A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle

Fouz Barman, Nora Alkaabi, Hamda Almenhali, Mahra Alshedi and Richard Ikuesan

Computing and Applied Technology Department, College of Technological Innovation, Zayed University, Abu Dhabi, United Arab Emirates

fouz.barman@hotmail.com
Noraalkaabi2001@gmail.com
Hamdaalmenhali@hotmail.com
mahralshedi2019@gmail.com
richard.ikuesan@zu.ac.ae

Abstract: Reconnaissance and enumeration are both equally significant phases of the penetration testing lifecycle. In hindsight, both reconnaissance and enumeration seem to be very similar as the pair involve information gathering. Whilst reconnaissance leverages passive approaches without direct interaction with the target, enumeration exploits susceptibilities and vulnerabilities in direct client-server communication. Both phases involve gathering information and pinpointing the attack surface within the network of the target. To do so, powerful tools such as Nmap and Netcat are utilized by ethical hackers and penetration testers to identify and resolve security vulnerabilities and weaknesses. Nmap is an open-source command-line tool used for information gathering, network discovery, and security auditing. Whereas Netcat is a back-end tool that manages networks, monitors traffic flow between systems, as well as allows port scanning and listening. However, the plethora of tools and approaches available for these two phases often introduce inconsistencies and time wastage, which can lead to frustration and poor outcome for inexperienced penetration testers. Additionally, not all commands found online are relevant and applicable. In such situations, there is a high probability that the user will feel overwhelmed and exasperated with the overflow of new and foreign information. To address this daunting challenge, this study developed a methodical framework that can provide a technical guide for the reconnaissance and enumeration phases of the penetration testing lifecycle. Furthermore, a clear and thorough step-by-step procedure and detailed explanations of each stage and commands initiated using Nmap and Netcat are provided. The output of this study will be extremely beneficial and informative to a vast group of audience, ranging from university students majoring in security to individuals interested in ethical hacking, and even someone looking for a job with a position of a penetration tester. Furthermore, this technical guide on Nmap and Netcat extends the common body of knowledge in penetration, as a bridge between the industry and academia.

Keywords: Penetration testing, Penetration testing framework, reconnaissance, enumeration, ethical hacking, Nmap, and Netcat.

1. Introduction

Ethical hacking, also known as white hat hacking, is the utilization of hacking techniques to identify vulnerabilities in computer systems, networks, and web applications to improve security. This proactive approach helps to identify and fix security weaknesses before they can be exploited by malicious actors. Furthermore, ethical hacking includes penetration testing, simulating an attack on a computer system, network, or web application to identify vulnerabilities and assess the effectiveness of security measures. Ethical hackers use the same tools, techniques, and tactics as malicious hackers, however, with the permission of the system or network owner and the intention of making the system or network more secure (Kebande, Karie, and Ikuesan 2020). Historically, ethical hacking can be traced back to the 1970s when the US government began to employ hackers to test the security of their systems. This practice was formalized in the 1980s with the creation of the US Air Force's Computer Emergency Response Team (CERT). As the internet became more widely used in the 1990s, private companies also began to hire ethical hackers to test their systems. Today, many professional organizations and certifications specialize in ethical hacking, such as the offensive security certified professional, International Association of Computer Science and Information Technology (IACSIT) and the Certified Ethical Hacker (CEH) certification, SANS GIAC web application penetration testing, as well as other non-prominent organizations. A summary of organizations that provide certifications to ethical hacking, penetration testing as well as other forms of offensive proactive security is further highlighted in word-cloud depicted in Figure 1.

Figure 1: Information Security Certification Word Cloud

Cybersecurity can be defined in many ways, however, it is always defined as the organization and gathering of resources, processes, and structures used to defend cyberspace and cyberspace-enabled systems from occurrences are known as cybersecurity (Craigen, Diakun-Thibault, and Purse 2014). Controlling access to data on the systems became a major point of worry when these time-sharing systems arose in the mid to late 1960s and many more jobs were using the web. Furthermore, the cybersecurity scan started in the 1970s after the researcher Bob Thomas designed and produced a computer program named Creeper that can move in the ARPANET's network. Moreover, the inventor of the email Ray Tomlinson designed a program named Reaper that is designed to capture and delete Creepers. The Reaper is one of the first antivirus malware-scanning software that is self-replicating. In the year 1987, the commercial antivirus software where Kai Figgie Andreas Luning released their antivirus (GeeksforGeeks 2022). Moving on to the early 2000s, criminal groups began to heavily fund professional cyberattacks, while governments started to crack down on the criminality of hacking, handing out large sums of money to responsible hackers. Information security continues to progress as the internet increases, but so do viruses (GeeksforGeeks 2022). Cyberattacks have been increasing during the past years which ensures that organizations and individuals must include mechanisms and defense systems to reduce their risk of them. The defense mechanism used can be multi-factor authentication to avoid malicious actors accessing the user account. In addition, creating long complex passwords and changing them regularly to avoid password attacks. Moreover, malware scanners are low-cost tools to scan devices for vulnerabilities in the devices. Additionally, using a VPN-capable firewall which is hardware to encrypt all communication between the device to reduce the risk of brute force attacks can also work as a filter to block access to malicious websites. Moving on to cyberattacks, the topmost common attacks are DoS Denial of Service, Phishing, SQL injection, Ransomware, and XSS Cross-Site scripting. DoS attacks are attacks that overwhelm a target to stop it from functioning. Phishing attacks are attacks that visually look like they are from a trusted party, however, it includes malicious code in them. SQL injection attacks are attacks that target websites that use a database to service their clients. SQL injection is when an attacker injects malicious code into the user input to gain access or modify code. Ransomware attacks are attacks where the victim's system is held captive by ransomware until they agree to pay the attacker a ransom. After receiving payment, the attacker instructs the target on how to retake control of their computer. The target of a ransomware attack is to download ransomware from a website or an email attachment. The malware is designed to take advantage of flaws that have not been addressed by either the system's vendor or the IT staff (A. Singh, Ikuesan, and Venter 2019). After that, the ransomware encrypts the target's computer. Ransomware can often be used to target several parties by limiting access to many machines or a central server critical to corporate operations. Cross-Site Scripting attacks XSS is when the attacker creates malicious scripts and transmits them into clickable content that is sent to a target victim browser. Once the victim clicks on the content, the malicious script will run on the victim's device.

2. Background

Penetration testing and ethical hacking are essential in the information security lifecycle for several reasons. Firstly, it helps to identify vulnerabilities in systems and networks before they can be exploited by malicious hackers. By identifying and addressing these vulnerabilities, organizations can prevent cyber-attacks and protect sensitive information, such as financial data and personal information. Secondly, ethical hacking is also important for compliance, as many industries are subject to regulations that require regular security testing. Thirdly, it also helps organizations to improve their overall security posture and stay ahead of the ever-evolving threat landscape. Furthermore, ethical hacking has been widely adopted by organizations as a key security strategy. In today's digital age, organizations are constantly at risk of cyber-attacks, and they must have the necessary security measures in place to protect their networks and data. Organizations that conduct regular ethical hacking and penetration testing are better prepared to detect and respond to cyber threats and are less likely to suffer data breaches and other security incidents. Fundamentally, the ethical hacking lifecycle contains five phases which are reconnaissance, enumeration, exploitation, post-exploitation, and clearing of tracks. The first two phases often play a critical success factor in any hacking exercise. However, this is often fraught with inconsistencies and subjective processes.

Given that some ethical hackers often lack formal training, experience, and understanding, ethical hacking has been susceptible to a diverse range of problems. The first problem relates to accessibility. Typically, ethical hackers need both physical and logical access to the target organization to conduct an assessment. In essence, the ability of ethical hackers to carry out their tried-and-true assaults depends on the access rights and privileges provided by the organization. This could be within the black, white, or grey box principle. The ability to effectively manage the first two phases of the hacking lifecycle is quintessential to the success of the process, especially with the least privileges (Yaacoub et al. 2021). Secondly, the problems regarding security and privacy must be taken thoughtfully, since organizations can be under simulated attacks, and their data, information, system privacy, integrity, and confidentiality are being targeted as well. Consequently, ethical hackers are severely required to explain, demonstrate, and document each phase performed. To provide a reliable baseline for developing trust and ensuring compliance, this study developed a conceptually practicable framework for the management of the first two phases of the ethical hacking cycle. The proposed framework is presented in the next section.

3. Proposed Framework

As a step towards enhancing the penetration testing process, this study presents a process model that can be used to reduce the daunting and confusing process of the first two stages in the penetration cycle. This is further illustrated in Figure 2. The process model details the process of managing the reconnaissance (reconn) and the enumeration (enum) phases in an agnostic alignment. The proposed management framework entails the process of ensuring ethical compliance during the reconnaissance and enumeration phases. Given that most ethical hacking process leverage diverse open-source tools and intelligence, the proposed framework further specify the potential platforms such as the use of Parrot OS and Kali Linux as the hacking platform. Within this platform, several off-the-shelf tools and open-source tools exist while others can be installed. To align with the principle of ethics, and the need for transparency in the process, the proposed framework integrates documentation and justification into every aspect of both phases. This includes the core process of curating the attack surface on the target based on the extensive use of the hacking platform. An implementation of this proposed framework is presented in the subsequent sections. Firstly, the methodology employed is discussed and then followed by the result obtained.

4. Methodology

This section of the report covers the methodology and steps undertaken to ensure a successful ethical hacking exercise. Additionally, this study highlights the two most important phases of the entire process, the reconnaissance and enumeration phases. To implement this process, kali-linux 2022.4-amd64 [1]was installed on a core i7 12GB RAM Windows 10 computing running using the virtual box as the virtualization technology. The default configuration for the Kali Linux platform with username and password as ‘kali’ was used. Furthermore, the victim machine was downloaded from Vulhub[2] open-source vulnerable machine repository. To demonstrate the documentation process, each step followed was carefully recorded using a combination of notes, and saved output (example, nmap –sP 192.168.170.0/24 >>output.txt). A synopsis of some common commands and their corresponding interpretation is further presented in Tables 1 and 2 for Nmap and Netcat respectively.

[1] https://www.kali.org/get-kali/#kali-virtual-machines

[2] https://www.vulnhub.com/entry/napping-101,752/

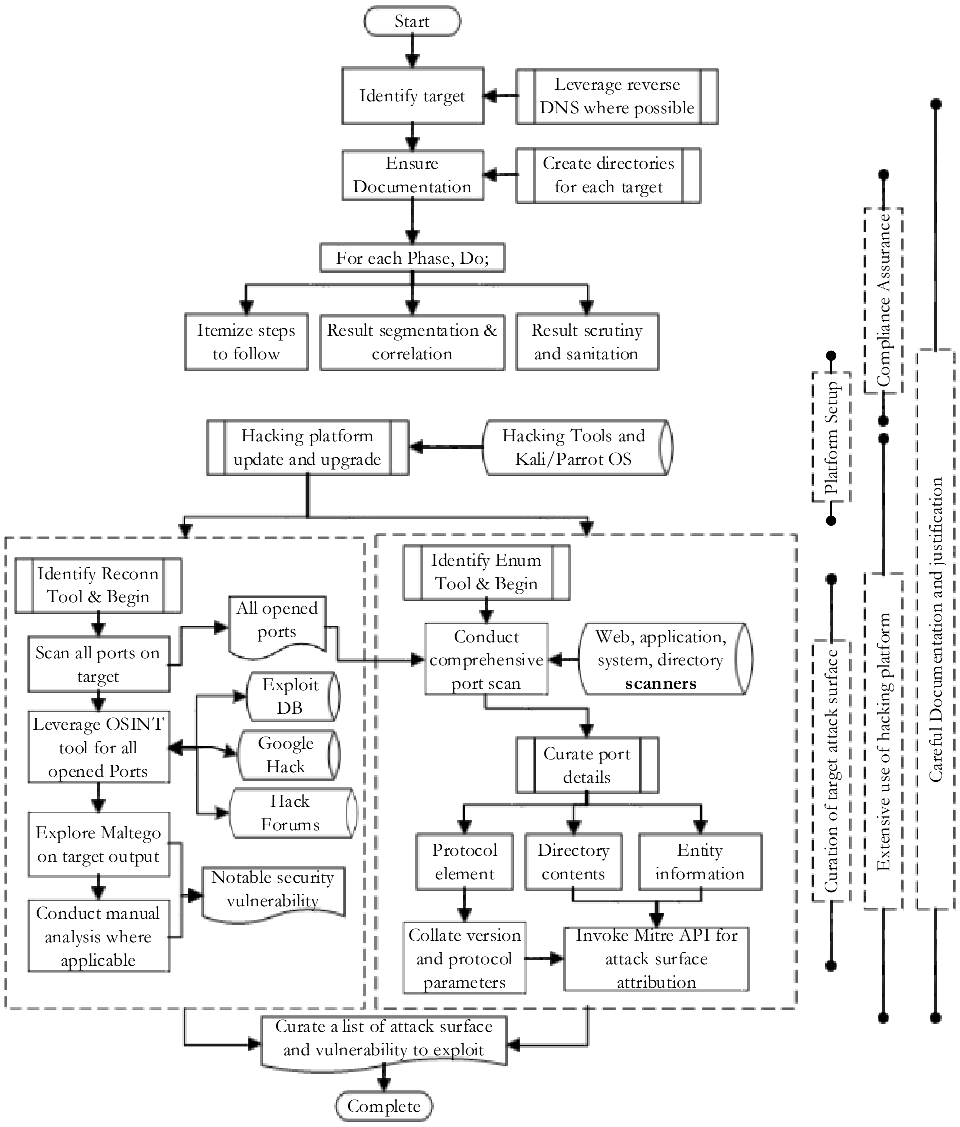
Start
Identify target
Leverage reverse DNS where possible
Ensure Documentation
Create directories for each target
For each Phase, Do;
Itemize steps to follow
Result segmentation & correlation
Result scrutiny and sanitation
Hacking platform update and upgrade
Hacking Tools and Kali/Parrot OS
Identify Reconn Tool & Begin
Scan all ports on target
All opened ports
Exploit DB
Leverage OSINT tool for all opened Ports
Google Hack
Hack Forums
Explore Maltego on target output
Notable security vulnerability
Conduct manual analysis where applicable
Identify Enum Tool & Begin
Conduct comprehensive port scan
Web, application, system, directory scanners
Curate port details
Protocol element
Directory contents
Entity information
Collate version and protocol parameters
Invoke Mitre API for attack surface attribution
Curate a list of attack surface and vulnerability to exploit
Complete
Platform Setup
Compliance Assurance
Curation of target attack surface
Extensive use of hacking platform
Careful Documentation and justification

Figure 2: Proposed Reconn and Enum management framework

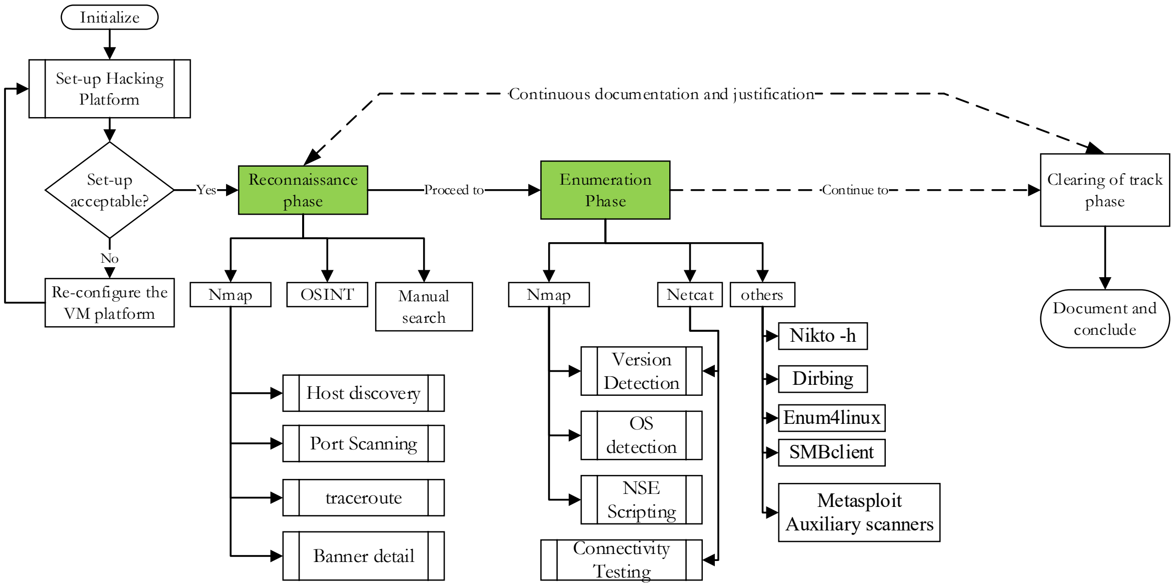

Figure 3: Operational framework for the experimentation process

5. Table 1: Reconnaissance Tools (Nmap)

USAGE	DEPLOYMENT	SUMMARY
Scanning IP Addresses: Command: nmap "ip address"	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	Scans every port on the computer with this IP address.
vulnerability scanning: scripts are in "/usr/share/nmap/scripts" then command: nmap –script= "chosen script" "target"	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	An open-source tool for security auditing and related network discovery. It can be used to identify the current running devices on the systems, hosts, and services available.
Scan multiple targets: Nmap t1,t2,t3..	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	One scan can be done including multiple targets ips at once.
Scan range of hosts: Nmap "range of ip addresses" Nmap 132.123.5.3-20	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	We can scan whole subnets, partial subnets, or file list targets. Nmap can generate possible new targets.
Performing fast scan: nmap -F "target"	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	-F will scan open services, domain names, and ports fast and quickly.
Scan specific ports or entire port ranges: Nmap -p x-xxx localhost Scan specific ports: Nmap -p x,xx x.x.x.x	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	Specifying port can filter the machine running a service on this specific port,
Scan hosts and IP addresses reading from a text file: Nmap -iL xx.txt	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	The "-iL" parameter lets you read from that file, and scan all those hosts for you:
Scan using TCP or UDP protocols: nmap -sT x.x.x.x nmap -sU localhost	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	Sending a UDP packet to each specified port is how the UDP scan operates. Most ports will have an empty packet.
Fragment packets. nmap -f <target IP address> -f split the ip address into tile fragment packets.	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	sending a probe to a network while fragmenting it into numerous smaller packets
Remote Networks:	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	Nmap also displays data about distant networks. In reality, you may use Nmap to analyze a website that you wish to look at, and it will parse the website and find the IP address for that web domain.
If host is vulnerable to DOS: Nmap –script dos -Pn x.x.x.x.	Linux, Windows, MAC OS X, BSD, Solaris and AmigaOS.	A script "NSE" is used to determine if the targeted host is vulnerable to DOS or not.

6. Table 2: Enumeration Tools (Netcat)

USAGE	DEPLOYMENT	SUMMARY
Port scanning: Nc -v -n x.x.x.x x-x	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	*To discover open doors and weaknesses in a network. The -v gives us a lengthier result.*
nc -lp port {host} {port}	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	Listen for incoming connections
Create a tunnel from one local port to another: nc – xxx | nc x.x.x.x x	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	*Using encrypted tunnels within the SSH protocol, tunneling is a method of port redirection. Using an SSH connection, two network devices can communicate by tunneling.*
Encrypt data before transferring over the network: openssl enc -des3 -pass pass:password | nc x.x.x.x x	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	sensitive data that is to be uploaded to the cloud should be encrypted on-premises, before upload.

USAGE	DEPLOYMENT	SUMMARY
TCP server mode: -l Nc -l -p x	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	Listens for network connections and establishes network connections.
-k Nc -k -l xx	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	Listen to the port & IP address after the connection closes
Displaying the IP routing table: Netstat -r	*Pre-installed in Linux and MAC OS. Need to be installed in Windows.*	*The -r displays the IP routing table. -s shows the protocol statistics for the UDP, TCP, SCTP, ICMP, and IP protocols.*

7. Result

Following the operational framework presented in Figure 3, this study explored the application of the proposed framework for an enhanced hacking experience. The testing was carried out on the identified target. A synopsis of the outcome is presented in this section.

a. The Reconnaisance Phase:

The reconnaissance phase is the initial and longest step of a hacking attack. This phase is essentially the preparatory phase in which useful details about a target are gathered; information such as their network, their open and active hosts, and the people involved. It is imperative to note that there are two types of reconnaissance: Active: **Directly** interacting with the target to collect information (Nmap), and Passive: Collecting and gathering information from the target **indirectly**. Common off-the-shelf tools include Nmap and Netcat (the Swiss army knife for network communication). A description of the respective terms used in this phase is provided in Tables 3 and 4. Whilst Table 3 addresses Nmap, Table 4 provides further clarity for Netcat.

7.1.1 Table 3: Description of Nmap Usage

Usage Perspective	Description
Host Discovery + Status	The main objective is to scan and discover which hosts are active and are worth conducting a deeper investigation.
Port Scanning	This forms one of the core operations of the Nmap tool. An attacker can send probes (both normal and carefully crafted probes) to determine if ports are open, closed, or filtered.
Version Detection	If a port is open, Nmap helps determine what version each software/application is running.
OS Detection	Allows attackers to determine and pinpoint the running OS which is extremely helpful as different OSs implement different network standards.
Traceroute	Aids in the finding of network routes
NSE Script Scan	Performs the tasks of detecting service vulnerabilities, gathering a greater amount of information, advanced version detections, as well as malware discovery.

7.1.2 Table 4: Description of Netcat usage

Usage Perspective	Description
Test Connectivity	Allows attacker to gain a shell or reverse connection to the target machine. Additionally, it helps establish numerous connections or backdoors simultaneously.
Port Scanning	Determines the range of ports as well as what ports are up and active.
Version Detection	Helps determine target information such as their running service version.
Banner Details Detection	Hunts down the target's banner details that can be used to exploit vulnerabilities.

Search Exploits	Websites and databases like “Exploit Database” allow attackers to search through any exploit for the specific versions they are looking for.

b. The Enermeration Phase:

The enumeration phase is the second phase of a hacking attack. This phase is extremely critical as it allows attackers to create active connections to the target to perform directed queries to gain additional information. In other words, it allows them to use the information to further enumerate the target to discover their vulnerabilities and weaknesses. Like the reconnaissance phase, the enumeration phase uses tools such as Nmap and Netcat. It is imperative to mention that the enumeration phase follows the same steps as the reconnaissance however, Nmap can be used for various enumeration techniques such as:

1. Nmap for NetBIOS Enumeration: This stands for Network Basic Input/Output System which essentially allows a connection and communication like sharing files to occur over a LAN.
2. Nmap for SNMP Enumeration: This stands for Simple Network Management Protocol in which Nmap gives attackers the ability to use scripts to enumerate and exploit targets.
3. Nmap for LDAP Enumeration: This stands for Lightweight Directory Access Protocol which is used to access directory listings.
4. Nmap for NTP Enumeration: This stands for Network Time Protocol, which is an enumeration process where attackers can pinpoint NTP servers on a network that can be used to implement further enumeration.

The typical output of the enumeration phase includes SNMP data, network shares, IP address table details, a list of password policies, as well as usernames on different systems. For completeness, the other phases of the hacking lifecycle are briefly explained.

c. *The Gaining Access Phase:* In this phase of a hacking attack, an attacker is granted the opportunity to initiate a sequence of attacks to gain access to the target’s machine and system by relying on the utilization of various tools, methods, and the gathered information regarding the target.

d. *The Maintaining Access Phase:* This phase of an attack is crucial to an attacker as it determines if they can linger in the target’s system long enough to successfully acquire all the information needed to carry out the attack.

e. *The Clearing Tracks Phase:* In the final phase of the Ethical Hacking Process, all traces and evidence of the attack are deleted and erased (Ushmani 2018; Yash et al. 2022).

A practical implementation of Nmap and Netcat is further covered in this section. Attackers use these tools to identify and test weaknesses/vulnerabilities in the target networks/web application. As an attacker or penetration tester, several tools and techniques are explored, and some entities prefer to use their speciated crafted private collection of tools for this purpose. A concise depiction of Nmap and Netcat usage is further provided in Table 5. Furthermore, the list of commands used during the process is further provided in Table 6.

Table 5: Summary of Nmap and Netcat command usage

NMAP Command	Description
nmap –sP 192.168.170.0/24	Nmap scan to perform Host discovery
nmap –sn192.168.170.16	Check target host availability with the (-sn) flag specified; this will disable port scanning.
Nmap –Pn –T4 192.168.170.16	Nmap command to perform regular or default scan to check top 100 ports, with (-T4) flag specified to impact the time and speed.
Nmap –Pn –T4 –p- 192.168.170.16	Nmap command scans all 65535 ports with (-p-) flag. Additionally, the (-Pn) flag will disable the host discovery and consider it active to improve scan speed.
Nmap –p80 –O 192.168.170.16	Nmap command to check the target machine's operating system with the (-O) flag. Additionally, I have added (-p80) HTTP port because OS footprinting is impossible without port scanning.

NMAP Command	Description
Nmap –Pn –T4 –p- -sV 192.168.170.16	Nmap command to scan all 65535 ports along with service versions, the (-sV) flag will detect the service version details.
Nmap –Pn –T4 -sV –sC –p 80,110,30109 192.168.170.16	Nmap command to scan to test NSE scripts for (80,110,30109) with (-sC) flag.
NETCAT	
Netcat 192.168.170.16 22	Netcat command to connect to a host on port 22.
Netcat –zv 192.168.170.16 22 Netcat –zv 192.168.170.16 80 Netcat –zvn 192.168.170.16 80	Netcat command with (-z) and (-v) flag performs port scanning and verbose results. Additionally, the (-n) flag prevents DNS resolutions and improves the scan speed.
Netcat –zvn 192.168.170.16 1-100	Netcat command to perform a port scan for the top 100 ports.
Netcat –zvn 192.168.170.16 1-65535	Netcat command to perform a full port scan for all 65535 ports.
Netcat –vn 192.168.170.16 80	Netcat command to grab the banner or version details of the web server.

During the enumeration phase, the attacker establishes an active connection to the system and launches directed queries to learn more about the target. The purpose of obtaining this information is to identify the vulnerabilities of the system of the target to exploit it and perform password attacks to gain illegal access to resources. Therefore, this type of enumeration could be a useful technique for attackers because the target cannot completely avoid being screened by the DNS. By applying the steps provided in Figure 2, the authors were able to extract a complete component of the target system. This includes the use of directory burster tools (dirb), and enhanced enumeration tools (nikto and enum4linux).

7.1.3 Table 6: List of All Commands Used During the Enumeration Phase

Command	Description
ip address (ip a)	display network information and IP address of a machine
netdiscover -r 10.0.2.5/24	Search for the connected machines/host on a specific range of subnets
nmap -sT 10.0.2.5/24	Display the TCP-connected hosts and their open ports
nc -zv 10.0.2.10 1-40000	Netcat command that scans the open ports on the victim machine without sending data, specifies searching area from 1 to 40000
nmap -Pn -sV -A -O 10.0.2.10	-Pn: ping without establishing a connection, -sV: service version, -A -O: discover information about the OS of the host
la /usr/share/nmap/scripts	List all Nmap/NSE scripts
nmap --script=nbstat.nse 10.0.2.10 nmap -sV -v -Pn --script=nbstat.nse 10.0.2.10	*Retrieve the target's NetBIOS names and MAC address*
nmap -sU -p137 --script=nbstat.nse 10.0.2.10 nmap -sU -p139 --script=nbstat.nse 10.0.2.10	sends a UDP/TCP probe on ports 137 and 139 to discover the name of the machine.
nmap -sU -p161 10.0.2.10 nmap -sU -p162 10.0.2.10 nmap -sU -p161 --script=snmp-brute.nse 10.0.2.10	Use brute force guessing to find an SNMP community string on UDP port 161
Nmap -p389 --script=ldap-brute.nse 10.0.2.10 nmap -p389 --script=ldap-search 10.0.2.10	LDAP authentication and searching attempts using brute force
nmap 10.0.2.10 -sU -Pn -p123 --script=ntp-info	uses an NTP server to obtain the time and configuration information
nmap -p25 --script=smtp-enum-users 10.0.2.10	Use the VRFY, EXPN, or RCPT TO commands to list all the users on an SMTP serv,
nmap -sSU -p53 --script=dns-nsec-enum 10.0.2.10	list domain names obtained from the DNS server

8. Discussion

Penetration testing is a crucial aspect of ethical hacking that involves simulating a cyber-attack on a computer system to identify any exploitable vulnerabilities. The testing process involves two key phases: reconnaissance and enumeration. In reconnaissance, information about the target system is gathered passively to inform the testing plan, while in enumeration, detailed information about the target's network resources, services, and usernames is extracted (A. S. B. Singh, Yusof, and Nathan 2021). This study used Nmap for reconnaissance and both Nmap and Netcat for enumeration. As part of the ethical hacking lifecycle, the goal of this report was to highlight the techniques used in the reconnaissance and enumeration phases of penetration testing. In these phases, access to sensitive information and common vulnerabilities can be gained. Netcat, as described, establishes a connection between two computers to transmit data across TCP and UDP transport layer protocols. It also enables banner grabbing to determine the operating system, service, and version on a specific port. On the other hand, Nmap is a versatile tool for network scanning and auditing that can identify security vulnerabilities, detect connected hosts, and determine open ports and running services on the target host and operating system. As highlighted in Figure 3, the exploration of Metasploit auxiliary modules for enumeration is a commonly misconstrued approach. This module can be leveraged like the Nmap, to conduct carefully crafted enumeration.

The ethical hacking lifecycle framework presented in this report outlines the steps involved in the reconnaissance and enumeration phases. It highlights the importance of identifying the target, documenting the process, and utilizing tools such as Kali Linux and Parrot. The report is a valuable resource for beginner hackers, students, and those looking to expand their knowledge in hacking and penetration testing, as it provides detailed explanations of the commands used and how they work. By leveraging this framework, limitations, and constraints often associated with the hacking processes can be easily remedied. This further supports the assertion postulated by Bellaby (2023) which posits that the development of a methodical process could help alleviate the frequent limitations associated with the hacking lifecycle. Ultimately, the goal of ethical hacking is to evaluate the security measures of an organization and potentially gain access to sensitive information. To achieve this, a certain level of trust must be established between the ethical hacker and the business hiring them to perform the test. The framework in this report serves as a guide for conducting the reconnaissance and enumeration phases of penetration testing in a compliant and ethical manner. Arguably, the use of other tools and techniques is also encouraged in this wise. Several off-the-shelf tools and tailored tools have been developed for this purpose. It is therefore worth mentioning that the process of conducting both active and passive information gathering is not limited to the presented framework in Figure 2 and the methodology identified in Figure 3. However, these steps provide a common baseline and a starting point for the same. This baseline aligns with assertions from other related frameworks (Zawali et al. 2021; Ellison, Venter, and Ikuesan 2017; Ellison, Ikuesan, and Venter 2019; Lagrasse et al. 2020; Patil et al. 2017).

9. Related works

Studies on existing ethical hacking frameworks are presented in this section, to highlight the contribution of this current study within the common body of knowledge. Findings in Rafay Baloch's Ethical Hacking and Penetration Testing Guide is a comprehensive book on ethical hacking and penetration testing. The book covers the fundamentals of ethical hacking, such as the different types of attacks, methods, tools, and techniques used in penetration testing. Furthermore, it provides readers with step-by-step instructions and examples to assist them in conducting ethical hacking and penetration testing. The book also emphasizes the significance of adhering to ethical guidelines and safeguarding user data (Baloch 2018). However, no specific detail is provided on the first two phases of the hacking lifecycle. Also, the work failed to provide a relevant methodical framework for conducting these phases. In a dissimilar approach, the study (Bellaby 2023) explored various penetration testing services with a specific focus on penetration testing service limitations. The authors surveyed penetration testing service providers and analyzed the results to determine these services' limitations. The identified limitations include a lack of customization, a limited scope, and difficulty testing real-world scenarios. The study also emphasizes the importance of taking these limitations into account when choosing a penetration testing service.

A study by Hawamleh et al. (2020) further highlights the Importance of Protecting User Data by applying the ethical hacking lifecycle. In this regard, an overview of the different types of hacking attacks, the methods used by hackers, and the consequences of these attacks. The paper also emphasizes the importance of protecting user data and the role of ethical hacking in cyberattack prevention. This source provides an excellent overview of the subject and emphasizes the importance of cybersecurity and ethical hacking. A similar work detailed by

Bhawesh (2022) discusses the different types of hacking attacks, such as SQL injection, cross-site scripting, and man-in-the-middle attacks, and describes the methods used to carry out these attacks. Mitigation strategies against these attacks, such as implementing security software and following best practices for web development are further provided. However, it fails to provide a directed method for conducting ethical hacking, particularly on the modalities for the first two phases. In attempting to identify challenges associated with conducting ethical hacking, a study conducted by Hartley (2015) discusses challenges, such as the increasing sophistication of hacking techniques, the difficulty of detecting and preventing cyberattacks, and the importance of user data protection. Whilst the study is good for information on cyber-attack, it fails to provide any direction or guide on the actual process of ethical hacking. Similarly, a review of cybersecurity risk management models, methods, and frameworks from a penetration testing perspective is presented by the study presented in Shah and Mehtre (2015). The authors examined the existing literature on cybersecurity risk management and identified the key components of effective risk management strategies. Based on the review of the extant studies, the authors discuss risk assessment, risk mitigation, and risk communication, as well as the importance of taking organizational culture and user behavior into account when implementing a risk management strategy.

These existing studies examined and discussed various methods and techniques that can be leveraged during the reconnaissance and enumeration phases of the penetration testing cycle. This framework, on the other hand, provides a more comprehensive and methodical approach to carrying out these phases, making it a valuable resource for readers. The framework provides a systematic and structured approach to reconnaissance and enumeration, lowering the possibility of missing information and increasing process efficiency. This academic paper also emphasizes the significance of understanding the target system and its network environment before proceeding to the next phase to ensure a thorough and complete penetration testing process. Other sources, by contrast, focus on specific techniques or tools and do not provide a comprehensive framework for conducting reconnaissance and enumeration. Overall, this framework is an important addition to the field of penetration testing because it provides a step-by-step guide to conducting effective reconnaissance and enumeration.

10. Conclusion

This study introduced a comprehensive methodology for conducting penetration testing, specifically focused on the reconnaissance and enumeration phases. These initial stages of the ethical hacking process aim to gather information about the target through passive reconnaissance methods and active enumeration techniques that exploit weaknesses and vulnerabilities in direct client-server communication. The proposed framework emphasizes compliance with ethical hacking principles and utilizes various hacking platforms. To assist new learners, users, and hackers, detailed tables (Tables 1, 2, 5, and 6) of Nmap and Netcat usage, deployment, and description are also provided as a clear and concise reference guide. As a future work, the authors intend to further develop a holistic framework that can adapt to any perspective of the hacking lifecycle with clearly stated detail and concepts. Furthermore, such a framework would provide a comprehensive view of the hacking process on which any stakeholder can reliably formulate a penetration testing process. Having such a framework can be a breakthrough for the ethical hacking community, as it would provide a reference model for ethical hacking. To date, the hacking community lacks such.

References

Baloch, Rafay. 2018. “Ethical Hacking and Penetration Testing Guide.” *International Journal of Advance Research in Computer Science and Management* 4 (4): 2253--2257.

Bellaby, Ross W. 2023. “An Ethical Framework for Hacking Operations.” In *The Ethics of Hacking*, 32–52. Bristol University Press.

Bhawesh, Kumawat. 2022. “Ethical Hacking Attacks, Methods, Techniques and Their Protection Measures.” *International Journal of Advance Research in Computer Science and Management* 4 (4): 2253–57. https://madhavuniversity.edu.in/ethical-hacking.html.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. “Defining Cybersecurity.” *Technology Innovation Management Review* 4 (10).

Ellison, Dagney, Richard Adeyemi Ikuesan, and Hein S. Venter. 2019. “Ontology for Reactive Techniques in Digital Forensics.” *2019 IEEE Conference on Application, Information and Network Security, AINS 2019*, 83–88. https://doi.org/10.1109/AINS47559.2019.8968696.

Ellison, Dagney, Hein Venter, and Adeyemi Ikuesan. 2017. “An Improved Ontology for Knowledge Management in Security and Digital Forensics.” In *European Conference on Cyber Warfare and Security*, 725--733. Academic Conferences International Limited.

GeeksforGeeks. 2022. “History of Cyber Security.” Computer Networks. 2022. https://www.geeksforgeeks.org/history-of-cyber-security/.

Hartley, Regina D. 2015. “Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack.” *Journal of International Technology and Information Management* 24 (4): 6.

Hawamleh, A M A, Almuhannad Sulaiman M Alorfi, Jassim Ahmad Al-Gasawneh, and Ghada Al-Rawashdeh. 2020. “Cyber Security and Ethical Hacking: The Importance of Protecting User Data.” *Solid State Technology* 63 (5): 7894–99.

Kebande, Victor R., Nickson M. Karie, and Richard A. Ikuesan. 2020. “Real-Time Monitoring as a Supplementary Security Component of Vigilantism in Modern Network Environments.” *International Journal of Information Technology (Singapore)*. https://doi.org/10.1007/s41870-020-00585-8.

Lagrasse, Maxime, Avinash Singh, Howard Munkhondya, Adeyemi Ikuesan, and Hein Venter. 2020. “Digital Forensic Readiness Framework for Software-Defined Networks Using a Trigger-Based Collection Mechanism.” In *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 296–305. https://doi.org/10.34190/ICCWS.20.045.

Patil, Sonali, Ankur Jangra, Mandar Bhale, Akshay Raina, and Pratik Kulkarni. 2017. “Ethical Hacking: The Need for Cyber Security.” In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 1602–6. https://doi.org/10.1109/ICPCSI.2017.8391982.

Shah, Sugandh, and Babu M Mehtre. 2015. “An Overview of Vulnerability Assessment and Penetration Testing Techniques.” *Journal of Computer Virology and Hacking Techniques* 11: 27–49.

Singh, Ammrish Singh Beker, Yusnita Yusof, and Yogeswaran Nathan. 2021. “EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration.” In *2021 14th International Conference on Developments in ESystems Engineering (DeSE)*, 97–101.

Singh, Avinash, Adeyemi Ikuesan, and Hein Venter. 2019. “A Context-Aware Trigger Mechanism for Ransomware Forensics.” In *14th International Conference on Cyber Warfare and Security, ICCWS 2019*, 629–38.

Ushmani, Azhar. 2018. “Ethical Hacking.” *International Journal of Information Technology (IJIT)* 4 (6).

Yaacoub, Jean-Paul A, Hassan N Noura, Ola Salman, and Ali Chehab. 2021. “A Survey on Ethical Hacking: Issues and Challenges.” *ArXiv Preprint ArXiv:2103.15072*.

Yash, Tathagat, Suresh Kumar, Kamlesh Sharma, and others. 2022. “Ethical Hacking: A Technique to Enhance Information Security.” In *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)*, 1:780–84.

Zawali, Bako, Richard A. Ikuesan, Victor R. Kebande, Steven Furnell, and Arafat A-Dhaqm. 2021. “Realising a Push Button Modality for Video-Based Forensics.” *Infrastructures* 6 (4): 54. https://doi.org/10.3390/infrastructures6040054.