Proceedings of the 28th SMART-iSTEAMS
Interteriary Multidisciplinary Conference
American International University West Africa
The Gambia

Full Research Paper

A Review of Common Tools and Techniques for Reconnaissance Attacks

Isaac Odun-Ayo, Gabriel Oyeyemi, Opeyemi Ogunsola, Etukudo , Deborah Okuoyo, Otavie

Department of Computer & Information Sciences
College of Science & Tech.
Covenant University
Ota, Ogun State, Nigeria

Corresponding Authors' Email
isaac.odun-ayo@covenantuniversity.edu.ng

Corresponding Authors' Phone
+2348028829456

ABSTRACT

Background: A reconnaissance helps the attacker gain valuable information on the target to help the attacker select the best tools that would make the attack successful.

Aim: This study aims to review tools for reconnaissance attacks which will be beneficial to professional ethical hackers and also enlighten organizations and the general public of the potential harm of successful reconnaissance attacks.

Methodology: The databases – Springer, Elsevier, Wiley, IEEE, ACM, ArXiv, and Google Scholar were explored. A quantitative evaluation was conducted on 19 selected articles.

Result: 95.2% of the reconnaissance tools allowed experts to gather information by use of the command line. While 4.8% of the tools do not provide a command-line interface. 61.9% of the tools are network-based – can be used to gather data about the target's network infrastructure.

Conclusion: The best-fit tool is massively dependent on the attacker or penetration tester. Therefore, a tool should be selected based on the user's preference and the attack style.

Keywords: Reconnaissance, cyber-attack, cybersecurity, social engineering, techniques.

Proceedings Reference Format
Isaac Odun-Ayo, G., Oyeyemi, O.O., Etukudo, D. & Okuoyo, O. (2021): A Review of Common Tools and Techniques for Reconnaissance Attacks.. Proceedings of the 28th iSTEAMS Intertertiary Multidisciplinary Conference. American International University West Africa, The Gambia. October, 2021. Pp 141-157 www.isteams.net/gambia2021.
DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2021/V28P11

1. INTRODUCTION

The internet is a public place and this opens users up to cyber-attacks. The phases of cyber-attack generally follow the same pattern as a traditional crime [1]. A reconnaissance attack, also known as information gathering, is the first phase of a cyber-attack. It is an unauthorized retrieval of information about a target to identify vulnerabilities that can be exploited by an attacker. The primary objective of the reconnaissance phase is to map a "real-world" target (a company, corporation, government, or other organization) to a cyber world target, where "cyber world target" is defined as a set of reachable and relevant IP addresses [2]. With the world being more digital as time goes by, we believe there would be a rise in cyber-attacks. Individuals and companies need to understand the need of safeguarding their cyber-space.

This paper aims to help individuals and companies comprehend the impact of reconnaissance attacks and how to mitigate them and also to help cybersecurity professionals, ethical hackers, make an educated decision in selecting the best-fit tool for performing a reconnaissance attack. The objective of this paper is to evaluate common reconnaissance attack tools, what they do, and their features. This paper also contributes to the United Nation's Sustainable Development Goals[3]. Section 2 discusses related works, while Section 3 examines the materials and method. Section 4 focuses on the results and discussion and the paper is concluded in section 5.

2. RELATED WORKS

The five pillars of information assurance are confidentiality, integrity, availability, non-repudiation, and authentication. An attack that violates at least one of these pillars is considered as a cyber-attack. Reconnaissance is the first phase of cyber-attack. In this phase, the weak points of the target are identified. Critical information like the victim's IP addresses, home address, telephone number, frequent hangout, dark secrets, security policies, etc. are collected and ways of by-passing the victim's defence systems are also noted [4].

Cyber-attacks are growing in, and according to Industry Week, in 2018 spear-phishing and spoofing attempts on business emails increased by 70% and 250% respectively, and ransomware campaigns targeting enterprises had an impressive 350% growth. This has led to economic damages. The average cost of a data breach has risen from $4.9 million in 2017 to $7.5 million in 2018. Attackers can now use a wide range of tools for compromising hosts, network appliances, and Internet of Things (IoT) devices simply and effectively, for example, via a Crime-as-a-Service business model [1].

Social engineering is non-technical [5] and it is probably the oldest form of technique used for reconnaissance and it is extraordinarily effective as it exploits the weakest link in security – humans. In essence, social engineering tries to manipulate and deceive victims by misusing their trust and convince them to share confidential information or to perform activities that can be useful to the attacker, for example, download and install a keylogger [1]. The attack first starts at getting the users' information, progresses to having access to the organization's computer and then to attack the control program of the organization [6]. Knowledge-based as discussed in [6] noted that the more education given to employees and users about social engineering, a decrease in the vulnerability to employee's activity performance online.

Also, a technique that was considered is email security, organizations should try to use Domain-based Message Authentication Reporting and Conformance (DMARC) and real-time blocking which maintain email security gateways through tools to identify origins of email (SPF) sent and include cryptographic signatures to know the validity of the email and also identifies malicious emails. [6].

A survey in [6] and the results showed that most people did not know about the intrusion they had experienced in past years. The authors stated that employees are responsible for securing the organization's data because if they are careless, they are exposing vital information to hackers that will gain access to them. Organizations can adapt neuro-fuzzy inference system which uses neural networks to create a self-predicting phishing detection that places hackers on blacklists making it difficult for them to generalize [6].

3. MATERIALS AND METHOD

The search techniques in Kitchenham (2004) were adopted and modified for this paper. To achieve the aforementioned objectives, research questions were prepared as shown below:

RQ1: What are the relevant values of the existing studies for reconnaissance tools and techniques?
RQ2: What are the existing reconnaissance tools and techniques?
RQ3: What are the methods of evaluating common techniques for reconnaissance attacks?

3.1 Search String

The search strategy utilized for this paper was done based on the following criteria:

1. Obtain relevant keywords from the research questions;
2. Recognize distinct synonyms and spellings for the keywords;
3. Identify keywords in relevant articles;
4. Utilize "AND" or "OR" to relate relevant keywords.

The search query used is as follows: (reconnaissance tools or techniques) AND (reconnaissance attack OR reconnaissance attack techniques) AND (reconnaissance evaluation OR reconnaissance evaluation metrics) AND (description of reconnaissance techniques OR concept of (reconnaissance tools).

3.2 Search Selection Strategy

The aforementioned search string was utilized for advanced search on the databases – Springer, Elsevier, Wiley, IEEE, ACM, ArXiv, and Google Scholar. The systematic review process is shown in Fig. 1.

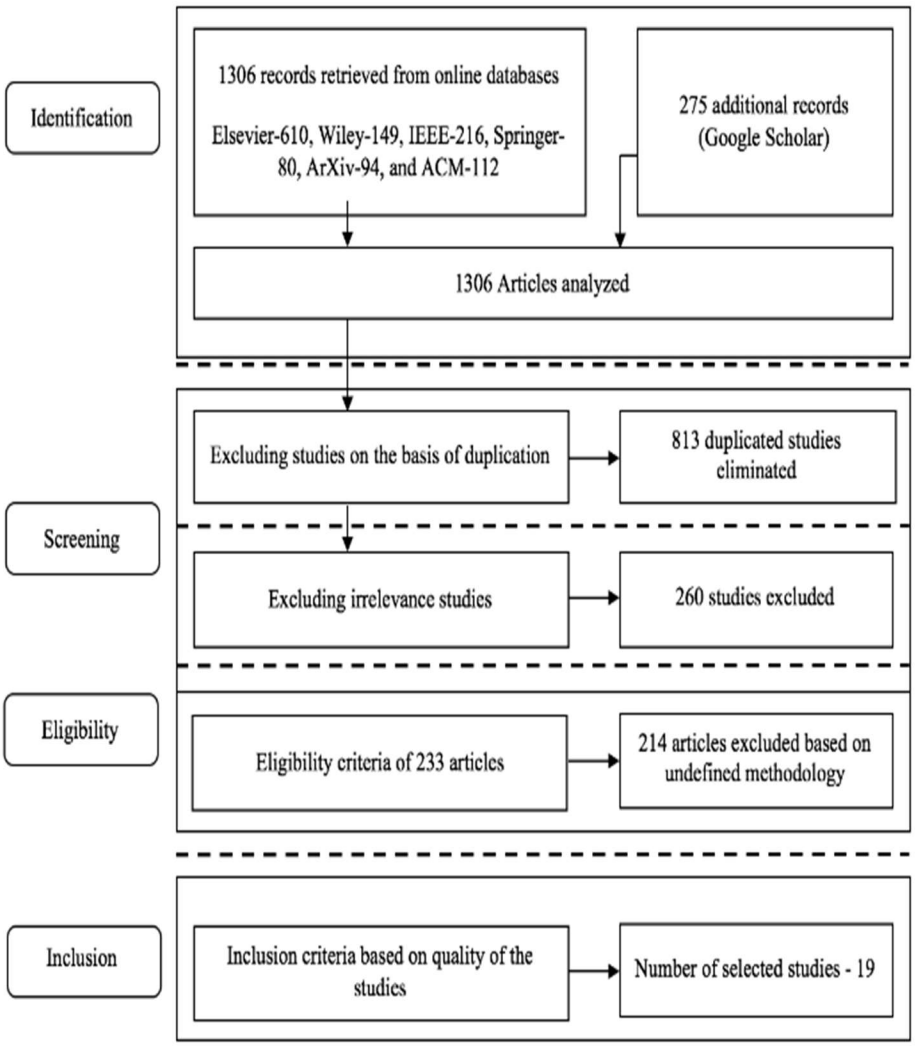

Fig. 1. PRISMA flowchart of the review process and selection of the articles

First, a search was executed in the seven databases with to 1306 articles retrieved. Then, 813 duplicates were found and 260 articles were considered irrelevant when screened through the titles and their abstracts. A full text selection criterion was executed to extract relevant studies, and 214 articles were removed based on undefined methodology. Finally, a quality assessment was initiated, and 19 primary studies were selected (Fig. 2.).

Table 1. Number of articles extracted from databases

S/N	Database	Number of Articles
1	Springer	80
2	Elsevier	610
3	Wiley	149
4	IEEE	216
5	ACM	112
6	ArXiv	94
7	Google Scholar	275

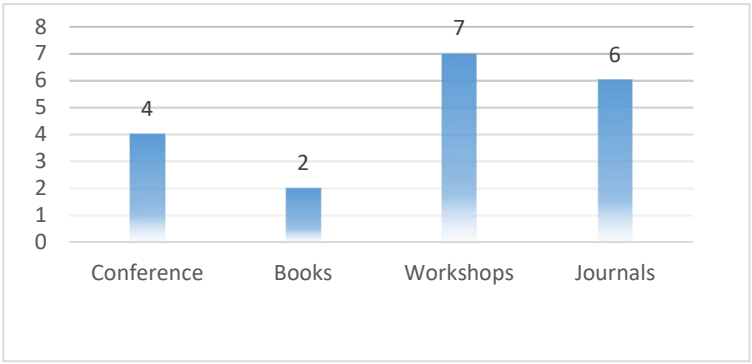

Fig. 2. The number of collated studies.

The keywords, titles, and abstracts were used to execute a search query in the seven (7) databases. Existing reconnaissance tools: Twenty-one (21) reconnaissance tools were used. Existing reconnaissance techniques: Seven (7) existing reconnaissance techniques. Evaluation Method: Fourteen (14) methods were discussed in section 4. A word cloud analysis (Fig. 3) was done using the titles of the selected studies on Orange machine learning development environment shows 'Penetration' as the most frequent followed by 'Testing' and 'Security'.

Fig. 3. Generated keywords from Titles of selected studies

A hierarchical search strategy was used to identify related articles using relevant keywords and the paper titles. Then, the search for related works was conducted for articles between 2013 and 2021. Fig. 4 shows the returned results for relevant studies while Fig. 5 shows the number of relevant articles based on the publication year.

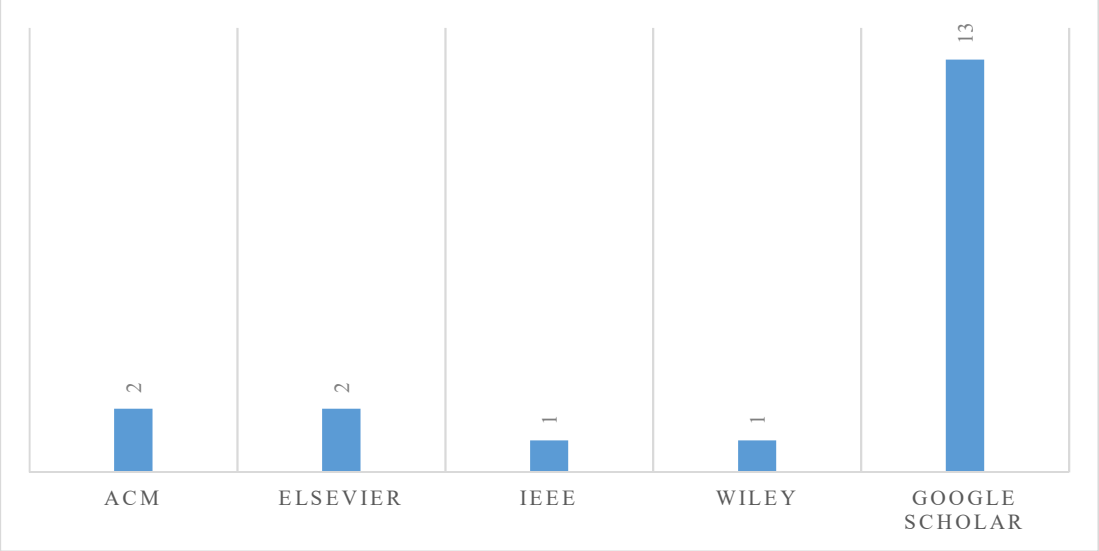

Fig. 4. Sources and number of relevant articles

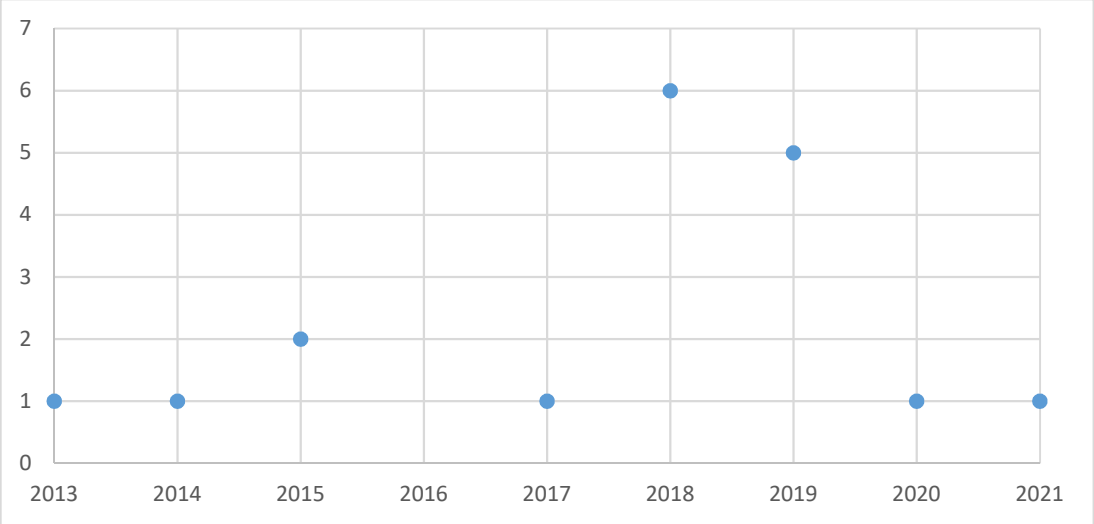

Fig. 5. Published Year and number of relevant articles

3.3 Reconnaissance Tools

MSFCONSOLE: It is an interface to the Metasploit Framework. It provides an all-in-one centralized console that allows one to efficiently have access to virtually all the options available in the MSF. It makes hacking way easier, and it is an indispensable toeol for the red hat hackers and blue hat hackers. Once a weakness has been identified all you need do is search the database of Metasploit for the exploit (a script or program software that helps hackers to have control over the system) that will crack open and give you access to the system. It provides CLI only [7].

DNSEUNM: It is a Kali Linux command-line tool used passively to gather DNS information about the target. It helps to locate all DNS servers and DNS entries for an organization. It is also used to perform Google scraping (the process of sending queries to Goggle to discover all the domain names linked to the target domain).

NMAP: Network Mapper (Nmap) is a free and open-source platform that can be used to perform initial device or network scanning like discovering accessible hosts, operating systems, and port discovery [8]. It scans individual IP addresses as well as IP ranges and returns valuable information such as the operating system, utilities found, and available ports [9]. It is the best port scanner and an excellent component of our host security equipment [10].

DNMAP: This framework uses a client/server architecture to distribute Nmap scans among several clients. The output from the Nmap scan is stored on both the server and client. Nmap is an open-source Linux command-line tool that helps a pen tester to gather information about hosts and services and also detect vulnerabilities on a network. It does this by sending packets and analyzing the response gotten. OS finger printing is done with it.

DNS RECON: It is used when conducting DNS enumeration. It provides the pen tester the ability to perform: goggle scanning for sub domains and host, reverse look up against IP range, et cetera. It runs on Linux OS.

DNSWALK: It is a tool that helps to check the target database for internal consistency and accuracy. It is a DNS debugger. It can be used to initiate zone transfer that is, copying contents of the zone file on a primary DNS server (a copy of part of its database) to a secondary DNS server (zone transfer). It runs on Linux operating system.

DNS TRACER: It is used to extract unique DNS information like NS (Name server records), MX (Mail exchanger records) etc. It determines where a given DNS gets its information from a given host name following the chain of DNS servers back to the DNS server hosting the primary copy of the DNS record that responded to your lookup.

SHODAN: Shodan is a search engine that can be used to locate individual devices and types of devices. Shodan scans the entire Internet and when the search is over, the information returned will most likely be about web servers and their models, as well as anonymous FTP servers if they operate in a specific area, and system model information. Shodan search engine for security analysis expected to grow ever further [8].

BURP SUITE: It is used for conducting web application security monitoring. It also helps with the whole testing process, from plotting and analyzing an application's attack surface to discovering and leveraging security flaws [8]. It can be used to search for popular site vulnerabilities automatically, but it also includes specialized manual scanning procedures to help with each step of penetration testing [9].

METASPLOIT: Metasploit is a vulnerability discovery, leveraging, and validation tool that includes Metasploit Framework and some commercial equivalents. The Metasploit Framework is an open-source initiative that offers infrastructure, content, and resources for penetration testing. Anti-forensics and specialized avoidance tools are also available, with some of them being integrated into the Metasploit Framework [8].

WIRESHARK: This is a network packet inspection tool (network sniffer) that captures and displays packets in a human-readable format in real time. Wireshark is a passive network traffic analyzer that does not transmit data. This ensures that if Wireshark is used on a network, other parties would not be able to spot it. It is open source and works for UNIX, Windows, and a variety of other operating systems. It has a graphical user interface, which distinguishes it from other packet analyzers like tcpdump, which shares several features with Wireshark [8].

SQLMAP: SQLmap is a free and open-source penetration testing platform that automates the task of manipulating SQL databases. It can also be used to determine the database and version being used. As a result, the tool can be used both during reconnaissance and during the gaining access process [9].

DMITRY: Dmitry is a data collection tool that can be used to find out who is who, uptime records, email addresses, and subdomains. Additionally, the instrument can be used to conduct port scans [9].
HPING3: hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a trace route mode, the ability to send files between a covered channel, and many other features. While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts [11].

NBTSTAT: Nbtstat is a network utility that is used to verify the status of ongoing TCP/IP connections. Nbtstat displays all of the network connections that are active in the Windows operating system. Because this utility is pre-installed in Windows, you won't need any additional program to utilize it. It's a useful tool for determining all of the Windows workstations' TCP/IP connections [12].

NBTSCAN: The NBTScan utility may be used to look for NetBIOS name information in IP addresses. It will generate a report with the related computers' IP addresses, NetBIOS computer names, services accessible, logged in usernames, and MAC addresses. This data will come in handy throughout the penetration testing process. The difference between nbtstat and Windows' NBTScan is that NBTScan can scan a wide range of IP addresses.
You should be warned that utilizing this program generates a lot of traffic, which the target computers may log [13].

NIKTO: Sullo, CIRT, Inc. was the first to write and maintain Nikto. David Lodge is the current maintainer; though other individuals have also contributed to the project. It was included in the Kali Linux Penetration Testing distribution and is designed to work on any platform having a Perl environment. It is an open-source program that supports SSL, proxies, host authentication, IDS evasion, and other features [14].

GHOST PHISHER: This is a wireless and Ethernet security auditing and attack software application built in Python with the Python Qt GUI framework. It can impersonate access points and distribute malicious code [15].

THE HARVESTER: This program's goal is to collect emails, subdomains, hosts, employee names, open ports, and banners from a variety of public sources, such as search engines, PGP key servers, and the SHODAN computer database. It helps pene testers to understand the client footprint on the Internet during the early phases of a penetration test. It is also valuable for anyone curious in what an attacker sees about their company [16].

FARADAY: IPE (Integrated Penetration-Test Environment), a multiuser Penetration-Testing IDE, was introduced by Faraday. Faraday is a program that distributes, indexes, and analyzes the information gathered during a security audit. It was created to allow you to use the community's various tools in a true multiuser manner [17].

MASSCAN: This is the quickest scanner for Internet ports. It can scan the whole Internet in less than six minutes and transmit ten million packets per second. It delivers findings that are comparable to those of nmap, the most well-known port scanner. Internally, it uses asynchronous communication and works similarly to scanrand, unicornscan, and ZMap. It is more adaptable, allowing for any address and port ranges [18].

3.4 Reconnaissance Techniques

PHISHING: This is the most common way to get information through the use of email, phone calls and SMS. Hackers observe the target by learning the types of messages, mails, etc. the target is interested in. The hacker then sends malicious emails to the target with familiar features such as passwords, bank etc. on what the target is used to, and when it is clicked on it gives the hacker access to personal information of the target. [19].

BAITING: This is a process of physically attacking an individual or an organization through the use of various mediums such as an infected USB drive [20].

DUMPSTER DIVING: This is another technique used for getting information from a target. Dumpster diving involves the monitoring of waste bin or dust bin of an organization by an attacker and collecting information such as important document that may have been disposed carelessly by a staff or worker in the organization. [20].

SPEAR PHISHING: It is used just like phishing; however, spear phishing focuses on specific persons, and sends emails based on the information gathered of that person. Once the emails are clicked on it gains access to private information, the success rate in spear phishing attack is higher than the phishing attack [21].

PRETEXTING: It involves pretending to be someone you are not to get information from an organization or individual, for example acting as an investigator just to obtain persona companies records. [21].

TAILGATING: This process involves an attacker gaining access into an organization simply by following an employee or an authorized person working in the organization. [20].

WATERING HOLE ATTACK: This attack involves tracking of all websites the target has visited and how frequent the target visits those websites. The hacker gets the gets the most visited websites and finds loopholes in those websites such as reflected XSS, host header etc. to obtain confidential information from the target. [19].

4. RESULTS AND DISCUSSION

Upon exploring the 19 selected relevant studies, the similarities and differences with respect to the features associated with them have been tabulated below. Table 2 illustrates the summary of our findings which answers RQ3

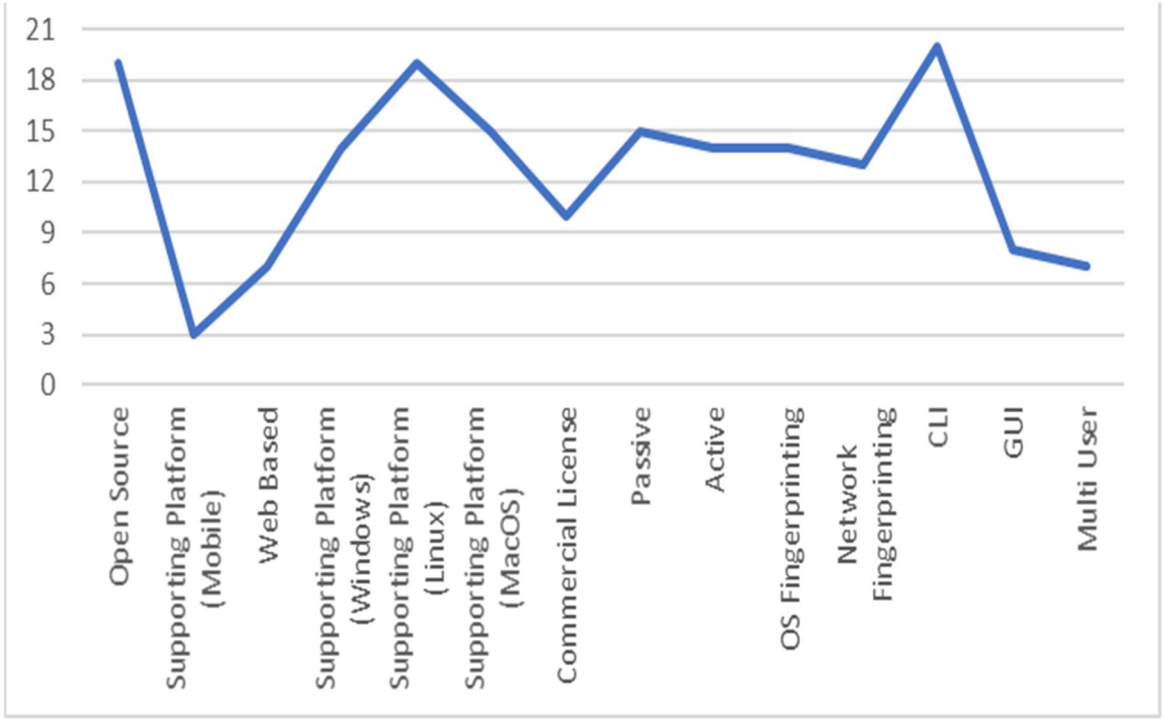

Fig. 6. Summary of the Tools Reviewed

Before considering and deploying tools to be used for information gathering, experts often review and gather information on them. Open-source tools promote trust and dependability as they offer readability into the coding structure and development history of these tools, and a community that supports it. However, experts need to be fully informed if they might need to pay for the tools in an enterprise environment.

Other important metrics used to evaluate these tools include: the Operating System supported; are they Command Line based, Graphical User based or both; are they used actively or passively. Most of these tools often gather information about a target host or a target network, which can be categorized as OS fingerprinting or Network fingerprinting. Experts may also want to know if their InfoSec team can collaborate within these tools, which defines the multiuser feature.

Table 2 Chart of Reconnaissance Tools and Techniques

Reconnaissance Tools	Open-Source	Supporting Platform (Mobile)	Web Based	Supporting Platform (Windows)	Supporting Platform (Linux)	Supporting Platform (MacOS)	Commercial License	Passive	Active	OS Fingerprinting	Network Fingerprinting	CLI	GUI	Multiuser
MSFCONSOLE	✓			✓	✓	✓	✓		✓	✓		✓		✓
DNSEUNM	✓				✓	✓		✓			✓	✓		
DNMAP	✓				✓	✓		✓			✓	✓		
DNS RECON	✓				✓			✓			✓	✓		
DNSWALK	✓				✓			✓			✓	✓		
DNS TRACER	✓				✓	✓		✓	✓		✓	✓		✓
NMAP	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
SHODAN	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓
BURP SUITE	✓	✓	✓	✓		✓	✓	✓	✓	✓			✓	✓
METASPLOIT	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
WIRESHARK	✓		✓	✓	✓	✓	✓	✓		✓		✓	✓	
SQLMAP	✓			✓	✓		✓		✓	✓		✓		✓
DMITRY	✓		✓	✓	✓	✓	✓	✓		✓		✓		✓
HPING 3	✓			✓	✓	✓	✓		✓	✓		✓		
NBSTAT				✓					✓	✓	✓	✓		
NBTSCAN			✓	✓	✓	✓			✓	✓	✓	✓		
NIKTO	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
GHOST PHISHER	✓				✓			✓	✓		✓	✓	✓	
THEHARVESTER	✓				✓			✓	✓		✓	✓		
FARADAY	✓			✓	✓	✓		✓	✓	✓	✓	✓	✓	
MASSSCAN	✓			✓	✓	✓		✓	✓	✓	✓	✓		

Platforms Supported: Operating Systems: Linux operating has more information-gathering tools. It supports 95.2% of all the tools evaluated. Some of these tools even come preinstalled on Kali Linux, Parrot Security OS, Backbox, and other Linux distributions that were built for hacking and penetration testing.

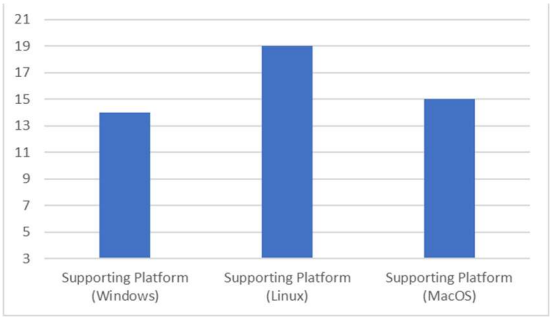

Fig. 7. PC Supported for the Tools Reviewed

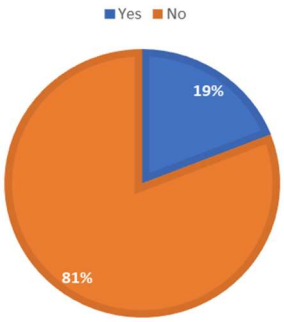

Fig. 8. Mobile Supported for the Tools

MacOS recorded more support for these tools while Windows recorded the lowest number of supports from these tools. This implies that Windows might not be the choice OS for ethical hackers and cybersecurity professionals.

IOS/Android Support: Mobile operating systems like Android and iOS have less penetration testing tool (19%). This low-rate support for mobile can be attributed to lack of shell or Command Line Interface (CLI).

Web-Based Support: 67% of the tools reviewed are web-based while 33% are not.

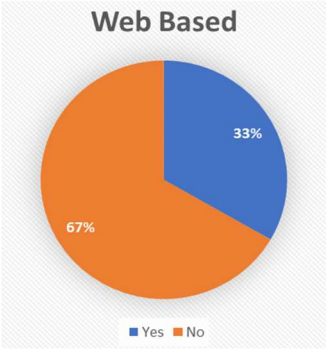

Fig. 9. Tools Reviewed That Are Web Based

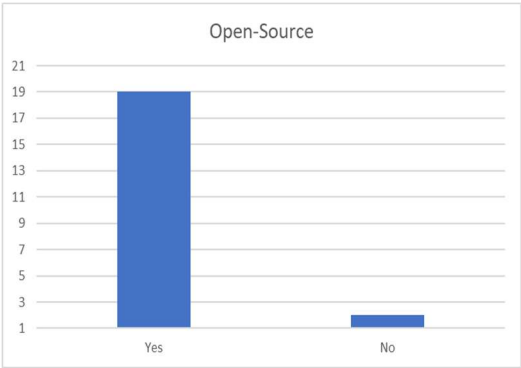

Fig. 10. Tools Reviewed That Are Open-Source

Open-Source: 90.4% of these tools are Open-Source, while 9.6% were not proprietary tools. This implies that majority of these tools have their source code hosted on public communities like GitHub where collaboration and contributions can be made.

Commercial/Enterprise Licensing: The result of the analysis on the tools reviewed indicates that about 48%, almost half of the tools reviewed have or require licensing for enterprise deployment. This would mean that they may need to adjust their IT budget or investigate alternative tools that may be "license-free".

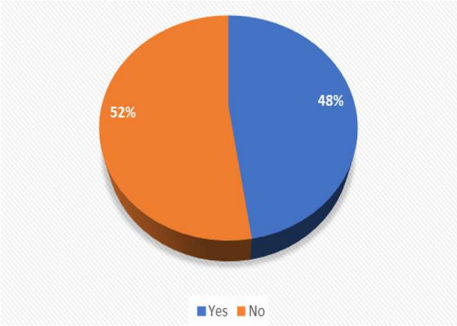

Fig.11. Tools Reviewed That Possesses Commercial License

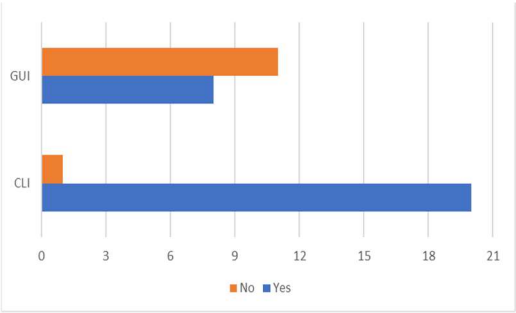

Fig. 12. User Interface Tools Reviewed

Command Line Interface (CLI) and Graphical User Interface (GUI): The CLI is preferred for ethical hackers with a solid scripting skill as it is faster and it gives more freedom. Only 38% of the tools evaluated actually provide GUI, while 95.2% of the tools provide a CLI. Even the 4.8% of the tools that do not provide CLI, allows users to launch it from the command line interface while specifying some parameters to customize how it runs.

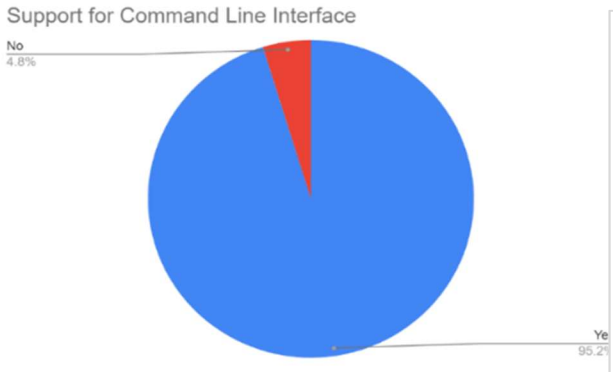

Fig. 13. Tools Reviewed That Support Command Line Interface

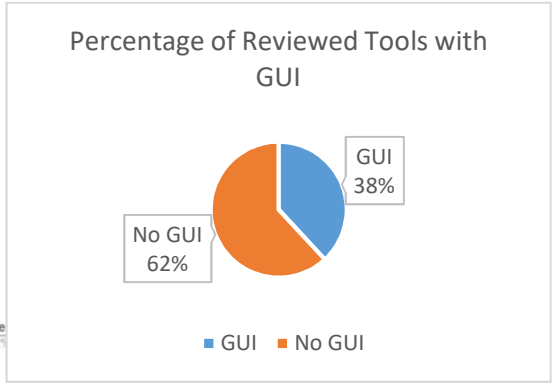

Fig. 14. Tools Reviewed That Support Graphical User Interface

Also, 95.2% of the tools reviewed allowed experts to gather information by running their necessary command from the command line. Although this option requires a level of coding skills and knowledge of the command for the application, it offers greater flexibility, faster management, greater control, and automation option. This means that ethical hackers can do faster within the designed scope of the application.

Network-Based and System-Based Fingerprinting*:* In this study we evaluated and classified these tools into two categories – OS fingerprinting and network fingerprinting tools. The means the tools can either be used to get information about the target system's hardware and operating system or gather data about the target network.

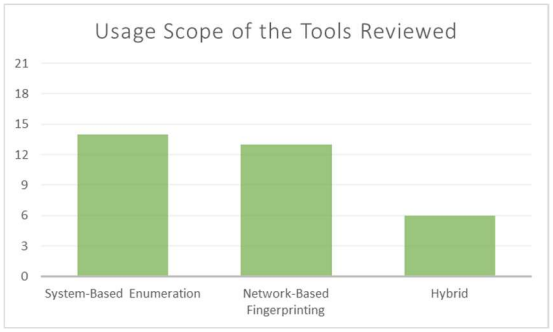

Fig. 15. Usage Scope Tools Reviewed

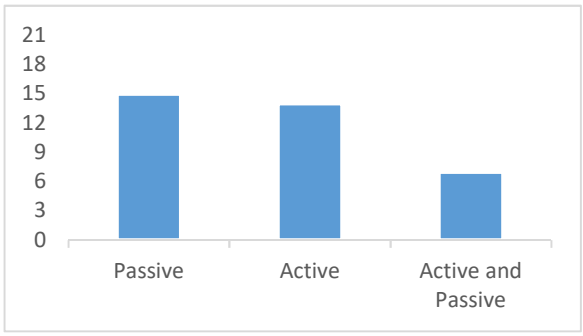

Fig. 16. Passive and Active Tools Reviewed

Out of the 21 tools that were reviewed, 66.7% of them could be used for gathering and extract information like machine names, operating system, usernames, network resources; 61.9% are network-based as they can be used to gather the target's network infrastructure information such as protocols, ports, DNS, IP address, hosts, and the general network architecture. While 28.5% could be classified as hybrid.

Active and Passive Information Gathering*:* Passive information gathering refers to gathering as much information as possible without establishing contact between the pen tester (yourself) and the target about which you are collecting information. Active information gathering involves contact between the pen tester and the actual target. Some tools be used actively and passively.

Multiuser Environment: Out of the 21 tools reviewed, 33.3% had basic communication features like chatting, however other features like task management, scheduling, and other multiuser features that could enhance collaboration were missing. One of the recent trends in IT is the implantation of Role Based Access Control (RBAC), to ensure that in organizations IT staffs only get just the privilege or permission they need to do their work, and nothing more. This means that information technology has evolved from traditional roles like system administrator and enterprise administrator, into job specific roles like Security Administrator, Compliance Administrator, User Access Administrator, Authentication Administrator, Security Operator and Password Administrator.

Unfortunately, this trend is not yet visible in the information gathering tools that were reviewed, as they still function as though only one person should perform reconnaissance and not a team.

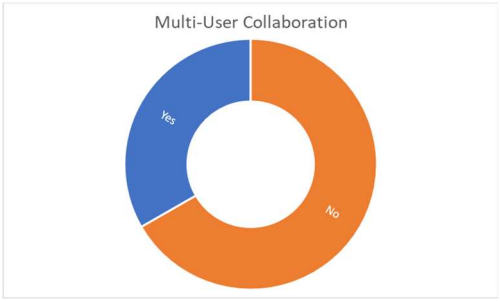

Fig. 17. Tools Reviewed That Support Multi-User Collaboration

5. CONCLUSION

Having evaluated 21 reconnaissance tools, the best-fit tool is dependent on the attacker's or penetration tester's style of attack. However, enumerating these tools and how they operate alongside the social engineering techniques in gathering information of victims, enlightens common users, cybersecurity professionals, and organizations about the risk of a successful reconnaissance attack and possible ways of avoiding the attack.

Acknowledgment

We acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation, and Discovery (CUCRID). There are no conflicts of interest.

REFERENCE

[1] W. Mazurczyk and L. Caviglione, "Cyber Reconnaissance Techniques," *Communications of the ACM,* pp. 86-95, 2021.

[2] J. Faircloth, "Reconnaissance," in *Penetration Tester's Open Source Toolkit*, Fourth Edition ed., Syngress, 2017, p. 32.

[3] United Nations, "Sustainable Development Goals," 17 May 2021. [Online]. Available: https://www.un.org/sustainabledevelopment/.

[4] H. P. Sanghvi and M. S. Dahiya, "Cyber Reconnaissance: An Alarm before Cyber Attack," *International Journal of Computer Applications,* pp. 36-38, 2013.

[5] A. Kumar, M. Chaudhary and N. Kumar, "Social Engineering Threats and Awareness: A Survey," *European Journal of Advances in Engineering and Technology, 2015, 2(11): 15-19,* p. 5, 2015.

[6] G. Skinner and H. Aldawood, "Contemporary Cyber Security Social Engineering Solutions,," *International Journal of Security (IJS), Volume (10) : Issue (1) : 2019,* p. 15, 2019.

[7] U. Timalsina, "Use of Metasploit Framework in Kali Linux," 3 April 2015. [Online]. Available: https://doi.org/10.13140/RG.2.2.12377.93284.

[8] K. Božić, N. Penevski and S. Adamović, "Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods," n.d. n.d. 2019. [Online]. Available: http://portal.sinteza.singidunum.ac.rs/paper/669.

[9] R. Ankele, S. Marksteiner, K. Nahrgang and H. Vallant, "Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing," 25 June 2019. [Online]. Available: https://arxiv.org/abs/1906.10416.

[10] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan and Ata-ur-rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," 25 March 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8673520.

[11] HPING, "hping," 19 May 2021. [Online]. Available: http://www.hping.org/.

[12] J. Gill, "NETBIOS OVER TCP/IP – NBTSTAT USAGE IN DETAIL," 25 April 2019. [Online]. Available: https://www.securitynewspaper.com/2018/11/28/netbios-over-tcp-ip-nbtstat-usage-in-detail/.

[13] Packt Publishing, "Kali Linux – Assuring Security by Penetration Testing," 7 April 2014. [Online]. Available: https://www.oreilly.com/library/view/kali-linux/9781849519489/ch06s03.html.

[14] L. Obbayi, "Introduction to the Nikto Web Application Vulnerability Scanner," 30 March 2018. [Online]. Available: https://resources.infosecinstitute.com/topic/introduction-nikto-web-application-vulnerability-scanner/.

[15] S. E. Ekiko, "Ghost Phisher Package Description," 24 November 2018. [Online]. Available: https://tools.kali.org/information-gathering/ghost-phisher.

[16] C. Martorella, "theharvester Package Description," 25 November 2018. [Online]. Available: https://tools.kali.org/information-gathering/theharvester.

[17] K. John, "Faraday - Penetration Testing IDE & Vulnerability Management Platform," 7 November 2020. [Online]. Available: https://computingforgeeks.com/faraday-penetration-test-vulnerability-management-ide/.

[18] R. Graham, "masscan Package Description," 23 December 2015. [Online]. Available: https://tools.kali.org/information-gathering/masscan.

[19] S. Lohani, "Social Engineering: Hacking into Humans," *INTERNATIONAL JOURNAL OF ADVANCED STUDIES OF SCIENTIFIC RESEARCH,* pp. 1-4, 2018.

[20] A. Y. Chouhan, R. Fatima, L. Liu, A. Yasin and J. Wang, "Contemplating social engineering studies and attack," *Wiley,* pp. 5-6, 2019.

[21] I. A. M. Abass, "Social Engineering Threat and Defense: A Literature Survey," *Scientific Research Publishing,* pp. 5-6, 2018.