**CFC 090423**

**PENTEST PROJECT**

**VULNERABILITY**

**GAN LAI SOON S19**

**Project report**

**Introduction:**

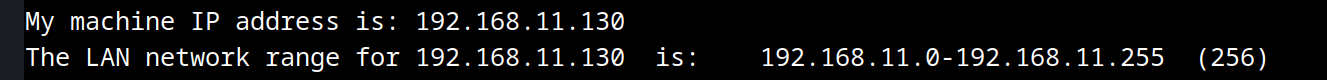
The project aims to enhance our ability to understand mapping of host machines within our local network and possibilities vulnerabilities that they have while running various network services.

For learning purposes, I will be using the Kali Linux machine and metasploitable machine (msf) to run the script.

In addition, attached will be ‘user.lst’ – a username list and ‘passwordlist.txt’ – a password list to run the bruteforcing in the script. For learning purposes, the username and password list I created will be short as the bruteforcing will take very long if the lists are long.

A screenshot of a computer

Description automatically generated



The commands and the results show my machine Ip address as well as the LAN network range.

<https://www.commandlinux.com/man-page/man1/hostname.1.html>

From the above link, I discover the command hostname -i can also display my kali Linux own Ip address.

A screen shot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

The detection of 3 live hosts is up

A white background with red and blue text

Description automatically generated

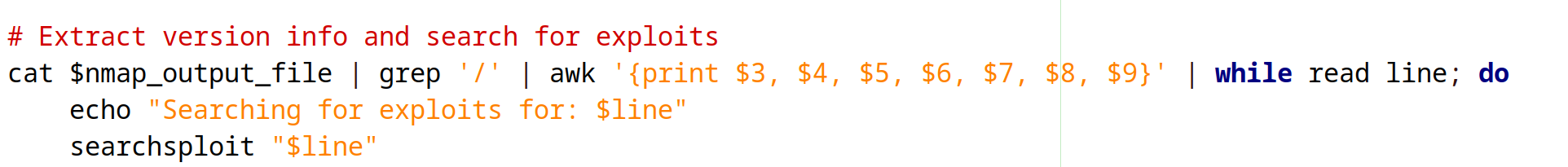
Running Nmap scans for each live hosts

A computer screen with white text

Description automatically generated

A computer screen shot of a computer program

Description automatically generated



As the output file from the Nmap scans is not a log file, we have to grep and awk and print the relevant fields for searchsploit to exactly scan the service names.

<https://www.cyberciti.biz/faq/unix-howto-read-line-by-line-from-file/>

Running searchsploit scans for each live host

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

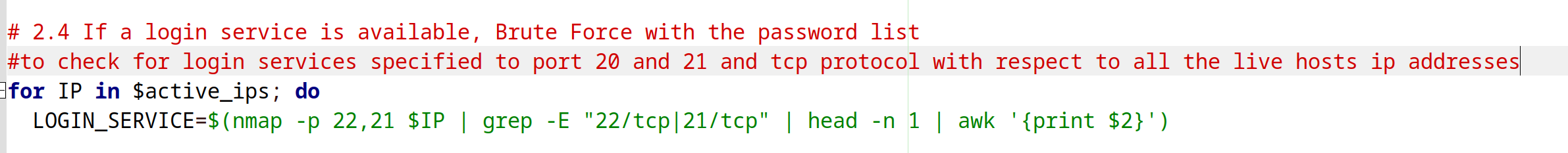
A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

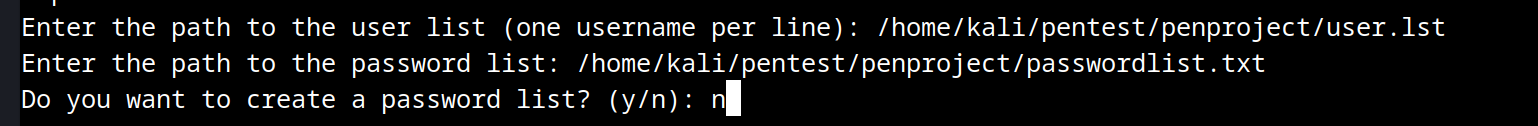
From searchsploit, above are the possible vulnerabilities in the metaploitable machine.



A black background with white text

Description automatically generated

There are no login services available for the 2 Ip addresses as stated above except for 192.168.11.134 which is the metasploitable machine where brute forcing is carried out.



Here brute forcing is carried out using the username list and password list which I have created, and results of successes are shown below. To run the brute forcing, make sure to key the correct paths where the username list and the password list are saved at.

2 services – ssh and ftp are being brute forced.

A computer screen shot of text

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

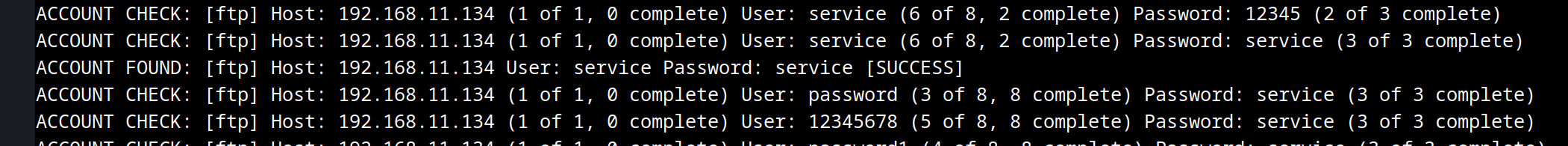
Using the created password list to bruteforce

A computer screen shot of text

Description automatically generated/

A screen shot of a computer screen

Description automatically generated



Results above show successful brute force on both ftp and ssh services with the user self-created password list.

A screen shot of a computer

Description automatically generated

Here we have an option to allow the user to key the relevant Ip address and a report based on nmap scans will be generated.

A screenshot of a computer screen

Description automatically generated

A number on a black background

Description automatically generated

A white screen with text

Description automatically generated with medium confidence

References:

<https://www.geeksforgeeks.org/tee-command-linux-example/>

With the tee command, we can display the output of the command as well as save it to the file.

Scan reports based on the Nmap scans of each possible live hosts are also generated within the same folder. Running the files will show their respective Nmap scan results.

Conclusion:

This project clarifies the possible vulnerabilities of host machines within our own network.

The scripting challenges us to automate the mapping and scanning process of the hosts, the services run and possible vulnerabilities that can exist. The scripting process lets us explore the various pen testing tools that we can attempt to incorporate to run scans on the hosts discovered. I was able to appreciate the significance of functionalities of such tools.

In addition, it also made me realize how possible vulnerabilities open opportunities for hackers to gain unlawful access to the host machine easily.

The project has been very instrumental in building up my understanding of network security in terms of host discovery and the vulnerabilities they could have while running various services on them. This has been very meaningful where it is insightful how much possible critical information can be gained from the scanning of machines.