USER MANUAL FOR THE TUI

* **OVERALL USE CASE**

This tool is a perfect start for users who are just beginning with their careers in cybersecurity and aim to learn the practical usage of tools. By creating this tool, we have integrated many existing tools to perform various attacks under one roof, to simplify things for the users and the cybersecurity enthusiasts. Rather than having to run individual commands, we have provided the users with the comfort of selecting the tool by just providing the option index number.

* **INDIVIDUAL TOOL USE CASE**

1. **Get HTTP Header**: The HTTP header is determined while performing web application fingerprinting. By the HTTP header, we can get to know the server version, technology.

Usage:- The user just needs to give the website URL as input to this option, then the header information for the given input is displayed.

1. **UDP scan**: It is used to evaluate the response packets which are sent to ports to determine the availability of the service on the host.

Usage:- The user just needs to give the IP address of the target as input to this option, then the result of the UDP scan for the given input is displayed.

1. **John the ripper tool**: It is an open-source dictionary style password cracker. The prerequisite of this tool includes having a wordlist ready or creating one by yourself. Furthermore, with the help of the wordlist, you perform bruteforce attacks on the target.

Usage:- The user just needs to give the name of the target file as input to this option, then the tool will extract and unzip the input file.

1. **SQLMap**: This tool is used to test a website for SQL Injection vulnerability. Now what is SQL Injection? It is a code injection technique where the attacker injects malicious SQL queries on a vulnerable website to gain access to the database of the website and the information stored in it.

Usage:- The user just needs to give the website URL as input to this option, then the resulting vulnerabilities found out by the tool for the given input is displayed.

1. **DNS Lookup**: All websites on the Internet have a particular DNS. In the worst-case scenario, where a website has no vulnerability, the attacker can try and penetrate inside the DNS server in order to gain access to the website. Therefore, to determine the DNS of a website, DNS lookup tool is used.

Usage:- The user just needs to give the website URL as input to this option, then the DNS information for the given input is displayed.

1. **Reverse IP Lookup**: It is also known as reverse DNS lookup, which is used to determine the domain name associated with an Internet Protocol address.

Usage:- The user just needs to give the website’s IP address as input to this option, then the associated domain name for the given input is displayed**.**

1. **Get Robots.txt file of a website**: The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index. The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents.

Usage:- The user just needs to give the website URL as input to this option, then the HTML DOCYTYPE document for the robots.txt file for the given input is displayed.

1. **IP Locator**: IP Locator helps in mapping of an IP address to the geographical location of the internet from the connected device. It provides you with location information such as the country, state, city, zip code, ISP and other information.

Usage:- The user just needs to give the IP address of a website or a host system as input to this option, then the location information for the given input is displayed.

1. **Host Finder**: It is used to find the host/hosting service of any website.

Usage:- The user just needs to give the website URL as input to this option, then the hosting service information for the given input is displayed.

1. **Recon-ng scan**: It is a tool to perform reconnaissance. Reconnaissance is the first phase of a penetration test and is the act of gathering preliminary data or intelligence.

Usage:- The user just needs to give the name of the workspace he wants to create to work in the recon-ng tool as input to this option, then this tools automatically creates & gets the user into the recon-ng tool interface with the created wordspace.

1. **GeoIP**: GeoIP is used to map the public IP address of a user with their location. The location might not be specific.

Usage:- The user just needs to give the website URL as input to this option, then the GeoIP information for the given input is displayed.

1. **Subnet Finder**: We can use subnet finder to find different subnets inside a specific IP. A subnet maps to different network number and host identifier.

Usage:- The user just needs to give the website URL as input to this option, then the information regarding the sub-domains for the given input is displayed.

1. **Whois Information**: A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name. Typically, each Whois record will contain information such as the name and contact information of the [Registrant](https://www.domaintools.com/support/key-terms-definitions/#registrant) (who owns the domain), the name and contact information of the registrar.

Usage:- The user just needs to give the website URL as input to this option, then the information for the given input is retrieved & displayed from the WHOIS databse.

1. **ARP Scan**: ARP scan allows a user to quickly collect device intel and stealthily. It discovers all IPV4 network connected devices, identify and map IP addresses to MAC addresses.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform ARP scan on the given address as input & display it’s result.

1. **ICMP ECHO Ping Scan:** Ping scans are used to determine if a host is online and responding. ICMP messages are used for this purpose, and hence ICMP ping scans use these types of packets to accomplish this.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform ICMP ECHO Ping scan on the given address as input & display it’s result.

1. **TCP SYN Ping Scan**: It sends a SYN request at a given port on the target host. If the port is open, the target host responds with a TCP SYN/ACK packet indicating that a connection can be established.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform TCP SYN Ping scan on the given address as input & display it’s result.

1. **TCP connect scan:** TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform TCP scan on the given address as input & display it’s result.

1. **Stealth scan:** SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform Stealth scan on the given address as input & display it’s result.

1. **XMAS scan**: These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header. When viewed within Wireshark, we can see that alternating bits are enabled, or “Blinking,” much like you would light up a Christmas tree.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform Xmas scan on the given address as input & display it’s result. If the port is close/filtered then the port will reply with a RST packet.

1. **FIN scan**: An adversary uses a TCP FIN scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the FIN bit set in the packet header.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform FIN scan on the given address as input & display it’s result**.**

1. **Service Discovery scan**: Service discovery is how applications and (micro)services locate each other on a network. Implementations include both a central server(s) that maintain a global view of addresses and clients that connect to the central server to update and retrieve addresses.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform Service Discovery scan on the given address as input & display it’s result. The output of the given option gives the tool user the services associated with different open/filtered ports of the target.

1. **OS Discovery:** As the name suggests, this scan discovers the operating system on which a particular system is running.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform OS Discovery scan on the given address as input & display it’s result. The result output gives the tool user the OS associated with the target.

1. **Display ARP cache table**: Displays and modifies entries in the Address Resolution Protocol (ARP) cache. The ARP cache contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses.

Usage:- The user just needs to give the IP address as input to this option, then the tool will display the ARP cache table of the associated input.

1. **Basic Website scan**: It will perform a basic scan on the webserver with the help of Nikto tool. It is a vulnerability scanner which will point out dangerous files/CGIs, outdated server software which could have vulnerabilities and other problems.

Usage:- The user just needs to give the website’s URL as input to this option, then the tool will perform vulnerabilities scan on the given address as input & display it’s result.

1. **Logs**: A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security.
2. **ARP Spoof**: An ARP spoofing, also known as ARP poisoning, is a Man in the middle (MitM) attack that allows attackers to intercept communication between network devices.

Usage:- The user just needs to give the IP address as input to this option, then the tool will perform ARP spoof attack on the given address as input & display it’s result as sending spoofed ARP requests to the target.

1. **IOT Device scan:** It makes use of the nmap scan to look for any IOT devices connected to the network. It further retrieves all the information of the device.

Usage:- The user just needs to give the IP address of a network as input to this option, then the tool will perform the scan on the given network address as input & display it’s result as explored iOT devices in the network.

1. **Website Footprinting:** Footprinting refers to the act of accumulating data related to a specific network/webiste environment. For website, the footprints involve subdomains, OS details, file name and file path etc.

Usage:- The user just needs to give the website address as input to this option, then the tool will perform footprinting on the given website address as input & display it’s result.

1. **Check for SQL vulnerabilities:** This command will check the website entered by the user for SQL vulnerabilities which can further be exploited by the attackers to gain control of the database of a website by modifying and writing their own SQL queries.

Usage:- The user just needs to give the website address as input to this option, then the tool will perform SQL vulnerability scan on the given address as input & display it’s result as explored SQL vulnerabilities.

1. **Load Balancing information of a website:** Load balancing is the process of distributing network traffic across multiple servers. This ensures no single server bears too much demand. By spreading the work evenly, load balancing improves application responsiveness. It also increases availability of applications and websites for users.

Usage:- The user just needs to give the website address as input to this option, then the tool will perform footprinting on the given address as input & display it’s result of the explored information about the Load Balancers.

1. **Discovery e-mail accounts of a company:** This will present a list of all the email accounts associated with a company. The user will be required to input the URL of the company.

Usage:- The user just needs to give the company’s website address as input to this option, then the tool will perform enumeration on the given address as input & display it’s result.

1. **Discover a website for directories and files:** This will look for important directories and files of a website. These sensitive files should not otherwise be visible to users because it might contain user data and other sensitive information.

Usage:- The user just needs to give the website address as input to this option, then the tool will perform enumeration on the given address as input & display it’s result of explored hidden files & directories.

1. **Mirroring a website:** When you mirror a website, you download a copy of the files that make up a website and then host this mirror website. You can then use this mirror website for phishing attacks.

Usage:- The user just needs to give the website’s address as input to this option, then the tool will perform the mirroring of the website and store it’s output in the tool’s parent directory.

1. **Embedding a text in a picture using Steganography:** This tool will embed your secret message into an image file using Steganography. You can then send this image to the destination so that the actual text message stays hidden.

Usage:- The user just needs to give the secret message, name of the image file in which you need to imbed the text as input to the interface & also give a password to it in order to retrieve it in future. The resulting encrypted image will be saved in the tool’s parent directory.

1. **Retrieving a text from an image:** This tool will retrieve the hidden message embedded in an image using reverse Steganography.

Usage:- The user just needs to give name of the image file from which you need to extract the text as input to the interface & also give a password to it in order to retrieve it. The resulting encrypted message will be displayed on the terminal.

1. **LLMNR/NBT-NR poisoning:** By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.

Usage:- The user just needs to give the IP address of a host as input to this option, then the tool will perform the scan on the given input & display it’s result.

1. **Email account footprinting:** Email tracking is used to monitor the delivery of emails to an intended recipient. Attackers track emails to gather information about a target recipient to perform social engineering and other attacks.

Usage:- The user just needs to give the IP address of a host as input to this option, then the tool will perform the e-mail footprinting on the given address as input & display it’s result.

1. **Create a customized dictionary:** This tool is used to create a custom dictionary to perform dictionary brute-forcing attacks.

Usage:- The user just needs to give the characters of the resultant dictionary, minimum length, maximum length of the resulting words in the dictionary, the name of the resulting dictionary file.

1. **Exit:-** This option of the tool will make the user exit from the TUI.

Usage:- The user just needs to select the option number in order to exit from the TUI.