

EzSec Manual

EzSec utilizes tools that need to be installed on the computer before it is ready to run.

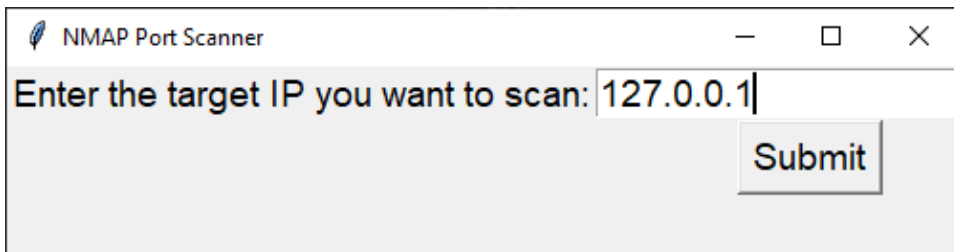
Software Dependencies

1. Nmap-python
 - a. Instructions to install: <https://pypi.org/project/python-nmap/>
2. Scapy
 - a. Instructions to install: <https://scapy.readthedocs.io/en/latest/installation.html>
 - b. Scapy also uses Python 3.9. It is necessary to have Python 3.9 installed and the interpreter for your IDE set to Python 3.9
 - i. Link to install Python 3.9: <https://www.python.org/downloads/release/python-390/>
3. Wireshark
 - a. Wireshark is not necessary for the program to run. However, it is used for the pcap file for Scapy.
 - b. Link to install Wireshark: <https://www.wireshark.org/download.html>
4. Hashcat
 - a. Instructions to install: <https://github.com/bannsec/hashcat>
5. Sublist3r
 - a. Instructions to install: <https://github.com/aboul3la/Sublist3r>

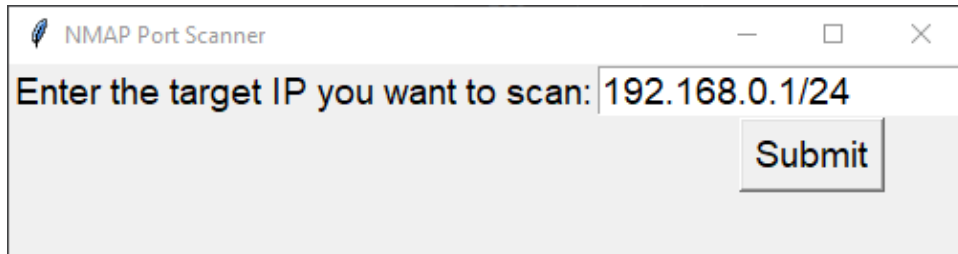
NMAP Function:

The NMAP function is used to scan a network and test for open ports on different hosts. The NMAP function in EzSec does not require any input besides the network location you are trying to scan. It will automatically check for open ports.

- 1) After choosing the NMAP function you will need to input an IP address. This IP address can be a single IP or a range of IPs based on CIDR notation as below:
 - a. Single IP



- b. CIDR Notation:



NMAP Port Scanner

Enter the target IP you want to scan: 192.168.0.1/24

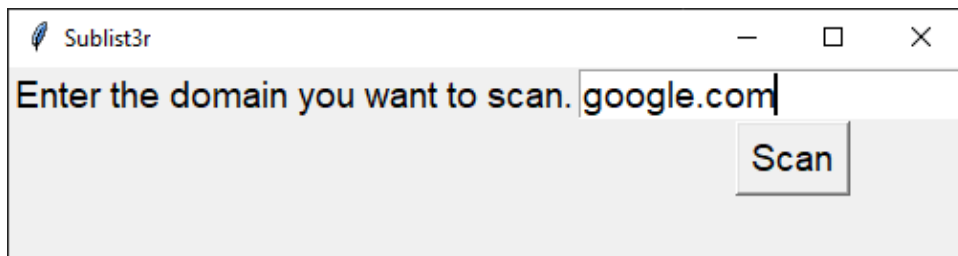
Submit

- c. Once the scan is complete you will receive a notification of where the results are stored.

Sublist3r Function:

Sublist3r is used for domain enumeration. It lists all subdomains so that cyber security engineers are aware of the possible attack surface. In EzSec Sublist3r only requires the domain. All other options for the command are hard coded for ease of use.

1. After choosing the Sublist3r function you will receive a popup requesting a domain name.



Sublist3r

Enter the domain you want to scan: google.com

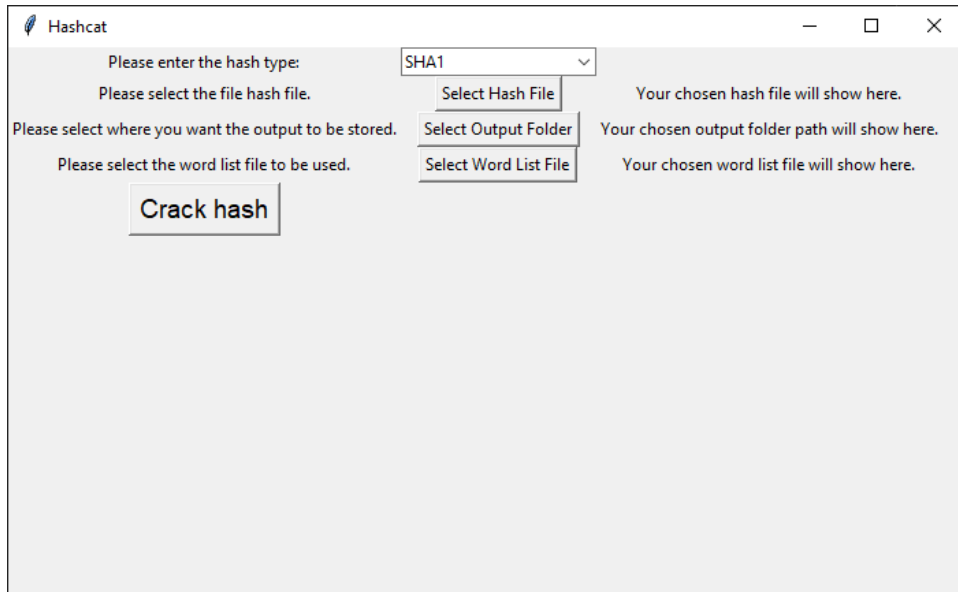
Scan

2. After pressing scan Sublist3r will begin to work and popup a notification once complete. This notification also tells you where the output is stored.

Hashcat Function

Hashcat is used to crack hashes for testing purposes. Also testing the strength of the hash and the password.

1. After choosing the Hashcat function you will be prompted with the below screen asking for user input:

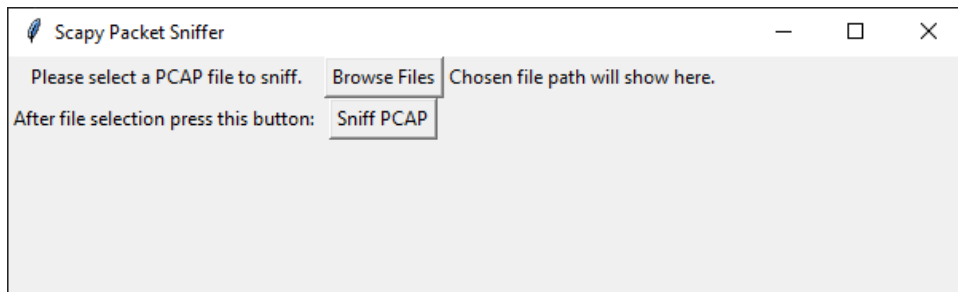


2. The first option is to choose the hash type from available hash types (SHA1, SHA256, SHA512, MD5 & NTLM).
3. Next you must submit the file that contains the hashed output.
4. The folder where you would like to output the results.
5. Lastly the word list file. We recommend using this word file: <https://github.com/praetorian-inc/Hob0Rules/blob/master/wordlists/rockyou.txt.gz>
6. After cracking the hash it will display results to your desired output folder.

Scapy

Scapy is a tool that allows for parsing through pcap files to export into an easier format to read. When opening the Scapy function the you will receive a window to upload a pcap. This is why it states in the above instructions it is good to have Wireshark installed.

1. When clicking on the Scapy function you will receive this below prompt.



2. After selecting a PCAP file and sniffing the PCAP the results will be output to a text file.
3. Once the process is complete a popup will occur stating where the results are saved.