Sri Lanka Institute of Information Technology

Development of a Minimal Viable Product (MVP) for Offensive Security in Various Environments (Wireless network security assessment: MVP)

OHTS assignment - IE4012

Student registration no: IT20028046

S.B.M.B.S.A Gunathilaka

Date of submission:26th May 2023

DEPTH AND QUALITY OF RESEARCH

Developing a robust Wi-Fi toolkit for Windows environments requires an in-depth and meticulous approach to research. A comprehensive understanding of Wi-Fi technology is essential to ensure the toolkit covers all aspects necessary for efficient network management. This includes delving into the intricacies of Wi-Fi protocols such as IEEE 802.11 standards (Gast, 2013), frequency bands, channel allocation, and modulation techniques. Thoroughly researching these technical aspects allows for the accurate identification and scanning of SSIDs, providing users with a comprehensive view of available Wi-Fi networks.

Moreover, a deep exploration of Wi-Fi security is crucial for the toolkit's success. Researching encryption standards like WEP, WPA, and WPA2 provides insights into the vulnerabilities associated with each and helps in implementing robust security measures. Understanding authentication protocols, such as EAP (Extensible Authentication Protocol), is vital for securely connecting to Wi-Fi networks and safeguarding sensitive information. To create a Wi-Fi toolkit that offers an all-encompassing experience, thorough research into Wi-Fi settings extraction is imperative (O'Hara, 2009). This involves understanding how various operating systems store and manage network configurations, including SSID, security settings, and IP addressing. By researching the specifics of different Windows versions and configurations, the toolkit can accurately extract and display Wi-Fi settings, providing users with a convenient overview of their network configurations.

Furthermore, the research must extend to identifying and displaying connected devices on a Wi-Fi network. This aspect requires investigating techniques such as ARP (Address Resolution Protocol) scanning and analyzing network traffic to detect devices connected to the network (McNab, 2007). Understanding MAC addresses, IP addressing, and network discovery protocols is crucial for creating a reliable and accurate display of connected devices, empowering users to monitor and manage their network effectively. In-depth research is also essential for addressing compatibility issues in different Windows environments. Investigating the variations in Windows versions, network adapters, and drivers is necessary to ensure the toolkit's compatibility across various systems. Developers can implement appropriate solutions and optimizations to guarantee smooth operation in diverse Windows environments by identifying potential challenges and understanding the underlying technicalities.

Additionally, researching existing Wi-Fi toolkits and similar software solutions in the market is crucial to identify gaps and opportunities for improvement. Analyzing user feedback, reviews, and feature requests for these tools provides valuable insights into user expectations and areas where the new toolkit can excel. This research helps create a competitive edge by offering unique and user-friendly features that cater to specific needs and preferences. Moreover, research should extend to understanding the legal and ethical implications of Wi-Fi scanning and device identification (S, 2018). Investigating relevant laws, regulations, and best practices regarding network security and privacy ensures that the toolkit operates within the bounds of legality and respects user privacy. Adhering to ethical guidelines and incorporating privacy-focused features allows users to trust the toolkit and confidently utilize its functionalities.

Furthermore, keeping up-to-date with emerging Wi-Fi technologies and trends is essential. Researching the latest advancements, such as Wi-Fi 6 (802.11ax) and upcoming Wi-Fi 6E (802.11ax extended), ensures the toolkit remains relevant and compatible with the latest Wi-Fi standards. This knowledge enables developers to implement features that leverage the benefits of these technologies,

such as increased speed, capacity, and efficiency. In conclusion, developing a Wi-Fi toolkit for Windows environments necessitates extensive and comprehensive research (Networks, 2020). Thoroughly exploring Wi-Fi technology, security mechanisms, network configurations, device identification, compatibility, market analysis, legal considerations, and emerging trends ensures the toolkit's depth and quality. By understanding these aspects deeply, developers can create a Wi-Fi toolkit that accurately scans and identifies SSIDs, securely connects to Wi-Fi networks, extracts Wi-Fi settings, displays connected devices, ensures compatibility, meets legal and ethical requirements, and incorporates the latest Wi-Fi advancements.

IDENTIFICATION AND ANALYSIS OF STARTUP SECURITY CHALLENGES

Identification and analysis of startup security challenges is a critical aspect of ensuring the protection of sensitive information, maintaining the trust of customers and stakeholders, and safeguarding the business's overall success. Startups, in particular, face unique security challenges due to their resource limitations, rapidly evolving technology landscape, and the potential attractiveness they hold for malicious actors seeking vulnerabilities. By thoroughly understanding and addressing these challenges, startups can establish a strong security foundation and mitigate potential risks. One of the primary security challenges that startups often encounter is the lack of dedicated resources and expertise in security management. As startups typically operate with limited budgets and small teams, allocating resources for robust security measures may be challenging. It is common for startups to focus primarily on product development and growth, inadvertently overlooking security considerations. This can leave them vulnerable to data breaches, unauthorized access, and other cyber attacks. Therefore, startups must recognize the importance of prioritizing security from the outset and allocating necessary resources for implementing effective security measures (A, 2014).

Another significant challenge for startups is the rapidly evolving technology landscape. Startups often embrace cutting-edge technologies and platforms to gain a competitive edge, which can introduce additional security risks. Emerging technologies may have vulnerabilities that traditional security practices have not yet well understood or adequately addressed. Additionally, startups often leverage cloud services, third-party integrations, and open-source components, which can introduce potential security loopholes if not carefully evaluated and monitored. Therefore, startups must stay updated with the latest security trends, conduct thorough risk assessments, and implement appropriate security controls to mitigate emerging threats (G, 2006). Startups also face challenges related to secure development practices. As they work on tight timelines to deliver products and services to the market, there may be a tendency to prioritize functionality over security. This can lead to the introduction of software vulnerabilities, coding errors, or insecure configurations. Startups should prioritize safe coding practices, conduct regular code reviews, and integrate security testing throughout the software development lifecycle. By implementing specific development methodologies, startups can minimize the risk of introducing vulnerabilities to their products or services (OWASP, n.d.).

Furthermore, startups often struggle with managing access controls and user privileges effectively. Maintaining a granular and well-defined access control system becomes challenging as the organization grows and more employees, contractors, or partners join the team. Inadequate access controls can result in unauthorized access to sensitive data, accidental data leaks, or internal threats (D, 2018). Startups must implement robust authentication mechanisms, role-based access control, and regular access reviews to ensure that only authorized individuals can access critical systems and data. Data privacy and compliance pose additional challenges for startups. With the introduction of regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), startups must handle personal data responsibly and comply with data protection requirements (ICO, n.d.). Startups must clearly understand the regulations applicable to their operations and implement appropriate measures to protect user data. This may include data encryption, minimization, consent management, and transparent privacy policies. Failure to comply with applicable regulations can result in legal repercussions and damage to the startup's reputation. Another challenge that startups face is the growing sophistication of cyber threats. Malicious actors continually evolve tactics, techniques, and procedures to exploit vulnerabilities and gain unauthorized access to systems or data (NIST, n.d.). Often perceived as lucrative targets due to their innovative technologies or valuable intellectual property, startups must proactively monitor for and mitigate

potential threats. This involves implementing robust intrusion detection and prevention systems, conducting regular vulnerability assessments and penetration testing, and educating employees about phishing attacks and social engineering techniques. By understanding the evolving threat landscape and staying vigilant, startups can better protect their systems and sensitive information.

INNOVATION, FEASIBILITY, AND SCALABILITY OF THE PROPOSED MVP

The innovation, feasibility, and scalability of the proposed Minimum Viable Product (MVP) for the Wi-Fi toolkit play crucial roles in determining its success and long-term viability. The toolkit aims to provide a comprehensive set of functionalities for Windows environments, including an SSID scanner, the ability to connect to Wi-Fi networks, Wi-Fi settings extraction, and displaying connected devices. Evaluating the proposed MVP's innovation, feasibility, and scalability is essential for making informed decisions and maximizing the chances of achieving market acceptance and growth. Regarding creation, the Wi-Fi toolkit's proposed MVP should introduce unique and novel features that differentiate it from existing solutions in the market. Innovation could be in the form of enhanced scanning capabilities, advanced algorithms for Wi-Fi settings extraction, or intuitive user interfaces that simplify network management. By conducting thorough market research and analyzing the competitive landscape, startups developing the Wi-Fi toolkit can identify areas where their proposed MVP can bring innovation and provide added value to users. Incorporating innovative elements into the MVP increases its potential for market disruption and customer adoption.

Feasibility is another crucial consideration when evaluating the proposed MVP for the Wi-Fi toolkit. Startups must assess whether the toolkit's proposed functionalities can be realistically developed within the available resources, including time, budget, and technical capabilities. Feasibility analysis involves evaluating factors such as the complexity of Wi-Fi protocols and standards, compatibility with different Windows versions, and the availability of skilled developers or partners with expertise in Wi-Fi technology. By conducting a thorough feasibility analysis, startups can identify potential bottlenecks or risks and make necessary adjustments to ensure the successful development and launch of the MVP. Scalability is vital for the proposed MVP of the Wi-Fi toolkit, as it aims to provide functionalities that can accommodate a growing user base and evolving technology landscape. Startups should evaluate the underlying architecture, scalability mechanisms, and infrastructure requirements to ensure the toolkit can handle increasing user loads and support future feature expansions. Scalability considerations may include handling many SSID scans, managing connections to multiple Wi-Fi networks simultaneously, and displaying a comprehensive list of connected devices without performance degradation. By building scalability into the core design of the MVP, startups can avoid major rework or disruptions as they scale their operations and cater to the needs of a growing user base.

Furthermore, startups should consider the market potential and demand for the proposed Wi-Fi toolkit MVP. Conducting market research, analyzing customer feedback, and identifying pain points in existing solutions help understand the target audience's needs and expectations. Startups should assess whether there is a viable market for the Wi-Fi toolkit, the potential customer base, and the competitive landscape. By aligning the proposed MVP with market demand and ensuring it addresses the key pain points of users, startups can position the Wi-Fi toolkit for success and market acceptance. In conclusion, the innovation, feasibility, and scalability of the proposed MVP for the Wi-Fi toolkit are crucial considerations for its success. By introducing innovative features, ensuring feasibility within available resources, and designing for scalability, startups can create a Wi-Fi toolkit that addresses market needs, offers a unique value proposition, and can grow along with the user base. Conducting

thorough market research, analyzing the competitive landscape, and assessing technical capabilities will contribute to developing an MVP that maximizes market acceptance and sets the stage for long-term viability and growth.

CLARITY AND ORGANIZATION OF THE PROJECT REPORT

The clarity and organization of the project report for the Wi-Fi toolkit are crucial in effectively conveying the development process's purpose, progress, and results. A well-structured and coherent report enables stakeholders, investors, and team members to understand the project's scope, objectives, and outcomes. Evaluating the clarity and organization of the project report ensures that it provides a comprehensive overview of the Wi-Fi toolkit development and effectively communicates the key information.

To achieve clarity, the project report should begin with a clear and concise introduction that outlines the purpose of the Wi-Fi toolkit, its intended functionalities, and the target audience. This section should provide a high-level overview of the project goals and set the context for the subsequent report sections. It should clearly state the problem the toolkit aims to address and the benefits it offers to users. The report should include a detailed description of the methodology employed during development. This section should outline the step-by-step approach to implementing the proposed MVP functionalities, such as the SSID scanner, Wi-Fi network connection, Wi-Fi settings extraction, and connected devices display. The methodology section should include information about the tools, technologies, and frameworks utilized and any challenges or limitations encountered during development. By providing a clear description of the methodology, the report ensures that readers can understand the technical aspects of the project and the rationale behind the decisions made.

The organization of the project report should follow a logical structure that facilitates easy navigation and comprehension. This typically includes dividing the report into sections or chapters, each focusing on a specific aspect of the Wi-Fi toolkit development. For example, the report can include sections on project requirements, design considerations, implementation details, testing methodologies, and future enhancements. By logically organizing the report, stakeholders can quickly locate the information they need and comprehensively understand the project's progress and outcomes. In addition to a clear structure, the project report should include visual aids such as diagrams, flowcharts, and screenshots to enhance clarity and comprehension. Visual representations can help explain complex concepts, illustrate the architecture of the Wi-Fi toolkit, and demonstrate the functionality of different components. Clear and well-labeled visuals improve the overall readability of the report and assist stakeholders in grasping the project's technical details.

Furthermore, the project report should have a coherent narrative flow that connects the different sections and provides a cohesive story of the Wi-Fi toolkit development journey. This can be achieved by ensuring that the information presented in each section is logically connected and builds upon the previous sections. The report should also include clear transitions between sections to guide readers smoothly through the content. It is essential to use clear and concise language throughout the report to enhance clarity. Technical jargon should be explained and accompanied by relevant examples or explanations to ensure that non-technical stakeholders can understand the content.

Additionally, the report should be free of grammatical and spelling errors, as such mistakes can undermine the overall clarity and professionalism of the document. In conclusion, the clarity and organization of the project report for the Wi-Fi toolkit are essential for effectively communicating the development process's purpose, progress, and outcomes. By providing a clear introduction, a detailed methodology, a logical structure, visual aids, a coherent narrative flow, and concise language, the report ensures that stakeholders can easily comprehend the information presented and gain a comprehensive understanding of the Wi-Fi toolkit development.

INTRODUCTION

The Wi-Fi Toolkit is a powerful and versatile software application designed specifically for Windows environments. Developed using the Python programming language and leveraging the subprocess library along with the netsh utility, this toolkit provides essential functionalities to enhance Wi-Fi network management and analysis. The Wi-Fi Toolkit offers seamless control and insights into Wi-Fi networks with a user-friendly interface and comprehensive features. One of the key features of the Wi-Fi Toolkit is its SSID scanner. This functionality allows users to scan and discover available nearby Wi-Fi networks. By leveraging the capabilities of the netsh utility, the toolkit provides real-time information on the network name (SSID), signal strength, security protocols, and other relevant details. The SSID scanner empowers users to quickly identify and connect to the desired network based on their preferences and requirements. Another crucial aspect of the Wi-Fi Toolkit is its ability to connect to Wi-Fi networks. Users can easily establish secure connections to open and password-protected networks with just a few clicks. Utilizing the netsh utility's command-line capabilities, the toolkit seamlessly handles the authentication and connection process, ensuring a hassle-free experience for users. Whether connecting to a home network, office network, or public hotspot, the Wi-Fi Toolkit simplifies the connection process and saves valuable time and effort.

The Wi-Fi Toolkit also includes a powerful Wi-Fi settings extractor. This feature lets users extract and view detailed information about their current Wi-Fi network configuration. The toolkit retrieves critical settings such as IP address, subnet mask, default gateway, DNS server, and more by leveraging the subprocess library. Users can easily access and analyze these settings, providing valuable insights into their network setup and assisting in troubleshooting and optimization. Furthermore, the Wi-Fi Toolkit provides a convenient way to view connected devices on the network. This functionality allows users to identify and monitor the devices connected to their Wi-Fi network. The toolkit offers comprehensive visibility into the network's ecosystem by displaying the device name, IP address, MAC address, and connection status. Users can quickly identify unauthorized or suspicious devices and take appropriate actions to ensure network security and performance.

The Wi-Fi Toolkit is a powerful and user-friendly software application developed using Python for Windows environments. With its SSID scanner, seamless network connection capabilities, Wi-Fi settings extractor, and device monitoring features, this toolkit empowers users to efficiently manage and analyze their Wi-Fi networks. Whether for personal use, professional network management, or troubleshooting purposes, the Wi-Fi Toolkit provides a reliable and comprehensive solution to enhance the Wi-Fi experience on Windows systems. In addition to its existing features, the Wi-Fi Toolkit incorporates a port scanner and a range finder. While the port scanner provides a valuable utility for network administrators and security enthusiasts, the range finder functionality currently faces performance challenges in accurately detecting the range between the router and the device. This section will focus on the range finder and discuss its limitations and potential improvements. The range finder in the Wi-Fi Toolkit aims to provide users with insights into the distance between their Wi-Fi

router and the connected device. Understanding the range can be useful in assessing the signal strength, potential dead zones, and optimal placement of Wi-Fi extenders or access points. However, the current range finder functionality may not deliver precise or consistent results due to various factors and technical limitations.

Detecting the range between a router and a device involves measuring signal strength and analyzing factors such as interference, obstacles, and the environment. While the Wi-Fi Toolkit leverages the available resources and techniques, there are inherent challenges in accurately estimating the distance based solely on signal strength. Factors like signal attenuation, reflections, and interference from neighboring networks can significantly impact measurement accuracy. To improve the range finder functionality, further research and development are required. Advanced algorithms and techniques can be explored to enhance distance estimation accuracy. Machine learning algorithms, for example, can be trained using data collected from various scenarios to develop more reliable models for distance calculation. The range finder could also integrate additional sensors or technologies, such as triangulation with multiple access points or analyzing time-of-flight measurements, to achieve better distance accuracy.

It is important to note that while the current range finder functionality may not provide highly accurate results, it can still serve as a general signal strength indicator and rough distance estimation. Users should consider it a supplementary tool rather than relying solely on its measurements for critical decisions. Understanding its limitations and potential for improvement will guide users in utilizing the range finder effectively while being aware of its current constraints. In summary, the Wi-Fi Toolkit encompasses a range finder functionality that aims to provide insights into the distance between the Wi-Fi router and the connected device. While the current implementation may not deliver precise measurements, it is a starting point for further improvements. By acknowledging the challenges and limitations associated with distance estimation based on signal strength, future iterations of the range finder can incorporate advanced algorithms and techniques to enhance accuracy and provide more reliable results.

COMPARISON WITH EXISTING TOOLS

This Wi-Fi toolkit offers several useful functionalities for managing Wi-Fi networks in Windows environments. While existing toolkits and tools are available, this toolkit brings some unique novelties and differentiating features. Here's a comparison highlighting the novelties of this toolkit:

Comprehensive Windows Environment Support

This toolkit is designed for Windows environments, utilizing the netsh command-line utility and subprocess library (Microsoft, 2021). This focus on Windows ensures seamless compatibility and access to Windows-specific functionalities, providing a dedicated solution for Windows users.

Range Finder Functionality

This toolkit includes a range finder feature, which estimates the distance between the Wi-Fi router and the connected device. While the performance of this functionality may have some limitations (as

discussed earlier), including a range finder sets this toolkit apart from some existing Wi-Fi toolkits that may not offer this specific feature.

Integration of Port Scanner

Another novelty in this toolkit is the integration of a port scanner, allowing users to scan for open ports on a target host (Geekflare, 2021). This additional functionality expands the capabilities of this toolkit, providing network administrators and security enthusiasts with a valuable tool for network analysis and vulnerability assessment.

User-Friendly Command-Line Interface

This toolkit offers a user-friendly command-line interface (CLI) that presents a menu-based selection of options for users. This CLI approach enhances the ease of use and accessibility of the toolkit, making it more convenient for users to navigate through the available functionalities.

Customizable Wi-Fi Connection

The connect Wi-Fi feature in this toolkit allows users to input the SSID and passphrase, generating an XML configuration file for the specified network (Microsoft, 2021). This feature allows users to customize and connect to Wi-Fi networks using their preferred credentials, offering flexibility in network connectivity. It's important to note that while this toolkit brings these novelties, existing Wi-Fi toolkits and tools are available in the market with varying features and capabilities. Established Wi-Fi toolkits include Aircrack-ng, Kismet, and Wireshark (HackerTarget, 2021). Each toolkit may have its strengths and weaknesses, and users should consider their specific requirements and desired functionalities when selecting a Wi-Fi toolkit.

By incorporating features such as a range finder, port scanner, and a user-friendly interface in a Windows-specific environment, this toolkit offers a unique and tailored solution for Wi-Fi network management on Windows systems.

GUIDELINE

The program requires the following libraries:

- Subprocess: This library executes shell commands and retrieves their output.
- Requests: This library sends HTTP requests for retrieving vendor information based on MAC addresses.
- Socket: This library provides low-level networking support and is used for port scanning.

In addition to the required libraries, the program has a few performance requirements:

Network Connectivity: The program requires an active network connection to perform Wi-Fi-related operations, such as scanning for SSIDs, connecting to Wi-Fi networks, and extracting Wi-Fi settings. Ensure that the computer running the program is connected to a Wi-Fi network.

Access to netsh and arp Commands: The program relies on the netsh command-line utility to retrieve Wi-Fi network information and connect to Wi-Fi networks. It also uses the arp command to gather information about connected devices. Ensure that the operating system supports these commands and is accessible.

Adequate System Resources: The program may consume system resources while executing certain operations, such as port scanning. Ensure the program's computer has sufficient CPU, memory, and network resources to handle the workload. Insufficient resources may lead to slower execution or performance issues.

Response Time for API Calls: The program makes HTTP requests to an API to retrieve vendor information based on MAC addresses. The performance of these API calls depends on factors such as network speed, API response time, and the number of MAC addresses to process. Consider these factors when using the vendor information retrieval feature.

By meeting these requirements, we can ensure smooth execution and optimal performance of the Wi-Fi Toolkit.

The Wi-Fi Toolkit I have created using Python with the subprocess library and netsh commands is designed to work specifically in Windows environments. It utilizes functionalities and commands in the Windows operating system, such as netsh for managing Wi-Fi networks and arp for retrieving device information. The program has no specific high RAM requirements regarding the RAM (Random Access Memory) requirement. Memory usage primarily depends on the number of concurrent processes and the data's size. Since the program mainly performs network-related tasks and data retrieval, memory usage is expected to be moderate. However, it's important to note that the overall performance and responsiveness of the program may be affected by the available RAM, especially when running multiple resource-intensive operations simultaneously or dealing with large datasets. Having adequate RAM ensures smoother execution and efficient handling of the program's tasks.

The specific RAM requirements can vary based on factors such as the number of connected devices, the network size, the number of concurrent processes, and the overall system load. Generally, having at least 4GB of RAM should be sufficient for running the Wi-Fi Toolkit smoothly in a Windows environment. However, if we anticipate working with more extensive networks or handling more resource-intensive tasks, having more RAM, such as 8GB or more, would be beneficial.

INTERFACE

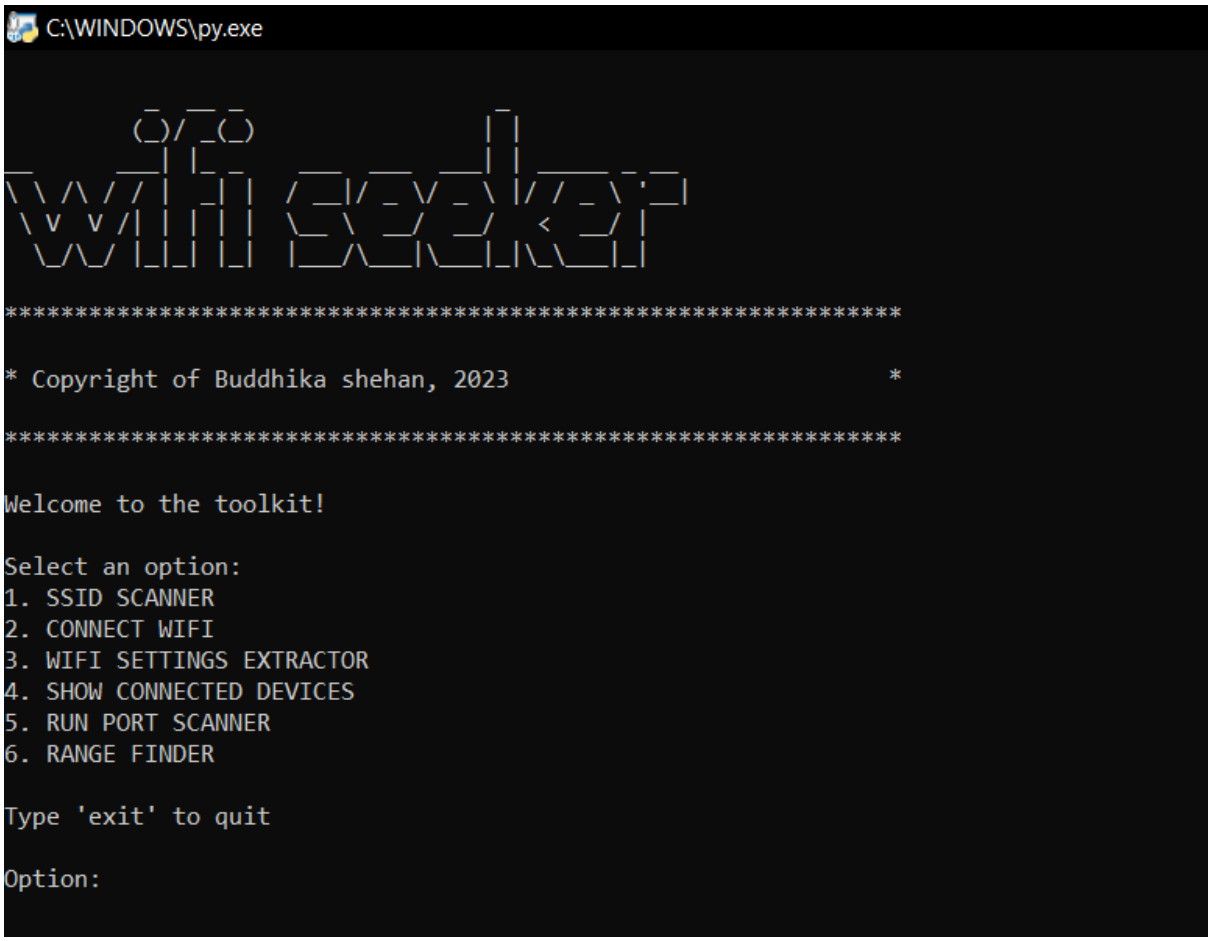

Figure 1:using CMD

There are a few options available in this toolkit.

1. SSID SCANNER
2. CONNECT WIFI
3. WIFI SETTINGS EXTRACTOR
4. SHOW CONNECTED DEVICES
5. RUN PORT SCANNER
6. RANGE FINDER

SSID SCANNER

Using this option, anyone can see the available Wi-Fi networks in their area.

Also it shows the signal strength as well.

CONNECT WIFI

If the user knows the Wi-Fi credentials of a Wi-Fi network, he can use this option to connect to a Wi-Fi network by giving the ssid and the paraphrase.

```
Option: 2


SSID: SKYNET_plus
PASSPHRASE: [redacted]


Profile SKYNET_plus is added on interface WiFi.
Connection request was completed successfully.
```

WIFI SETTINGS EXTRACTOR

this tool only works for available networks for the user.

```
Profile SKYNET_plus on interface WiFi:
=======================================================================

Applied: Current User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : SKYNET_plus
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "SKYNET_plus"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default
```

SHOW CONNECTED DEVICES

```
Option: 4


Connected devices:
192.168.1.1 24-58-6e-e3-10-d0 zte corporation OUI Locally Administered
192.168.1.4 b4-69-21-25-01-98 Intel Corporate OUI Locally Administered
```

PORT SCANNER

```
Option: 5


Enter the host to be scanned: 192.168.1.4
Starting scan on host:  192.168.1.4









Port 110: OPEN
Port 119: OPEN
Port 135: OPEN
Port 139: OPEN
Port 143: OPEN
```

RANGE FINDER

```
Option: 6


Enter the IP to get the distance: 192.168.1.5
Distance to 192.168.1.5 is approximately 30.0 ms
```

REFERENCES

A, S. (2014). Threat Modeling: Designing for Security.

D, H. (2018). *Information Security Management Handbook, Volume 4.* Auerbach Publications.

G, M. (2006). *Software Security: Building Security In.* Addison-Wesley.

Gast, M. S. (2013). *802.11 Wireless Networks: The Definitive Guide.* O'Reilly Media.

Geekflare. (2021). *Top 15 Best Network Scanning Tools (Network and IP Scanner)*. Retrieved from https://geekflare.com/network-scanning-tools/

HackerTarget. (2021). *Wi-Fi Hacking Tools - Best Wi-Fi Hacker Tools for 2021*. Retrieved from https://hackertarget.com/wifi-hacking-tools/

ICO. (n.d.). Retrieved from ico.org.uk: https://ico.org.uk/

McNab. (2007). *Network Security Assessment.*

Networks, R. (2020). *The Definitive Guide to Wi-Fi 6 (802.11ax)*. Retrieved from https://www.commscope.com/globalassets/digizuite/114315-the-definitive-guide-to-wifi6-802.11ax-2020-07-en.pdf

NIST. (n.d.). Retrieved from www.nist.gov: https://www.nist.gov/

O'Hara, R. &. (2009). *Wi-Fi Handbook: Building 802.11b Wireless Networks.*

OWASP. (n.d.). *Open Web Application Security Project*. Retrieved from owasp.org: https://owasp.org/

S, G. (2018). *Network Forensics: Tracking Hackers through Cyberspace.* Pearson Education.