REMOTE ACCESS USING LINUX

A PROJECT REPORT

Submitted in partial fulfilment for the award of the degree of

B.TECH

In

COMPUTER SCIENCE

By

EASHAN SINGH GILL	16BCE0899
KURAKULA MONA TEJA	16BCE2110
KONAPALLI PAVAN KUMAR REDDY	16BCE0073
JASDEEP SINGH	16BEC0364

Under the Guidance of PROF.VIJAYARAJAN.V

School of COMPUTER SCIENCE & Engineering

NOVEMBER, 2017.

DECLARATION BY THE CANDIDATE

I hereby declare that the project report entitled **"REMOTE ACCESS USING LINUX"** submitted by me to VIT University, Vellore in partial fulfilment of the requirement for the award of the degree of **B.Tech(Computer Science)** is a record of J component of project work carried out by me under the guidance of **Prof.VIJAYARAJAN.V** I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: Vellore

Date: 8th November, 2017.

EASHAN SINGH GILL
KURAKULA MONA TEJA
KONAPALLI PAVAN KUMAR REDDY
JASDEEP SINGH

➢ CONTENTS

INTRODUCTION

- In the real world the major threat to our society is cyber-crime and un-authorized access to our data.
- so we will discuss the ways how the criminals are getting the unauthorized data from the users and we will suggest the users how can we reduce this crimes and how can they protect their own data from the third party
- Here we are discussing the one of the main problems in public networks and how they can get the private data from us like our bank details , passwords etc.
- The best way we can reduce these attacks just not connecting to the public wi-fi and creating strong passwords to our accounts cannot be cracked by the brute force method.
- So for understanding the ways they are doing let us understand the concept behind the method.

INSTALLATION OF LINUX

Basically in my context LINUX is a Unix-like computer operating system assembled under the model of free and open-source software development and distribution.

ABSTRACT

In, our project we are trying to access other devices or restrict other devices by using Linux on our pc.

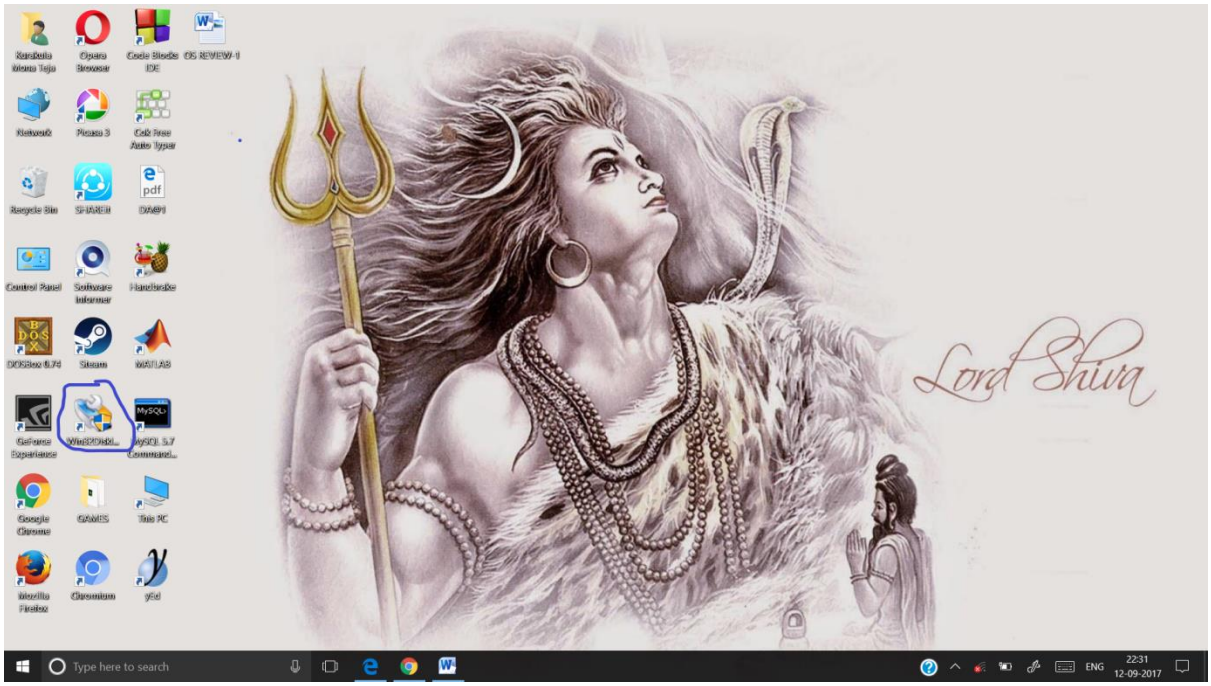
PROCESS OF INSTALLATION

STEP1:-

Download the LINUX image file.

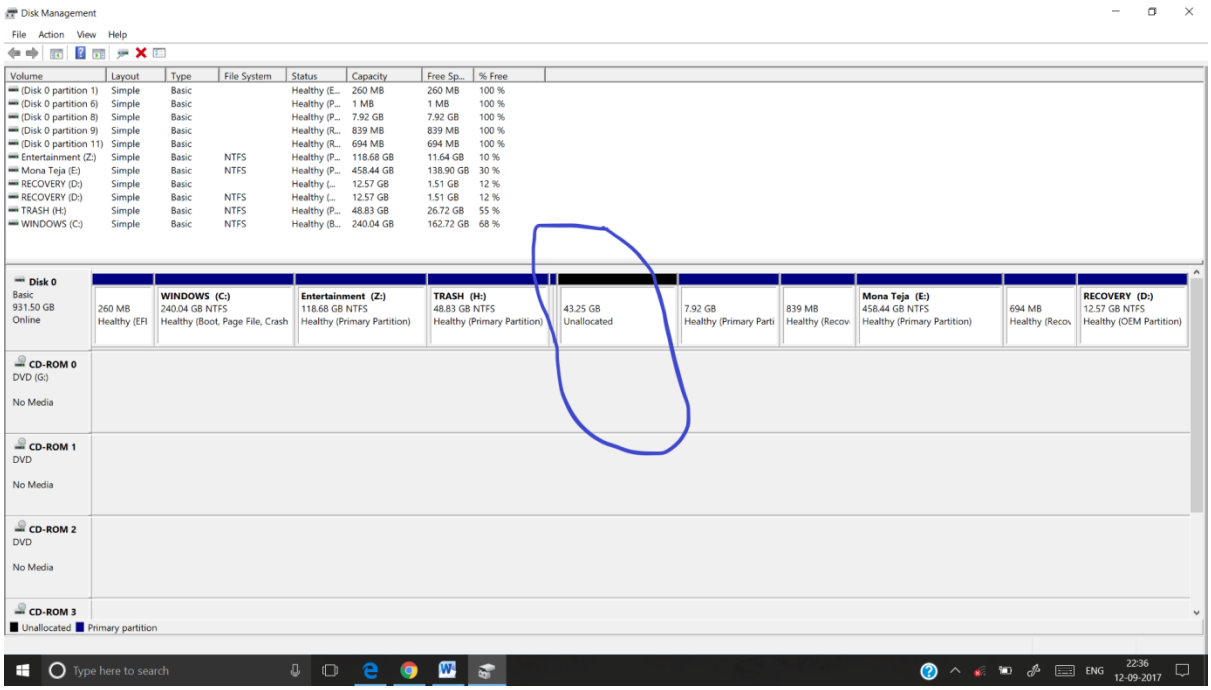
STEP2:-

Take a USB and make it a bootable USB using win32 Diskette and it will copy then required boot files into the USB and make it useful for booting.



STEP3:-

Go to disk Management and create a partition and unallocated the memory because we need some space to work with other OS i.e. Linux in our case.



STEP4:-

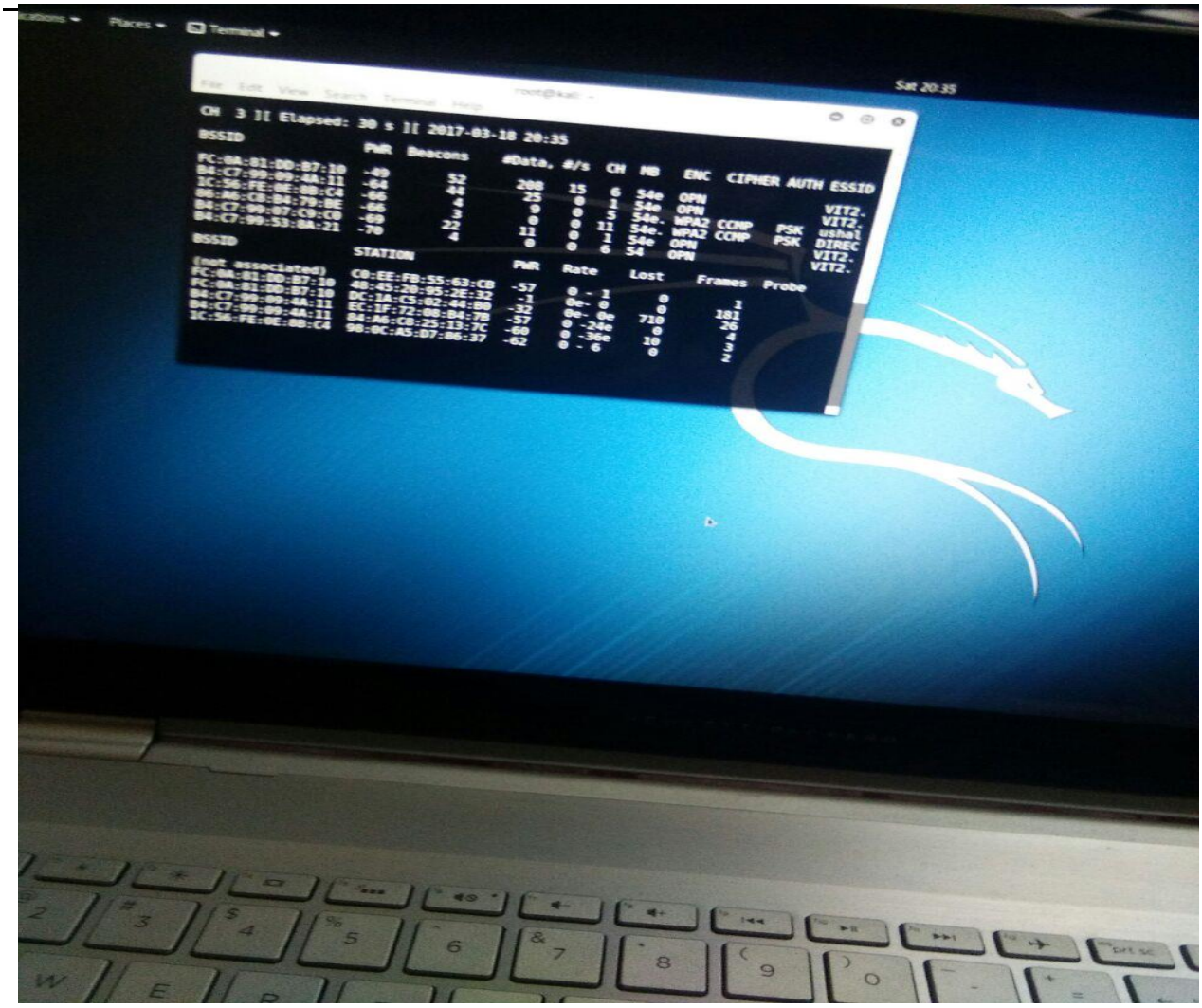
Now while booting by pressing F10 got to Boot Menu and change the priority to USB from OS in Hard drive of the PC then save changes and exit then it will live boot using the files in the USB the boot strap loader will load the files into

the unallocated memory which serves as RAM for our secondary OS or else we can install on the same hard drive and dual boot the PC. (After installation of LINUX)

STEP5:-

Then for now we used some inbuilt commands in the LINUX called KALI LINUX we have accessed the networks around us and learnt how to use it and access other pc so in Future we thought of working on system calls and payloads.

EXECUTION OF LINUX AFTER INSTALLATION:



ABSTRACT

- In this project we are going to explain the methods and ways to exploit the devices which are connected in the same network.
- Here we going to explain the step by step procedure to exploit the device which is connected in the same network.
- So in this way we can describe the drawbacks of present technology and we can also suggest to ways to improve the security of the devices .
- In this project we are going to explain the methods and ways to exploit the devices which are connected in the same network.
- Here we going to explain the step by step procedure to exploit the device which is connected in the same network.
- So in this way we can describe the drawbacks of present technology and we can also suggest to ways to improve the security of the devices.

PEN TESTING (PENETRATION TESTING)

- Penetration testing (additionally called pen testing) is the act of testing a PC framework, system or Web application to discover vulnerabilities that an assailant could misuse.
- Pen tests can be computerized with programming applications or they can be performed physically.
- In any case, the procedure incorporates gathering data about the objective before the test (surveillance), recognizing conceivable passage focuses, endeavouring to soften up (either basically or without a doubt) and revealing back the discoveries.
- The principle target of penetration testing is to decide security shortcomings.
- A pen test can likewise be utilized to test an association's security arrangement consistence, its representatives' security mindfulness and the association's capacity to recognize and react to security occurrences.

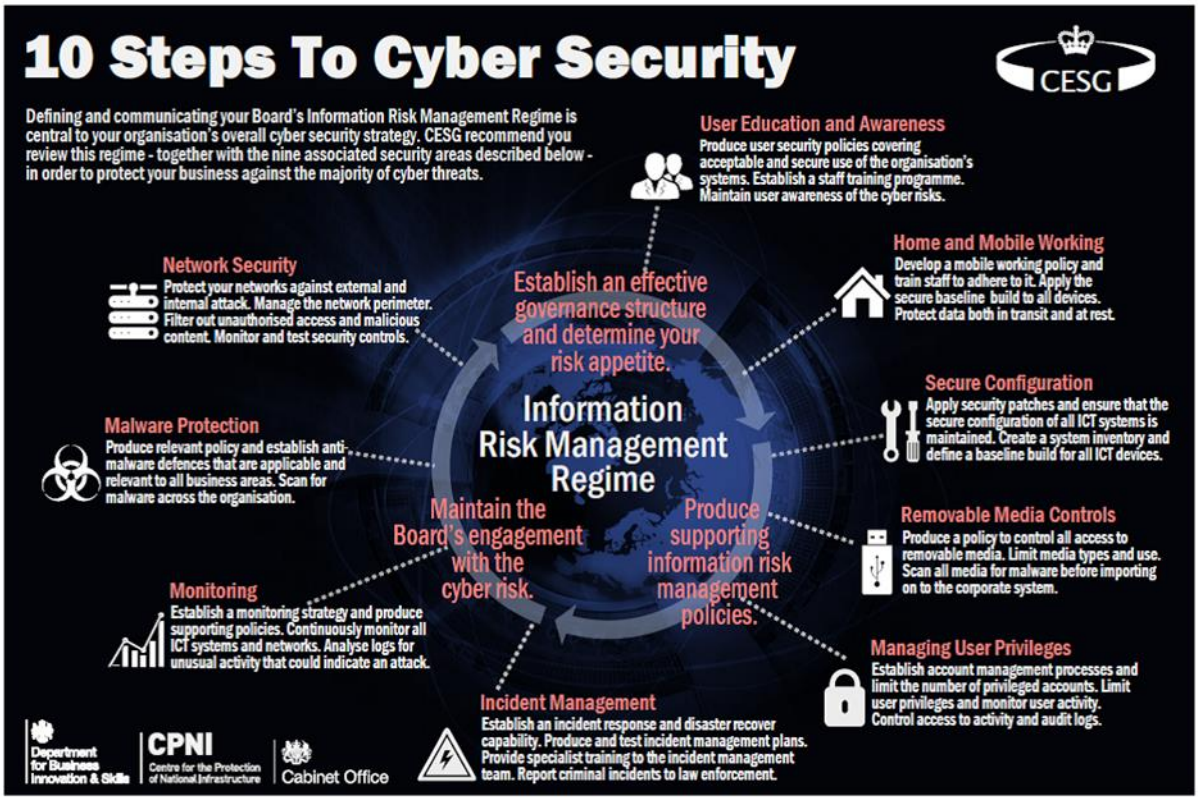
USAGE

- Penetration tests are now and then called white hat hacker methods because they use these methods to find the vulnerabilities in their network and they start modifying it and they also strengthens the security of the system
- Pen test procedures also include Targeted testing, external testing , internal testing ,blind testing, double blind testing . for our convenience we have chosen the kali Linux plat form to explain the problems that occurs in the real world.

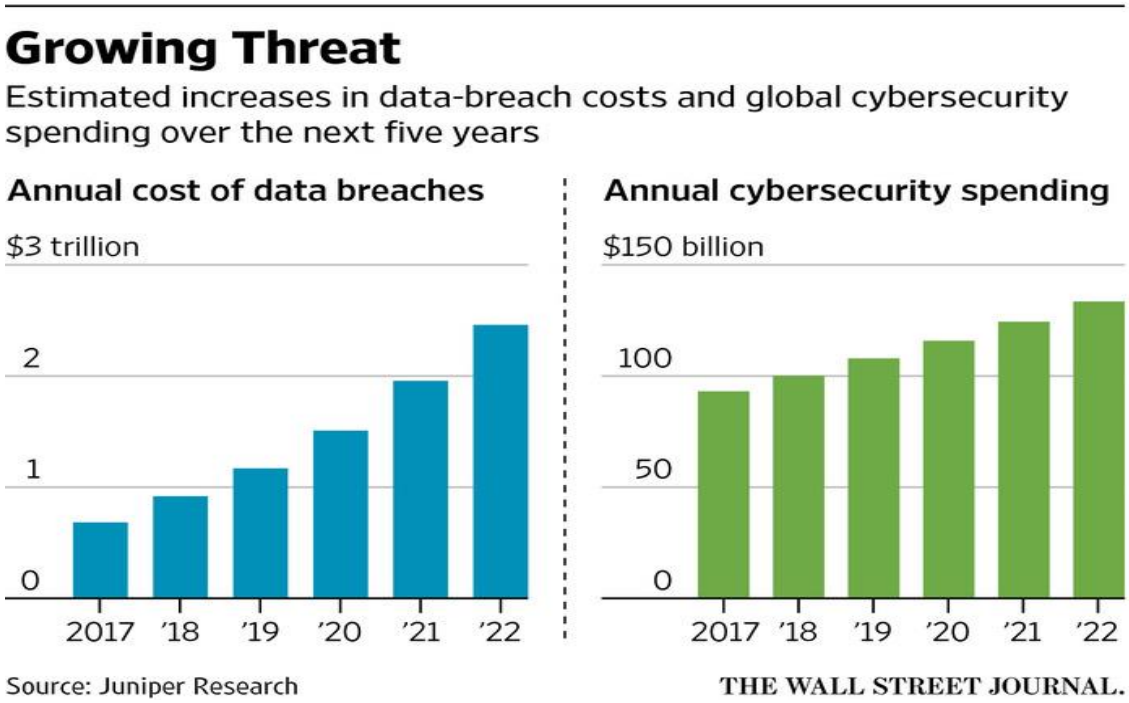
PROBLEM IN PRESENT DAY LIFE

- The major security problems is Virus, Hacking problems, malware, Trojans , password cracking. Here we are discussing one of the main problems in public networks and how they can gain access to our private data like our bank details, passwords etc.

SAFETY MEASURES



ANALYSIS OF GROWING THREAT



PROCEDURE

- As per review 2 requirements we have created a temporary payload and sent it to the victim device offline we can also do this online in any corner of the world by port forwarding.
- We are creating a payload using Metasploit framework and sending it to the victim by attaching to any file.
- When the victim downloads the file (payload) which we have sent, it gives us remote access.
- After it is installed, we setup the Metasploit console which is basically used for monitoring and sending commands.
- In order to understand what can be done using this, we are showing how to access the camera of the phone in our pc without the victim's consent and knowledge.

CONCLUSION

- We have successfully shown how to create a payload and how it works.
- We clearly showed how to gain remote access of another device without the victim's knowledge.
- It is mainly used for ethical hacking and for testing system security in order to curb modern crimes.

EXECUTION SCREENSHOTS: (OUTPUT)

YOU CAN SEE THE PROCESS ID'S IN THE BELOW SCREENSHOT

REFERENCES

https://www.offensive-security.com