**Get from user a network to scan**

A screen shot of a computer

Description automatically generated

Using if else statement to check if the user input matches the format of a network (numbers 0-9, minimum of 1 and maximum of 3 characters, with a separator . after the first 3 sets). Program to exit if the input is invalid.

**Get from user a name for the output directory**

A screen shot of a computer

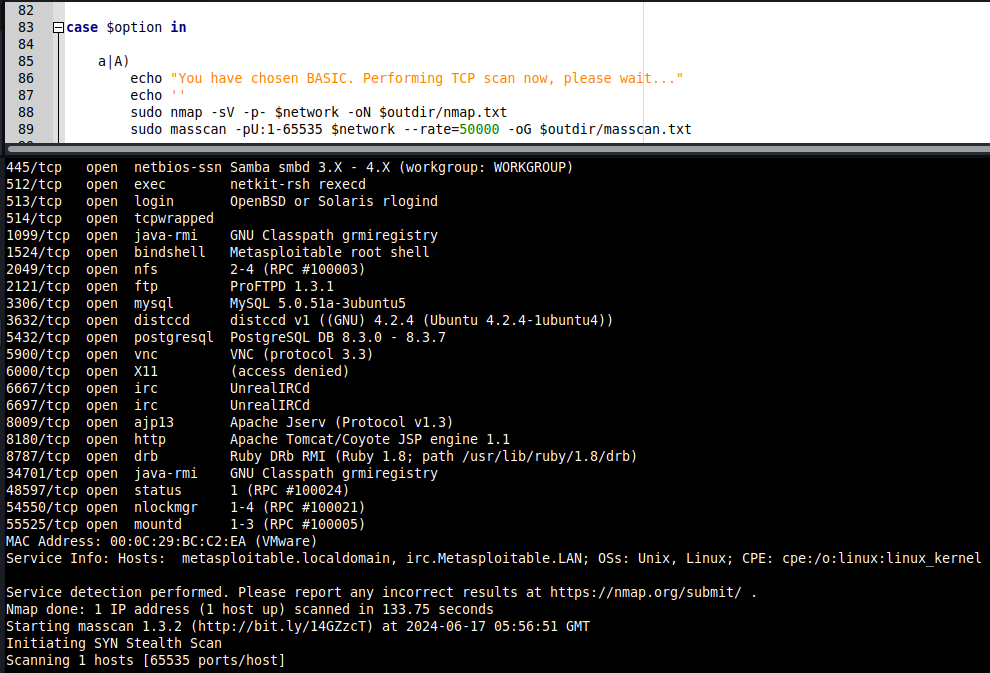
Description automatically generated

**Allow the user to choose ‘Basic’ or ‘Full’**

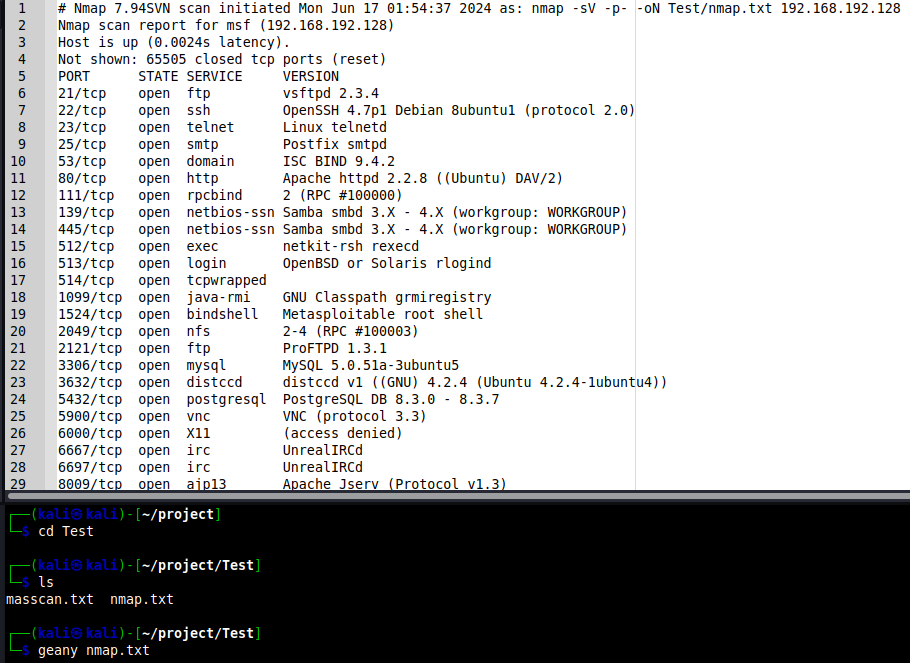
A screenshot of a computer program

Description automatically generated

Using case to provide user with options of Basic or Full scan. Case insensitivity for options A and B. All other inputs will prompt the program to exit.

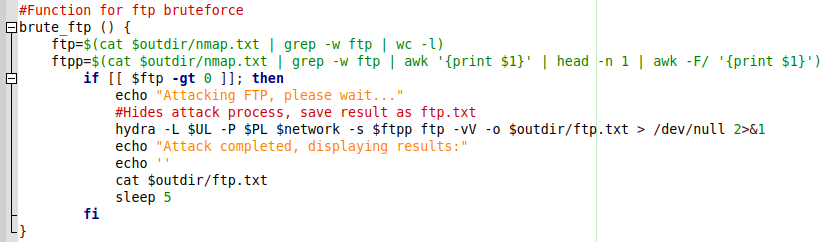
**Basic Scan**

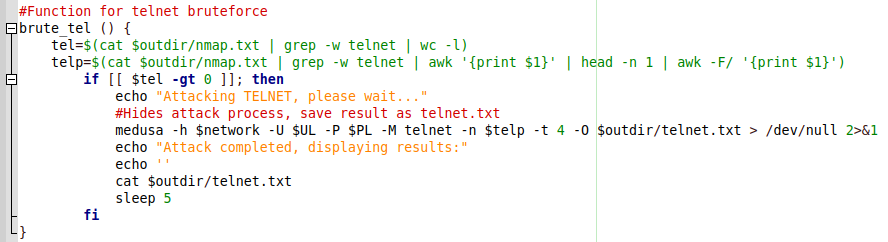
Using nmap -sV for TCP and service version scan. Output saved in normal format. For UDP, masscan is used and output is saved in greppable format. Both files are saved to the previously provided output directory.

A screenshot of a computer

Description automatically generated

**Weak Passwords**

A computer code with text

Description automatically generated with medium confidenceA computer code with text

Description automatically generated with medium confidenceA black screen with text

Description automatically generatedA black background with white text

Description automatically generated

Functions are defined at the start of script to be called upon to check for available services (FTP, SSH, Telnet, RDP). To check if the service is open, an if statement will check from the nmap result for the specific keyword. A wc -l will be performed for word count. If it is available, the word count would be more than 0, starting the brute force process. Telnet uses medusa instead, as hydra is unstable for Telnet brute-forcing. If services are found during nmap scans, they will be tested for weak passwords. Attack process hidden to declutter the user’s screen. Attack result shown after attack is completed. Results are all saved in the specified output directory.

**Full Scan**

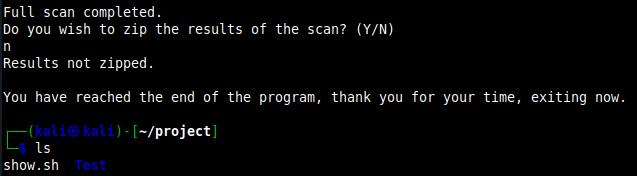
A screen shot of a computer screen

Description automatically generated

The only add on from the Basic scan is the vulnerability assessment. Vulners script used to produce results. Again, results are saved in the specified output directory. Only exploitable results are shown on screen to prevent information overload.

**Allow to save all results into a zip file**

**A screenshot of a computer program

Description automatically generated**

At the end of the script, an option is provided for the user to zip the result.

**References**

Ask Ubuntu. (n.d.). *Hiding output of a command*. [online] Available at: https://askubuntu.com/questions/474556/hiding-output-of-a-command [Accessed 17 Jun. 2024].