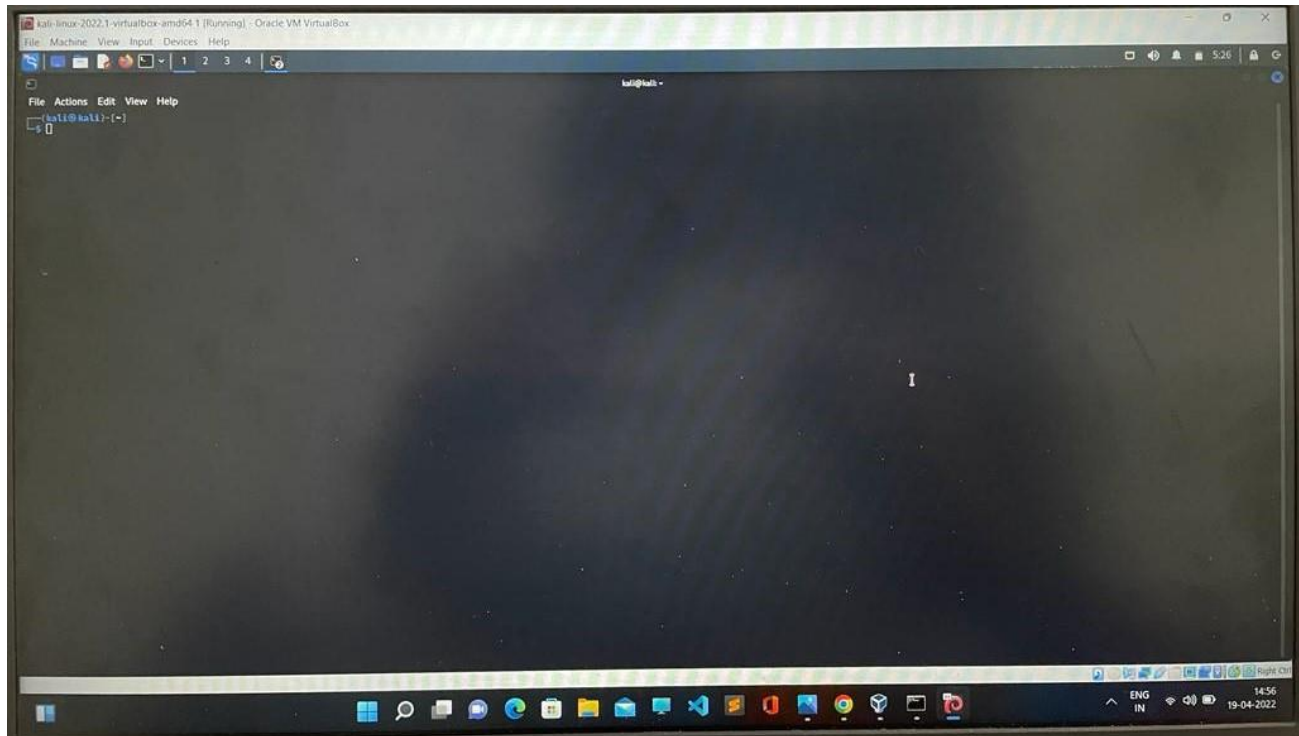
By passing or evasion of IDS and Firewall devices are not only for Bypassing and sending up for payload. Its all about the evaluation of security measures at place.

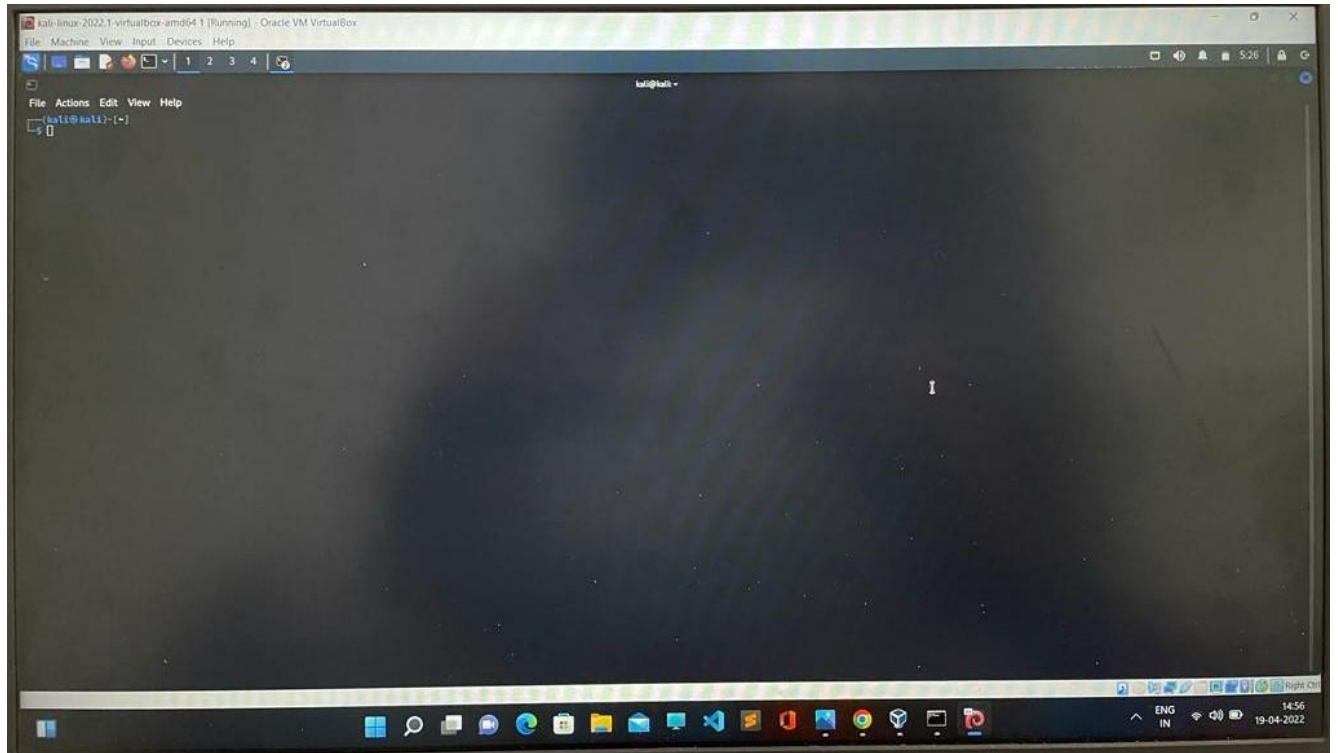
REFERENCES:

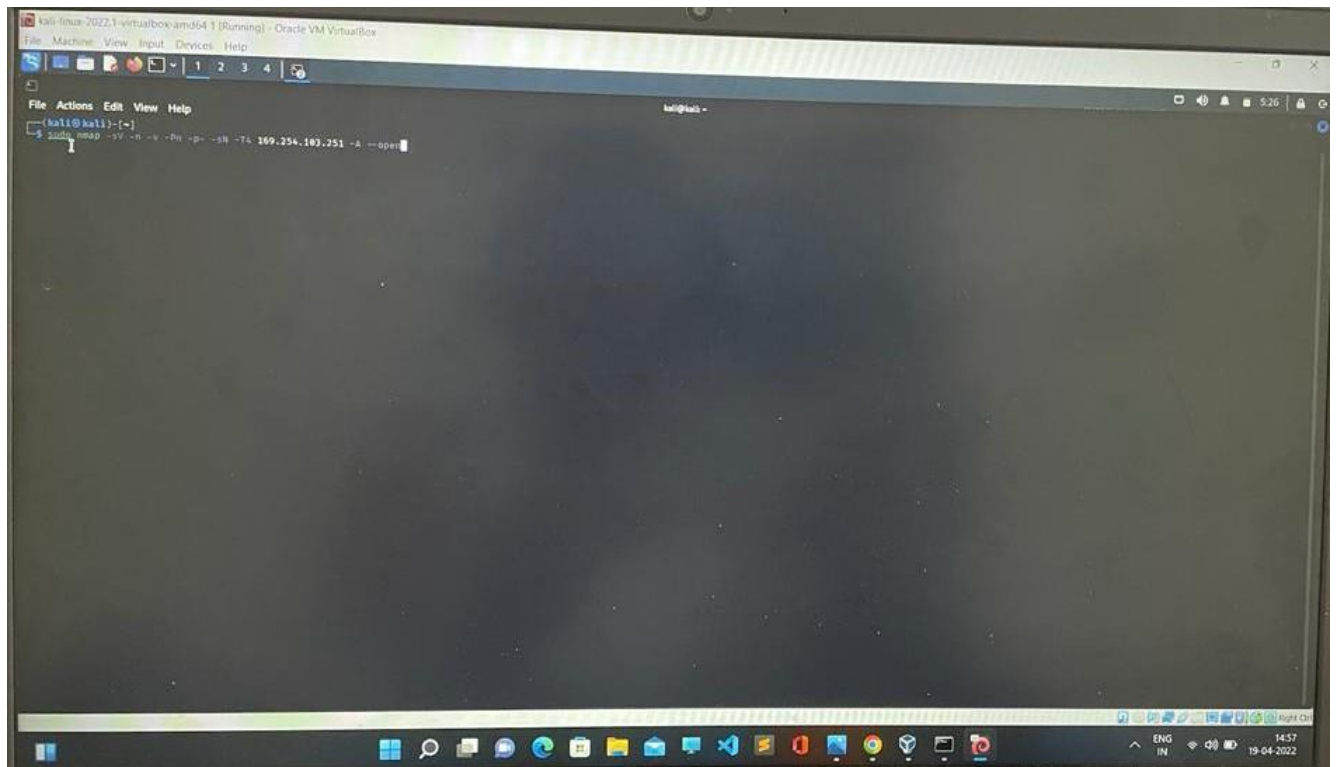
1. Try me hack(website)
2. Google.com
3. YouTube

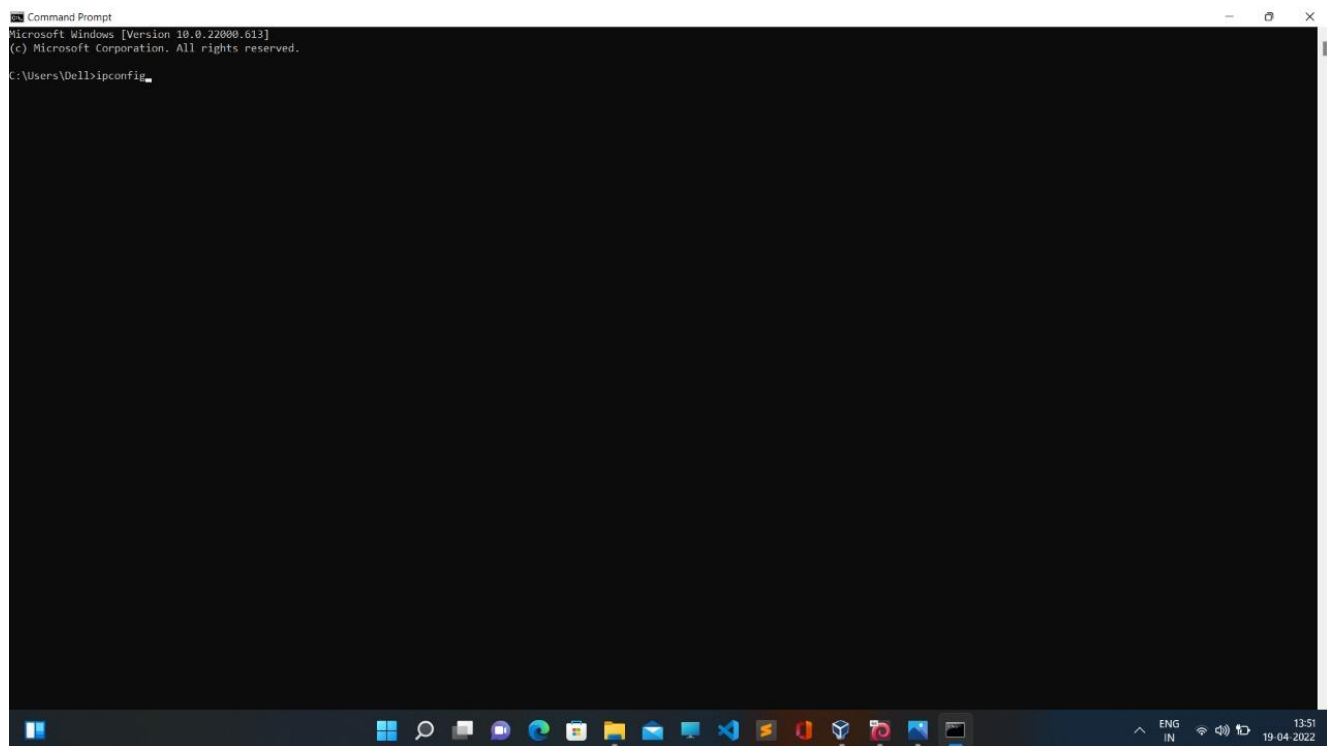
APPENDIX

A. SOURCE CODE

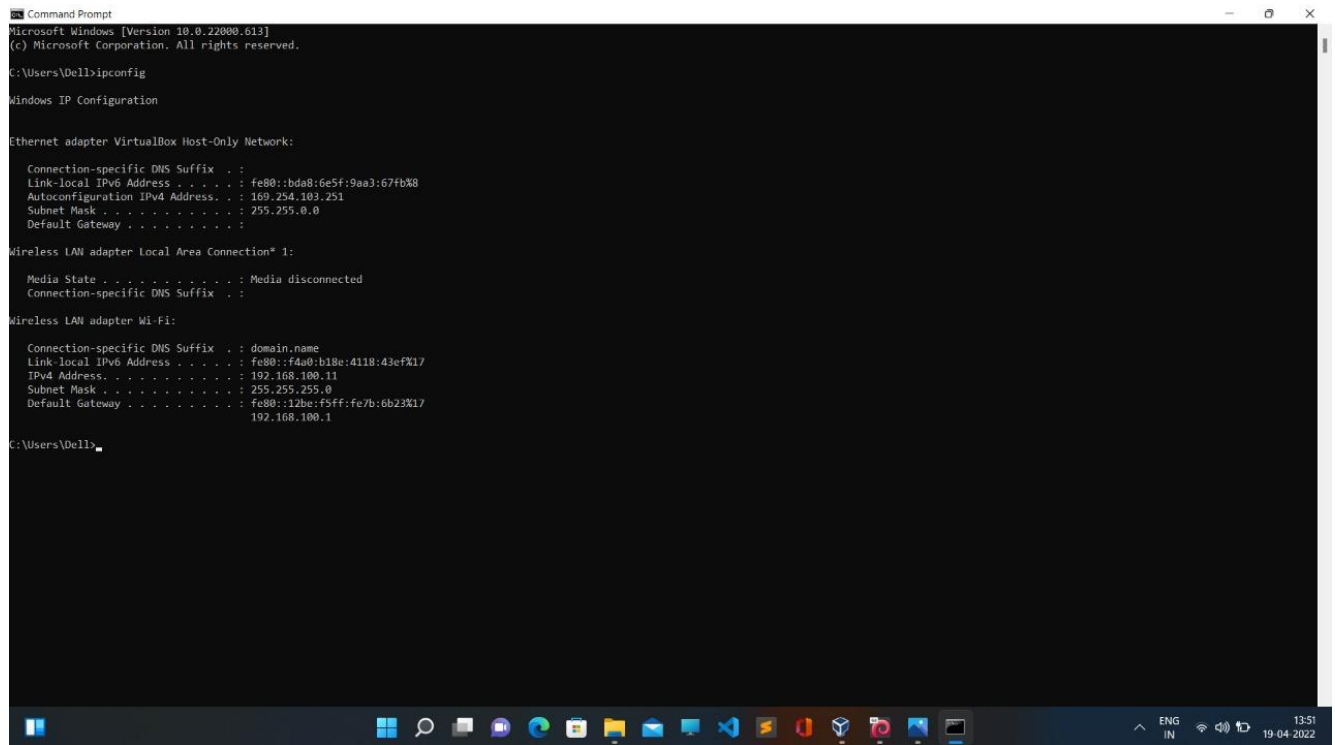








B. SCREENSHOT



```
Command Prompt
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Dell>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bda8:6e5f:9aa3:67fb%8
    Autoconfiguration IPv4 Address. . : 169.254.103.251
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : domain.name
    Link-local IPv6 Address . . . . . : fe80::f4a0:b18e:4118:43ef%17
    IPv4 Address. . . . . : 192.168.100.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::12be:f5ff:fe7b:6b23%17
                                192.168.100.1

C:\Users\Dell>
```



```

Select C:\Windows\system32\cmd.exe
U=Certification Services Division, O="thawte, Inc.", C=US" added to store.
virtualbox-iso: CertUtil: -addstore command completed successfully.
virtualbox-iso:
virtualbox-iso: C:\Users\vagrant>cmd /c certutil -addstore -f "Root" A:\utn-userfirst.cer
==> virtualbox-iso: Gracefully halting virtual machine...
virtualbox-iso: Removing floppy drive...
==> virtualbox-iso: Preparing to export machine...
virtualbox-iso: Deleting forwarded port mapping for the communicator (SSH, WinRM, etc) (host port 3487)
==> virtualbox-iso: Exporting virtual machine...
virtualbox-iso: Executing: export packer-virtualbox-iso-1497355880 --output output-virtualbox-iso\packer-virtualbox-iso-1497355880.ovf
==> virtualbox-iso: Unregistering and deleting virtual machine...
==> virtualbox-iso: Running post-processor: vagrant
==> virtualbox-iso (vagrant): Creating Vagrant box for 'virtualbox' provider
virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\packer-virtualbox-iso-1497355880-disk001.vmdk

virtualbox-iso (vagrant): Copying from artifact: output-virtualbox-iso\packer-virtualbox-iso-1497355880.ovf
virtualbox-iso (vagrant): Renaming the OVF to box.ovf...
virtualbox-iso (vagrant): Using custom Vagrantfile: vagrantfile-windows_2008_r2.template
virtualbox-iso (vagrant): Compressing: Vagrantfile
virtualbox-iso (vagrant): Compressing: box.ovf
virtualbox-iso (vagrant): Compressing: metadata.json
virtualbox-iso (vagrant): Compressing: packer-virtualbox-iso-1497355880-disk001.vmdk
Build 'virtualbox-iso' finished.

==> Builds finished. The artifacts of successful builds are:
--> virtualbox-iso: 'virtualbox' provider box: windows_2008_r2_virtualbox.box

C:\Users\admin\Desktop\metasploitable3-master\metasploitable3-master>_

```

