PROJECT NAME : nmapAutomator

nmapAutoMater : A script that you can run in background

FEATURES :

1.Quick : Shows all open ports quickly (~30 sec)

2.Basic : Runs Quick scan ,then runs a more through scan on found ports(~5 mins)

3.UDP : Runs “Basic” on UDP ports (~ 5-7 mins)

4.FULL : Runs a full range port scan ,then runs a through scan on new ports (~ 8 mins)

5.Vulns : Runs CVE scan and nmap vulns scan on all found ports (~ 12 mins)

6.Recon : Runs “Basic” scan if it doesn’t run then runs recon (~ 20 mins)

7.ALL : Runs all the scans consecutively.

I make the script as efficient as possible ,that user can get the result as soon as possible.

Requirements :

Gobuster v3 or higher.

You can update Gobuster in kali-

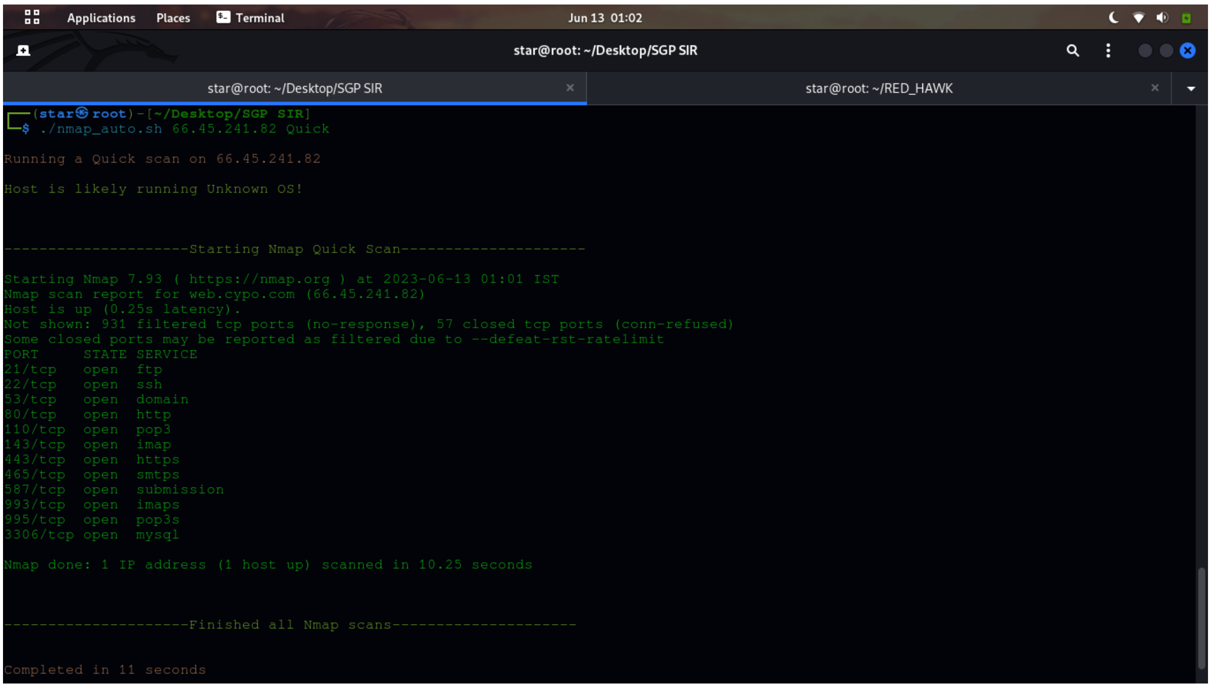
1. Sudo apt-get update
2. Sudo apt-get install gobuster --only upgrade

Other recon tools used within the script
1.nikto
2.sslscan
3.nmap vulns
4.joomscan
5.wpscan
6.droopescan
7.smbmap
8.enum4linux
9.dnsrecon
10.odat

Example of use:

$ chmod +x nmap_auto.sh

$ ./nmap_auto.sh <TARGET IP> <TYPE>



```
┌──(star㉿root)-[~/Desktop/SGP SIR]
└─$ ./nmap_auto.sh 66.45.241.82 Quick

Running a Quick scan on 66.45.241.82

Host is likely running Unknown OS!



---------------------Starting Nmap Quick Scan---------------------

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-13 01:01 IST
Nmap scan report for web.cypo.com (66.45.241.82)
Host is up (0.25s latency).
Not shown: 931 filtered tcp ports (no-response), 57 closed tcp ports (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 10.25 seconds



---------------------Finished all Nmap scans---------------------


Completed in 11 seconds
```

BETTER TO EXPLAIN:

The provided script is a bash script that appears to be a port scanning tool based on Nmap. It takes two command-line arguments: the target IP address and the type of scan to perform. The script defines various functions for different types of scans, such as quickScan, basicScan, UDPScan, fullScan, vulnsScan, and recon.

Here is a breakdown of the script's main parts:

- The script starts by defining some color codes for output formatting.
- The usage function displays information about how to use the script, including the available scan types.
- The header function displays information about the target IP, the detected OS, and the scan type.
- The assignPorts function assigns port values based on the scan results.
- The checkPing function checks if the target IP is responsive by sending a ping request.

- The checkOS function determines the operating system based on the TTL value from the ping response.
- The cmpPorts function compares the basic ports with all ports and generates a list of extra ports.
- The various scan functions (quickScan, basicScan, UDPScan, fullScan, vulnsScan) perform different types of scans using Nmap with different options.
- The recon function suggests reconnaissance commands and prompts the user to choose which commands to run.
- The reconRecommend function provides recommendations for reconnaissance commands based on the scan results.

It's important to note that running port scans or any type of network scanning without proper authorization may be illegal and unethical. Make sure to obtain proper permissions and follow the laws and guidelines of your jurisdiction before conducting any scanning activities