T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADUATE EDUCATION

CYBER SECURITY THESIS PROGRAM

A STUDY ON PENETRATION TECHNIQUES

DISSERTATION

PREPARED BY

AHMAD WAHEED MOHAMMAD SHRATEH

ANTALYA – 2022

T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADUATE EDUCATION

CYBER SECURITY THESIS PROGRAM

A STUDY ON PENETRATION TECHNIQUES

DISSERTATION

PREPARED BY

AHMAD WAHEED MOHAMMAD SHRATEH

ADVISOR

PROF. DR. CAFER ÇALIŞKAN

ANTALYA - 2022

APPROVAL/NOTIFICATION FORM

ANTALYA BİLİM UNIVERSİTY

INSTITUTE OF POST-GRADUATE EDUCATION

AHMAD WAHEED MOHAMMAD SHRATEH, a master student of Antalya Bilim University, Institute of Post Graduate Education, cyber security with student ID 2071102, successfully defended the thesis/dissertation entitled "A STUDY ON PENETRATION TECHNIQUES", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Academic Tittle, Name-Surname, Signature

Jury Member (Chairman) **:** Prof. Dr. Cafer Çalışkan **....., ...**

Jury Member **:** Dr. Öğr. Üyesi Aslı Bay **....., ...**

Jury Member **:** Dr. Onur Koçak **....., ...**

Directore of The Insitute **: .....**

Thesis Submission Date : .....

Thesis Defence Exam Date : .....

PREFACE

This master's thesis on cyber security presents the issue of cybercrime, which is one of the biggest threats to the security of an organization. Within the scope of this study, preliminary research has been conducted and many documents have been examined. I would like to thank my dissertation adviser, Prof. Dr. CAFER ÇALIŞKAN, for guiding me during the preparation of this study, as well as Asst. Prof. Dr. Aslı BAY, who gave her thoughts and suggestions at different phases of the research. I would also want to thank my family and friends for their support.

Full Name

Ahmad Waheed Mohammad Shrateh

ÖZET

PENETRASYON TEKNIKLERI ÜZERINE BIR ÇALIŞMA

Siber suçların artmasıyla siber güvenlik hiç bu kadar önemli olmamıştı. Her işletme, veri sızıntıları ve korsanlık gibi siber suçları önlemeye çalışır. Her kuruluşun benzer senaryolara hazırlanmak için çeşitli koruyucu mekanizmaları vardır. Yine de, penetrasyon testi bu koruyucu mekanizmaların verimliliğini değerlendirmek için geçerli bir yöntemdir. Sürecin her aşaması için en iyi araçları seçmek amacıyla her penetrasyon test cihazı, maliyet, zaman ve kuruluşun penetrasyon testinin kapsamı gibi önemli öğeleri incelemelidir. Bu tez, en önemli 10 aracı tartışacak ve nasıl çalıştıklarını gösterecektir. Ayrıca, uzman olmayanların penetrasyon testi hakkında bilgi sahibi olmasını sağlar ve ağ bölümünü kapsamaz.

Anahtar Kelimeler: Siber Güvenlik, Etik Bilgisayar Korsanı, Sızma Testi Araçları.

ABSTRACT

A STUDY ON PENETRATION TECHNIQUES

With cybercrime on the rise, cybersecurity has never been more crucial. Every business seeks to prevent cybercrime such as data leaks and hacking. Every organization has several protective mechanisms in place to prepare for similar scenarios. Still, penetration testing is the current method for assessing the efficacy of these protective mechanisms. To choose the best tools for each phase of the process, every penetration tester must examine important elements such as cost, time, and the scope of the organization's penetration testing. This thesis will discuss the top 10 tools and demonstrate how they work. This thesis will help non-expert to be familiar with penetration testing and will not cover network part.

Keywords: Cyber Security, Ethical Hacker, Penetration Testing Tools.

TABLE OF CONTENTS

TABLE OF FIGURE

ABBREVIATIONS

NIST : National Institute of Standards and Technology

IP : Internet Protocol

PECB : Professional Evaluation and Certification Board

DNS : Domain Name Server

CVSS : Common Vulnerability Scoring System

ICMP : Internet Control Message Protocol

SNMP : Simple Network Management Protocol

WPA : Wi-Fi Protected Access

SQL : Structured Query Language

SET : Social Engineering Toolkit

Lan : Local Area Network

NIST : National Institute of Standards and Technology

IT : Information Technology

DNS : Domin Name Server

PEN : Penetration

ARP : Address Resolution Protocol

ESSID : Extended Service Set Identification

1. INTRODUCTION

Penetration testing is referred to as a pen test. According to the National Institute of Standards and Technology (NIST), penetration testing is a type of security testing that simulates cyber-attacks in order to detect a system's or network's vulnerabilities before they can be exploited in the real world by adversaries. Weissman (Weissman,1995) defines penetration testing as "a fictitious adversary attack on a target computer system by a friendly evaluation team to discover ways to breach the system's security controls, to penetrate the security perimeter of protection in order to obtain sensitive information, unauthorized services, or to cause system damage that prevents legitimate users from accessing the system. Additionally, the United Kingdom's National Cyber Security Center describes penetration testing as "a strategy for assuring the security of an information technology system by attempting to compromise some or all of that system's security using the same tools and tactics as an adversary might." As Bishop points out, the "aspect" being examined does not have to be a computer system or network. Additionally, it can be a structure or a collection of people, an office, and a computer system (Bishop, 2007). In his book, Osborne defines pen testing as "a test to confirm that gateways, firewalls, and systems are constructed and set effectively to protect against unwanted access or efforts to interrupt services" (Osborne, 2006).

IT systems have become a vital part of many modern firms in the current business environment. Not only can a well-implemented system guarantee seamless operations, but it can also significantly enhance management processes. Despite the incredible benefits afforded by IT systems, businesses may suffer catastrophic losses and repercussions if cybercriminals compromise the systems. In order to dissuade intruders, a variety of protection mechanisms must be implemented (Bacudio, Yuan, Chu, and Jones, 2011).

After the implementation of security measures, the question of their efficiency unavoidably arises. At this point, penetration testing becomes significant. As one of the most prevalent techniques for examining system security, penetration testing may be viewed as the simulation of hacker attempts to infiltrate an IT system. In contrast to hacking efforts, which ultimately seek to cause damage and loss, the primary purpose of penetration testing is to identify any existing security vulnerabilities in the system. This

procedure enables testing teams to build realistic solutions to address such vulnerabilities, thereby enhancing the overall security of the firm. Penetration testing can find out how much the security of IT systems is at risk from attacks by hackers, crackers, and others. It can also find out if the security measures in place are enough to protect IT security (Bacudio, Yuan, Chu, and Jones, 2011).

Nowadays, businesses place a premium on data and information protection. All businesses must safeguard their information to maintain a competitive edge. Information is safeguarded through the use of well-defined protocols and well-documented organized methods. Additionally, they are required to adhere to security standards and regulations. Security assurance methods, secure software engineering environments, proof of correctness, and penetration tests are only a few of the regulatory processes (Kumar, 2014).

A security test examines the behavior of a system's security controls, whereas a PEN test measures the difficulty of an attacker penetrating a business's computing network. In a PEN test, an unauthorized attack on the test target system is demonstrated using automated programmed tools, human tools, or a combination of the two (Kumar, 2014).

One of the primary objectives of PEN testing is to instill an understanding of the significance of IT security at all levels of an organization through structured training and awareness programs to prevent security incidents that compromise confidentiality, integrity, relationships, and customer trust.

A PEN test allows a business to evaluate the security awareness of its personnel, the efficacy of its existing security policies and processes, and the productivity of its goods. It contributes to the decision-making process by evaluating the organization's security and planning security investments and information technology strategy.

Additionally, penetration testing contributes to the development of essential components of an information security strategy by promptly and precisely identifying weaknesses. In addition, it aids in improving test configurations to proactively mitigate identified risks. It allows businesses to evaluate the possibility and effects of vulnerabilities. As a result, the organization can prioritize and implement a mitigation action plan for the identified vulnerabilities. Depending on the intricacy of the business,

penetration testing needs a substantial amount of time, effort, and knowledge. Consequently, penetration testing adds to the growth of the knowledge and abilities of people involved in the process. It is viewed as a quality-control instrument that improves the company and its operations (Doshi and Trivedi, 2015).

Penetration testing is typically time-limited, and with cause. There is insufficient time to conduct all possible tests. Even if the software passes every test imaginable, this does not guarantee that it is safe. Lack of evidence of vulnerability does not necessarily imply the absence of any vulnerability; The tester may have simply overlooked anything. Since no test can be guaranteed that it has covered everything, the conventional method is to impose a time constraint and prioritize the most critical tests first. Penetration testing is not a process that can be automated. The entire purpose of the test is to uncover the flaws, the things that fell through the gaps and were overlooked. While an automatic check may protect the system from problems we were aware of yesterday, it cannot guarantee that no new vulnerabilities will be identified the following day. (Kaufmann, 2017).

Penetration testing is a rewarding professional path. It is difficult and demands a diverse set of technical skills and knowledge, including programming, networking, cryptography, and creativity. The worst aspect, though, is that we may notice defects in a program but are unable to exploit them. When this occurs, we are left concerned but without the facts necessary to persuade developers to adjust (Kaufmann, 2017).

2. PRELIMINARIES

In this chapter, we will cover the overview of the penetration process, Penetration categories and types, how security companies do penetration testing, and finally, the technical perspective of penetration testing.

2.1 Penetration Testing Categories

In general, penetration testing can be of the black box, the white box, or the gray box variety. The distinction between the two, according to the author, is the amount of knowledge and information offered; the black box is when the tester has no understanding of the organization's information structure and the source code. White box penetration testing is performed when the tester is granted a complete access to an organization's structure and source code. Gray box testing is a combination of black box and white box testing in which the tester has just a rudimentary understanding of the network or source code (Ami and Hasan, 2012).

According to the National Institute of Standards and Technology (NIST), there are four phases for penetration testing: planning, discovery, attack, and report (Baloch, 2017).

Penetration testing begins with the **planning** phase, which is a pre-engagement attack, which involves how the attack will be launched, the scope and goals of the attack. The second phase is **discovery**, this phase is divided into two parts: The first part includes information gathering, network scanning, service identification, and operating system. In this part the tester discovers and collects source information about the target system, network infrastructure, IP addresses, server type, opening ports, active service. The aim of this phase is to capture a big picture of the system. The second part is vulnerability assistant, which involves discovering a subset of input space with which a malicious user can exploit logical errors in a system to drive it into an insecure state (Sparks, 2007). Vulnerability detection and analysis attempts to scan the target system against all possible test scenarios and enlist a comprehensive set of existing gaps and weakness point.

After discovery phase, the **attack** phase begins, which it is the heart of the penetration testing process, the previous phase's vulnerabilities are attempted to be

exploited once a system has been exploited however, if a new target is discovered during this process, we return to the discovery phase (Baloch, 2017).

Last phase is **reporting**; as a documentation, this phase consolidates information about all the results and their impacts, in addition, the report should be simple, understandable.

Until recently, penetration testing has been limited to advanced security specialists with many years of relevant knowledge to perform a complicated manual process, however manual penetration testing takes time, and it is costly. However, it has long-term benefits in terms of efficiency. Where in automated penetration testing a group of specialists can get together to create a professional automated tool based on the experience of experienced penetration testers; so that non-expert users may utilize automated tools to replace the penetration team in order to acquire a comprehensive perspective of the security situation on the organization's system (Stefinko, Piskozub, and Banakh, 2016).

2.2 Types of Penetration Testing

There are several types of penetration testing, however those mentioned below are the most prevalent.

2.2.1 Network Penetration Testing

In network penetration testing, the tester evaluates the network architecture for exploitable weaknesses and threads. There are two classifications for network penetration testing (Shivayogimath, 2014):

1. External: This test demonstrates what a hacker may see in the network and exploits vulnerabilities found over the internet. The threat, in this case, comes from an external network connected to the internet. This test is run via the internet, avoiding the firewall.

2. Internal: This test identifies threats from within the network itself. It considers the risk that a dissatisfied internal employee might bring the risk to the network. More over Internal network penetration testing simulates an assault on the organization on the

assumption that the attacker already has access to the internal network. The test then attempts to document and evaluate exactly what the attacker is capable of doing once inside. In this test, a connection to the local area network (LAN) is used.

2.2.2 Web Application Penetration Testing

Web applications are the most common areas of vulnerability in today's organizations. Web app weaknesses have led to the theft of millions of credit cards, huge financial loss, and threat on sensitive data (Baloch, 2017). This type of penetration tester will simulate unauthorized attacks from within or outside the company in order to get access to sensitive data.

2.2.3 Mobile Application Penetration Testing

Mobile application development is currently one of the most essential forms of software development, and many businesses have included it in their operations; as a result, companies should be sufficiently safe and secure while providing services and sensitive data.

2.2.4 Social Engineering Penetration Testing

A social engineering attack is completely based on human mistakes (Al Shebli, 2018). The tester in this type may be asked to attack a user in the organization, such as utilize speared phishing attacks to fool the user into doing anything they do not intend to do.

This will assist the company in evaluating its employees' commitment to the organization's policies and procedures.

2.2.5 Physical Penetration Testing

Physical penetration testing involves the tester physically entering restricted areas and personally engaging with employees to persuade them to break the rules or provide credentials (Pieters and Dimkov, 2011).

2.3 Penetration Testing Methodology Provided by Companies

In this section, Based on white paper for random companies,We will focus on how the security companies conduct penetration testing services.

2.3.1 Bulletproof

Generally, all security companies have the same flow of penetration methodology, which are basically summarized in seven steps (bulletproof penetration testing white paper, 2021):

2.3.1.1 Scope Definition & Pre-engagement Interactions

Starting with setting some goals, and limitations, and agree which penetration type will be used.

2.3.1.2 Intelligence Gathering & Threat Modelling

Intelligence gathering is collecting all the possible information about the target; this information will help the tester in the vulnerability assessment and exploitation phases.

2.3.1.3 Vulnerability Analysis

This phase aims to find weaknesses in networks, systems, or applications, which might include host and service misconfiguration, and unsafe application design.

2.3.1.4 Exploitation

Depending on the preview phase the system is attacked, using custom-made, available exploits and methods to bypass system security, get sensitive information, and gain access to the system.

2.3.1.5 Post-exploitation

The goal of this phase is to determine the value of the compromised targets by attempting to escalate privileges, pivot to different systems and networks identified within the scope.

2.3.1.6 Reporting

In this phase the penetration company provide simple and easy to read the documentation and include the above information:

a. All System risks
b. Vulnerabilities and active service
c. Actions should be taken in the near and long term

d. What steps have been taken to exploit each vulnerability flow

2.3.1.7 De-brief Session

This additional step occurs after the report has been provided and consists of a discussion of the report's findings and an opportunity to ask any questions.

2.3.2 Professional Evaluation and Certification Board (PECB)

Every company should prioritize fixing IT vulnerabilities and secure them from all kinds of attacks. When doing a PEN test, there are six key steps to follow (Arta, Era, and Muhadri, 2021):

2.3.2.1 Information Gathering (Reconnaissance)

Before conducting a PEN test, it is essential to obtain as much information as possible about the target; the more information gathered, the more likely it is that vulnerabilities or flaws will be uncovered. During reconnaissance, The tester may also gather information on a company's network infrastructure, operating systems, apps, and users.

Footprinting is the process of collecting as much information as possible about a network, system, or individual. There are many sorts of footprinting, including open-source footprinting, network-based footprinting, and domain name server (DNS) interrogation. It helps the tester obtain access to the system, and there are footprinting tools such as Whois Lookup, NS Lookup, and IP Lookup.

2.3.2.2 Scanning and Enumeration

Scanning is a procedure to identify hosts, ports, and other network services. Network scanning is a retrieval process for information that is used to build an overview picture of the target’s organization; in addition, there are different tools for each type of scanning such as Nmap, Wireshark, OWASP ZAP, and nslookup.

Enumeration is used to collect data such as usernames, hostnames, IP tables and routing tables, as well as applications and banners. Automated vulnerability scanning and enumeration are commonly used to indicate the existence of vulnerabilities without taking any action.

2.3.2.3 Gaining Access

During this phase, PEN testers use a variety of attack methods to aggressively attack the system's vulnerabilities. The Common Vulnerability Scoring System (CVSS) ratings of the detected vulnerabilities are compared. The higher the CVSS score, the more easily the vulnerability may be exploited. The scope of penetration testing determines the techniques for gaining access. The major goal of this phase is to determine how much harm a hacker may wreak. PEN testers will attempt to escalate their access privileges and pivot, or access other sections of the network. Once initial access has been achieved, credential harvesting and structured passwords are two methods for privilege escalation.

2.3.2.4 Maintaining Access

After gaining access to systems and networks, the tester tries to maintain that access. The goal is to stay as long as possible within the system. This enables them to harvest useful information, pivot to other regions, or exploit the environment even more. It can also be used to find additional weaknesses that are not readily apparent.

2.3.2.5 Cleaning Up

Any artefacts generated during the PEN test should be cleaned and destroyed by the penetration tester, agents, scripts, backdoors, temporary files, and shell sessions are examples of all these. Cleaning up and erasing artefacts allow PEN testers to think like hackers and identify activities that possible hackers could take to erase their footprints.

2.3.2.6 Reporting

The penetration test results are examined and documented in a written report. During all phases of the test, PEN testers keep a record of everything they do. This phase's major goal is to offer details on how access points and vulnerabilities were found.

2.3.3 Lifars

Penetration testing is divided into seven industry-accepted phases (LIFARS Penetration Testing Whitepaper, 2017).

2.3.3.1 Scoping

The early phase of a penetration test consists of planning and preparing to run a successful test. Next, the tester and company determine and agree upon the test's objectives and goals. The most common objectives of penetration testing are to detect system vulnerabilities and increase security.

2.3.3.2 Discovery, Reconnaissance, and Information Gathering

This step's main goal is to gather information about the target. A tester scans the target with automated tools to discover knowledge about an organization's system. This data is used to execute a more successful attack. Utilizing a variety of tools, the target is scanned for existing vulnerabilities. These programs have their own database containing information about the most current vulnerabilities.

2.3.3.3 Network Enumeration and Scanning

The third step of penetration testing partially intersects with the second phase. Using Network Enumeration, testers discover hosts and devices on the network. Various discovery protocols, including ICMP and SNMP, are utilized to scan the networks. Since hosts and devices are fingerprinted, testers are on the lookout for well-known services. This step includes using a vulnerability scanner on the target network or a network mapper to determine the versions of services operating on a host.

2.3.3.4 Vulnerability Mapping

All automated or manual tests and scans are examined in this step. This process allows testers to find, measure, and rank vulnerabilities methodically.

2.3.3.5 Exploitation

This is the most critical phase of the entire testing scenario since it determines whether the test will be successful or will fail. Testers are likely to exploit weaknesses or bypass security limitations to gain access to a system or resource. Since exploits are customized based on the vulnerabilities discovered in the system, the tools and techniques utilized in the second phase (discovery, reconnaissance, and information gathering) are critical to successful exploitation.

2.3.3.6 Clean Up

After gaining network access, testers aim to collect data as much as possible, but they must stay stealthy during the process to avoid being detected. Testers utilize a variety of techniques to keep access, including privilege escalation, establishing a backdoor, and sending phishing emails,

2.3.3.7 Reporting

Actions from the previous six phases are documented and professionally presented to the client. The scope, information, attack path, vulnerabilities, used attack vectors, advice, and remedy are all included in the report.

2.4 Technical Penetration Testing

The following are technical procedures used by the most of experts in real-world penetration scenarios.

2.4.1 Pre-connection Attacks

This phase is the most important phase of the penetration testing process since it allows the tester to know about the target system. In this phase, the tester collects information about the target system with direct or indirect interaction. Some of the tools, frameworks and commands utilized during this phase are covered below.

AIRODUMP-NG tool is a part of the aircrack-ng suit. It is a packet sniffer and allows the tester to discover and capture packets that are in his range and show the tester detailed information such as (MAC address, clients connected, and encryption type) (Sabih, 2021). Starting airdump tool by using **airodump-ng {Interface Name}** command will run the airdump tool to detect all networks within the interface range.

The result, it will show us the network's target MAC address, signal strength, beacons, number of data packets, channel number, maximum speed supported by the network, and encryption type. Additionally we will detect the ESSID which is the name of the network ,cypher and authentication used in the network . This information will help the tester to get a bigger picture of the target (Sabih, 2021).

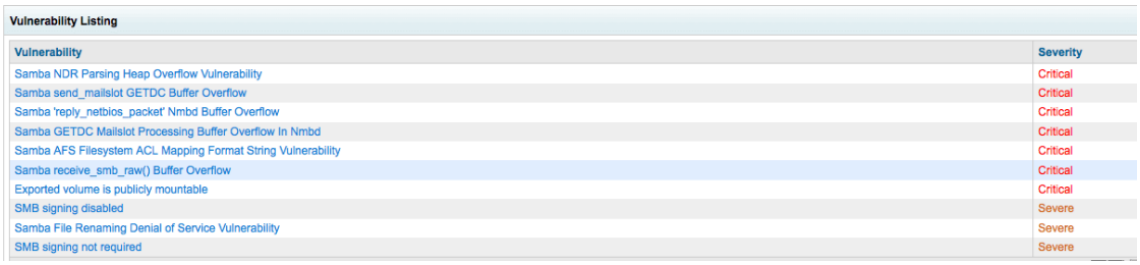
ZENMAP is another another tool that is used in the process of discovering and scanning networks. It is the graphical user interface for the network scanner known as

Nmap, and it basically discovers open ports, running services, operating system, and determines the connected clients. In addition, the tester can go deep into each port or service that we have discovered and search for any misconfiguration or backdoor to use later to gain access to the target. The output in Figure 1 below shows the ZENMAP scanning on a specific IP Address.

Figure 1. Zenmap Output

Source: Rahalkar, 2019

NEXPOSE is a management framework that can cover the whole life cycle of penetration testing; it can scan open ports, discover running services, find vulnerability and exploits them. Moreover it can also use to automate these scans and schedule them (Sabih, 2021). The outputs of Nexpose on a specific target are shown in Figure 2.



Vulnerability Listing

Vulnerability	Severity
Samba NDR Parsing Heap Overflow Vulnerability	Critical
Samba send_mailslot GETDC Buffer Overflow	Critical
Samba 'reply_netbios_packet' Nmbd Buffer Overflow	Critical
Samba GETDC Mailslot Processing Buffer Overflow In Nmbd	Critical
Samba AFS Filesystem ACL Mapping Format String Vulnerability	Critical
Samba receive_smb_raw() Buffer Overflow	Critical
Exported volume is publicly mountable	Critical
SMB signing disabled	Severe
Samba File Renaming Denial of Service Vulnerability	Severe
SMB signing not required	Severe

Figure 2. Nexpose Output

Source: Offensive-security, 2009

2.4.2 Gaining Access

The following stage, based on the output of the AIRODUMP-NG program, is to utilize this information to evaluate if there are exploitable vulnerabilities. In practice, the network's encryption method is the most important detail of gathered information, since there are two encryption mechanismsthat can be used in wireless networks; WAP (hard to crack) and WEP (Easy to crack) due to their poor quality encryption (Sabih, 2021).

To exploit WEP vulnerabilities and crack networks that use this encryption . The tester must catch and analyze big data packets to obtain the key. The initial stage is to focus on the target's network to collect and save all data in a file. This can be achieved with the following command: **airodump-ng -c {network channel} --bssid {target network} -w {file name} {interface name).** The next step is to execute AIRCRACK-NG against the file in that we have stored our data, **aircrack-ng {file name}**. After a thorough analysis, the key will be found in ASCII format.

Using the output from Zenmap tools in Figure 1 there are many open ports that can be a weakness, The tester should go through all these ports and check them one by one if there is any weakness, misconfiguration, or exploited command (Sabih, 2021). However, the port number 512 with execute service and netkit-rsh version ; is a remote executing program, using it we will be able to execute commands on the target's computer. The netkit-rsh version uses RSH rlogin, Which mean we can use rlogin program to get access on the target

The tester will use the rlogin program to facilitate the login process using the following command **rlogin –l {user} {IP address}**, tester writes root as the user, which is the highest privilege on the system followed by the target's IP address

2.4.3 Post Connection Attacks

This phase comes after we gain access to the computer, whether the tester used social engineering, server-side exploitation or a backdoor. We are assuming that the tester gains access to that computer. In this phase, we can maintain our access or use the target computer as a pivot to exploit all the other computers on the same network. Testers can upload any tools required for use, such as Nmap or ARP spoof, and run them on the hacked computer that is connected to the network, after which they can run a port scanner or perform a man-in-the-middle attack (Sabih, 2021). Moreover, we can set up a route between the hacker and the hacked device to use any metasploit auxiliary. To do that, we are going to use a module called AutoRoute. Starting with the **ifconfig** command to see all connected devices on the network and get the IP address of the target's computer. After the tester has the target's IP address, the tester sets up the route using the **post/multi/manage/autoroute** modul command, The next step is to set up the session, and subnet setting to target IP address set **SESSION {number}**, set **SUBNET {target IP address}**, exploit to execute the commands.

The last phase of penetration testing is generating a report that summarizes the tester's penetration process; this phase can be done manually or automatically. One of many tools that can generate a report is NEXPOSE which is not just a scanning framework, as we mentioned before it is a framework that covers post and pre-connection phases as well. Nexpose can generate reports to detail everything that it has discovered as well as a technical report for technical people and high-level reports to share with less technical people such as admins and managers (Muñoz, 2018). Nexpose report is shown in Figure 3.

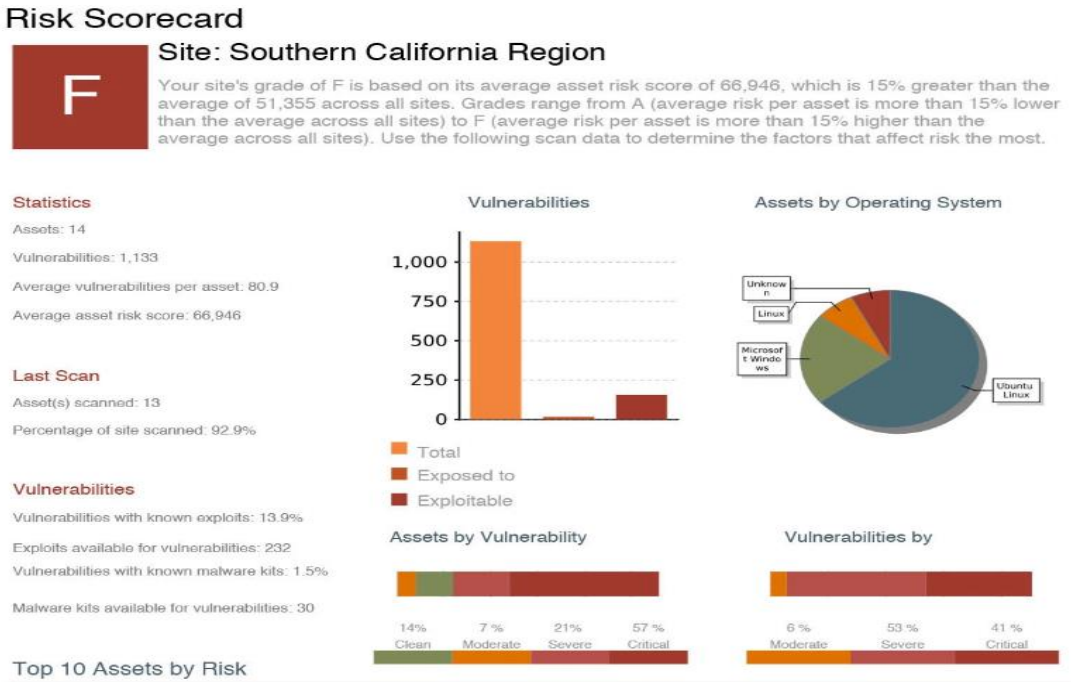


Figure 3. Nexpose Remediation Reporting

Source: Rapid7, 2016

3. METHODOLOGY

After giving an overview of the penetration process, we discussed the categories and types of penetration. This chapter will provide an introduction to some tools and illustrate how they work.

The purpose of penetration testing is to evaluate the security of a system until it can be improved, therefore avoiding real threat actors from exploiting vulnerabilities. Despite the fact that businesses are aware that they cannot guarantee the security of every system, they are extremely curious about the nature of the security issues they face. This is where penetration testing of ethical hacking methods is useful. Penetration testing differs from vulnerability analysis and scanning since it simulates an actual hacker assault.

Due to financial constraints, an actual penetration test will typically not employ all available test modules. This would assure a comprehensive examination, but it would be incredibly time-consuming and hence incompatible with the client's objectives and specific security requirements. When security requirements are especially stringent, the test should be as thorough as possible. This implies that all or most modules must be applied, and client's entire system must be tested. Certain components can be omitted and/or just exposed, and/or externally visible systems can be tested if the security requirements are low. The extent of the penetration test should be determined by financial concerns. The cost or dangers of the testing activities must be evaluated against the possible cost and risks of an attack.

As part of a penetration test, penetration testing tools are used to automate activities, increase productivity, and find vulnerabilities that would be difficult to detect using manual analysis alone. When determining which tools to use during the different stages of a penetration test, there are a variety of available strategies. Several penetration testing tools and frameworks can be used to evaluate a variety of products and execute a variety of attacks. These tools are classified into numerous groups based on their respective functions.

3.1 Penetration Testing Tools

There are several commercial and open-source penetration-testing tools available to assist the tester in evaluating the security of the system. The following are the top 10 free penetration-testing tools for 2021 (Balaji, 2021).

Metasploit: Metasploit is a free, open-source framework for executing exploits on remote target machines (Timalsina and Gurung, 2015). Metasploit is a tool for identifying vulnerabilities in operating systems and applications. This tool in penetration testing is based on the concept of "exploit." It executes a set of codes on the target, therefore establishing a framework for penetration testing. It is compatible with Linux, Mac OS X, and Windows. Framework components include tools, libraries, modules, and user interfaces. The primary component of the framework is a module launcher that enables users to configure exploit modules and launch them against a target system. Unlike other tools, however, the majority of them are built for a specific function. Metasploit is a tool for penetration testing that can perform a variety of tasks throughout the entire life cycle of a penetration test (Rahalkar, 2017). More information on how to use Metasploit can be found in the steps listed below:

Starting with scanning targets, which currently exist in the process of discovering hosts and enumerating open ports to gain visibility into network services. Metasploit features a built-in discovery scanner that uses Nmap to do basic TCP port scanning and gather additional information about the target hosts. The tester starts scanning from within a project's menu bar, shown in Figure 4.

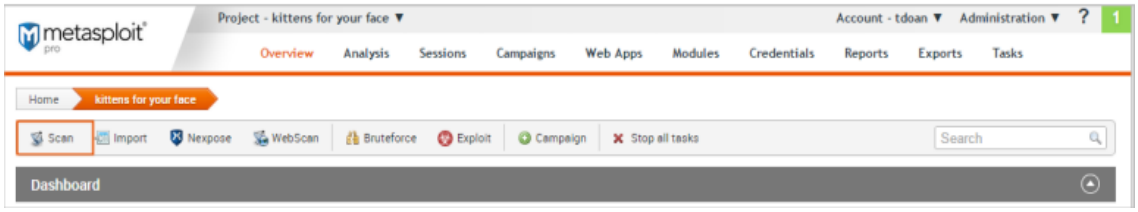


Figure 4. Step for Run Metasploit

When the New Discovery Scan form appears, the tester must enter the IP address of the target before running the scan. Check Figure 5.

Figure 5. Step for Run Metasploit

Additionally, The tester may export and import data between Metasploit projects. This allow the tester to sharing findings with other team members.

Select the Import button inside of the Quick Tasks box to import data into a project. Select the Import from File option when the Import Data screen displays. Figure 6.

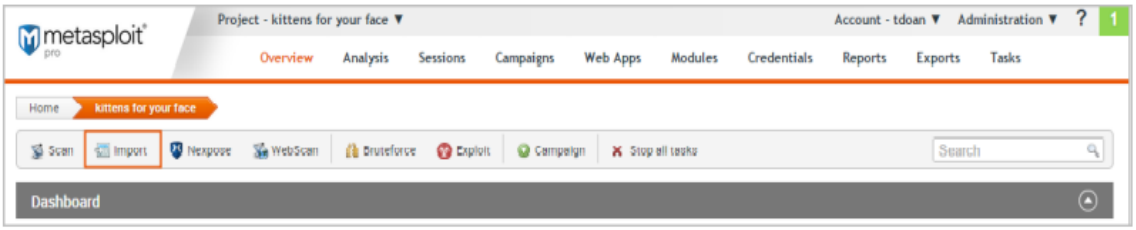


Figure 6. Step for Run Metasploit

After scanning is complete, To examine further information about a host, the tester should click on the host's IP address to access the single host view. After that, he will be able to view a target host's services, vulnerabilities, and ports. Check Figure 7.

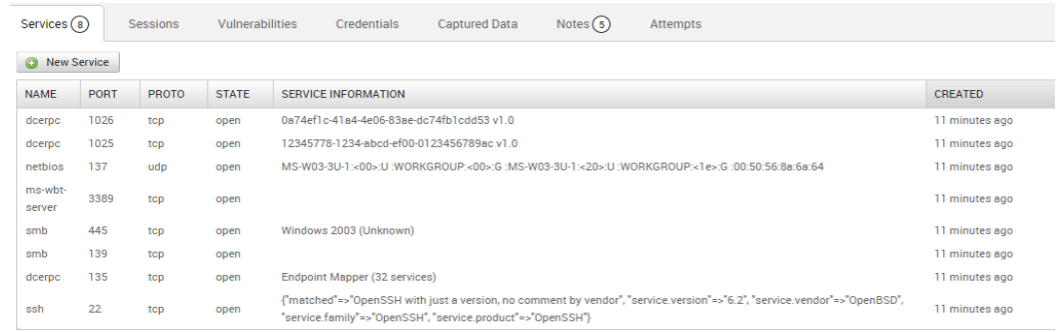


Figure 7. Step for Run Metasploit

After adding target data to the project, the tester can start a vulnerability scan to identify exploitable security vulnerabilities. Scanners for vulnerabilities utilize vulnerability databases and scans to identify known vulnerabilities and configuration issues on target machines.

The integration with Nexpose enables the tester to immediately initiate a vulnerability scan through the Metasploit web interface. Click the Nexpose button available in the Quick Tasks bar to start a Nexpose scan on the target. Figure 8.

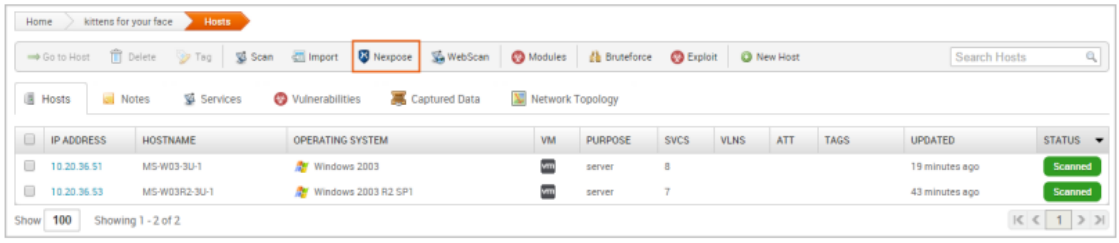


Figure 8. Step for Run Metasploit

Next, To view all of Nexpose's potential security vulnerabilities, go to Analysis Vulnerabilities. To discover the modules that may be used to exploit a vulnerability by clicking on the vulnerability's name, Figure 9. This information helps with the next step of the penetration testing, which is called "exploitation".

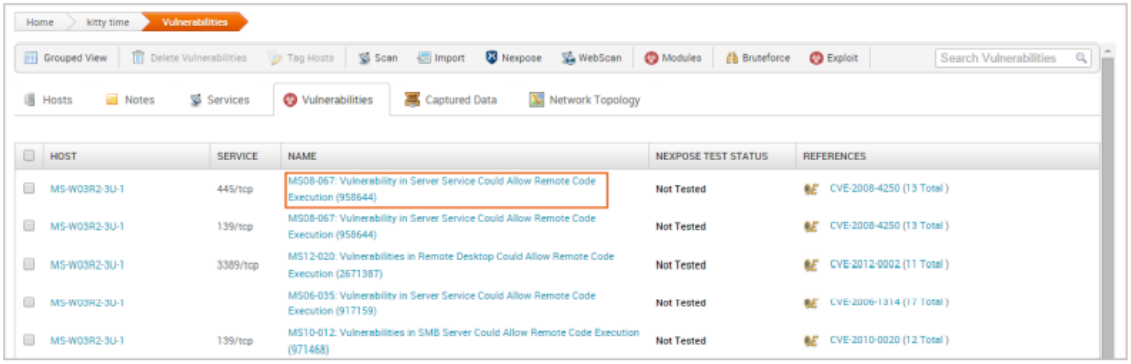


Figure 9. Step for Run Metasploit

Tester can move on to the exploitation phase after gathering information about the target and identifying possible vulnerabilities. Metasploit offers automation and manual exploitation, Click the Exploit button in the Quick Tasks tab to start auto-exploitation. Figure 10.

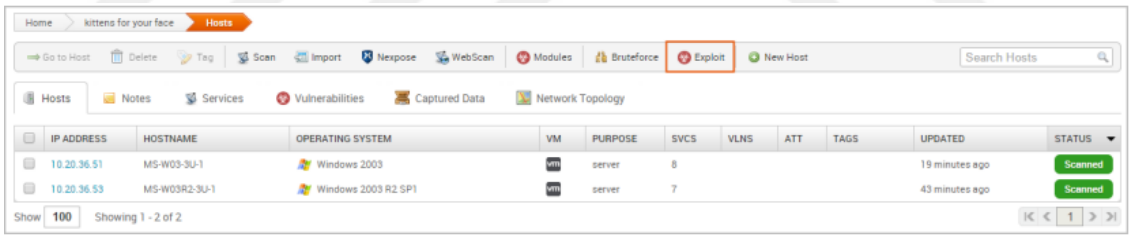


Figure 10. Step for Run Metasploit

Manual exploitation is a more comprehensive and systematic way for exploiting vulnerabilities. It enable the tester to run a selected exploit individually. This strategy is very handy when a specific vulnerability need to be exploited.

To search for modules, choose Modules > Search and type the target module's name. The most effective method for finding a perfect module match is to search by vulnerability reference.

One of the simplest methods to find an exploit for a vulnerability is on the vulnerability page directly. To examine all project vulnerabilities, choose Analysis > Vulnerabilities. Moreover, the tester may click on the name of the vulnerability to examine the modules that can be exploited. Figure 11.

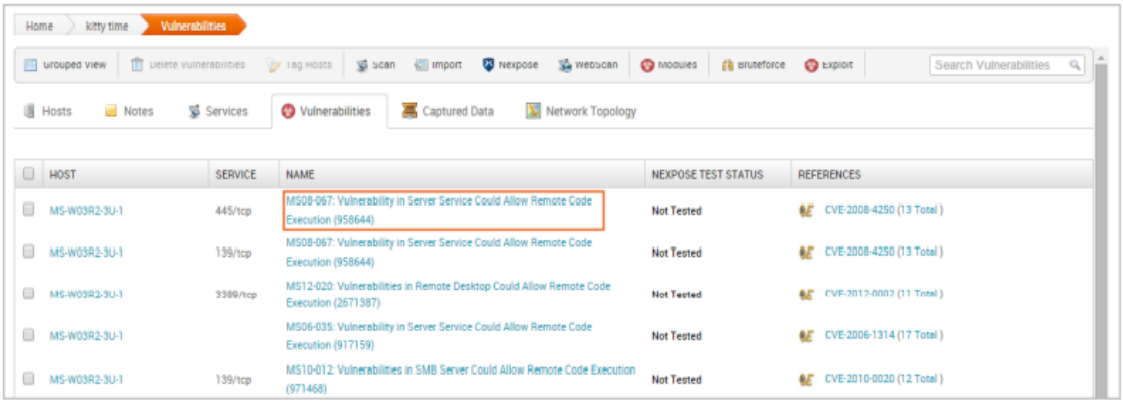


Figure 11. Step for Run Metasploit

A list of exploits that can be used against the host is displayed in the single vulnerability view. Tester may open the module's configuration page by clicking the Exploit button. Figure 12.

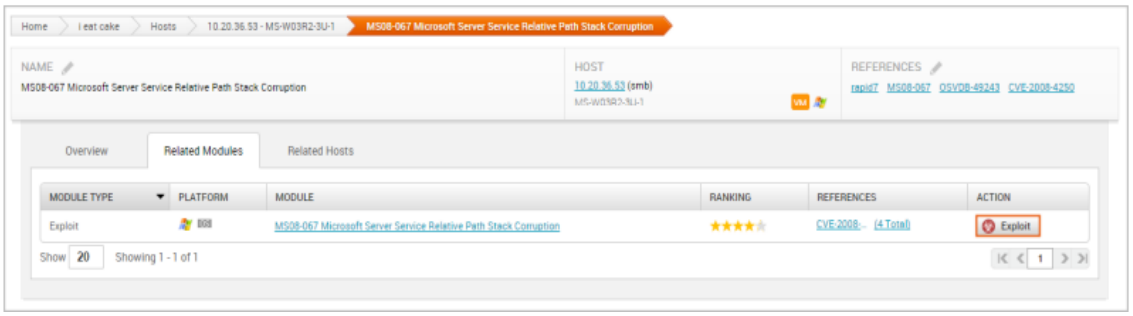


Figure 12. Step for Run Metasploit

NMAP: Nmap (Network Mapper) is a free and open-source network discovery and security auditing program. Nmap examines raw IP packets in unique ways to determine what hosts are on a network, what services they offer such as application name and version, what operating systems they are running, and what type of packet filters/firewalls they are employing, amongst hundreds of other details. It was designed to efficiently scan large networks as well as single hosts. Nmap is a powerful tool with a simple interface. Tester may utilize the Zenmap graphical user interface or use its command-line options, which are simple to use and scrip (Orebaugh and Pinkard, 2011). In addition, Nmap is compatible with all major computer operating systems, it runs on Windows, Linux, and Mac OS .

Zenmap aims to simplify security scanning for both beginners and experts. The UI of Zenmap offers three fundamental setting options. **Target**: This can be a single target address, multiple target addresses, or a subnet range. **Profile**: the type of scan; neither tester enables customized scans. **Command**: Nmap command that will be executed in the background (Rahalkar , 2018).

In scanning using Zenmap, the tester simply enters the IP address of the target device or server in the "Target" field, then chooses the required scan type in the "Profile" drop-down menu, and finally clicks the "Scan" button to start a scan, as seen in Figure 13.

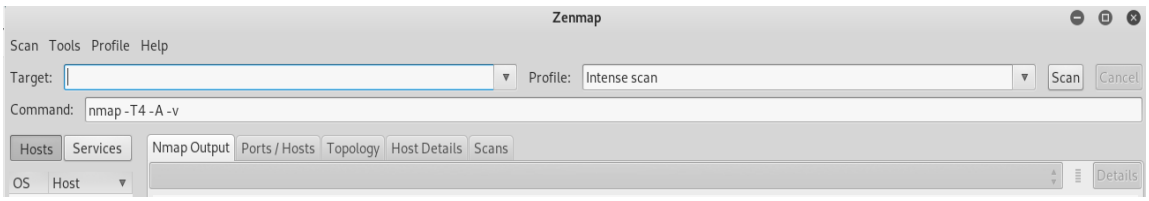


Figure 13. Start Zenmap

Zenmap allows the tester to scan the whole range on the same network, Figure 14 shows the output of Zenmap scan by discovering all the hosts on the subnet and displaying the information about them such as the open ports, running services.

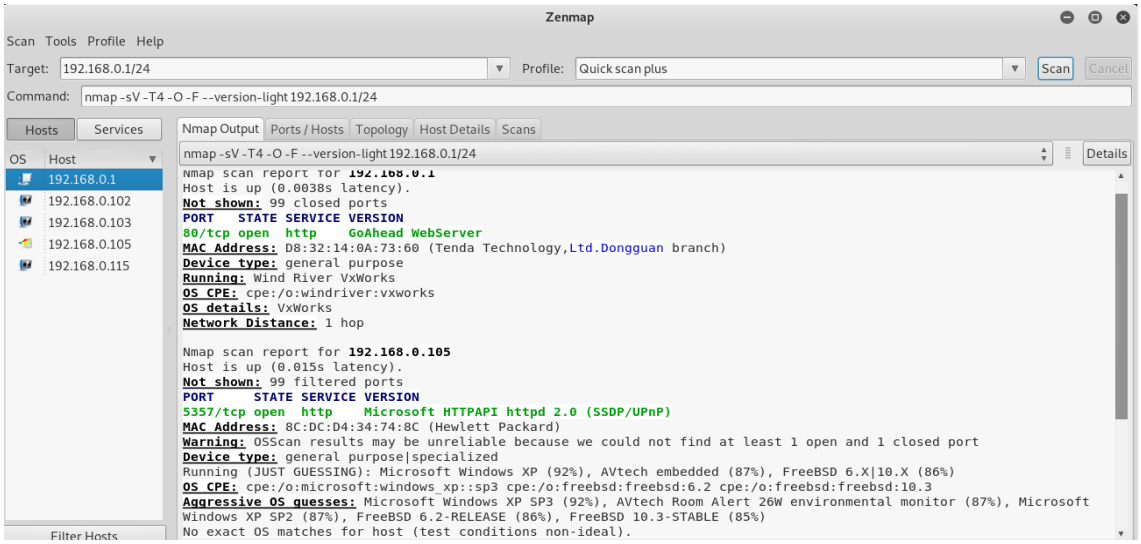


Figure 14. Zenmap Scan Output

Wireshark: Wireshark is a free and open-source network sniffing tool (Sandhya, Purkayastha, Joshua, and Akash, 2017). Wireshark is a network protocol analyzer with a graphical user interface and TShark for text mode, display filters, live capture, and offline analysis, as well as the ability to read a number of capture file types and support hundreds of protocols. Wireshark is a flexible tool that may be used on several systems. It's compatible with Windows, Linux, and Mac OS. Wireshark captures and archives network traffic on a local network for later analysis. Wireshark is capable of capturing network data from several media types, including Ethernet, Wireless LAN, Bluetooth, and USB. These packets will assist to detect network issues, and many hackers use Wireshark to steal sensitive data. (McRee, 2006).

Start Wireshark by choosing the interface for live packet capture. Otherwise, a captured file may be imported. Figure 15 used a wireless adapter interface.

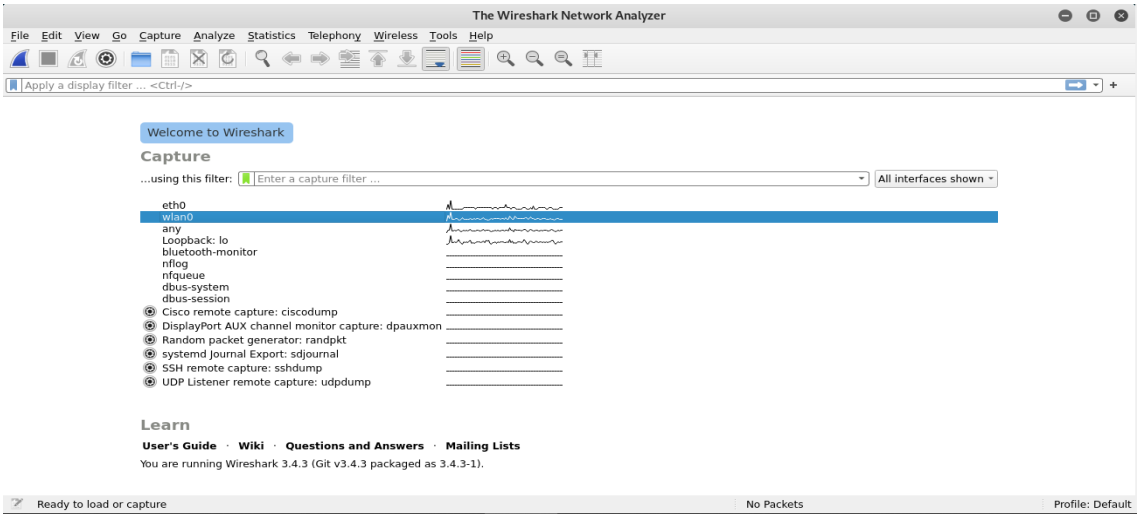


Figure 15. The Wireless Adapter

The live packet capture that is shown in Figure 16 represents the data transfer in a range of the wireless adapter. A tester can easily determine the origin and the final destination of a packet.

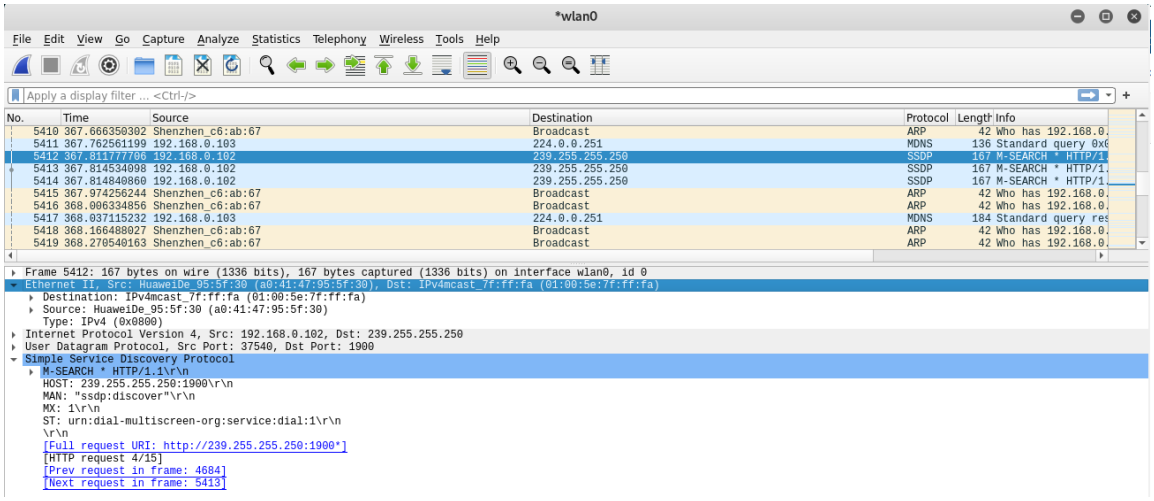


Figure 16. Live Packet Capturing

Wireshark offers a data filter that facilitates it is management. For instance, to only display packets transmitted or received from a specific IP address, set **IP.addr=={target IP address}** command. Filtering command output is seen in Figure 17.

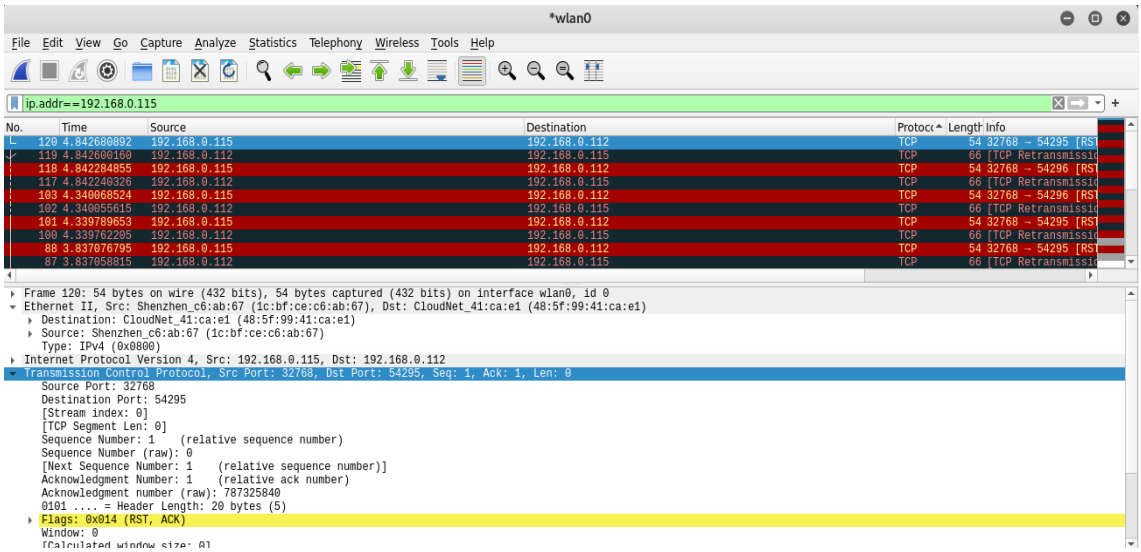


Figure 17. Filtering Output

Aircrack: The Aircrack-ng package contains tools for capturing packets, handshakes, de-authentication of connected clients, generating traffic, brute-force, and dictionary attacks. The main purpose of this tool is to assess the security of wireless networks. It may be used to capture wireless traffic, inspect Wi-Fi cards, and verify password strength (Čisar and Čisar, 2018). Aircrack is a very useful tool for Wireless Local Area Networks (WLANs), especially on Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) protocols (Kumkar, Tiwari, Tiwari, Gupta, and Shrawne, 2012).

Aicrack-ng is a multi-tool suite that consists of the following tools: **aircrack-ng** for cracking wireless passwords, **Airplay** for client de-authentication and traffic generation, **Airodump** for packet capture, **Airbase** for creating fake access points (Čisar and Čisar, 2018). Aircrack-ng is a tool that is pre-installed in Kali Linux . Using Airodump-ng tools, begin capturing all packets in the Wi-Fi card's range.

The techniques are listed below; Start monitoring mode on the wireless interface with **airmon-ng start {interface Name}**, then run airodump **airodump-ng {interface}**, the tester will be able to detect all access points within range. Figure 18.

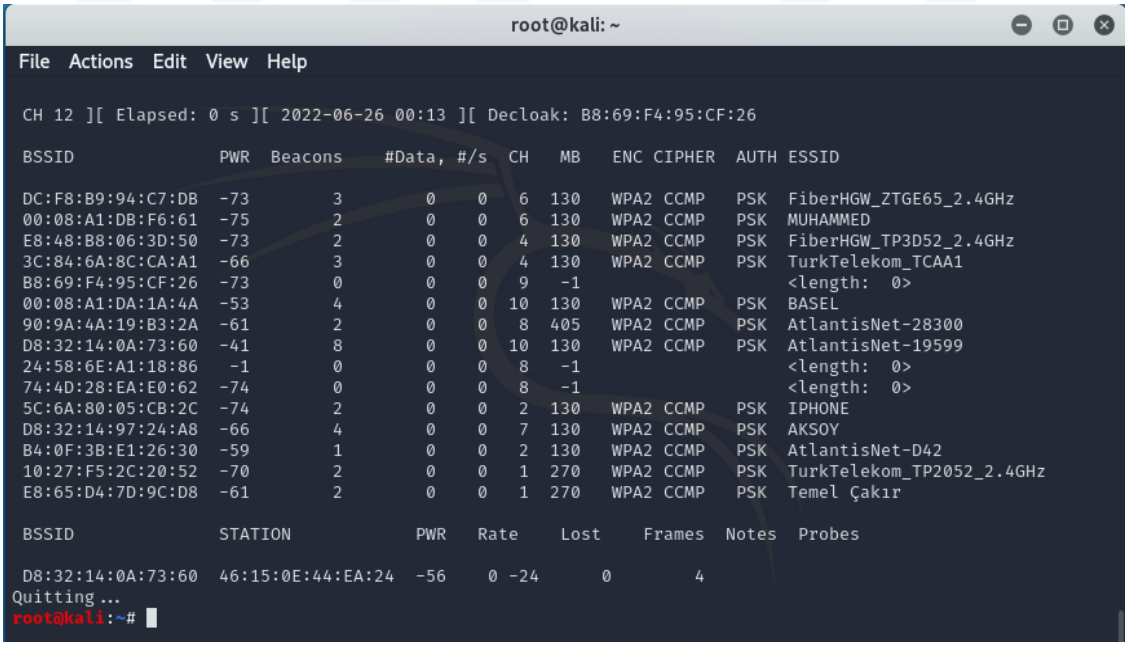


Figure 18. Airodump Scanning

The target will be picked by the tester. Depending on the captured information about the target, it shows that the target uses WPA encryption. In addition, for breaking such a WPA-encrypted network, the tester must use a 4-way handshake and a password-containing wordlist.

Use the following command to focus on a single target and store all available data and handshake packets into a file: **airodump-ng—channel {channel} —bssid {bssid} —write {filename} {interface}**. Check Figure 19.

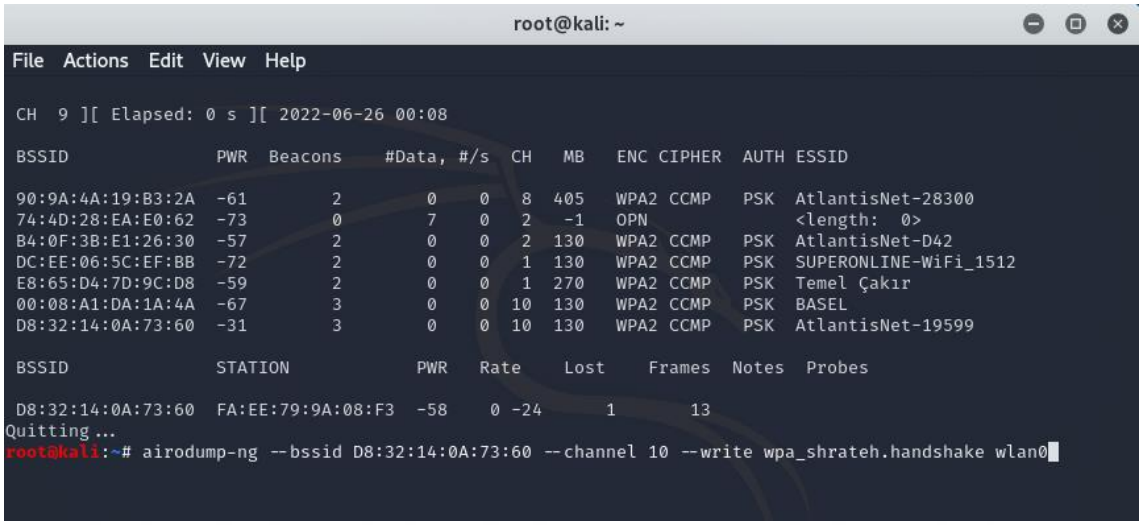


Figure 19. Airodump Output

The tester will wait until the handshake is captured, which will happen when a new client connects to the network. Alternatively, we may use a de-authentication attack to temporarily disconnect a client. Whenever a client reconnects to a network, a handshake packet will be captured. Using the command below to de-authentication attack **aireplay-ng –deauth {number of packet} –a {MAC address of the target network} –c {MAC address of the clinet} {wirless adapter}.** After that, the handshake packet will be captured.Figure 20.

Figure 20. Handshake Captured

Once the handshake packet has been saved to a file, the tester will execute **aircrack-ng {handshake file} –w{word list file}.** This command will use a handshake packet and test each password in the list to confirm the correct password.

Nessus: Nessus is a powerful remote security-scanning tool that scans devices and informs the tester if it detects any vulnerabilities that might be exploited by hackers to obtain access to a network-connected device. More than 1200 tests were performed on a specific device to determine if any of these attacks could be used to break into or harm the computer. Nessus scans network devices, virtual hosts, operating systems, databases, web applications, and IPv4/IPv6 hybrid networks for vulnerabilities (Wang and Yang, 2017). There are three unique versions of Nessus. The free version is available for non-commercial users such as educators, students, and individuals, whereas the professional version for consultants, pen testers, and security practitioners, and the Nessus Manager version, offer vulnerability management for small, medium, and large organizations.

Figure 21 depicts how to start Nessus scanning by clicking "new scan" and selecting "scan template. After that will show up many options that can be used and each option has a specific test. host discovery is used if the tester wants to examine the network that he connecting with). The advanced scan is used when scanning a target device or target range.

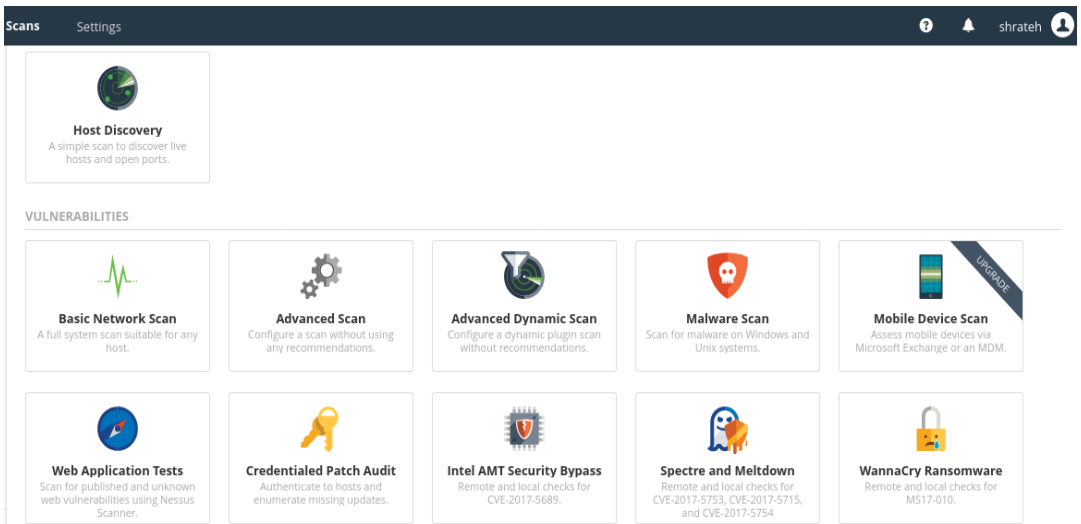


Figure 21. Nessus Scanning

Next, After entering the target information, the tester may scan a local target or a number of networks. Figure 22 showse the advance scan.

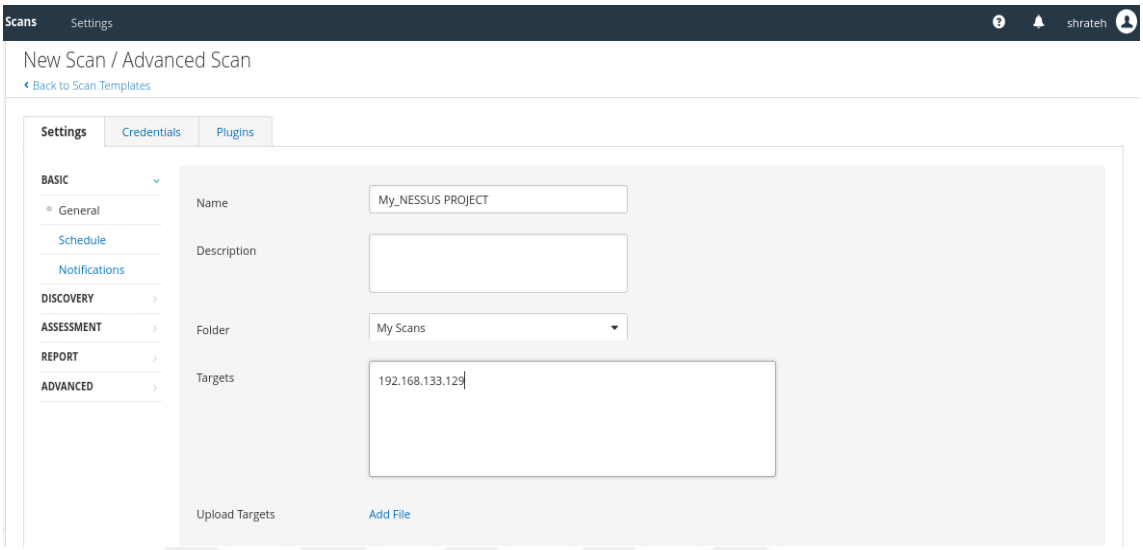


Figure 22. Advanced Scan

The result of the advanced scanning report is shown in Figure 23, which shows all of the identified vulnerabilities and their respective risk ratios.

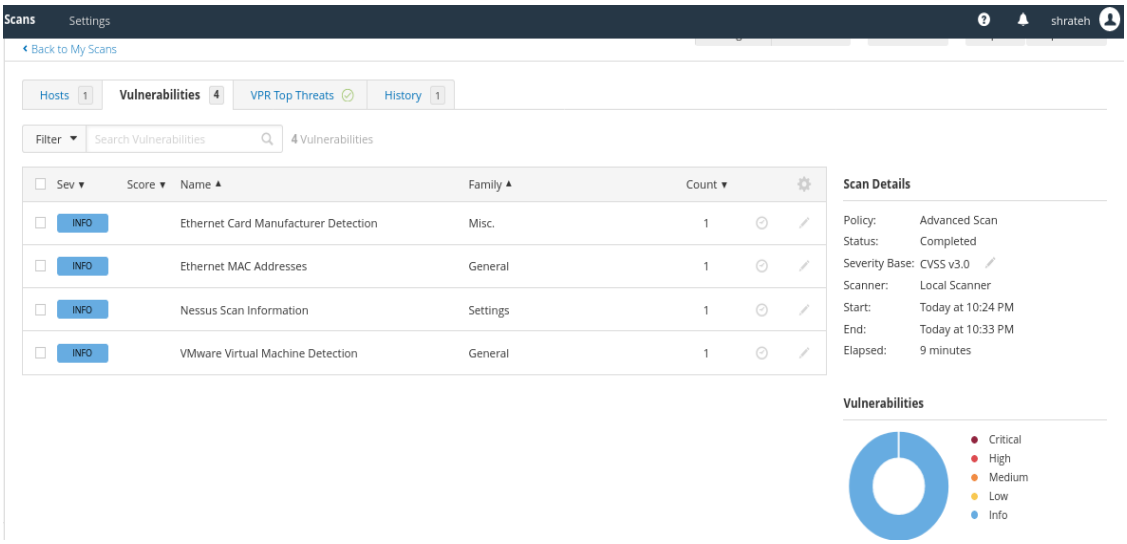


Figure 23. Addvance Scaning Report

Social Engineering Toolkit (SET): Software-based social engineering refers to attacks that use system software such as a computer or a mobile device to obtain the required information (Salahdine and Kaabouch, 2019). The Social-Engineer Toolkit is

one-of-a-kind suite of tools that detect this type of attack. Creating spear-phishing attacks, website attacks, infection media generator, mass mailing, qrcode attacks, and powershell attack vectors can be used. Moreover, it is an open-source python-driven tool for social-engineering penetration testing and it is pre-installed in kali Linux. To execute a successful spear phishing attack, adhere to the guidelines listed below.

After launching the toolkit, the tester will be presented with all of the options that may be performed in general; chose option 1 to see all of the available attacks that (SET) can launched. See Figure 24.

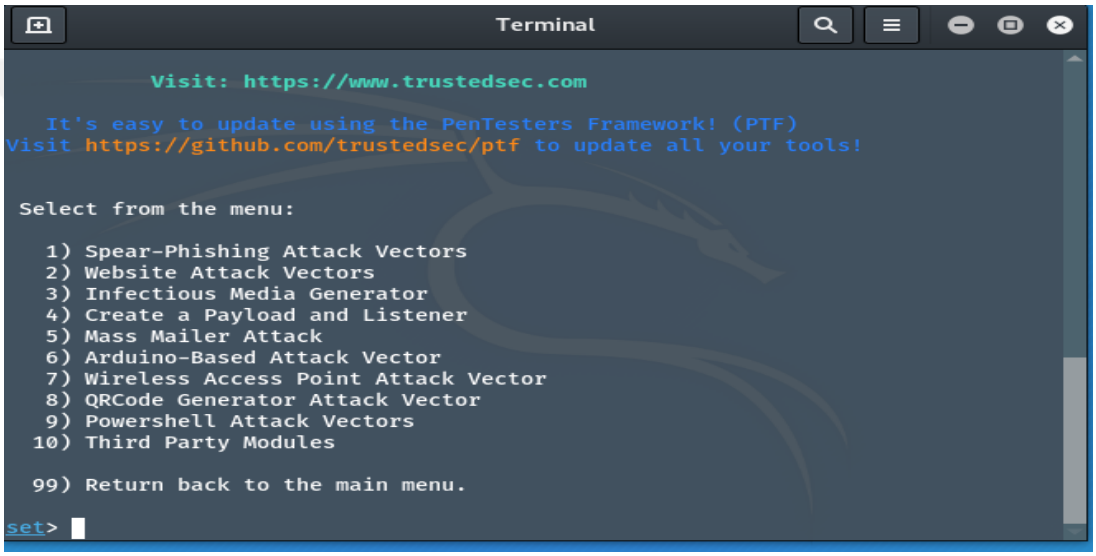


Figure 24. Available Attack Options

Next, we will use option 5, which is a mass mailer attack to send a link or file that has been infected with malware to the target's email ID. It is shown in Figure 25.

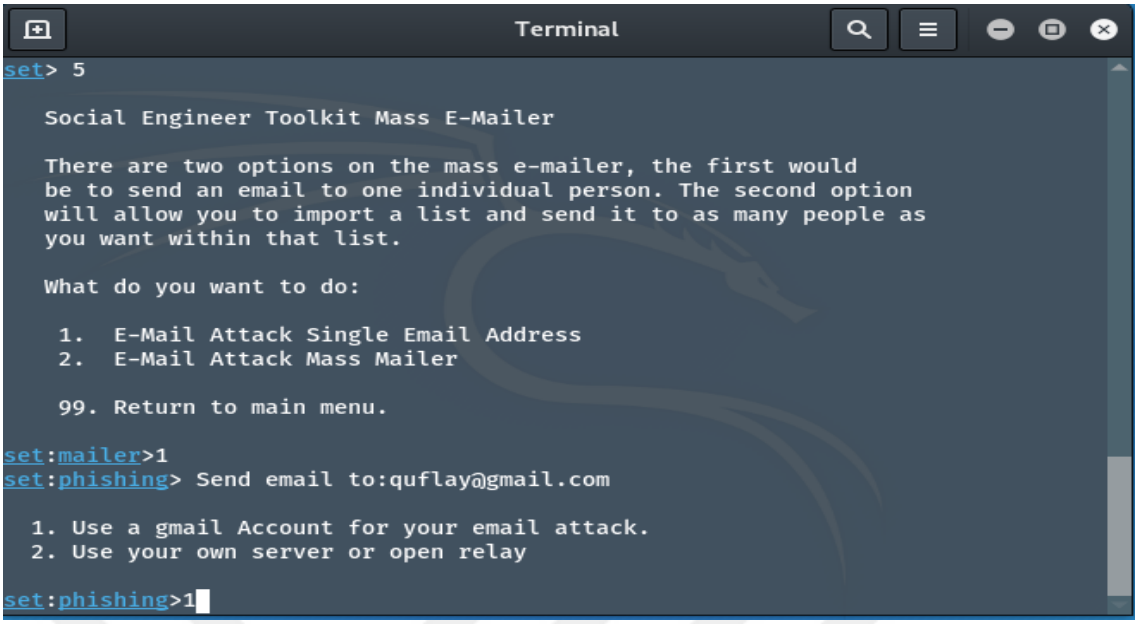


Figure 25. Mass Mailer Attack

Next, we must choose one of two available options. In this example, we will be target a single person; hence, we choose the option "1". Option “2” for multiple targets.

Next, we will enter the victim's email address, and choose the option "1". Then choose option "1" or "2" to specify how the mail form would be sent; we would choose option "1" to utilize Gmail account.

The last step requires the tester to enter the email address, password, as well as all email content details ending with “END” in order to send the email. It is shown in Figure 26.

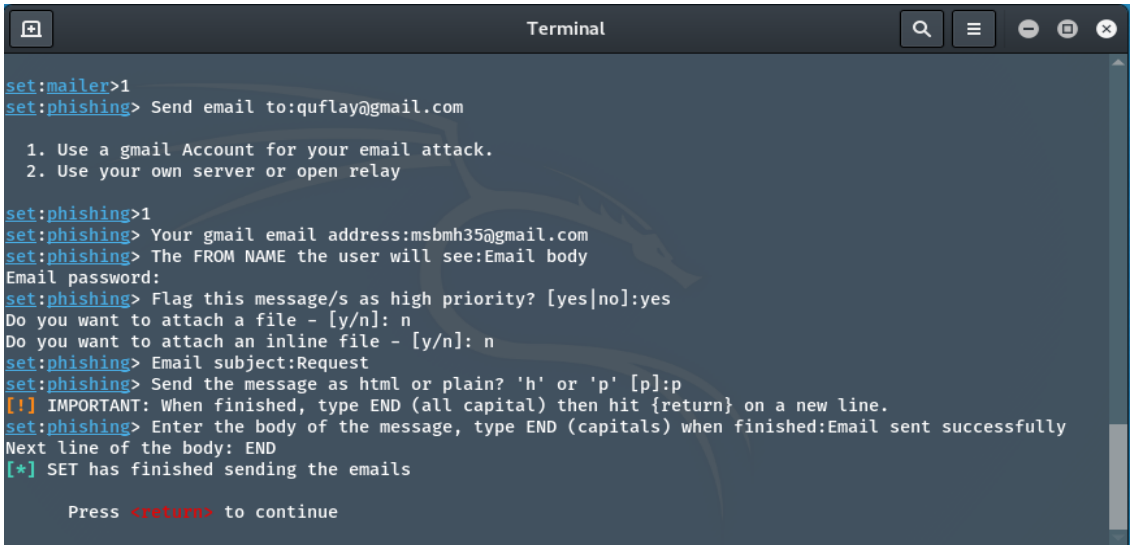


Figure 26. Mass Miler Email Configuration

W3AF: Web application attack and audit framework, popularly known as W3AF, is a commercial web application security scanner and exploitation tool .W3AF attempts to create a framework to assist users in securing their web applications by exploring and exploiting web application vulnerabilities. Both the W3AF core and plugins are written in Python. In addition, the framework's more than 130 plugins make it simple to discover the majority of known vulnerabilities (Ansari, 2015). Figure 27 displayed the graphical user interface.

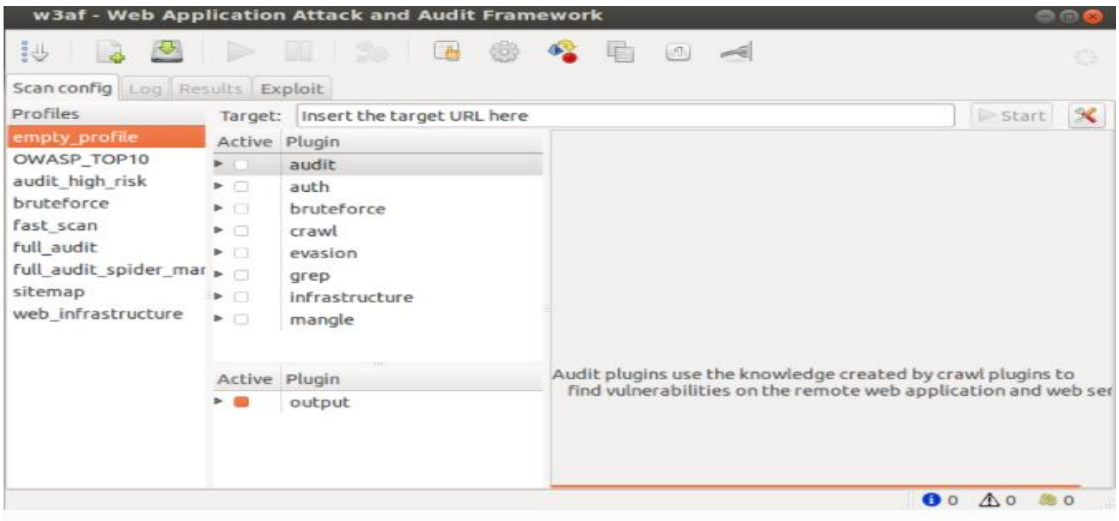


Figure 27. W3AF Graphical User Interface

Burp Suite: Burp Suite is one of the most popular tools for web application penetration testing. It is composed of the following modules as shown in Figure 28 (portswigger, 2022).**Web vulnerability scanner** which detects flaws in advanced web technologies

Proxy; It functions as a web proxy server between the browser and the target apps, allowing the tester to intercept, analyze, and change the raw traffic traveling on both sides.

Repeater; Repeater is a straightforward tool for manually manipulating and reissuing HTTP requests and evaluating the application's response. The tester may make a request to Repeater from any area inside Burp, change them, and return it repeatedly.

Sequencer; This modules for evaluating the randomness of a sample of data objects. It can be used to test an application's session tokens or other significant data items that are meant to be unexpected, such as anti-CSRF tokens, password reset tokens, and password reset tokens.

The Burp Suite is a complicated tool that needs a certain level of user skill. Burp Suite is available in two versions: free with limited functionality and professional with full functionality

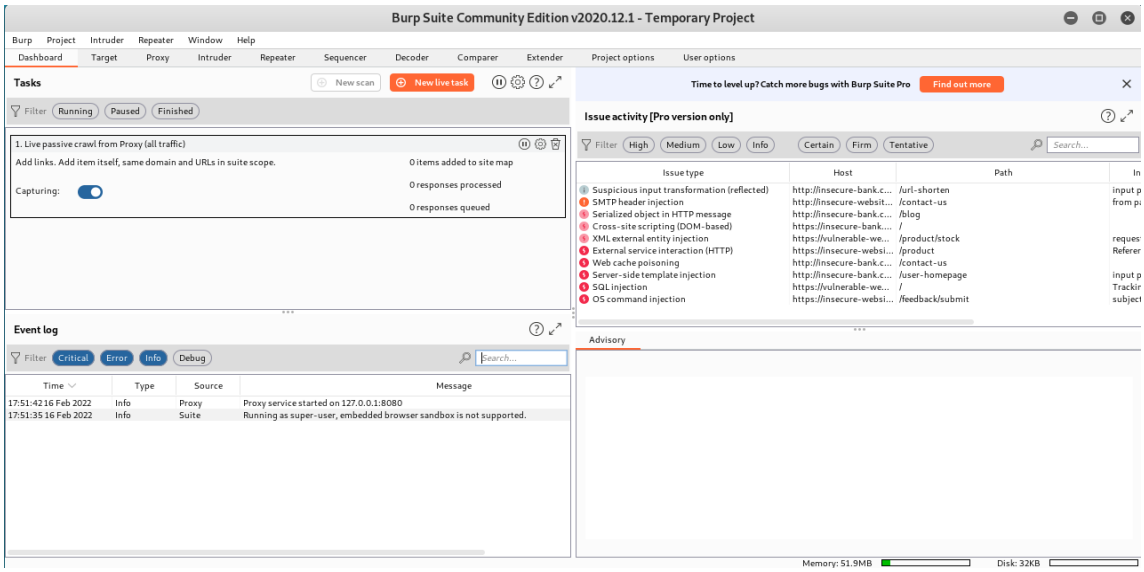


Figure 28. Burp Suite Application

BeEF: The Browser Exploitation Framework is a well-known open-source penetration testing framework that focuses on cross-site scripting (XSS) attacks. Penetration testers can use client-side attack vectors to analyze the security posture of a targeted system with BeEF. BeFF uses one or more web browsers to launch commands and attacks against the system. Moreover, BeEf is working at vulnerabilities in context web browsers (Williams, 2020). BeEF is pre-installed in Kali Linux and other penetration testing operating systems with powerful user interfaces. It is shown in Figure 29.

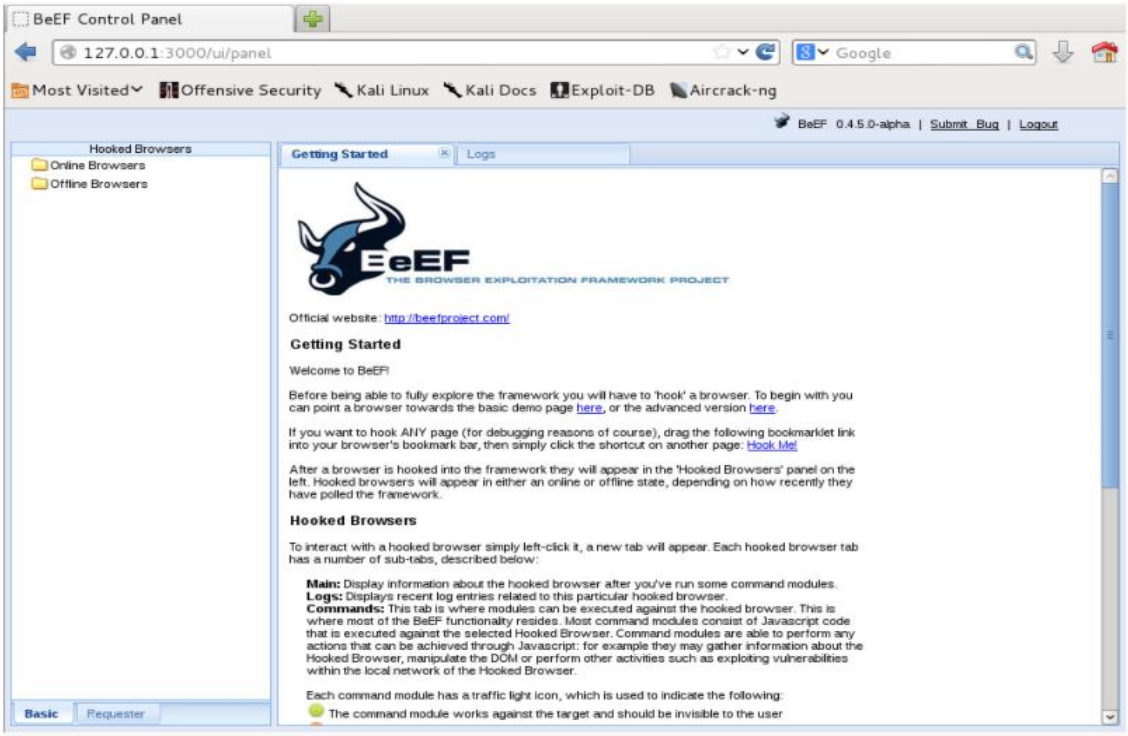


Figure 29. BeFF Application

SQLmap is an open-source penetration testing tool that automates the detection and exploitation of SQL injection vulnerabilities (Damele and Stampar, 2020). It is command-line driven and compatible with all major operating systems. Additionally, all versions of this tool are available for free download. The authors (Charania and Vyas, 2016) explain that an attacker or tester may utilize SQLmap to perform database fingerprinting, execute commands on the operating system, extract database management system, read or delete database, and even access the server's file system.

SQL injection may occur if the url parameter of a website is incorrectly configured, as in http://testphp.vulnweb.com/listproducts.php?**cat=1**. The following demonstrates the SQLmap scanning procedure for the *testphp.vulnweb.com* website, which is designed to practice SQL injection vulnerabilities.

Before running SQLmap, we can manually determine if the website is vulnerable by changing the "GET" parameter to " * ". If we receive an error message, the website is vulnerable. The result is shown in Figure 30.

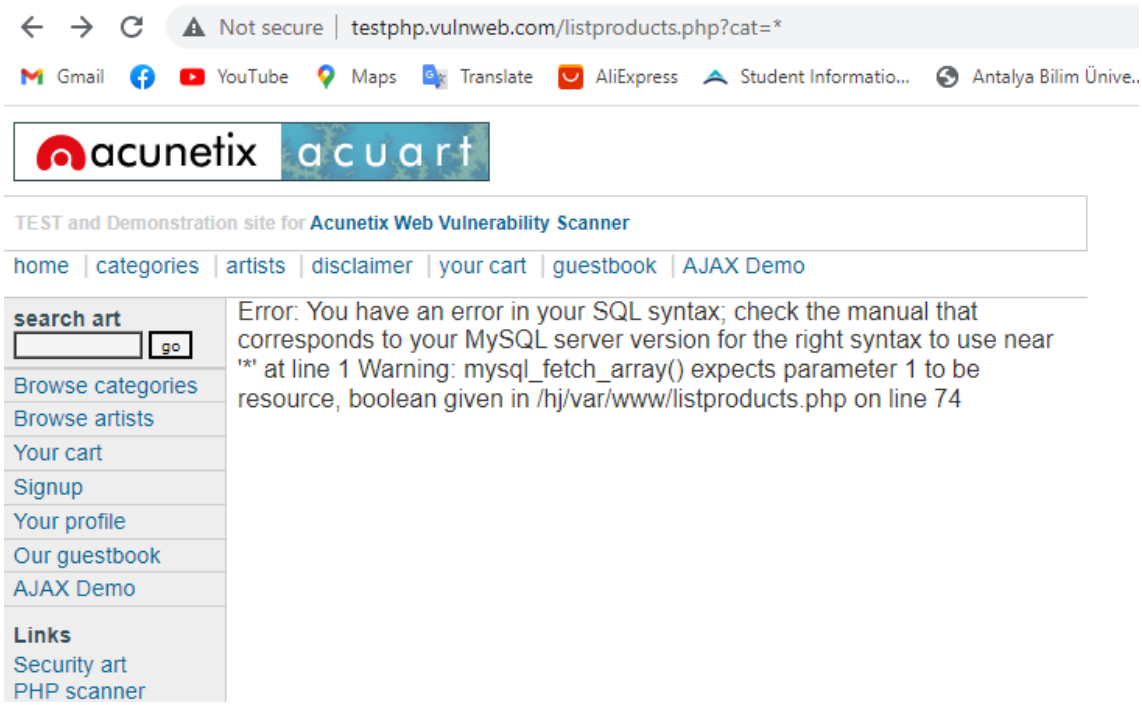


Figure 30. Checking The Website Manually

Now we know the website is vulenebre. Next step is test the connection with the target website using the following command : **SQLmap –u "yourtarget.website.com"**. the result is shown in Figure 31.

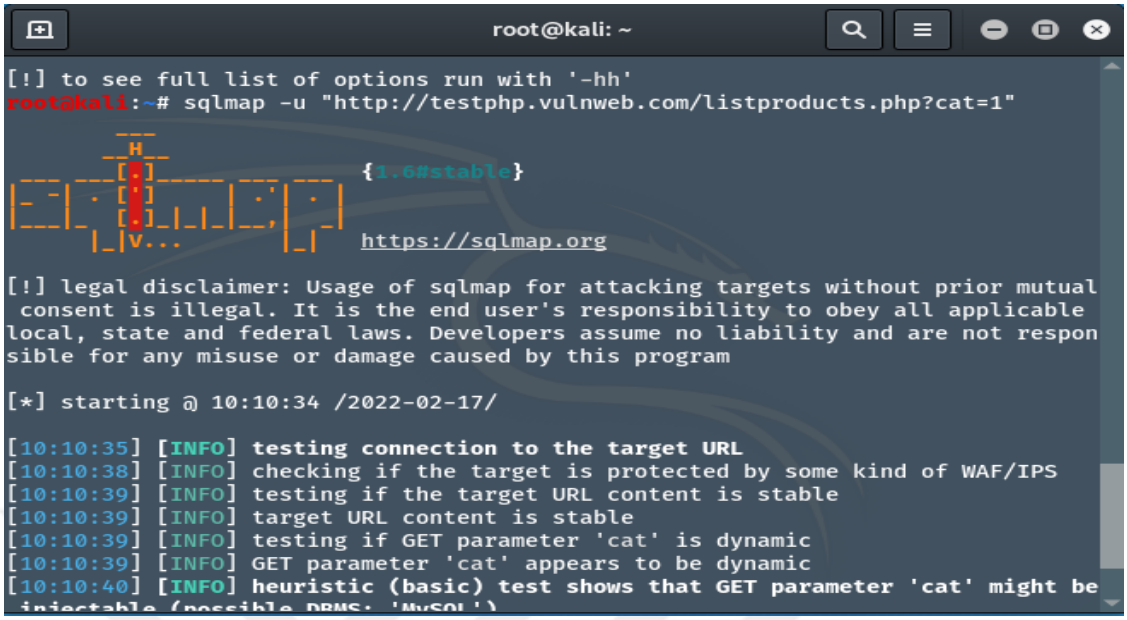


Figure 31. Connect To Target Website

Now generally, we would want to determine if database access is available. Therefore, we use the **–dbs** option. **–dbs** displays a list of all available databases, **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs**. Figure 32

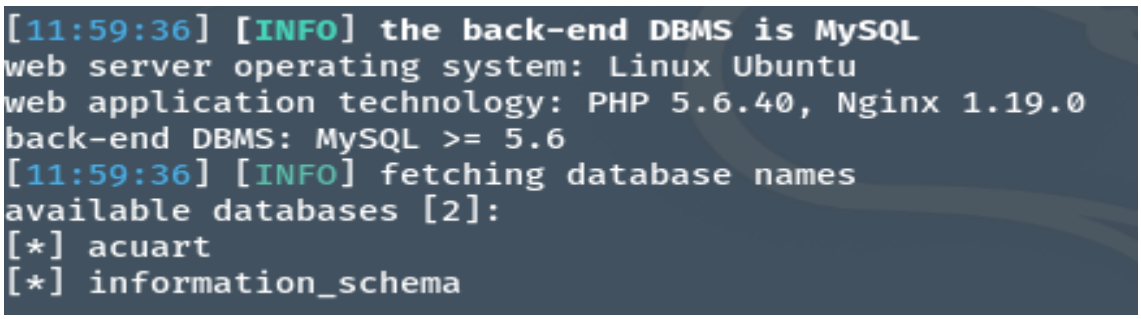


Figure 32. Available Databases

We see there are two databases, acuart and information schema. Now, we use **-D** to indicate the name of the database we need to access, and after we have access to the database, we will check to see whether the tables are accessible. Next, we utilize the **–tables** query option. **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –tables**. Figure 33.

Figure 33. Acuart Tables Database

We can see that eight tables were obtained. Now we are certain that the website is vulnerable. In order to check the columns of a certain table, we can use the command **-T table name –columns** to query the column names. The command will be like: **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists –columns**.Figure 34.

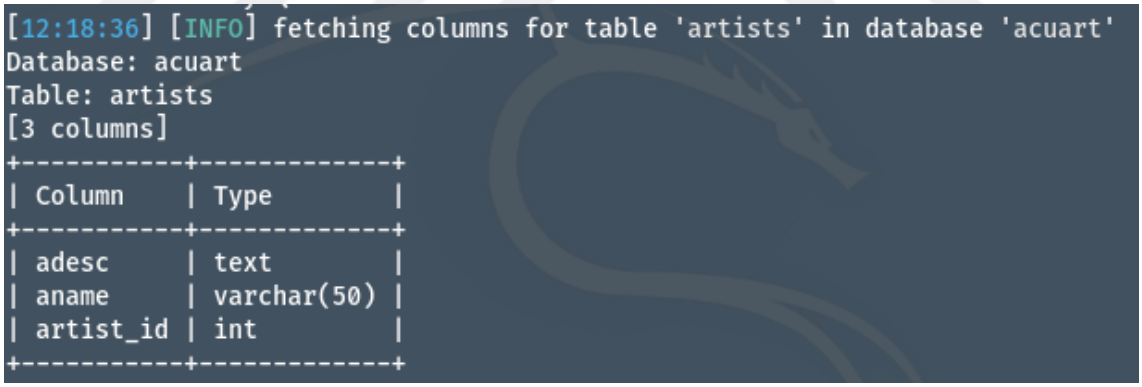


Figure 34. Artists Colums Database

We can obtain the data in a particular column with the following command, where **-C** to select the column and the **–dump** query extracts the data, This can done using the following command, **sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname –dump**. Figure 35.

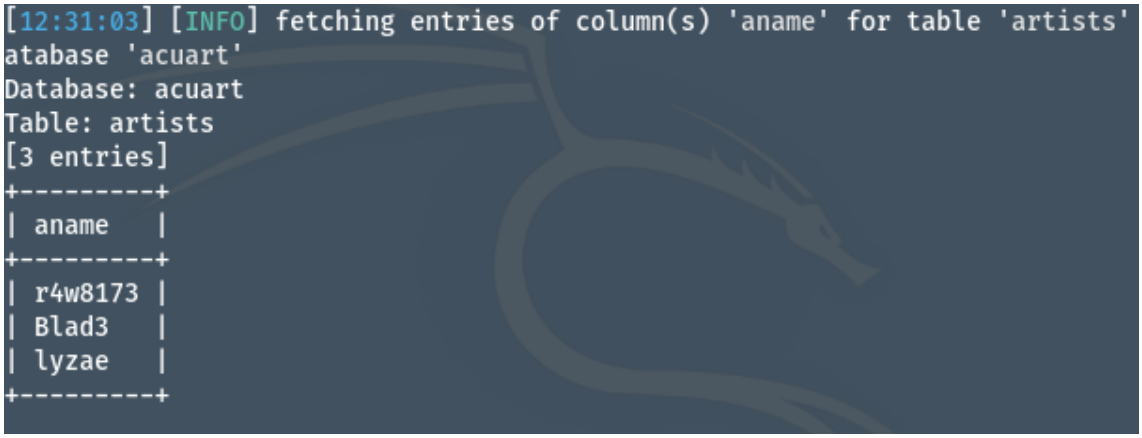


Figure 35. Extract The Information

4. DISCUSSION

In this chapter, we will talk about the results of this work and the advantages, disadvantage of each tool.

The **Metasploit** framework can be utilized by both cybercriminals and security engineers to explore networks and servers for vulnerabilities. Since it is an open-source framework, it is highly adaptable and compatible with the most of operating systems. This framework's advantages are existing vulnerabilities, different workspaces for different projects, and constantly updated exploit databases.

The Metasploit dashboard must be improved enough so C-level executives can understand the issues, export the data, or integrate it with reporting systems, as well as enhancing plugins compatibility and providing options for controlling payloads. Moreover, these disadvantages have made Metasploit a complicated tool that requires deep knowledge.

Nmap is a free and open-source network discovery, mapping, and security auditing tool. The main functionalities are including port scanning, identification of unknown devices, testing for security vulnerabilities, and identification of network issues. This tool is quite useful for rapidly scanning big networks. It uses raw IP packets to detect available hosts and services on the network. The advantages are it is open source, so users can verify how it works, it is comprehensive, with many-advanced networking functions, as well as it is incredibly small and easy to install. Nmap has a significant disadvantage since if users did not restrict the scanning range, a command might take a very long time to complete. Moreover, not all functionalities are available on the Windows version.

Wireshark is a tool for network scanning that analyzes packets sent across a network. It will show every package with its contents. Professionals use it to analyze the network and solve issues if they detect any. Wireshark has several capabilities, one of the most important being the ability to capture packets in a live network. Wireshark enables network users to discover and solve infrastructure issues by checking packets. Disadvantages of using Wireshark is that new users may find Wireshark difficult to use unless they take the time to understand how the program works, since Wireshark cannot transmit packets; it can only capture them.

Aircrack-ng is a well-known network scanner able to display Wi-Fi network traffic and signals. However, the program can also transmit packets and is notorious for encryption key recovery (WEP). A well-known, open-source hacking tool with versions for Windows, Unix, Linux, and MacOS; pre-installed in Kali Linux; and capable of cracking wireless network encryption. Aircrack-ng is outdated technology and a tool developed for skilled specialists, since it only has a command-line system and no graphical user interface. This makes the tool difficult to use and susceptible to defeat by other systems.

Nessus is a remote security-scanning tool that scans a system and sends an alarm if it finds any vulnerabilities that malicious hacker may exploit to obtain access to any linked network. Nessus scans OS systems, network devices, hypervisors, databases, tablets, mobile phones, web servers, and key infrastructure for vulnerabilities, and threats. However, in order to get the full benefits, users must use the professional version.

The Social Engineering Toolkit (SET) is a very effective instrument designed to attack one of the most vulnerable aspects of any information security program such as the users. It is generally simple to contact someone and convince them to visit a website that infects their computer and completely compromises it. The tester might use convincing emails to persuade recipients to click a link. Often, the effectiveness of social engineering depends on plausibility and trustworthiness. The SET makes it quite easy construct effective assaults. In addition to being free, SET offers many tools for phishing campaigns, such as the ability to copy an existing website for landing page and the ability to capture passwords and other information entered on the landing page.

Probably the most significant feature of **Burp Suite** is its ability to intercept HTTP requests and responses, we are able to modify a request and send it back to the server. Most security teams, researchers, and experts use this framework, since it is easy to use. Unfortunately, the community edition is difficult to learn and is missing a lot of functions.

The browser exploit framework (**BeEF**). BeEF exploits browser vulnerabilities to take full control of the victim machine. BeEF offers an Application-programming interface that we may utilize to develop our own web browser attack modules. BeEF can be used to run a malicious website, which the user will visit. The BeEF is used to deliver codes that will be executed on the target computer's web browser.

Web application attack and audit framework **(W3AF)** advantages include discovery of over 200 vulnerabilities in web applications, flexibility of use for learners, and the ability to setup as a MITM proxy.However, The occurrence of false negatives is a disadvantage of this testing tools.

SQL Map is a popular tool. Most security professionals across the world use it to evaluate the security of both web applications and databases that store data. The main goal of using different types of attacks, such as SQL injection, is to gain control of the database instance and SQLMap is one of the greatest tools for this type of attack. The tool provides a quality detection engine with quick and reliable results, automated identification of SQL vulnerabilities, full vulnerability scanning, and command customization for unique outcomes.

In a summary of the top ten penetration testing tools and their purposes, the tester should identify the tools that will be used during the initial phase of the penetration process. The tester must choose the right tool depending on the type of penetration testing and the procedure's stage. For example, the Metasploit framework is compatible with all penetration testing techniques and is integrated with the vast majority of penetration tools. In network penetration testing, the tester may use NMAP for information collection, Wireshark for packet capture and advanced packet analysis, and the Aircrack suite for professional wireless network work. Nessus can determine whether there are any vulnerabilities in the target network and provide reports describing these weaknesses.

A variety of tools, such as W3AF, SQLMap, and Burp Suite, may be used to test web applications. Web application testers, on the other hand, must have advanced programming skills, in-depth knowledge of all known vulnerabilities, and a complete understanding of how web applications behave.

Given the scope constraint of penetration testing, a weakly scoped test cannot meet the goal of PEN testing, even if it passes a compliance requirement. However, some companies with realistic restrictions, such as a limited budget, that force them to limit the scope of the PEN test do not get the full benefits. Consequently, if some or the most of PEN testing processes were automated in the future, requiring little to no human engagement, it would be of great benefit to everyone afflicted by this limitation. Given that this technique requires minimum human involvement, it may also assist PEN testers

overcome their limited skill level. In the future, including Artificial Intelligence and Machine Learning in this automation can significantly enhance the effectiveness of the PEN test.

When doing penetration testing, common starting points or points of attack include firewalls, web servers, RAS access points, and wireless network infrastructure. Firewalls, since of their position as a gateway between an organizational network and the internet, are natural attack target and points of entry for penetration testing. This is because of the function that firewalls play. Web servers have a significant potential for risk owing to many functions they perform and the resulting vulnerabilities in those functions. In addition to "regular" workstations, test should be done on servers that provide services accessible from the outside, such as email, FTP, and DNS.

The aim of "crackers" is to obtain data that has been protected or even to interrupt the processing of data. In contrast to penetration testing, the purpose of IT audits and security audits is to conduct an investigation into the compliance, efficiency, and effectiveness of an IT infrastructure. They are not necessarily intended to identify weaknesses. For instance, a penetration test does not involve determining if certain data could be recovered from a normal backup in the event that particular hardware fails; rather, it just examines whether such data can be accessed. This could also be done during a security or IT audit, but from a different angle and with less technical depth than a penetration test

Before proceeding, it is important to evaluate and assess the huge amount of information that is usually gathered. The evaluation must include the set goals, potential system threats, and an estimate of how much it will cost to look for security problems. The evaluation will always be subjective, for example, because the tester's experience and knowledge play a big role in figuring out how much time and money it will take, the tester's expertise and knowledge have a significant impact in determining how much time and money will be required for the evaluation.

After evaluating the threat, the tester must evaluate the individual cost of a successful attack that exploits the various vulnerabilities and compare it against its likelihood of success. The times listed in the module descriptions can be used to generate a rough timetable for the testing procedures (time required: medium, high, very high).

This comparison should then be used to determine priority. The priority should be higher, the better the possibility of success and the lower the time/cost necessary. The tester should capture both the estimated time/cost and the chosen priorities.

In addition, the report should provide suggestions on how the client can eliminate the vulnerabilities that were discovered during the penetration test. The final report should also include an action plan for removing vulnerabilities based on the client's priorities and the results of the vulnerability assessment. The action plan should include a timetable for the elimination of each key vulnerability and identify the individual or group accountable for its elimination.

The sensitive personal data obtained during penetration testing, such as passwords or private e-mails, should not be included in the final report due to data protection concerns; instead, they should be provided to a designated person, such as the data protection officer. However, the client must be able to clearly trace the test findings, and all information acquired in the various phases must be included in the working papers, or at least as an appendix. This provides complete information on the tools used work steps (which tool was used with which options), log files, and work hours (when attacks were performed).

The tester must uninstall any software, such as keyloggers, a tool that can record and report on a computer user's activity as they interact with a computer during the penetration testing, as well as any other modifications made to the client's IT system, and restore the system to the condition it was in before the testing.

Once the penetration testing process has been compiled, the next step is to deliver advisory and diverse reports to senior management through the reporting process. IT management and IT technical personnel will likely view the entire report or a portion of it. The report contains the following sections: Executive Summary, Technical Details, Evaluation Results, Risk Level Indication Overview, Patch Information Advisory, Budget Information, and Time Estimation. Using this report, penetration testers can show the full process to IT management to get and apply the final solution. After the penetration testing, a mitigation plan is developed.

Kali Linux is the most current version of the Linux operating system to be built by Offensive Security. It was designed specifically for conducting forensic investigations and network security audits. It is a free security auditing operating system and toolkit that includes more than 300 penetration testing and security auditing techniques. It offers an all-in-one solution for IT administrators and security experts to test the efficacy of their security measures by providing a solution that includes both testing and auditing techniques. The improved penetration testing experience that Kali Linux offers makes it more accessible to IT generalists as well as security professionals. Additionally, since it adheres to the standards established by Debian Development, the operating system provides IT administrators with a more comfortable setting.

Kali is a good environment for conducting vulnerability assessments that require minimal configuration. In the Information Gathering, Vulnerability Analysis, and Web Application Analysis categories of the Kali Applications menu, There are a variety of tools for vulnerability assessments. Such as the Kali Linux Tools Listing, the Kali Linux Official Documentation website, and the free Metasploit Unleashed course, offer good tools for utilizing Kali Linux during vulnerability assessments.

Kali Linux can be installed on a variety of computers, including the laptops of penetration testers, servers of system administrators who wish to monitor the network, workstations of investigative investigators. Due to their small size and low power consumption, a great range of ARM devices are also suitable for our needs. Kali Linux may also be installed in the cloud to quickly build a password-cracking farm, as well as on mobile devices and tablets to enable full mobile penetration testing. In addition, penetration testers need servers to utilize collaboration software within a pen-testing team, configure a web server for use in phishing campaigns, and run vulnerability scanning tools, among other things. Once Kali is up and running, We will notice that the main menu is set up for penetration testers and other information security professionals based on the tasks and activities they do.

Since there are so many things that affect the real risk of a discovered vulnerability, predetermined risk ratings from tools should only be used as a starting point to figure out the real risk to the organization.

When examined by a trained professional, a vulnerability assessment can serve as a foundation for later examinations, such as compliance penetration testing. Consequently, it is crucial to understand how to acquire the best possible outcomes from this initial review.

However, because the examples testbed used in this thesis is comparatively simple and straightforward, the research results, including the information gathering of the tools (in the first phase) and attack outcomes (in the second phase), may vary significantly when conducted on a more complex system. To give the community more accurate and reliable sources of information, similar research should be done on fully operational systems with multiple protection mechanisms or real scenarios, such as firewalls, intrusion detection systems, and security rules.we used simple examples since our target audience is not experts and requires advanced skill.

Perhaps it is the increase in the number of costly data breaches or the ever-expanding attacks and proliferation of sensitive data, as well as the attempt to secure them with increasingly complex security technology, which organizations lack the in-house competence to manage successfully. Therefore, organizations demand the expertise of a penetration tester.

It would be fascinating to observe the development of artificial intelligence in penetration testing as a means to eliminate any deficiencies.

The future of penetration testing depends on the use of AI to produce more accurate and efficient evaluations. However, it is also essential to recognize that pen testers must eventually use their experience and expertise to determine the optimal way to conduct the examination.

In order to test the vulnerabilities of information technology (IT) and security systems, penetration testers must have penetration testing skills and have a good understanding of information technology (IT) and security systems.

Enrolling in a specialized course or training program is one of the best ways to begin acquiring the abilities that are needed as a penetration tester. With the systems described in this thesis, it is possible to acquire several skills in a more structured environment.

Consider enrolling in the IBM Cybersecurity Analyst Professional Certificate, which includes a complete unit on penetration testing and incident response, whether you are new to cybersecurity. You may obtain job-ready skills while managing other commitments since the complete program is available online.

For the foreseeable future, there will be a significant and accelerating demand for information security personnel. In fact, there is a major lack of infosec specialists across all disciplines, and it is anticipated that the deficit will endure for the foreseeable future. As networks, applications, and information requirements continue to grow in complexity and importance to corporate and government operations, these systems become more directly targeted and vulnerable. Pen testers are at the vanguard of technological skill, assuming the role of would-be attackers as nearly as possible. There are no indications that this perception will change in the foreseeable future.

Methodologies for penetration testing should be flexible enough to take into account how different organizations work and what they need. Moreover, it should also have a strong base that covers all the important areas and parts. By using penetration techniques, the tester will go through and make sure to do a thorough penetration test and protect IT infrastructure.

5. CONCLUSION

In this thesis, we have covered penetration tests; criteria to consider when running penetration tests; the process of conducting a penetration test; and commonly used tools and software for conducting penetration tests. The procedure becomes effective if steps are taken to address the identified vulnerabilities. The management of risk and vulnerabilities concludes with the organizational process and individual morality. Consequently, we have also discussed in this thesis the function of the professional ethical and technical competence essential for executing the penetration test. Given that each phase of penetration testing is conducted with suitable tools, the most significant component of a tool is its dependability.

Technically, penetration testing is one of the most used approaches for evaluating security. Penetration testing may properly assess the effectiveness of the security measures installed on the tested system. With several community and commercially accessible supporting tools, it is very challenging for practitioners to make effective decisions when looking for relevant tools.

6. BIBLIOGRAPHY

6.1 Books

Kaufmann, M. (2017). Penetration testing. In R. Zabicki, R. Scott, and R. Ellis, Computer and Information Security Handbook (pp. 1031-1038).

Ansari, A. J. (2015). Web penetration testing with Kali Linux. Packt Publishing Ltd.

Baloch, R. (2017). Ethical hacking and penetration testing guide. Auerbach Publications.

Orebaugh, A. and Pinkard, B. (2011). Nmap in the enterprise: your guide to network scanning. Elsevier.

Osborne, M. (2006). How to cheat at managing information security. Elsevier.

Pieters, W. and Dimkov, T. (2011). Physical Penetration Testing: A Whole New Story in Penetration Testing. Centre for Telematics and Information Technology (CTIT).

Rahalkar , S. (2019). Introduction to NMAP. In A. Berkeley, Quick Start Guide to Penetration Testing.

Rahalkar, S. (2017). Metasploit for Beginners. Packt Publishing Ltd.

Weissman, C. (1995). Handbook for the computer security certification of trusted systems.

Wang, Y. and Yang, J. (2017). Ethical hacking and network defense: choose your best network vulnerability scanning tool. In 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), (pp. 110-113).

Al Shebli, H. M. (2018). A study on penetration testing process and tools. 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 1-7.

Sandhya, S., Purkayastha, S., Joshua, E. and Akash, D. (2017). Assessment of website security by penetration testing using Wireshark. In 2017 4th International Conference on Advanced Computing and Communication Systems, (pp. 1-4).

Stefinko, Y., Piskozub, A. and Banakh, R. (2016). Manual and automated penetration testing. Benefits and drawbacks. Modern tendency. 13th international conference on modern problems of radio engineering, telecommunications and computer science (TCSET) (pp. 488-491). IEEE.

Arta, H., Era, M. and Muhadri, F. (2021, 08 20). Ethical Hacking Whitepaper. Retrieved from pecb.com: https://pecb.com/whitepaper/ethical-hacking-whitepaper.

Automatic SQL injection and database takeover tool. (n.d.). Retrieved from sqlmap: https://sqlmap.org.

Balaji, N. (2021, 04 18). Top 10 Best Free Penetration Testing Tools 2022. Retrieved from cybersecuritynews.com: https://cybersecuritynews.com/penetration-testing-tools

bulletproof penetration testing white paper. (2021). Retrieved from bulletproof: https://www.bulletproof.co.uk/white-papers/pen-test.

Damele , B. and Stampar, M. (2020). Automatic SQL injection and database takeover tool. Retrieved from sqlmap: https://sqlmap.org.

LIFARS Penetration Testing Whitepaper. (2017, 08 01). Retrieved from lifars.com: https://lifars.com/knowledge-center/penetration-testing-whitepaper/

portswigger. (2022). Burp Suite documentation: desktop editions. Retrieved from portswigger.net: https://portswigger.net/burp/documentation/desktop

Sabih, Z. (2021). Learn Ethical Hacking From Scratch.

Timalsina, U. and Gurung, K. (2015). Metasploit Framework with Kali Linux.

Williams, J. (2020). Introducing BeEF. Retrieved from Github: https://github.com/beefproject/beef/wiki/Introducing-BeEF.

6.2 Articls

Bacudio, A. G., Yuan, X., Chu, B.T. B. and Jones, M. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications, 3(6), 9.

Ami, P.and Hasan, A. (2012). Seven phrase penetration testing model. International Journal of Computer Applications, 59(5), 16-20.

Bishop, M. (2007). About penetration testing. IEEE Security & Privacy, 5(6), 84-87.

Charania, S. and Vyas, V. (2016). SQL Injection Attack: Detection and Prevention. IRJET Journal, 2395-56.

Doshi, J. and Trivedi, B. (2015). Comparison of vulnerability assessment and penetration testing. International Journal of Applied Information Systems, 8(6), 51-54.

Čisar, P. and Čisar, S. M. (2018). Ethical hacking of wireless networks in kali linux environment. International Journal of Engineering, 16(3), 181-186.

Kumar, V. S. (2014). Ethical Hacking and Penetration Testing Strategies. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11(2), 976-1353.

Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A. and Shrawne, S. (2012). Vulnerabilities of Wireless Security protocols. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(2), 34-38.

McRee, R. (2006). Security analysis with Wireshark. ISSA Journal, 39-45.

Salahdine, F. and Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internet, 11(4), 89.

Shivayogimath, C. N. (2014). An overview of network penetration testing. International Journal of Research in Engineering and Technology, 3(7), 5.

Muñoz, F. R., Armas Vega, E. A. and Villalba, L. J. G. (2018). Analyzing the traffic of penetration testing tools with an IDS. The Journal of Supercomputing, 74(12), 6454–6469.

offensive-security. (2009). WORKING WITH NEXPOSE. Retrieved from offensive security.https://www.offensive-security.com/metasploit-unleashed/working-with-nexpose.

rapid7. (2016). Remediation Reporting. Retrieved 06 20, 2022, from rapid7: https://www.rapid7.com/products/nexpose/features.