East West University

Ethical Hacking Using Penetration Testing

Presented by

Redoan Hossain (2016-1-50-004)

Supervised by

Dr. Anup Kumar Paul

Associate Professor

Department of Electronics and Communications Engineering

East West University, Dhaka

This Project submitted in partial fulfilment of the Requirement for the Degree of
Bachelor of Science in B.Sc. in Information and Communications Engineering

To the

Department of Electronics and Communications Engineering

East West University
Dhaka, Bangladesh.

Date of Submission: 06-08-2022

APPROVAL

This research report presented to the Department of Electronics and Communications Engineering, East West University submitted to partial fulfillment to the requirement for the degree of B.Sc. in Information and Communications Engineering under complete supervision of the undersigned.

Approved By

……

(Signature of Supervisor)

Dr. Anup Kumar Paul

Associate Professor

Department of Electronics and Communications Engineering

East West University,

Dhaka, Bangladesh

DECLARATION

I hereby declare that this research project report is an original piece of work carried out by me, under the guidance and supervision of Dr. Anup Kumar Paul. This report is the requirement for the successive completion of B.Sc. Information and Communications Engineering under the Department of Electronics and Communications Engineering.I state that the report along with its literature that has been demonstrated in this report paper is my own work with the masterly guidance and fulfill assistance of our supervisor for the finalization of our report successfully.

Countersigned

……

(Supervisor)

Dr. Anup Kumar Paul

……

Redoan Hossain

ID: 2016-1-50-004

Signature of Student

……

DEDICATION

This paper is dedicated

To

My beloved Parents and Honorable Faculties

Acknowledgement

I would like to thank my supervisor, Dr. Anup Kumar Paul for his advice and investigation throughout the experiment of our model and also give guidance about the topic. Through my research, I learned a lot from him. His relentless encouragement gives me the confidence to do our work. Without his support and continuous monitoring, this research would not have been possible. Lastly, I thank the Almighty Allah, my parents, and friends for the support and encouragement that I have received during the period of this research. Their unconditional support made it possible for me to finish the thesis.

Abstract

Ethical hacking word realize us that hacking is for ethical purpose and helping purpose, on the other hand, penetration testing is one of the practical tools in the cybersecurity world and this makes an organization a secure and safe environment. Cyber-attacks increasing day by day in the entire world, and now network security is becoming a vital issue. This has influenced a large quantity of ethical hackers to improve methodologies and scripts to defend against security attacks. As it is to maintain and monitor attacks on individual hardware and software programs in an organization, the demand for new methods to control security systems invoked the concept of penetration testing. Many research organizations have designed algorithms relying on the size, type, and reason of application to secure networks. At present, the cyber world takes the whole world so ethical hacking and penetration testing are very important. In my thesis paper, I try to keep in paper overall knowledge about the pen test and ethical hacking. I try to complete this paper in an easy way to all readers can understand the topic easily. I attach to picture of some attacks on the network, software, and web application and describe it very shortly.

Table of Contents

Subject **Page**

List of Figures

List of Table

CHAPTER ONE

Introduction

1.1 Introduction

Today's world is becoming more and more technology dependent. The security of personal information in the present-day world depends on far greater than simply a locked door. Safeguards, procedures, and policies that are put depend heavily on security today into place and are left to be. Are these measures sufficient to provide actual security? Without checking out the security measures to show they work, is it really secure! The only way to be aware of an organization's devices is secure them from hackers. [9] [7]

The reason for this thesis paper is to explore, explain, and consider the significance of ethical hacking and pen testing out to our Internet world.

1.2 The Impact of Cyber Attack

Cybercrime is developing as one of the most annoying trends. A cyber attack's main intention is to steal money via the internet. Valerie McNiven, a U.S. Treasury Advisor, stated, "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion". She delivered that "cybercrime is moving at such a high speed that law enforcement cannot capture up with it." It looks clear that the problem will solely irritate in the subsequent few years. Recently, there has been good sized discussion over the amalgamation of organized criminals and cybercrime. Most of the criminal agencies running out of Eastern Europe, Russia, and Asia, where legal guidelines and enforcement are scanty, there is little hope of containing and neutralizing the risk via usual means. [11]

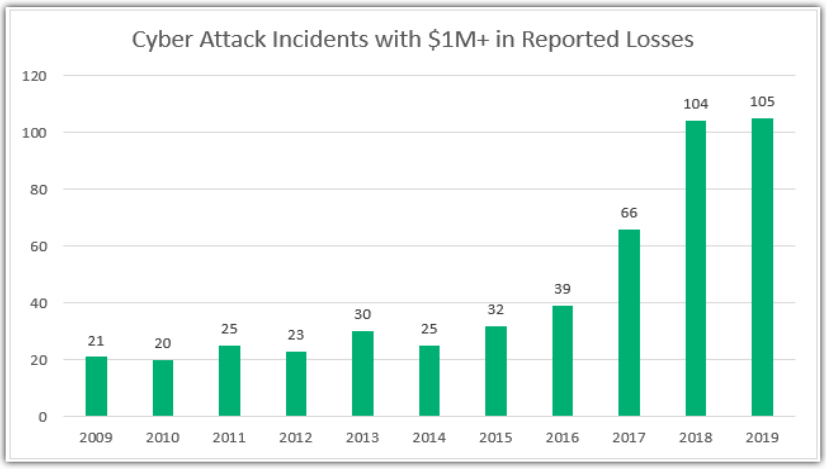

Figure 1.1: Cyber-Attack 2009 to 2019 [13]

Figure 1.1 shows the cyber-attack from 2009 to 2019. CSIS tracks “cyber-attacks on government agencies, defense, and high-tech companies, or economic crimes with losses of more than a million dollars." Four hundred ninety significant cyber incidents were tracked by them. [14]. In 2016 Bangladesh faced a cyber-attack. North Korea used fraudulent orders on the SWIFT repayment system to steal US$951 million, which used to be near all the cash from Bangladesh's central bank account. The hackers used a Federal Reserve Bank account in New York. They effectively managed to steal $81 million that was once transferred to accounts at Manila-based Rizal Commercial Banking Corporation. that cyber-attack has Bangladesh a massive impact on the Bangladesh banking system. [12]

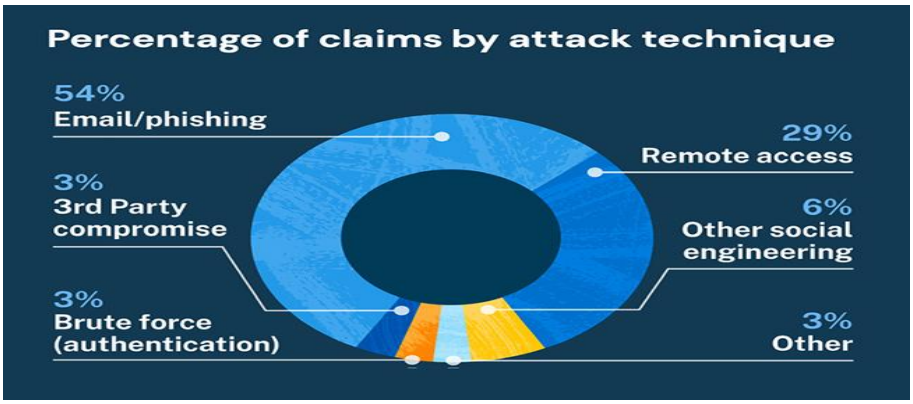

Figure 1.2: Most Attacks Happened as a Percentage of Claims [15]

The most types of attack shown in figure 1.2, which is happening till now. States have mentioned hackers affiliated with Russian intelligence have tried to steal information associated to the

COVID-19 vaccine. In August 2020, an Iranian hacking team used to be recognized as targeting essential U.S. companies and government agencies with the aid of exploiting newly published vulnerabilities in high-end network tools to construct backdoors for different businesses to use. [17]

1.3 The Overview of Book Organization

I divided my thesis into five chapter

In chapter one which is includes an introduction part. Where I discuss the impact of cybercrime. So, for readers can understand how much important cyber security and the importance of penetration testing and ethical hacking.

In chapter 2, included background. This section will give information about Ethical hacking Penetration Testing definition, the necessity of it, when to need it, also added a description of the CIA triad, types of attackers,

In Chapter 3, included the perform, stage, types of penetration testing and their information

In chapter 4 includes Hacker's type and their information, Different types of thread

In Chapter 5 there do some practical things.

In Chapter 6 their conclusion part.

CHAPTER TWO

2.1 Background Study

The World Economic Forum (WEF) now regards cybercrime as one of the largest threats to organizations and the economy, as mentioned in its 2019 Global Risk Report **[6].** The company will want to alternate its safety strategies as breaches can appear via the cloud, vulnerabilities in hardware chips, open-source DevOps, and infecting Internet of Things (IoT) devices. This type of adaptation is no longer An easy method for a company to achieve, particularly when it is more and more challenging to recruit and continue technically adept cybersecurity experts **[7].** All the organizations become alert and must have an idea about Cyber security. Give employees the necessary step to protect their important data, and personal information, Must need to keep an employee who has the knowledge of pen testing and ethical hacking. Cybersecurity should surely be a section of any organization's necessary values and additionally, and Penetration testing is one way to make positive that this occurs [8].

2.2 Ethical Hacking, What is it!

Firstly, we must understand what ethical hacking is; ethical hacking not only means hacking Facebook ID, YouTube, or other software, but it has different types of essential duties like various bound attacks and very important to find the security flow, weakness of databases office or company network so for giving strong protection to save from future attacking risks and must-have skill of using penetration testing. Ethical hacking is a term that covers all types of hacking techniques and other related computer attack techniques. It can find out security flaws, and vulnerabilities, and make sure the security of the target system. It hacks a system with permission in order and stands to safeguard security for future purposes. Ethical hacking one the key feature is penetration testing. [1]

2.3 Why is Ethical Hacking Needed?

We can think of this as an example a company owner runs a trading company, and he does online training with the money, which is customer invest, his company goes very well, and it's increasing with profit, but unfortunately, hacker decides to hack company server and starting to find server weakness when they find unprotected server and devices then they succeeded to attack the server and stolen customer accounts with a large amount of money after this situation company lost the customer trust. So, the owner of the company decides to find a person who can protect company information from a hacker, so the owner of the company applies an employee who thinks like a hacker and runs a test attack to find vulnerable system ware before the hacker penetrates the network and identifies the vulnerabilities in his office network and close all the loopholes. So, this type of work is called ethical hacking.

An ethical hacker can only know how to defend the server and protect it from hackers. If we keep our house unprotected, then a thief easily comes home and steals necessary items, similar like if we kept our device and server unprotected, then hackers easily use their hacking technic to steal our necessary documents.

A hacker always tries to find multiple ways to enter a system and find possible entry points that can let the hacker enter the system. So ethical hackers try to find those loopholes and quickly fix that.

2.4 Is Ethical hacking ethical!

Doing Ethical hacking for a good purpose, on the other hand, black hat hacking is totally different from an ethical hacker. Black hat hackers identify as criminals and Black hat hacking is a crime. Ethical hacking does the same process, but ethical hacking only does for the company who hired them to perform testing to protect from outside unethical hacking. Ethical hacking is ethical because the bad hackers always do unethical work and tries to harm people worldwide by hacking personal information or damaging devices and taking access without permission which is unethical. Where the good hacker always helps people, organizations, and governments to protect their personal information with permission. They work as an organization employee or government

agencies. Without a good hacker, no one is safe on the internet. So ethical hacking is needed, and so ethical hacking is ethical. [1]

2.5 What Is Penetration Testing

A penetration test or pen test can check for exploitable vulnerabilities in operating systems and application software. A pen test can expose the weakness of OS and software and find and secure vulnerabilities before attackers can create any damage.

Penetration testing is essential because DDoS attacks phishing, ransomware, and countless tactics used by increasingly sophisticated cybercriminals, but pen testing's best defense is strength and weakness to find it. Penetration testing works for addressing and fixing the issues that were discovered during the test, and this process is used to help secure computers and networks against future attacks

Penetration testing is also considered as

1. Pen Testing
2. PT
3. Hacking
4. Ethical Hacking
5. White Hat Hacking [10]

2.6 Why need penetration testing?

in May 2017, we have to have heard of the WannaCry ransomware attack that started. It locked more than 2 lakh computer systems round the world and demanded ransom repayments from the Bitcoin cryptocurrency. This attack has affected many large companies around the globe.

With huge & risky cyber-attacks going on these days, it has come to be unavoidable to do penetration testing at ordinary intervals to defend the data structures towards safety breaches. **[4]**

Penetration testing is important now in the present time. It's important because

2.6.1 Identify Risk Condition:

Penetration testing helps to find out which of the organization and applications are most at risk and helps to find what types of security tools are needed to make the organization or application make risk-free. This process helps to uncover the system where it has the weakness and where to fix the security issue.

2.6.2 Detect and Protect from Error

Developers, after penetration testing, can get reports and by considering reduce the reported error when developers understand where and how many malicious attacks on applications, software, and operating system then they are fixing that and alert for a future attack.

2.6.3 Preparation for Future Attack

Penetration testing helps to break in from future attacks such as malicious entities. Penetration testing is effective for testing the organization's security policy and can protect against future attacks. Penetration testing provides a solution for an organization not only to prevent or identify attackers but also to expel such intruders from their systems in an efficient manner.

2.6.4 Security Issue

Some attacks, such as ransomware attacks, network intrusions, and data theft, can disrupt and disrupt system processes, which undermines customer confidence and trust, which undermines customer satisfaction, and affects its market value.
Many companies take the necessary steps to provide a safe life cycle to maintain safety and reliability. There are four basic steps in the safety life cycle:

2.6.4.1 Identity: The first step is to know the details of what you want to protect and how to protect the resources, such as network maps, identifying servers, and understanding which applications are running. Must know and of a clear idea of what to protect

2.6.4.2 Assess: The security process is created at the identification stage, and if features are identified, the next step is to perform a security assessment. The evaluation phase can

cover several different areas and from evaluating the processes and procedures. It can scan vulnerabilities. If you have a large organization, the best idea is preferred. Evaluates and consider the potential risk assets associated with each variable.

2.6.4.3 Protect: If success finds the vulnerabilities, then need to bring the infrastructure into line with corporate security policy. Now is the time to secure the systems, and this life-cycle process refers to as the 'mitigation' process. Any risks found during the evaluation then the phase aims to minimize.

2.6.4.4 Monitor: The last step in the security life cycle is to seek security. After the upgrade, make sure that these improvements affect the security of the server, firewall, and router. It would also help if tracked with the latest frameworks implemented in the organization. Computer systems are complex and continuously updated. It can be changed by administrators and developers who have access to them. All of these are done by security experts and their management of the company by penetration testing.

2.7 When do we need to perform penetration testing?

Penetration does perform depending on the organization's condition; some organizations perform it once a year, some twice a year about their security condition. It also depends on newly invented hacking threats or emerging vulnerabilities that might be exploited by malicious hackers.
But there are also some specific when needed to perform penetration testing; those are

1. When new network infrastructure or applications are added, then penetration testing is needed.
2. Upgrades or modifications are applied to applications or added to new software.
3. When office location is changed, replacement or new office locations are established, then need to perform penetration testing.
4. If changing, the user policies are modified.
5. When security patches are applied, they then need to perform penetration testing.

2.8 All About CIA Triad

CIA triad is the organization's guideline for information security. CIA triad means the combination of three key elements together called CIA triad. And the three combinations are

i. "C" for Confidentiality

ii. "I" for Integrity

iii. "A" for Availability

Figure 2.1: CIA Triad

There all, everything for data and services. In figure 2.1, Where Confidentiality gives data privacy by restricted access through authentication encryption like a key. Integrity gives surety that the information is correct and trustful. Availability ensures that the information is available to the right or who deserve persons.

2.8.1 Confidentiality:

It means others should not understand except the parties who are involved in that transaction.

For example: if someone sends a message or letter to his relative and if it mentions that it is confidential. This confident message means it should be known to the sender as well as to the receiver because two parties are legitimate parties involved in this transaction. Now

an anonymous person receives this latter or message and if he sees the message or the content what is their privacy obviously, they haven't any confidentiality. If somebody sees this message so we need to prevent unauthorized access and disclosure. Unauthorize access means nobody else can access the right entities who are involved in the transaction, and disclosure means the message should not be open enough to be simple if the message is encrypted. No one else can see what the message except the sender and the receiver is because the sender and the receiver only will know what the message is and what is the key to the encryption algorithm. Generally, encryption algorithms are kept public, and keys only are kept secret.

Confidentiality means we need to protect the data that is being transmitted. If it is encrypted then obviously provides confidentiality because no one can see the original message or text so no one can understand, so that message is that being transmitted between the sender and receiver.

2.8.2 Integrity:

The 2nd element of the CIA triad is integrity. Here is the equation Sender = receiver, because if Sender sends the message, then the receiver only received that message. For example, if a person performing a banking transaction of 1000 Doller, then must transaction involve only 1000 Doller. If an attacker modified this as 10000 Doller, then not only modification of amount by the attacker. Let's assume the destination address or destination account is given as the attacker account then we don't want modification message to get unauthorized people. If any sender transfers some fund to a receiver, then, unfortunately, the fund is being transmitted or transferred to somebody else account which is the attacker's account. This is for the reason of modification of that message, and that is being transmitted between the sender and the receiver by the attacker. So, this transaction should be permitted by the system and the security system should be able to find out that this is not to message that was sent by the sender. In other words, the security system ensures that this is not a transaction because that was initiated by the sender. So, integrity means we need to ensure that there is no modification of the message being transmitted, so

the sender is sending that and only the receiver should receive any modified message that is being transmitted. The system should be able to find out and it should be discarding that message.

2.8.3 Availability

In availability, it means that in an organization or company there have available resources. The network and data are accessible to approved users by maintaining infrastructure, performing hardware maintenance, maintaining operating systems and applications up to date, and making backups. Denial of service attack creates serious damage but if we use security devices like firewalls which can give defend against DoS.

when hackers try to overload resources then users can't access the services then denial of service occur

The availability threats are

i. When Denial of Service attacks are Distributed

ii. If before a form of payment has been sent, then Ransomware attacks or blocks access to files.

iii. Interruptions to the Internet.

iv. if defects have in the server.

v. Bugs in software.

vi. If there are any viruses and malware virus and malware.

Chapter Three

3.1 What are the Penetration Stages?

The hackers are using 6 steps phases in ethical Hacking; it also can tell the stages of penetration testing. The points are described below [18]

3.1.1 Reconnaissance:

The whole concept of ethical hacking is not only based on practical knowledge. It is not limited to knowing how it's done, and how to access the account. It is lots more than that. The main thing is we need to gather knowledge and need to have lots of knowledge or information about it.

It is knowing

a. what the target is?
b. What is the scope of a target?
c. How many devices are in the company?
d. The number of employees of the company?
e. Who is the owner of the company?

- Every single piece of information must collect in reconnaissance, so this is the first process of Hacking. In this process, hackers collect all the necessary information about an organization, also called the Foot printing and information gathering phase. [2] It consists of gathering target information and sorting out necessary sources, which would possibly help in other phases. Planning. Research is the first step in any work, and by deeply preparing for a mission, the extra will possibly succeed. The man who builds the Linux Backtrack is fond of quoting Abraham Lincoln, who said, "If I had 6 hours to chop down a tree, I'd spend the first 4 of them sharpening my axe." [3] This is an extremely good introduction to each PT and reconnaissance phase. Active Reconnaissance is 2 types which are:
- Active Reconnaissance:
- Passive Reconnaissance

3.1.1.1 Active Reconnaissance: In active reconnaissance, the attacker is directly involved with the target system, basically it tries to find the open port so for it conducting a port scanning. In the figure 3.1.1.1 we can how attacker involved directly with the target system.

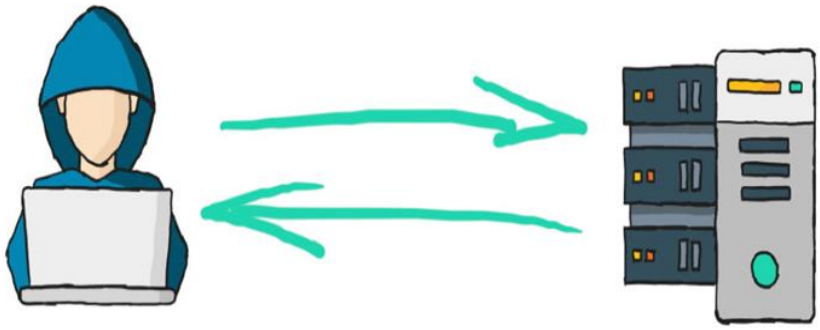

Figure 3.1: Active Reconnaissance [5]

I find figure 3.1 it on a google search where can see the attacker directly targets the targeted system, no media have in the middle, It directly target the system.

3.1.1.2 Passive Reconnaissance: In Passive Reconnaissance which not directly attack, where attackers without interacting with the target extract information from the target.

In below in the figure 3.2 where we can see in the middle there is a media for attack in target system

Figure 3.2: Passive Reconnaissance [5]

Here, attacker did not target the system directly.

They use tools like

1. NMAP
2. h-ping

Their information is collected as possible about the target and usually collected information about three groups,

1. Network
2. Host
3. People involved

3.1.2 Scanning

Once all the applicable information has been gathered in the reconnaissance phase, it's time to move on to scanning. In this phase, the tester makes use of a range of tools to discover open ports and test network visitors on the goal system. Since open ports are possible entry points for attackers, the aim of this phase is to locate as many as feasible so that the tester can take benefit of them in the subsequent phase.
Spot the vulnerabilities if in the target system using something like Nmap and expose.[16]

From internet and book research got different types of scanning:

- Determining if a system is alive
- Port scanning the system
- Vulnerabilities scanning of the system
- OS Scanning/ Fingerprinting
- Network Scanning

3.1.2.1 Determining if a System is Alive:

One of the primary steps in mapping out a network is performing an automated ping sweep on a range of IP addresses and network blocks to decide if individual gadgets or structures are alive.

Ping is traditionally used to send ICMP ECHO (Type 8) packets to a target system in an try to elicit an ICMP ECHO_REPLY (Type 0) indicating the target system is alive. Although ping is perfect to decide the range of systems alive in a small-to-midsize network, it is inefficient for larger organization networks. Scanning large Class, A networks can take hours if no longer days to complete. You must analyze several methods for discovering live systems; the following sections current a pattern of the available

3.1.2.2 Port Scanning:

Port scanning is used to determine what ports a system may additionally be listening on. This will assist an attacker to decide what services may additionally be running on the system. Port scanning on a network or server displays which ports are open and receiving data as well as revealing the presence of safety devices such as firewalls that are currently between the sender and the target. This method is known as fingerprinting. Some port scanners scan via ports in numeric order This involves scanning the target for the information example, open ports, live systems, and various services running on the host.

Based on the table 3.1 UDP and table of 3.2 TCP table of common Port Numbers and Their Corresponding Service

Based on UDP

Application	Port Number(s)
DNS	53
DHCP	67-68
TFTP	69
NTP	123
SNMP	161

Table 3.1: UDP

Based on TCP

Application	Port Number(s)
FTP	20-21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP	110
NNTP	119
HTTPS	443

Table 3.2: TCP

3.1.2.3 Vulnerabilities Scanning of the System:

Weaknesses or vulnerabilities are finding and checking the target for which can be exploited, and it's done with the help of automated tools. Vulnerability scanning is recognized as ‘vuln scan. This is a computerized process. It can discover the network, application, and protection vulnerabilities. Vulnerability scanning is usually performed via the IT branch of an organization. This scan is additionally carried out by attackers and tries to locate points of entry into your network.

The scanning method detects and classifies system weaknesses in networks, communications equipment, and computers. In addition to figuring out security holes, the vulnerability scans additionally predict how effective countermeasures are in case of a risk or attack.

3.1.2.4 OS Scanning/ Fingerprinting

Nmap's most effective feature is f OS. If a developer makes use of this kind of scan, then Nmap sends TCP. UDP packets to a specific port and then analyzes its response. It compares this response to a database of 2600 running systems. it returns data on the OS of a host

The fingerprint of the working device is the method of gaining knowledge of what running system is running on a specific device. By examining some protocol flags, options, and information on packets that a device sends to the network, we can make an enormously correct estimate of the OS that sends these packets. It is an effective tool for focusing on a system. Nmap's most effective feature is f OS. If a developer makes use of this kind of scan, then Nmap sends TCP. UDP packets to a specific port and then analyzes its response. It compares this response to a database of 2600 running systems. it returns data on the OS of a host

3.1.2.5 Network Scanning

Network scanning refers to the use of a pc network to collect data related to computing systems. It is basically used for safety assessment. It can additionally system maintenance and perform attacks by using hackers.

The purpose of network scanning

i) Recognize available
ii) UDP and TCP community offerings running on the centered hosts
iii) Recognize filtering structures for the user and the focused hosts
iv) operating systems in use via assessing IP responses
v) Evaluate the target host’s
vi) TCP sequence quantity predictability to decide sequence prediction attack
vii) TCP spoofing

3.1.3 Network Mapping:

It's essential to find the network's topology, routers, firewalls, servers, and any host information and draw a network diagram with the available information. This mapping process serves as valuable information for the hacking process.

3.1.4 Gaining Access:

In this step, locating the vulnerabilities that try to exploit them is known as gaining access. Attacker breaks into the system/network using various tools or methods and entering a system. The hacker must increase his privilege to the administrator level. The hacker can install an application he needs or modify data or hide data.

3.1.5 Maintenance Access:

After gaining access process, hackers make his through the organization's network; they try to maintain the access for future attacks by installing backdoors in the target system,
Using Metasploit tools can help with this process.

3.1.6 Clearing Track:

No bad hacker wants to get caught, so an intelligent hacker always clears all evidence. Later, no one will find any traces leading to them. In this phase, modifying, corrupting, and deleting the values of Logs and modifying registry values, and uninstalling all applications. Hacker always tries to use and delete all folders he created.

3.1.7 Reporting

In this phase hacker documents a summary of the entire attack, the vulnerabilities spotted, the tools the hacker uses, and the success rate of the attack.

3.2 Types of penetration testing:

In my thesis research, I get different types of penetration testing, which is

1. Network Service Penetration Testing
2. Web Application Penetration Testing
3. Client-Side Penetration Testing
4. Wireless Penetration Testing
5. Social Engineering Penetration Testing
6. Physical Penetration Testing

3.2.1 Network Service Penetration Testing

This is the most common type of penetration testing. The main reason is to become aware of the most uncovered vulnerabilities and security weaknesses in the network infrastructure like servers, firewalls, switches, routers, printers, workstations, and more of a company earlier than they can be exploited

Network penetration tests performing to protect against common network attacks like

i. Router Attacks
ii. DNS Level Attacks:
iii. Zone Transfer Attacks
iv. Switching Or Routing Based Attacks
v. SSH Attacks
vi. Proxy Server Attacks
vii. Unnecessary Open Ports Attacks
viii. Database Attacks
ix. MITM Attacks

x. FTP/SMTP Based Attacks

xi. IPS/IDS Evasion Attacks

In network service, penetration testing recommended that 2 types of penetration tests be performed at least annually, which are

3.2.1.1 Internal Testing: This pen-testing starts when the external penetration testing completing. it reduces an insider risk and identifies how an attacker with inner get entry might also compromise or harm the network, systems, or data. This type of inside threat comes from malicious insiders, careless employees, insecure third-party vendors, and even clients or customers

3.2.1.2 External Testing: In external access, there is no internal data, and no need to access information on the network. External testing limits the availability of system knowledge because the tester stays outside the firewall. In external testing here the tester gathers the information about security settings and protocols

These types of threads can come from:

i. Weak passwords or shared passwords

ii. access controls are weak

iii. Insecure file sharing

iv. unencrypted data

v. Network misconfigurations

vi. Lack of awareness about social engineering

vii. phishing

viii. Ransomware attacks

ix. Insecure remote networks and

x. Insecure remote devices

3.2.2 Web Application Penetration Testing

Web application penetration testing basically works in the web-based application. It's used to discover vulnerabilities or security weaknesses in web-based applications. It can use different penetration techniques, and assaults with the purpose to destroy the web software itself.

Web application penetration test includes web-based applications, browsers, and their components such as

i. ActiveX,
ii. Plugins,
iii. Silverlight,
iv. Scriptlets, and
v. Applets.

This type of test is very helpfull and it considers to be a more complex test. These types of tests needed enough time for planning and executing the test and for this can compile a useful report. web application penetration testing is continuously evolving day by day and increases threats coming from web applications day by day.

This thread increases very highly, more than 600% increase in cybercrime when the covid pandemic outbreak.

The reason behind the performing web application testing is

a. To identify security weaknesses or vulnerabilities within the web-based applications and their components like Database, Source Code, and the back-end network.
b. helps by determining weaknesses or vulnerabilities and provides possible solutions to them
c. in software application development continuously improves the codebase
d. balancing daily code deployment with security in mind.
e. It’s common for enterprise software companies to employ pen testers. This is for privacy continuously test their code.

3.2.3 Client-Side Penetration Testing

Client-side penetration testing find or discover the vulnerabilities or security weaknesses in client-side applications, like program or applications such as

i. Putty,
ii. email clients,
iii. web browsers like Chrome, Firefox, Safari, etc. and
iv. Macromedia Flash, and others.

for marking the specific cyber-attack which for client tests are needed. The Reason behind Performing a Client-Side Penetration Test is

a. Cross-Site Scripting Attacks
b. Clickjacking Attacks
c. Cross-Origin Resource Sharing (CORS)
d. Form Hijacking
e. HTML Injection
f. Open Redirection
g. Malware Infection

3.2.4 Wireless Penetration Testing

Wireless penetration testing identifies the connections between devices of the business's Wi-Fi. These devices are laptops, tablets, smartphones, and any other IoT devices. Wireless penetration tests are usually carried out on-site as the pen tester desires to be in the range of the wi-fi sign to get the right of entry to it. Can be deployed onsite to remotely operate the test which is a NUC and Wi-Fi Pineapple .

Wireless communications are an invisibly running provider that approves information to flow in and out of the network. Therefore, this wi-fi network needs to be secured from any weaknesses like unauthorized get right of entry or data leakage. Performing a wireless penetration test should consider the following:

A. Have all access points been recognized and how many use negative encryption methods?
B. Is the information flowing in and out of the network encrypted and if so, how?
C. Are there monitoring systems in the area to discover unauthorized users?
D. Is there any opportunity the IT group should have misconfigured or duplicated a wi-fi network?
E. What are the current measures in location to defend the wireless network?
F. Are all wireless get entry to point the use of WPA protocol?

3.2.5 Social Engineering Penetration Testing

Social engineering penetration testing is the place a malicious actor tries to persuade or trick users into giving them sensitive information, such as a username and password.

By using penetration tests can find the common types of social engineering attacks which are

a. Phishing Attacks
b. Vishing
c. Smishing
d. Tailgating
e. Imposters like Fellow Employees, External Vendors, or Contractors.
f. Name Dropping
g. Pre-texting
h. Dumpster Diving
i. Eavesdropping
j. Gifts

The reason behind Perform Social Engineering Tests is because social engineering is directly involved in the recent 98% of all cyber-attacks. For defending the attacks where social engineering tests and awareness programs have proven to be one of the most effective methods, here example KnowBe4, an email phishing platform, simulates an email phishing attack. When the user clicks on the link, they're taken to a page that affected them in the phishing test.

3.2.6 Physical Penetration Testing

At present Physical penetration testing simulates a real-world threat where a pen tester tries to compromise physical limitations to access a business's infrastructure, building, systems, or employees. For business purposes most of the time use a physical barrier, if any malicious attacker can physically access of server room, then they can own that network. They could also take the business, business partners, and customers.

So, the benefit of a physical penetration test can provide safety from this type of attack. which is to expose weaknesses and vulnerabilities in physical controls. so that problem can be possible to quickly find out. So, figuring out these weaknesses can be put in place to improve the physical security posture.

Chapter Four

4.1 Hacker Types

Basically, Hackers can be classified into three different categories they are

- Black Hat Hacker.
- White Hat Hacker.
- Grey Hat Hacker

In my thesis research, I get 14 types of hackers from a different source.

Types of H0acker	Known as	Who's most at risk
1. Black Hat	Criminal Hackers	Black hat hackers are the most risk to organizations, they target to steal sensitive data that can compromise a business financially.
2. White Hat	Ethical Hacker	Criminal hackers
3. Grey Hat	"Just for Fun" Hackers	Nobody doesn't want unauthorized access to their systems and networks
4. Script Kiddies	Ametuer Hackers	Organizations with unsecured networks and systems
5. Green Hat: Hacker	in-Training or new in this field	No one
6. Blue Hat	Authorized Software Hackers	Criminal hackers
7. Red Hat	Government-Hired Hackers	Black hat hackers
8. State/Nation Sponsored Hackers	International Threat Prevention	International hackers and criminals
9. Malicious Insider	Whistleblower Hackers	Internal executives and business leaders
10. Hacktivists	Politically Motivated Hackers	Government agencies

11. Elite Hackers	The Most Advanced Hackers	High-revenue corporations
12. Cryptojackers	Cryptocurrency Mining Hackers	Any individual or organization with unsecured networks
13. Gaming Hackers	Game related hacker	High-profile gamers
14. Botnets	Large-Scale Hackers	Individuals with unsecured routers and Wi-Fi-connected devices

Table 4.1: Types of Hacker and Who's Most Risk

Here the hacker's information given

4.1.1 Black Hat:

Black hat hackers can be known as cybercriminals; they break into computer systems with malicious intent. They have advanced technical knowledge, and they can navigate the cybersecurity landscape. This has made them skilled in carrying out their attacks. They always try to find vulnerabilities in computer systems and software. They exploit for financial gain or other malicious purposes. They can do serious harm to individuals and organizations by stealing sensitive or personal data, and they are compromising entire computer systems, or altering critical networks. 4.1 is the fictional example collected from internet.

Figure 4.1 : Black Hat

4.1.2 White Hat:

White hat hackers are also known as Ethical Hackers. They can also a Penetration Testers, but they are cybersecurity experts who use their skills to find vulnerabilities in organizational networks and computer systems. The key difference between black hat hackers, unethical or security creaker, and white-hat hackers are ethical hackers; White hat hackers are authorized to hack these systems for the purpose of spotting security vulnerabilities before a criminal hacker can, and they hack for helping purpose. They are doing the job as employees or hired by governments or large businesses; they identify, and fix loopholes or weaknesses found in organizational security systems to help prevent an external attack or data breach. 4.2 is the fictional example which collected from internet.

Figure 4.2: White Hat Hacker

4.1.3 Grey Hat:

A grey hat hacker is a cybersecurity expert and finds ways to hack into computer networks and systems, but they are not like a black hat hacker. Basically, they are hacking activities for the pure enjoyment of finding gaps in computer systems, and they can let the owner know if any weak points are found. However, they don't always take the most ethical route when employing their hacking activities—they may penetrate systems or networks without informing the owner's permission, but they aren't trying to cause any harm. In Figure 4.3 is the visualization example collected from internet.

Figure 4.3: Grey Hat Hacker [20]

4.1.4 Script Kiddies:

Script kiddies are amateur hackers. They are not at the same level of skill or expertise as more advanced hackers in the field. To make up for this, they turn to existing malware created by other hackers to carry out their attacks. They are harming organizations with unsecured networks and systems.

4.1.5 Green Hat:

A green hat hacker is new to the hacking world, but they focus on increasing their cyberattack skills. They are learning and primarily focus on how to perform cyberattacks on the same level as their black hat counterparts. Their main intent is to eventually evolve into full-expert hackers, so they spend their time learning opportunities from more experienced hackers.

4.1.6 Blue Hat:

Blue hat hackers are hired by organizations to bug-test a new software or system network. They find loopholes or security vulnerabilities in the new software and remedy them before it launches.

4.1.7 Red Hat:

Figure.4.4: Red Hat Hacker Information [20]

In 4.4 where Information of Red Hat Hacker information given, where Red Hat Hacker mainly hired by government agencies and they attack with government permission.

4.1.8 State or Nation Sponsored Hackers:

State/nation-sponsored hackers are appointed by a country's government. They gain access to another nation's computer systems, and their cybersecurity skills are used to retrieve confidential information from other countries in preparation for a potential upcoming threat or attack that could pose a threat in the future. These types of hackers are hired solely by government agencies.

4.1.9 Malicious Insider:

Malicious insider hackers are individuals who employ a cyberattack from within the organization where they work. They are also known as whistleblowers. They are working for their motivation for attack can vary from acting on a personal grudge they have against someone they work for to finding and exposing illegal activity within the organization.

4.1.10 Hacktivists:

A hacktivist is someone who hacks into government networks and systems to want attention to a political or social cause. They use hacking as a form of protest, retrieving sensitive government information basically which is used for political or social purposes.

4.1.11 Elite Hackers:

Elite hackers are the strongest cybercriminals globally, and they are the highest skilled hackers in their field. They discover cutting-edge attack methods and are known to be the experts and innovators in the hacking world**.**

4.1.12 Crypto Jackers

Figure 4.5 : Crypto Jackers Information [20]

From figure 4.5 where describe about the Crypto Jackers and they spread malware in many ways, often by planting infectious viruses across the web. These viruses and ransomware-like tactics are used to plant malicious code on victims' systems, which work quietly in the background without the victims' knowledge. If the code is planted, then it sends the results back to the hacker**.**

4.1.13 Gaming Hackers

Gaming hackers focus their hacking efforts on competitors in the gaming world. When the gaming industry boomed, then its specialized category of gaming hackers emerge as a result. Professional gamers spend thousands of dollars on high-performance hardware and gaming credits, but hackers typically carry out their attacks to steal competitors' credit caches or cause distributed denial-of-service (DDoS) attacks to take them out of the game.

4.1.14 Botnets:

Botnet hackers are the high-volume attacker's type hackers in the world, and they are malware coders who create bots to perform high-volume attacks across as many devices, mainly targeting routers, cameras, and other Internet of Things (IoT) devices. The bots search or operate by looking for unsecured devices to plant themselves in. Botnets can be used directly by the hacker who created them, but they are also available for purchase on the dark web for other hackers to take advantage**.** [20]

4.2 Disadvantages or Drawbacks of Penetration Testing

In the cyber world, pen-testing helps a lot, but there have some drawbacks and issues which can create a very devastating situation. Which is the risk of penetration testing. Some of those common mistakes are discussed below

Sometimes penetration testing goes wrong and involves hacking some or all the systems and can lead to the disclosure of a sensitive security issue for the company's customer information.

i. If the penetration testing is not carried out accurately, it can cause a lot of damage and server crash, important data can be corrupted. Dangerous situations can arise when criminal attacks occur.

ii. It must create a serious situation if the important data or private data is handed to the criminal hacker or opponent company.

4.2.1 DETERMINING THE TEST CONDITIONS

i. The advantages and disadvantages of the penetration test need to be considered while testing, as it can be very complex and costly to determine the test conditions and opportunities.

ii. Sometimes analyzing only, a specific area of that network can be risky for a company's security. Disadvantages of penetration testing if it's discussed it may be better to make the most of each test with a better scope.

iii. If Pentest occurs in a company's entire network and infrastructure, then one must have the right knowledge then be sure to be ready to explore the penetration test.

iv. Currently, some businesses want to test penetration. Hackers do not issue a single warning about cyber-attacks. So, when you need to take a penetration test, make sure that the test gives accurate and perfect results

4.2.1.1 Unwanted Situation:

Sometimes outages and breakages can't stop or fail penetration testing but sometimes application or software can have the manufacturing issue and can-do wrong configuration network, which can create very bad traffic. unfortunately, there have fewer options to solve this problem. but have an option which is practices patching, change management, and thorough code reviews.

4.2.1.2 False Negative

False Negatives are vulnerabilities that exist but are not detected easily. A penetration tester always does their best to detect all types of vulnerabilities in their penetration testing but there is no surety to finding all vulnerabilities and there have many reasons for this type of miss situation.

By contracting with an organization that how much does the penetration tester team normally perform their penetration testing in a fixed time. Some of the vulnerabilities are detecting too much critical, but there have some tools which help to detect vulnerabilities but not all types of vulnerabilities. There can have some vulnerabilities which are not invented so sometimes unprofessional pen-testers or good hackers they are failed to detect these types of vulnerabilities.

4.3 What is the Internal and External Security thread?

4.3.1 Internal Security thread

Internal security means the thread from the inside of an organization that can create internal damage to an organization and can expose or leak the internal private documents is called internal security thread. This is very dangerous than an external thread because it can take direct access to an organization. Can invite malware to the network with malicious e-mails, and websites.

For example, in an organization, there have lots of employees. And if there have any employees who access data using this in a bad manner or sell the important data to others, so this type of thread is an internal security thread. This type of thread can create a huge problem.

4.3.2 External Security Thread

External means outside so from here we can understand this attack comes from outside of an organization. So, in an organization black hat hacker or an employee tries to take access to organization devices to collect important data from outside of an organization is called external data.

They are like professional attackers and can exploit vulnerabilities in the networks of an organization.

4.4 Which types of tools are used in a penetration test?

Penetration tools are very important for doing pen tests. In my thesis purpose, I am finding here are most pro-level tools using for penetration testing which are

4.4.1 Kali Linux

Kali Linux is the most popular software for penetration testing. It is the most advanced Linux distribution used for penetration testing. Many experts like to use this tool for both injecting and password snipping. It's a most beneficial tool for gaining basic skills in both TCP/IP protocols.

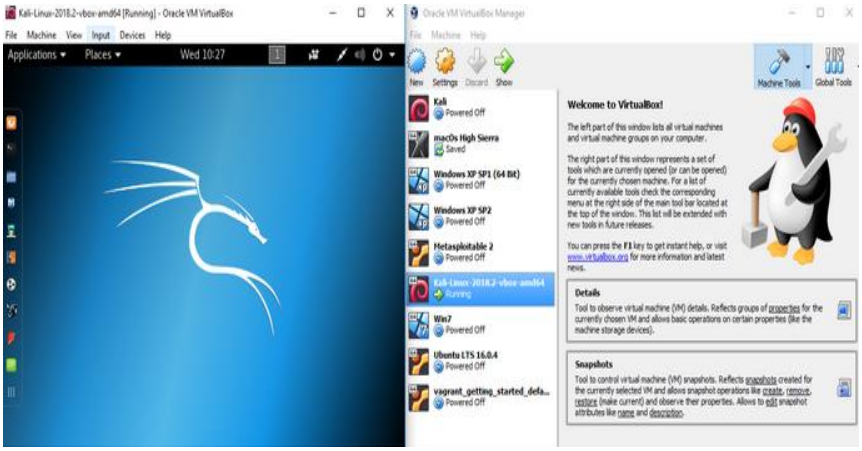

Figure 4.6 : Kali Linux

In the figure 4.6, where showing picture of the Kali Linux opening tool and their options and benefits of using this tool. Web applications, data gathering, wireless attacks, reverse engineering, password cracking, forensic tools, web applications, spoofing, sniffing, exploitation tools, and hardware hacking are available in Kali Linux integration with different penetration checking out tools like Wireshark and Metasploit.

The BackTrack gives tools for WLAN and LAN vulnerability assessment scanning, digital forensics, and sniffing. With 64-bit support useful to use this tool for brute force password cracking. The great tool for gaining knowledge of the security skills for ethical hackers.

Kali has over 600 ethical hacking tools. Various security tools for vulnerability can analysis

4.4.2 Netsparker:

Netsparker Security Scanner is a popular penetration testing tool for ethical hacking. By using this, the hacker can identify everything from cross-site scripting to SQL injection and developers use this tool on websites, web services, and web applications. This is a powerful system because it can

scan at the same time 500 to 100 web applications. Netsparker automatically finds out weak spots in a read-only way and also can find out exploitation is produced so for the impact of vulnerabilities is instantly visible to the tester. The benefits of the Netsparker are

(i) Add multiple team members for collaboration and easy shareability of findings.
(ii) Automatic scanning ensures a limited setup is necessary.
(iii) Searches for exploitable SQL and XSS vulnerabilities in web applications.
(iv) Legal internet application and regulatory compliance reports.
(v) Proof-based scanning Technology ensures correct detection.

4.4.3 Wireshark

Wireshark this software program can shortly locate and interpret network packets. This tool is open-source and useable for various systems example as Windows, Solaris, FreeBSD, and Linux.

Benefits of Wireshark

i. Provides each offline analysis and live-capture options.
ii. Capturing information packets permits you to discover various traits, such as source and destination protocol.
iii. It provides the capability to investigate the smallest details of activities all through a network.
iv. Optional including coloring policies to the pack for rapid, intuitive analysis.

4.4.4 Metasploit

The world's most usable pen tester tool is Metasploit. Metasploit helps the expert teams verify and control security assessments and improves the consciousness and gives inspiration to the defenders

to be confident in the game. The new hacker uses these tools for improving them. The benefits of using this tool are because

(i) For network segmentation tests.
(ii) Using this to discover older vulnerabilities inside the infrastructure.
(iii) Available on Mac Os X, Windows, and Linux.
(iv) Used on servers, networks, and applications

4.4.5 BeEF

This pen-testing tool is best used for checking a web browser. It is mainly useful for mobile clients because defending against web attacks. BeEF is most useful for Browser Exploitation Framework and uses GitHub to locate issues.

The benefit of using this tool because

(i) Can use client-side attack vectors to check security posture.
(ii) Connects with more than one web browser.
(iii) Can launch directed command modules

4.4.6 John The Ripper Password Cracker

Hackers are most interested on to steal or cracking passwords. Hacker mainly wants to use a password to steal important documents and enter sensitive systems. John the Ripper is the necessary tool for password cracking and offers a range of systems for this purpose. Using purpose

Identifies unique password hashes Automatically. Discovers password weaknesses Available for Linux, Mac OS X, Hash Suite, and Hash Suite Droid. Includes a customizable cracker. Users can explore documentation online.

4.4.7 Cain & Abel

Cain & Abel is best for collecting network keys and passwords. Using purpose The Windows-based software can recover passwords using network sniffers, cryptanalysis attacks, and brute force. Can recover lost passwords.

4.4.8 Wapiti

Black box testing perfect and suitable security tool is wapiti. when the black box testing process occurs then the web pages are scanned, and the testing data is injected to check for any weaknesses can have in the security.Using purpose Experts will find ease-of-usability with the command-line application. Wapiti identifies vulnerabilities in file disclosure, Can find XSS Injection, Can identifies Database injection, Identifies XXE injection,Command Execution detection, easily bypassed compromised .htaccess configurations.

4.4.9 (SET) Social Engineer Toolkit

Tool kits are suitable for pen testing for Social engineering. This uses purpose for top cybersecurity conferences, which include ShmooCon, Defcon, DerbyCon for penetration tests, this is an industry-standard SET has been downloaded over 2 million times. An open-source checking-out framework designed for social engineering detection.

4.4.10 SQLmap

For databases, SQLmap uses SQL injection, which is supported by database platforms example MySQL, SQLite, Sybase, DB2, Access, MSSQL, and PostgreSQL. SQLmap is open-source and automates the technique of exploiting database servers and SQL injection vulnerabilities. The purpose of using this Detects and maps vulnerabilities. support for all injection methods like Union, Time, Stack, Error, Boolean. The software runs at the command line Can be downloaded for Linux, Mac OS, and Windows systems

Chapter Five

5.1 Domain name service (DNS):

A DNS server is a computer server that has a data set of public IP addresses and related hostnames. The server's motivation is to determine or make an interpretation of those names to IP addresses, as mentioned. DNS servers run unique programming and speak with one another utilizing exceptional conventions. Different names might mean the same thing as the DNS server incorporate name server or space name framework server.

It's significantly simpler for individuals to recall a space name like SoftwareKeep.com than it is a series of numbers (an IP address); however, for PCs, it's easier to use numbers because they don't work well with names. All we do is type in the area name we need, and the DNS servers got to resolve to figure out where we need to go by utilizing IP addresses. A DNS server does this. [21]

5.1.1 How Hackers Use DNS Server to Hack

Programmers make malware programs that can change our DNS server settings. For instance, assuming our PC utilizes Google's DNS servers and needs to go to a bank's site, type in the URL of the bank and hope to be taken to the bank's genuine site. If downloaded malware can changes DNS server settings, the framework will never again utilize Google's DNS servers. It will reference the programmer's servers, which will imitate our bank's site. The site will closely resemble our bank's site, yet rather than logging into our bank account, it takes our username and secret word whenever we've composed it. This gives programmers all the data they need to then get to our ledger. DNS server data can be changed despite our good faith without knowing. Once visited a "counterfeit" bank site and entered the data without acquiring passage into a casualty account, they might expect the site isn't working accurately and attempt some other time. The issue here is that it will be passed the point of no return by then, at that point. The programmers have proactively gotten into the casualty's financial balance and can wipe out before the loss realize there has been an issue. These malware assaults can do different things too. Whenever they have changed our DNS server settings, they can take us to sites that are loaded with pornography, have lots of

vindictive promotions on them, or to a phony site that fools you into accepting our PC has been contaminated with an infection. We might have seen this previously, and in the event that we have, our DNS server settings have been modified. This trick has been liable for getting many individuals to pay for something they don't require in light of the fact that they dread their PC will be obliterated by an infection or secured. NEVER accept an infection on the grounds that a site springs up, letting us know that our PC is contaminated. The main issue we are having is that our DNS server settings have been changed. Hackers are startling our information. They can cause such a lot of harm to our PC. They can plant infections on our PC, take our data, assume command over our framework and make it seem as though victim are downloading child pornography, taking data from government organizations, or doing quite a few other criminal operations that can land the victim in prison or cost immense fines.

Probably the most fantastic way they can get to us is by utilizing our DNS server. [21]

5.1.2 Using Nmap Switches and Techniques to perform TCP Connect() scan:

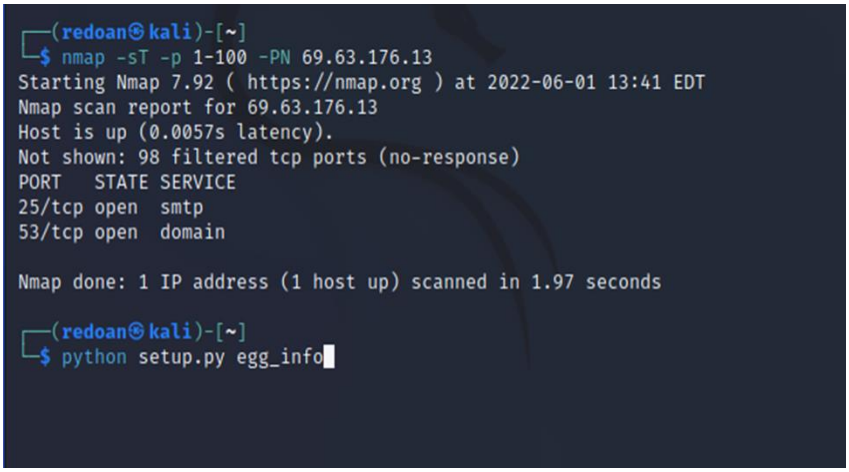

Figure 5.1: TCP Connect Using Nmap

TCP scan for port 1-1000 and TCP connect scan is the default which is showing in figure 5.1. The first computer connects to the second computer by sending an SYN packet to a specified port number. If the second computer is listening, it will respond with an SYN/ACK. When the first computer receives the SYN/ACK, it replies with an ACK packet

5.2 What is bug bounty hunting?

Bug bounty hunters do ethical hacking using penetration testing tools and discover the security of vulnerabilities and weaknesses in systems**.**

Bounty hunters can find and give an accurate report about valid bugs, they also can discover the security gaps before bad hackers do. So, bug bounty hunting is very important in an organization

5.2.1 How to bug bounty hunting to find the vulnerabilities

Here I use Kali-Linux in a virtual box for pen testing to find the vulnerabilities or bugs in my university server. And use the very easiest method to find vulnerabilities in website

Note: Firstly, I need to open my virtual box and login into Kali-Linux, and then open the terminal to start to find out the vulnerabilities on the network. For doing this I have need to open the github website

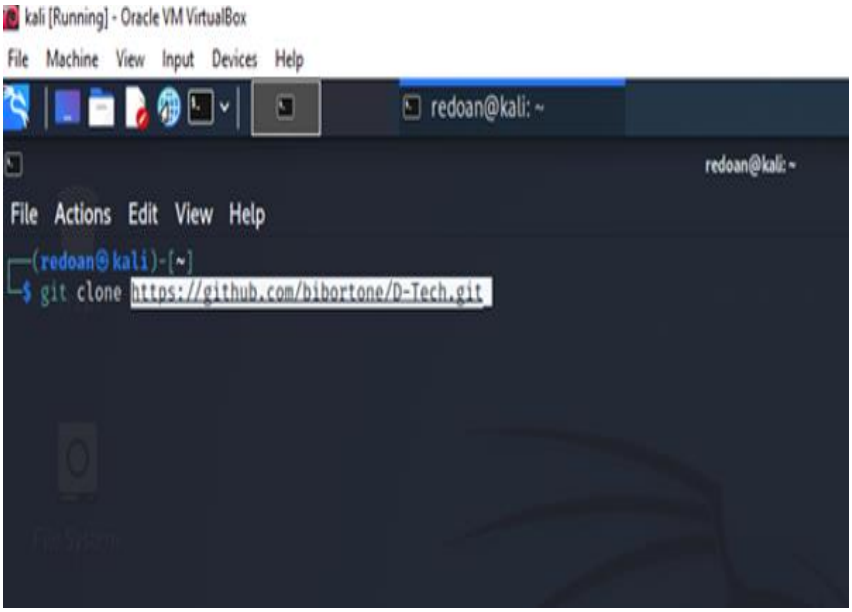

Figure 5.2: GIT Hub Code

Note: In my research in this field, I found a code which given in figure 5.2 given by via the internet. GitHub code or tool for pen-testing and YouTube, which can easily scan the vulnerabilities. After in the terminal, I copy-paste the code and press enter

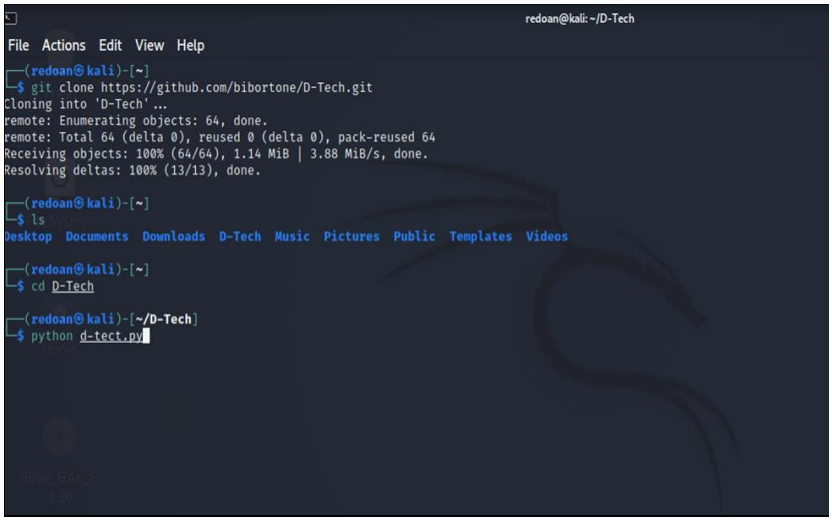

Figure 5.3: Using Python Command

Note: Now figure 5.3 where the code processing the system. Here so I need to write the python command to run the code. The code in this process can generate automatically.

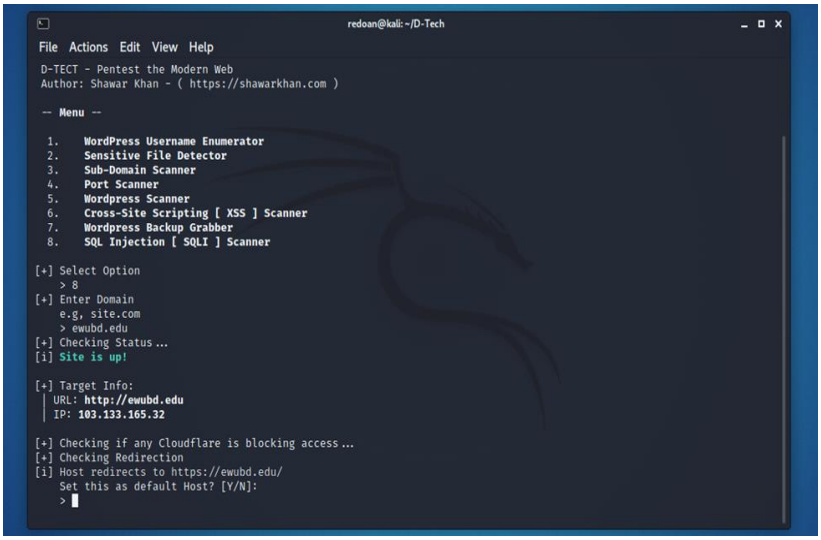

Figure 5.4: List of Option

Note: Now the tool is activated and now we can see in figure 5.4, there have some menu options, by selecting that we can find the vulnerabilities and do very easy penetration testing

Sub Domain of ewubd.edu

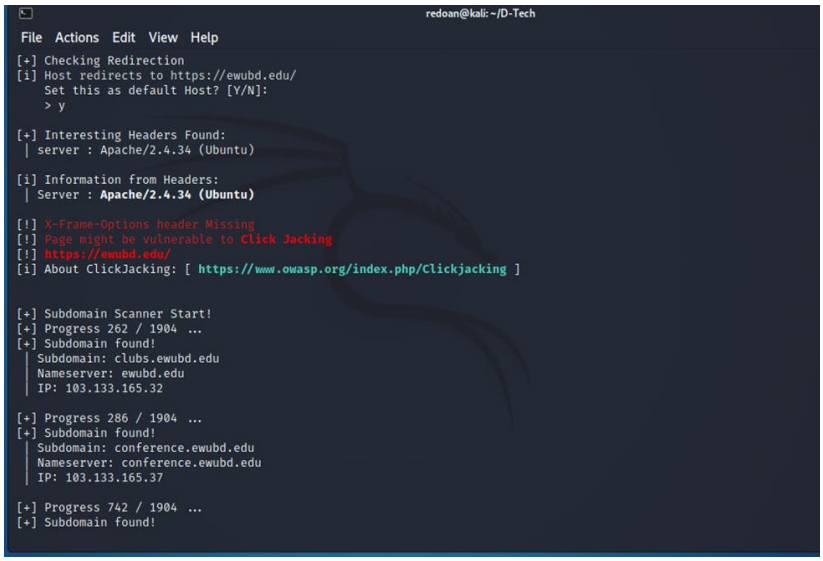

Figure 5.5: Finding Sub-domain, Server, Name-Server, IP Address

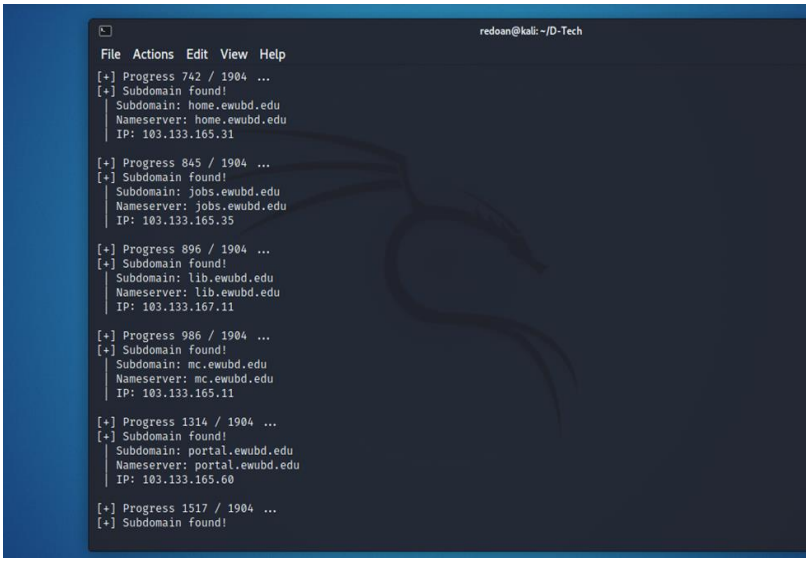

Figure 5.6: Finding Subdomain

Note: In here the figure 5.5 and 5.6, we found a Subdomain from the website of ewubd.edu. Subdomains are trustful for some applications and so they permit them to make cross-origin HTTP requests. Hackers can penetrate a subdomain if an app whitelists a subdomain with CORS headers so that it allows it to steal data. the hacker can steal data on the main application from an authenticated user

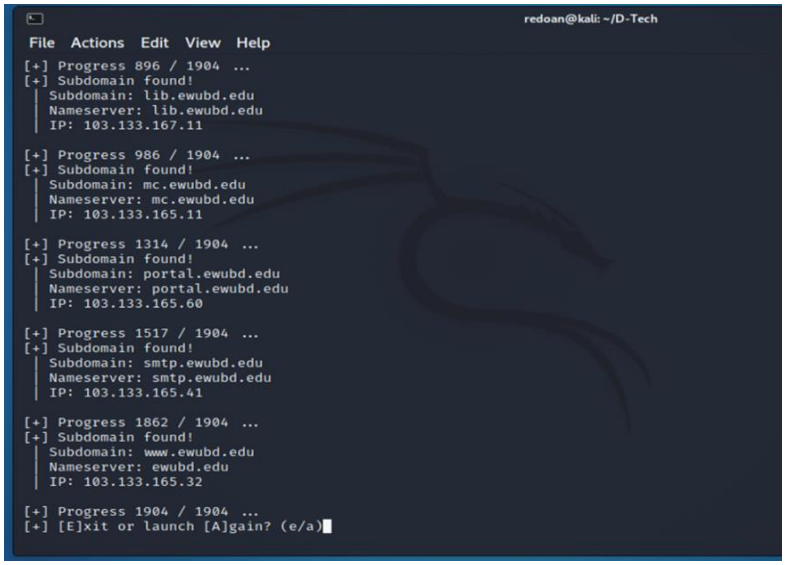

Figure 5.7: Finding Subdomain

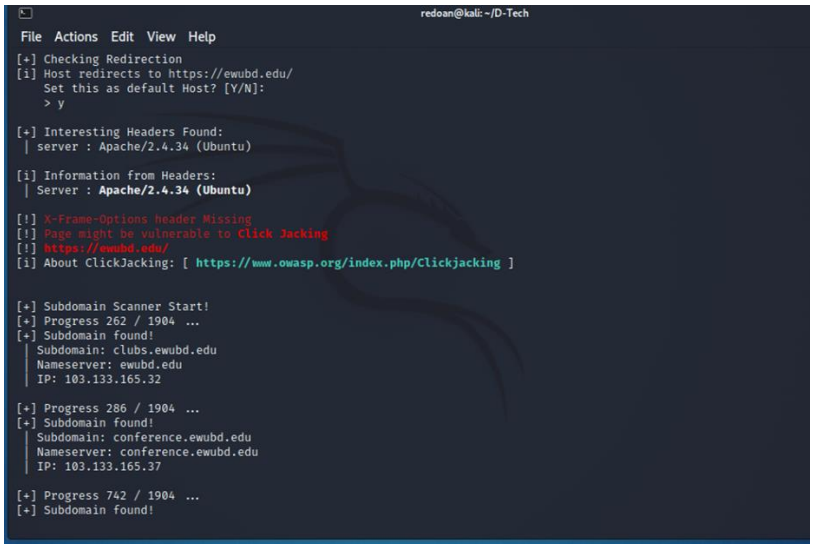

Figure 5.8: Finding Subdomain, Server Name and IP address

Note: we can see in figure 5.7 and 5.8 where server very easy to access, for taking that facility hacker easily hack, and in here we can see their show server accurate name. There Have vulnerabilities because showing the IP address and subdomain name and the server's name. If a hacker knows the IP address, then they can easily find out the user's location and know the important information and online identity and use this information beginning point. knowing IP address which easily can hack this information as a starting point, they could potentially hack device and can find out user identity, etc.

Port

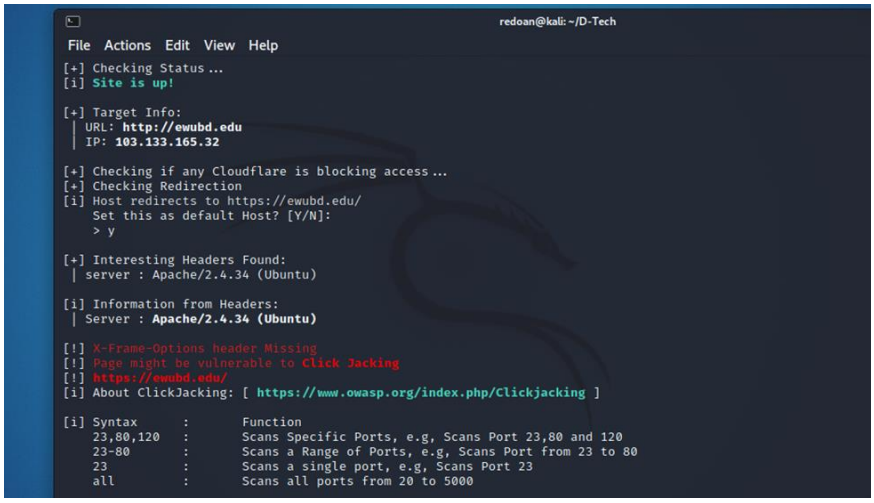

Figure 5.9: Finding Apache Server

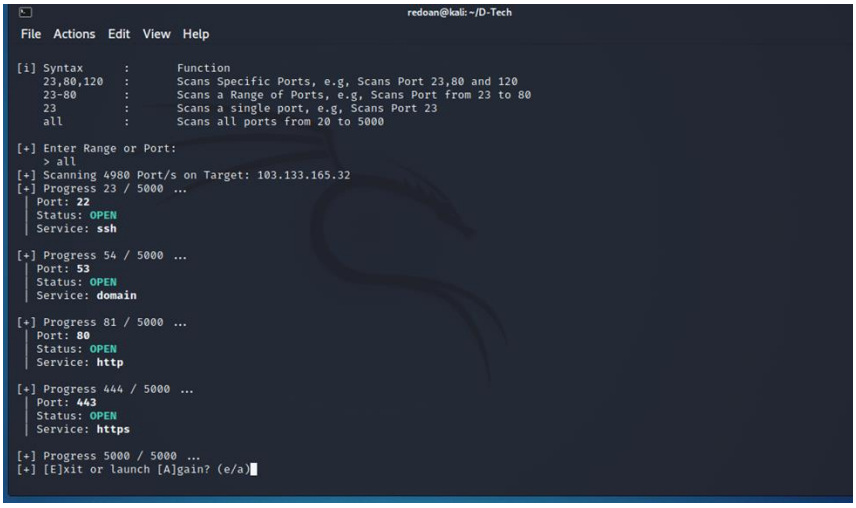

Figure 5.10: Finding Port and Service

Note: In figure 5.9 and 5.10, if hackers found any open port, then they try to connect or can easily connect to the computer for malicious use. they also try to find ports to find the vulnerabilities service. Hackers try to understand whether telnet or FTP port is password protected or not and vulnerable MySQL service running on some port.

Cross-Site Scripting [XSS] Scanner

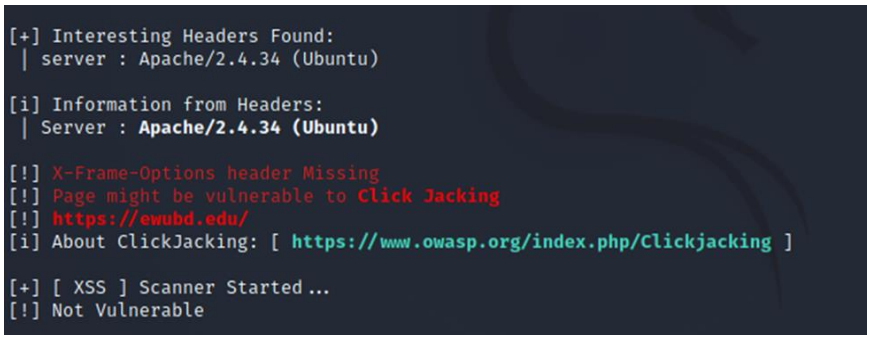

Figure 5.11: Find Vulnerable

Note: Here figure 5.11, I cannot find any vulnerabilities. The site is safe. But if it is found then hackers try to manipulate forms to keep the place of harmless forms or replace harmless forms with manipulated ones DBy the way, even SSL encryption cannot protect users from this.

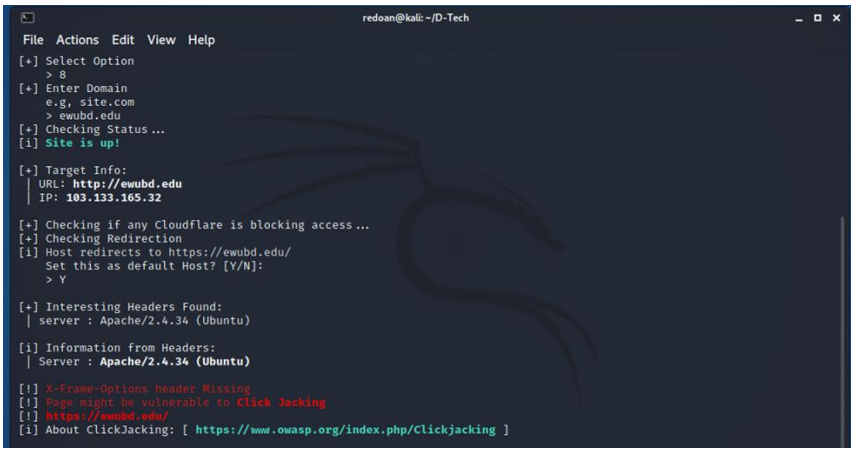

Figure 5.12: Find Vulnerable

Note: After that, I select option 8 shown in figure 5.12 where to find the SQL injection scanner. And choose my university web address there we saw that one site is up and showing the IP address. So those sites can be at risk.

5.3 About Information Gathering Tool Dimitri

Dmitry is a tool which used for information gathering tool. First need to download the tool and install in Kali Linux. Dmitry stands for Deep Magic Information Gathering Tool. It's a command-line tool Using Dmitry tool, can gather information about the target, this information can be used for social engineering attacks. It can be used to collect a quantity of valuable pieces of information

5.3.1 How to use Dimitry

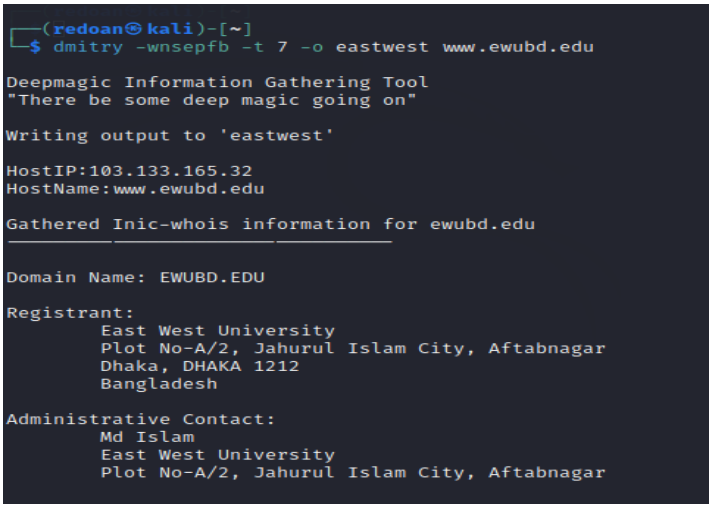

Figure 5.13 : Using Information Gathering Tool (Dmitry)

In figure 5.13, for running this command type tool we need to command that in the Kali Linux terminal "demitry -wnsepfb -t 7 -0 eastwest www.edubd .edu"

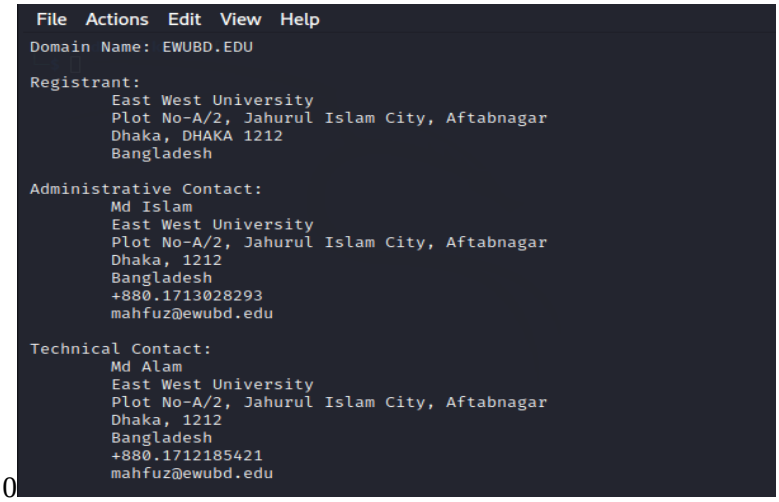

Figure 5.14: Finding EWU university Registrant, Administrative Contact and information

In figure 5.14, After command that this type of things will running for giving us the values. And find important information of an organization.

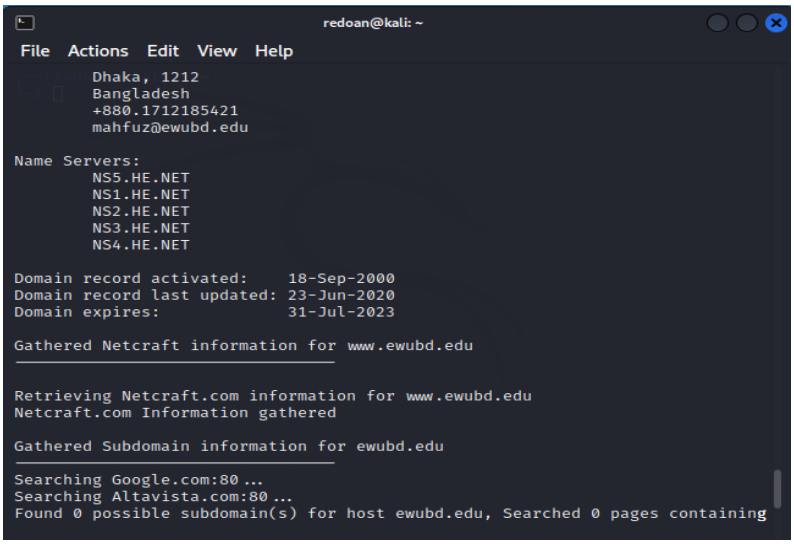

Figure 5.15: Finding Name server and domain record (DNS)

Then in figure 5.15, where finding Name server and domain record (DNS). Ordinarily, name servers use names like ns1.example.com and ns2.example.com, where example.com addresses your Domain A DNS record is an information base record used to plan a URL to an IP address. DNS records are put away in DNS servers and work to assist clients with associating. At the point when the URL is placed and looked through in the program, that URL is sent to the DNS

servers and afterward coordinated to the web server in name. In IP Address text box, type the IP address related with the name server.

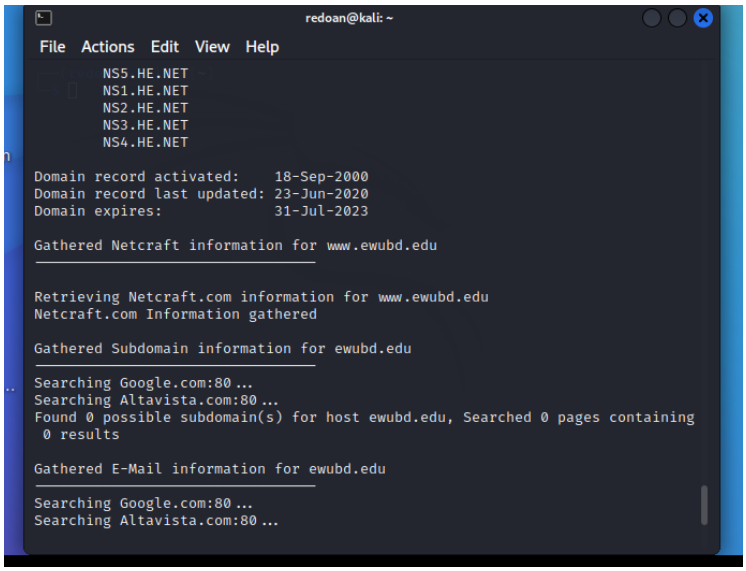

Figure 5.16: Gathered Subdomain information

In figure 5.16 where Gathered Subdomain information, In this example, ‘ewtbd’ is the subdomain, and ‘.edu’ is the top level domain.

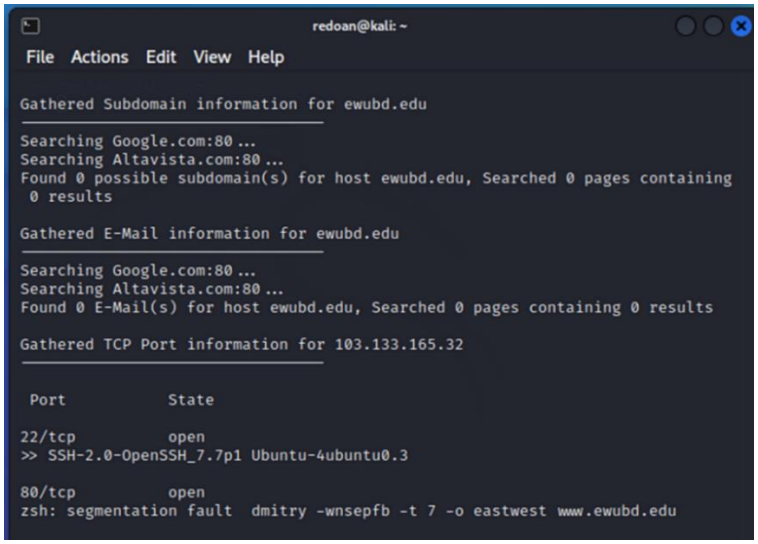

Figure 5.17: Port and State Conditions

In the figure 5.17 where find the port and condition, in here Port are the channel through what capacities on the client PC can accomplish the software program on the server. Administrations, for example, website pages or FTP, require their separate ports to be "open" on the server can be accessible for all.

Chapter SIX

6.1 Conclusion & Future Work

The development of the internet is increasing step by step, as are the quantities of information breaks and cyber-attacks. Cybercrime is a danger to all associations, and Ethical hackers use advanced tools and strategies to prevent such attacks. Ethical hacking saves an organization from fortifying its security ability in the present cyber-attacks.

With this proposal as a base, the most suitable future work would be going after weaknesses in the BGP convention to block traffic by sending vindictive bundles among confided-in looks inside the network. Creating Metasploit scripts with a clever means to run fruitful endeavors against the protected bugs in different Windows conditions utilizing ruby language will be smart. Moreover, fuzzier coding is captivating to learn and plan, which helps send produced bundles to different weak applications. Above all, computerizing the course of infiltration testing as any other programming application will assist associations with unhesitatingly protecting their organization with required insignificant information. Moreover, Social design is typically disregarded, making an unexplored world indirect access. Consistent strategies in stressing the classification during get-togethers and sites will assist with limiting the data gathering by an aggressor.

REFERENCES

1. Mike James “Ethical hacking (also referred to as white hat hacking) has become an essential way for businesses to identify and address cybersecurity exposures” Access May 1, 2019
2. https://intellipaat.com/blog/reconnaissance-in-cyber-security/ Access Jan 25,2019
3. RunRunner “Runrun.it Blog” Access Jan 25,2019
4. SoftwareTestingHelp“A Complete Penetration Testing Guide with Sample Test Cases” Last Updated: Access May 11, 2022
5. INTRODUCTION “FIVE PHASES OF HACKING” Access Posted: October 2, 2012
6. ‘Internet Security Threat Report: Volume 23’. Symantec. Accessed Apr 2019. www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.
7. Touhill, Gregory. 'Challenges on Cyber security Landscape Demand Strong Leadership.' ISACA, 20 Mar 2019. Accessed Apr 2019. www.isaca.org/Knowledge-Centre/Blog/Lists/Posts/Post.aspx?ID=1154.
8. Nicholson, S. (2019). How ethical hacking can protect organizations from a more significant threat. Computer Fraud & Security, 2019(5), *15–19.* https://doi.org/10.1016/S1361-3723(19)30054-5
9. Michael Wulff “Making the Case for Ethical Hacking” accessed July 25, 2009
10. Patrick Engebretson, ed (2013) “THE BASIC OF HACKING AND PENETRATION TESTING." 2nd ed. USA: Syngress.
11. Sumanjit Das and Tapaswini Nayak “IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES” Accessed October 2013.
12. The India Express “Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank” Accessed June 30, 2021 8:30:15 am
13. wallarm “What is a Cyber Attack?” https://www.wallarm.com/what/what-is-a-cyber-attack Retrieve by on 1th April,2022
14. Casey Crane “42 Cyber Attack Statistics by Year: A Look at the Last Decade” accessed February 21, 2020

15. Help Net Security “Cyber losses are increasing in frequency and severity” Accessed September 14, 2020
16. https://www.helpnetsecurity.com/2020/09/14/cyber-losses-are-increasing-in-frequency-and-severity/ Retrieve by on 4th March,2022
17. Nicholas Handy “Penetration Testing Introduction: Scanning & Reconnaissance” Accessed Aug 15, 2018
18. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents Retrieve by on 2th April,2022
19. https://www.simplilearn.com/ Retrieve by on 4th April,2022
20. https://www.tutorialspoint.com/penetration_testing/penetration_testing_vs_ethical_hacking.htm Retrieve by on 7th April,2022
21. https://www.pandasecurity.com/en/mediacenter/security/14-types-of-hackers-to-watch-out-for/ Retrieve by on 10th April,2022
22. Calvince Nyawara “How Hackers Use DNS Server to Hack (and How to Protect Yourself)” Retrieve by on 10th April, 2022