Maximizing Penetration Testing Success with Effective Reconnaissance Techniques Using ChatGPT

Sheetal Temara

Asian Journal of Research in Computer Science

Volume 17, Issue 5, Page 19-29, 2024; Article no.AJRCOS.112467
ISSN: 2581-8260

Maximizing Penetration Testing Success with Effective Reconnaissance Techniques Using ChatGPT

Sheetal Temara [a*]

[a] Department of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY, United States.

Author's contribution

Author ST designed the study, conducted the research, collected and analyzed the data, and wrote the manuscript.

Article Information

DOI: 10.9734/AJRCOS/2024/v17i5435

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/112467

Original Research Article

Received: 15/12/2023
Accepted: 20/02/2024
Published: 24/02/2024

ABSTRACT

Background/Objective: The study investigates the integration of ChatGPT, a generative pretrained transformer language model into the reconnaissance phase of penetration testing. The research aims to enhance the efficiency and depth of information gathering during critical security assessments offering potential improvements to traditional approaches.
Research Problem: The research study addresses the challenge of optimizing the reconnaissance phase in penetration testing. It seeks to provide a solution by exploring the capabilities of ChatGPT in extracting valuable data, such as various aspects of the digital footprint or infrastructure of a system or an organization. The scope of the research relies in demonstrating how ChatGPT can contribute to the planning phase of penetration testing, guiding the selection of tactics, tools, and techniques for identifying and mitigating potential risks that could be used to assist with securing Internet accessible assets of a system or an organization.

**Corresponding author: E-mail: stemara22276@ucumberlands.edu;*

Methodology: The research adopts a case study methodology to assess the effectiveness of ChatGPT in reconnaissance. Tailored questions are formulated to extract specific information relevant to penetration testing. The study highlights the importance of prompt engineering emphasizing the need for carefully constructed questions to ensure usable results.
Results: The research showcases the ability of ChatGPT to provide diverse and insightful reconnaissance information. The extracted data includes IP address ranges, domain names, vendor technologies, SSL/TLS ciphers, and network protocols. The information gathering improves efficiency of the reconnaissance phase aiding penetration testers in planning subsequent phases of the assessment.
Discussion: The research study extends to the broader field of cybersecurity where artificial intelligence language models can play a valuable role in enhancing the success of reconnaissance in penetration testing. The research suggests that integrating ChatGPT into penetration testing can bring about positive changes in the efficiency and depth of information obtained during reconnaissance.
Conclusion: The results of the study determine that incorporating ChatGPT in the reconnaissance phase significantly benefits penetration testers by offering valuable insights and streamlining subsequent assessment planning. The results affirm ChatGPT as a pivotal tool in maximizing success in penetration testing, contributing to ongoing advancements in cybersecurity practices.

Keywords: ChatGPT; penetration testing; reconnaissance; artificial intelligence; cybersecurity.

ABBREVIATIONS

ALPN	:	*Application-Layer Protocol Negotiation*
API	:	*Application Programming Interface*
AWS	:	*Amazon Web Services*
BGP	:	*Border Gateway Protocol*
CDN	:	*Content Delivery Network*
ChatGPT	:	*Chat-based Generative Pre-trained Transformers*
CIDR	:	*Classless Inter-Domain Routing*
CRM	:	*Customer Relationship Management*
CT	:	*Certificate Transparency*
DNS	:	*Domain Name Service*
DHE	:	*Diffie-Hellman Ephemeral*
ECC	:	*Elliptic Curve Cryptography*
ECDHE	:	*Elliptic Curve Diffie-Hellman Ephemeral*
FQDN	:	*Fully Qualified Domain Name*
gTLD	:	*Generic Top-Level Domain*
HSTS	:	*HTTP Strict Transport Security*
HTTP	:	*Hyper Text Transfer Protocol*
HTTPS	:	*Hyper Text Transfer Protocol Secure*
IP	:	*Internet Protocol*
IPv4	:	*Internet Protocol Version 4*
NLP	:	*Natural Language Processing*
NTP	:	*Network Time Protocol*
OCSP	:	*Online Certificate Status Protocol*
PFS	:	*Perfect Forward Secrecy*
PIN	:	*Personal Identification Number*
PKP	:	*Public Key Pinning*
RSA	:	*Rivest-Shamir-Adleman*
SAP	:	*System Analysis Program Development*
SMTP	:	*Simple Mail Transfer Protocol*
SNMP	:	*Simple Network Management Protocol*
SSH	:	*Secure Shell*
SSL/TLS	:	*Secure Socket Layer/Transport Layer Security*
SSO	:	*Single Sign-On*

TCP : Transmission Control Protocol
TTP : Tools, Techniques, and Procedures
UDP : User Datagram Protocol
VPN : Virtual Private Network

1. INTRODUCTION

Web applications are a vital part of modern computing as they provide access to sensitive information and services. These applications also present a significant attack surface making them vulnerable to various threats. Many security processes can be used to help organizations identify security vulnerabilities and to ensure those vulnerabilities are understood and remediated [1]. One such process is known as a penetration test which is an assessment performed by authorized individuals meant to mimic an actual attack against a computer system in order to analyze the implemented security controls and to identify exploitable vulnerabilities. Penetration testing is a widely accepted technique for identifying vulnerabilities which can be resource-intensive and time-consuming [2]. In this research study, the penetration testers will make use of identical tools, techniques, and procedures (TTPs) as used by actual malicious actors in order to discover and prove that particular vulnerabilities or design flaws exist.

The initial stage of a penetration test is known as reconnaissance or information gathering. The reconnaissance phase of penetration testing is a crucial step in the overall security assessment process. During the reconnaissance stage, a penetration tester will collect detailed data regarding the scope of the assessment which could be an application, system, network or more [3]. The data collected can include information such as technology components deployed, the SSL/TLS versions and cipher suites configured, cookies and their attributes used by websites, third-party relationships, network topology, and operating systems utilized. With knowledge of these details regarding the scope of the assessment, the penetration tester will have a comprehensive understanding of the target in order to better plan for actual testing to evaluate where potential risks may be present.

The rapid growth of web applications has introduced a myriad of security threats making penetration testing an essential component of cyber security [4]. The advent of Artificial Intelligence (AI) has the potential to transform and enhance penetration testing improving accuracy and enabling more efficient and effective identification of vulnerabilities. ChatGPT is an open-source dialogue system trained on billions of exchanges based on human-to-human conversations that are powered by the latest advancements in natural language processing (NLP). ChatGPT provides users with a virtual assistant that can cognize and analyze natural language to answer questions, hold a conversation, and interact with the user through a chat interface. This presents an opportunity for ChatGPT to contribute significantly to the reconnaissance phase of penetration testing.

The capabilities of ChatGPT in natural language processing and data extraction make it an ideal tool for information gathering and analysis from various sources such as online databases, search engines, network scans, system logs, social media, and domain registration records [5]. By harnessing the strengths of ChatGPT, penetration testers can automate and streamline the reconnaissance phase which enable them to identify potential vulnerabilities and weaknesses, enhance the accuracy and comprehensiveness of the reconnaissance report, reduce the overhead time and resources required to perform manual testing and ultimately improve the overall security poster of an organization.

2. METHODOLOGY

The research analysis employed a case study methodology by selecting various common penetration testing reconnaissance data types that were provided as an input into the artificial intelligence engine known as ChatGPT. The reconnaissance data will provide knowledge needed to guide the later phases of a penetration test such that the test execution and exploitation can be crafted to vulnerabilities and technologies with a greater chance of existing on the target. The types of information that is expected to be retrieved from ChatGPT would provide as much background information about the selected target as possible [6]. This information would include contextual data such as technology stack deployed, vendor relationships, encryption techniques implemented, and network topology. The objective was to gather information crucial for further guidance with the multiple stages of a penetration test.

A structured and strategic approach is critical in order to ensure the efficiency and effectiveness of information gathering as part of implementation of the research methodology for the reconnaissance phase of penetration testing. The research methodology consists of six stages commencing with Planning and Preparation where the scope and objectives of the penetration test were defined. This stage involves the identification of the target system, network, and/or application including the extraction of critical identifiers and the selection of information about the network topology, operating system and applications, online databases, system, logs, user accounts and other publicly available information. This is followed by the Information Gathering stage where the natural language processing capabilities are leveraged in order to retrieve and collect pertinent data from multiple online sources. The analysis and summarization of this information can be supplied to ChatGPT which utilizes the text analysis capabilities and contributes to a nuanced understanding of the findings provided. In the third stage of the reconnaissance stage known as Network Scanning and Discovery, ChatGPT crafts custom queries for network scanning tools such as Nmap which should be followed by a rigorous examination in order to customize the scan results responsible for identification of the potential vulnerabilities. The subsequent phases of Log Analysis use ChatGPT to analyze system logs in order to identify unusual patterns or anomalies that may indicate security threats, Vulnerability Research can research and summarize information about potential vulnerabilities identified during the reconnaissance phase, and Report Generation can help write executive summaries using the gathered information, identified vulnerabilities, and security recommendations through the creation of a comprehensive final automated report.

The following diagram illustrates the six stages of reconnaissance for gathering information and ensuring a comprehensive and methodical examination of the target.

In order to gain better insights into the reconnaissance process for penetration testing, information gathering will benefit from reusable questions constructed in a manner to provide valuable reconnaissance data that can be requested of ChatGPT as part of a standard practice for each assessment performed [7]. From a research perspective, questions had to be tailored in a specific way to obtain information usable for the reconnaissance phase of a penetration test. Substantial trial and error was required as customizing questions requesting specific types of data did not always deliver desirable results.

The research analysis is conducted through a case study methodology by strategizing reconnaissance to enhance penetration testing using ChatGPT. Prompt engineering for ChatGPT is an indispensable skill necessary in order to procure usable information including the reconnaissance research performed for this use case study. Prompt engineering can aid with reconnaissance for penetration testing using ChatGPT in several ways:

1. **Crafting Structured Queries:** ChatGPT provides information in a certain format that can be used as an intel mechanism to retrieve relevant data from online sources which will result in identifying potential vulnerabilities. The quality of responses should be regularly assessed based on the acquired information to probe for further refinement.
2. **Specific Iterative Questioning:** Prompts can be used to generate tailored queries making the process more efficient. For instance, if the initial response is vague, specifying the level of detail required using follow-up prompts to narrow down the information can facilitate comprehensive and accurate responses.
3. **Incorporating Additional Context:** Frame prompts with contextual threat intelligence data in order to accumulate information on possible threats, risks, and attack vectors. For example, inquire about specific security controls, recent vulnerabilities, and/or known issues associated with the target system.
4. **Soliciting Open and Close-Ended Questioning:** The mixed-method approach can provide specific context in order to ensure that ChatGPT combines the open-ended questions for a broader overview delving through in-depth aspects of a particular topic whereas the closed-ended questions can offer intricate details in response to the questions asked. Moreover, detailed exploration of multiple dimensions of reconnaissance data including technical, risk-related, and security related information associated with

the target or a system can provide targeted and meaningful insights for identifying vulnerabilities for penetration testing [8].

The table below outlines the multiple stages and purpose of the reconnaissance process. Each stage represents a crucial step in gathering information about a target system, network, or application to assess its security posture.

Utilizing the current literature from the existing scholarly discourse, this research study leveraged search tools including but not limited to Google Scholar, ResearchGate, IEEE Access, IEEE Xplore, Springer, Taylor & Francis, and the Grover Hermann Library at UC. The objective was to discern pertinent scholarly journal entries, conference proceedings, preprint repositories, and articles. In addition to academic repositories, authoritative independent news articles and blog posts were also considered to supplement the research. The examination process entailed a thorough assessment of each question included in the Results section with the extensive usage of ChatGPT.

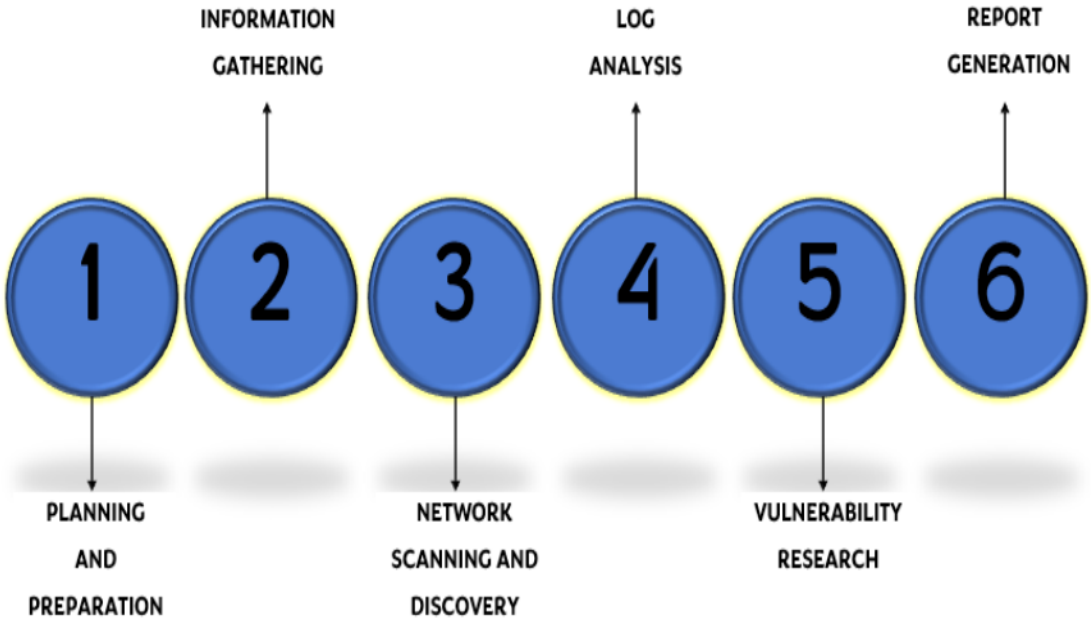

Fig. 1. Six stages of reconnaissance

Table 1. Multiple stages and purpose of the reconnaissance process

Stage	Purpose/Activities
Planning and Preparation	Define the scope and objectives, identify the target, and determine sources of information for the reconnaissance phase.
Information Gathering	Retrieve and analyze information about the target system, network, or application from various online sources.
Network Scanning and Discovery	Generate custom queries for network scanning tools, analyze scan results, and identify potential weaknesses for further testing.
Log Analysis	Analyze system logs, identifying unusual patterns or anomalies that may indicate security threats.
Vulnerability Research	Research and summarize information about potential vulnerabilities identified during the reconnaissance phase.
Report Generation	Automate the generation of a detailed reconnaissance report, summarizing gathered information, vulnerabilities, and recommendations.

3. RESULTS

A significant portion of the information available in ChatGPT regarding the selected target of a penetration test would be considered footprinting. The accumulation of information that can be applied in order to attack a target is known as footprinting [9]. The first technique that will be discussed is obtaining the IP address space utilized by the target organization. It is important to know the full scope of IP addresses used by the target organization as the comprehensive list of IP address ranges represents the attack surface. It is critical to ensure the entire attack surface is included in an assessment as all network nodes could have vulnerabilities that need to be identified. ChatGPT will return a list of IP addresses by asking a question similar to the following: "What IP address range related information do you have on [insert organization name here] in your knowledge base?" A list of IP addresses belonging to the target organization will be returned. These IP addresses will be listed in a classless inter-domain routing (CIDR) format. CIDR addresses concludes with a forward slash and a trailing number [10]. The trailing number following the slash denotes the quantity of IP addresses included in the range.

One of the data points that could be used as part of the reconnaissance phase are domain names. Domain name information provides details that are specific to ownership, registration, name server, IP address, and Domain name Service (DNS) records. Subdomain enumeration can help identify assets related to an organization [11]. ChatGPT will return information on domain names that are actively in use when prompted with the following: "What type of domain name information can you gather on [insert target website here]?" In response to this question, ChatGPT will provide a comprehensive list of information on domain names used by the organization such as primary domain, subdomains, other domains, international domains, generic top-level domains (gTLDs), and subsidiary domains. Acquiring this type of information on domain names can help a penetration tester in mapping out the network through identification of IP addresses with a domain name associated with the organization's infrastructure and discovering potential risks such as vulnerable software components.

Another important piece of information to obtain during reconnaissance is to understand vendor technologies that are used by the penetration testing target [12]. By understanding these technologies, it allows the penetration tester to perform planning on the potential types of vulnerabilities that may be present on the target which in turn will affect the tools to be used as well as the attacks that will be simulated. ChatGPT will provide vendor technologies used by particular website with a question similar to the following: "What vendor technologies does [insert target website fqdn here] make use of on its website?" As response to this query, ChatGPT will provide a variety of different technologies such as the content delivery networks (CDNs), the web server, advertising engines, analytics engines, customer relationship management (CRM) capabilities, and potential marketing automation tools, libraries used, application programming interface (API) technologies deployed, single sign-on (SSO) implementations, technologies for data exchange and integration.

Sensitive data consists of data such as passwords, account numbers, personal identification numbers (PINs), and personal health information. In order to ensure the continued privacy of this information, it must be secured while at rest or in motion [13]. Websites do this through security control referred to as encryption. It is possible that the websites could be misconfigured to use a weak SSL version, or a weak cipher which would allow a malicious actor to view sensitive information. ChatGPT can provide details about the encryption security by submitting a question as follows: "Provide a comprehensive list of SSL ciphers based on your research used by [insert target website fqdn] in pursuant to your large corpus of text data present in your knowledge base." ChatGPT would respond to this request with a list of SSL ciphers such as AES128_GCM_SHA_256, AES_256_GCM_SHA_384 to name a few as well as certificate authority issuers like DigiCert and Extended Validation (EV) Certificates. The penetration tester will need to understand which ciphers have deficiencies as some can result in issues that can put sensitive data at risk [14].

Deprecated versions of SSL/TLS present the possibility that malicious actors can decrypt data transmitted between clients and servers [15]. As this vulnerability could lead to sensitive information becoming compromised, it is critical that a secure version of SSL/TLS is implemented. ChatGPT can provide information related to SSL/TLS versions by asking a question similar to "What kind of SSL version related information can you provide on [insert target

website here]?" ChatGPT will return a list of SSL/TLS versions used by the target website which may include but not limited to TLS 1.0, 1.1, 1.2 & 1.3, SSL 3.0 and widely used encryption standards such as Perfect Forward Secrecy (PFS), HTTP Strict Transport Security (HSTS), Application-Layer Protocol Negotiation (ALPN), Elliptic Curve Cryptography (ECC), Public Key Pinning (PKP), Certificate Transparency (CT), Rivest-Shamir-Adleman (RSA) Encryption, Online Certificate Status Protocol (OCSP) Stapling, Forward Secrecy with DHE and ECDHE using key exchange algorithm such as Elliptic Curve (EC) Diffie-Hellman Ephemeral (DHE).

According to [5], it is important to understand all connectivity to and from a particular website as these relationships can also represent a component of the target's attack surface. From this perspective, links from the target website or to the target website from other related web properties can represent entry points into the target that should be explored during a penetration test [16]. ChatGPT can help with this through a particular question such as: "Please list the partner websites including FQDN based on your research that [insert target website here] has direct links to according to your knowledge base." When receiving this request, ChatGPT will provide the list of partner websites that the selected target website has direct links to.

Reconnaissance can provide additional information that will assist the penetration tester to understand the selected target in more detail in the form of the technology stack [17]. Understanding the technology stack is similar to comprehending the services running as this information provides background necessary to select the specific attacks, exploits, and tools in order to establish objectives and determine the focus in the way of vulnerabilities. ChatGPT can assist with providing information about a selected target's technology stack by asking a question similar to "Provide a vendor technology stack based on your research that is used by [insert organization name here]." The type of information that will be returned may include application server type, database type, operating systems, big data technologies, logging and monitoring software and other infrastructure related information specific to the organization. These vendor technologies usually improve the performance and reliability of the target website or protect its digital infrastructure [18]. The output generated by ChatGPT can include several vendor technologies such as Akamai, Amazon Web Services (AWS), Cisco, Microsoft, Salesforce, Oracle, SAP, Google, and Workday.

During a penetration test, knowledge of network protocols that can be easily exploited and carry a high degree of risk is vital [19]. The network protocols used by a target can be expended to establish an initial foothold into the organization's network and potentially could lead to direct access to sensitive information as well as the ability to laterally move within the target's network. ChatGPT can provide a list of network protocols with a request such as "Provide a list of network protocols related information that is available on [insert organization name here]." From this question, ChatGPT will return a list of network protocols used by the target organization which potentially could include protocols such as Hyper Text Transfer Protocol (HTTP) and Hyper Text Transfer Protocol Secure (HTTPS), Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), Network Time Protocol (NTP), Secure Shell (SSH), Border Gateway Protocol (BGP), Simple Network Management Protocol (SNMP), Transmission Control Protocol (TCP) & User Datagram Protocol (UDP), Internet Protocol Version 4 (IPv4), Virtual Private Network (VPN).

4. DISCUSSION

The primary purpose of this research was to understand and assess how ChatGPT can deliver high- quality information that can be used to assist penetration testers with the reconnaissance phase of a penetration test. The reconnaissance phase used by penetration testers serves the dual purpose of identifying potential vulnerabilities within the system and focusing on specific areas that might attract threat actors [20]. This distinction is crucial because penetration testers generally have a finite amount of time to perform a test in contrast to real threat actors who generally have indefinite amounts of time. Due to the remarkable growth of artificial intelligence, the capacity to streamline laborious and repetitive tasks within penetration testing has significantly expanded. For instance, ChatGPT possesses the potential to produce shell commands, code fragments, and even mimic social engineering attacks allowing penetration testers to allocate their attention to the more intricate facets of the testing process.

ChatGPT possesses an exceptional ability to understand natural language inputs allowing for intuitive, user-friendly queries and providing

contextually relevant information [21]. In this study, it was determined that ChatGPT has the ability to provide valuable insight into the deployment of the target organization's technology stack as well as specific information about web applications deployed by the target organization. This included information about the overall attack surface as well as insights into specific web properties. Another important reminder is that ChatGPT can provide additional information on any question by prompting the word "continue" and this may retrieve additional information containing the desired response. All of these will assist a penetration tester in the reconnaissance phase as such to enable them to perform appropriate planning relative to the technologies discovered as well as the potential vulnerabilities that could exist in the target's environment [22]. A penetration tester's cognitive thinking formed by experience can result in the tester discovering hard-to-find or complex issues using ChatGPT which can serve as a motivation for the usage in the field of penetration testing including reconnaissance. This planning can include the selection of tools to be used while executing the penetration test, the configuration of certain tests, and the selection of specific exploits to be performed.

Findings from this research indicate that multiple types of information can be returned from ChatGPT such as the IP address range used by the target organization, the SSL/TLS versions as well as cipher suites enabled to protect data in transmission, the vendor partner websites that are linked from the selected target's websites, the technology stack used by the target and the network protocols enabled by the target organization. This background information provides a large amount of data needed to perform reconnaissance in order to prepare for the next phases of a penetration test [23]. The efficiency of the reconnaissance phase is therefore greatly improved as ChatGPT consolidates together capabilities found today in several different tools.

The research performed on ChatGPT required trial and error in the prompting as certain requests can either be outright rejected or may result in responses that do not contain usable data for the reconnaissance phase of a penetration test. However, the research also revealed challenges as certain requests to ChatGPT were rejected or yielded responses lacking usable data for reconnaissance. Over time, the model generated invalid responses emphasizing the need for penetration testers to carefully structure their questions for effective results. Research on reconnaissance using ChatGPT can continue by selecting additional types of reconnaissance data needed in specific penetration test scenarios [24]. The study performed during this research concentrated on obtaining some reconnaissance data that is useful in most scenarios to represent examples of ChatGPT's capabilities. The set of reconnaissance information that could be gathered from ChatGPT can be greatly expanded on for a wide range of penetration testing scenarios in the future. An additional item that can be further examined is prompt research into the language that will assist in ensuring appropriate responses can be retrieved from ChatGPT [9].

The collaborative efforts between AI models like ChatGPT and human penetration testers can result in a more comprehensive and robust approach to cybersecurity. Integrating the cognitive thinking of experienced penetration testers with the analytical capabilities of ChatGPT can lead to the discovery of nuanced vulnerabilities that might be challenging to identify through automated processes alone. While ChatGPT exhibits notable capabilities, it is necessary for penetration testers to refine their questioning techniques in order to ensure relevant and accurate responses [3]. The iterative nature of trial and error in the research process emphasizes the dynamic relationship between human input and AI output. Moreover, the discussion about ChatGPT's ability to provide information on SSL/TLS versions, cipher suites, vendor partner websites, and technology stacks demonstrates the diverse range of data that can be extracted. In addition, the adaptability of ChatGPT in delivering information such as details about cloud services, network configurations, or even social engineering risks could further solidify its role as a valuable tool in the hands of penetration testers [25]. This variety of information equips penetration testers with a comprehensive understanding of the target environment enabling them to make informed decisions during subsequent testing stages.

5. CONCLUSION

The synergy of AI in web application penetration testing holds substantial potential for enhancing security and efficiency and explores how ChatGPT's capabilities can be harnessed to optimize the reconnaissance phase, providing

valuable insights for improved planning and enhanced security in penetration testing scenarios. This research presents some observations regarding penetration test reconnaissance from ChatGPT and highlights some of the insights that can be gathered about penetration testing targets. Information gathered can be used directly for planning the next phase of a penetration test and can provide some meaningful insights that a penetration tester would have previously needed to use multiple tools to obtain and possibly would not have been able to acquire very easily. The results of this research indicate ChatGPT is a valuable tool for the reconnaissance phase of penetration test given the insightful information that can be returned. ChatGPT is continually being trained and therefore responses can change over time especially regarding security details of organizations targeted for a penetration test. This requires penetration testers to be flexible and determined when tailoring prompts in order to procure the desired results pertaining to reconnaissance related information. The research suggests promising avenues for further exploration. The focus on specific penetration test scenarios and the identification of additional types of reconnaissance data can contribute to a more nuanced understanding of ChatGPT's capabilities. Additionally, delving into the nuances of language prompts can enhance the reliability of responses and streamlining the interaction between human testers and the AI model. In addition, the information received through this research is meant to be the inception for reconnaissance with ChatGPT and built on over time as it has been proven that ChatGPT does add value for maximizing penetration testing success with respect to research of selected targets.

DISCLAIMER

This paper is an extended version of a preprint document of the same author.
The preprint document is available in this link: https://www.researchsquare.com/article/rs-2707376/v1
[As per journal policy, preprint article can be published as a journal article, provided it is not published in any other journal].

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ACKNOWLEDGEMENTS

I want to extend my heartfelt appreciation to Chris Howser whose significant contribution was instrumental in every stage of the research. Chris graciously dedicated his time and expertise offering invaluable feedback on my research question and methodology. His astute insights and constructive suggestions motivated me to enhance the robustness of my arguments and explore the research more profoundly. Chris' encouragement pushed me to strive for excellence and I am truly grateful for his steadfast support and guidance without which completing this research would not have been possible.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Aljanabi M, Ghazi M, Ali AH, Abed SA. ChatGPT: Open possibilities. Iraqi Journal For Computer Science and Mathematics. 2023;4(1):62-64.
Available:https://doi.org/10.52866/ijcsm.2023.01.01.0018
2. Bahrini A, Khamoshifar M, Abbasimehr H, Riggs RJ, Esmaeili M, Majdabadkohne RM, Pasehvar M. ChatGPT: Applications, opportunities, and threats. In 2023 Systems and Information Engineering Design Symposium (SIEDS). IEEE.2023; 274-279.
3. Chowdhary A, Huang D, Mahendran JS, Romo D, Deng Y, Sabur A. Autonomous security analysis and penetration testing. 16th International Conference on Mobility, Sensing and Networking (MSN). 2020;508-515.
Available:https://doi.org/10.1109/msn50589.2020.00086
4. Dash B, Sharma P. Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review. International Journal of Engineering and Applied Sciences. 2023;10(1).
5. Denis M, Zena C, Hayajneh T. Penetration testing: Concepts, attack methods, and defense strategies. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT); 2016.

Available:https://doi.org/10.1109/lisat.2016.7494156

6. Gupta M, Akiri C, Aryal K, Parker E, Praharaj L. From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and Privacy. IEEE Access. 2023;11:80218–80245. Available:https://doi.org/10.1109/ACCESS.2023.3300381
7. Gundu T. Chatbots: A framework for improving information security behaviours using ChatGPT. In international symposium on human aspects of information security and assurance. Cham: Springer Nature Switzerland. 2023;418-431.
8. Hadi M, Najm M. Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. Sci. Arch. 2023;4:276-285.
9. Iqbal F, Samsom F, Kamoun F, MacDermott Á. When ChatGPT goes rogue: exploring the potential cybersecurity threats of AI-powered conversational chatbots. Frontiers in Communications and Networks. 2023;4.
10. Javaid M, Haleem A, Singh RP. A study on ChatGPT for Industry 4.0: Background, potentials, challenges, and eventualities. Journal of Economy and Technology. 2023;1:127-143.
11. Kalla D, Kuraku S. Advantages, disadvantages and risks associated with ChatGPT and AI on cybersecurity. Journal of Emerging Technologies and Innovative Research. 2023;10(10).
12. Khadka B, Aryal R. ChatGPT: Applications, opportunities and challenges. International Journal of Advances in Engineering and Management (IJAEM). 2023;5(11):396-407. Available:https://doi.org/10.35629/5252-0511396407
13. Langford T, Paynen B. Phishing faster: Implementing chatgpt into phishing campaigns. In Proceedings of the Future Technologies Conference Cham: Springer Nature Switzerland. 2023; 174-187
14. Mateo E. A deep dive into artificial intelligence and its integration into cybersecurity (Doctoral dissertation, Utica University), ProQuest; 2023.
15. Merve Ozkan-Ozay, Akin E, Aslan Ö, Selahattin Kosunalp, Iliev T, Stoyanov I, Beloev I. A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEE Access. 2024;12:12229–12256. Available:https://doi.org/10.1109/access.2024.3355547
16. Mihai IC. The Transformative impact of artificial intelligence on cybersecurity. Int'l J. Info. Sec. & Cybercrime. 2023;12(9).
17. Mijwil M, Aljanabi M. Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. Iraqi Journal For Computer Science and Mathematics. 2023;4(1):65-70. Available:https://doi.org/10.52866/ijcsm.2023.01.01.0019
18. Moatsum Alawida, Sami Mejri, Mehmood, A., Belkacem Chikhaoui, & Oludare Isaac Abiodun. A comprehensive study of ChatGPT: Advancements, limitations, and ethical considerations in natural language processing and cybersecurity. Information. 2023;14(8):462–462. Available:https://doi.org/10.3390/info14080462
19. Muna Al-Hawawreh, Ahamed Aljuhani, Yaser Jararweh. Chatgpt for cybersecurity: Practical applications, challenges, and future directions. Cluster Computing. 2023;26. Available:https://doi.org/10.1007/s10586-023-04124-5
20. Prasad SG, Sharmila VC, Badrinarayanan MK. Role of artificial intelligence based chat generative pre-trained transformer (ChatGPT) in Cyber Security. IEEE Xplore; 2023. Available:https://doi.org/10.1109/ICAAIC56838.2023.10141395
21. Qammar A, Wang H, Ding J, Naouri A, Daneshmand M, Ning, H. Chatbots to ChatGPT in a Cybersecurity Space: Evolution, Vulnerabilities, Attacks, Challenges, and Future Recommendations. arXiv; 2023. Available:https://doi.org/10.48550/arxiv.2306.09255
22. Saraswathi VR, Ahmed IS, Reddy SM, Akshay S, Reddy VM, Reddy SM. Automation of recon process for ethical hackers. IEEE Xplore. 2022;1-6. Available:https://doi.org/10.1109/ICONAT53423.2022.9726077
23. Sebastian G. Do ChatGPT and other AI chatbots pose a cybersecurity risk? International Journal of Security and Privacy in Pervasive Computing. 2023; 15(1):1–11.

Availablehttps://doi.org/10.4018/ijsppc.320225

24. Suthar F, Khanna S. Analysis of Network Vulnerability through Pen Testing. Indian Journal of Cryptography and Network Security (IJCNS). 2021;1(1):2582–9238. Available:https://www.ijcns.latticescipub.com/wpcontent/uploads/papers/v1i1/A1404111121.pdf

25. Svendsen A, Garvey B. (Prompt-engineering testing ChatGPT4 and Bard for assessing Generative-AI efficacy to support decision-making.SSRN; 2023.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/112467