**CFC 090423**

**SOC ANALYST PROJECT**

**SOC CHECKER**

**GAN LAI SOON S19**

**Project report**

**Introduction**

This project aims to allow a user to choose between various attacks on a remote machine though an automatic attack system. Once an attack is chosen, it will be executed and logged for analysis.

For the purpose of the project and learning, I will be using my kali linux (192.168.11.130) machine as well as the MSF metalsploitable(192.168.11.134) machine.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Here I have created host discovery in mine local network.

In addition, I have created 3 types of attacks for a user to select from; from which they can choose the host they want to execute that attack on.

A screenshot of a computer

Description automatically generated

So, we know that the only probable ip addresses that we can choose to attack is 192.168.11.134

The 2>/dev/null is to filter out the the error messages from the sudo arp-scan –localnet command to dev/null.

<https://serverfault.com/questions/1074648/what-is-the-meaning-of-the-dev-null-21-in-a-cronjob-entry#:~:text=It%20means%20that%20stderr%20(%202,issued%20by%20the%20executed%20command>.

grep -oE '\b([0-9]{1,3}\.){3}[0-9]{1,3}\b' as taught in class was to filter only the ip addresses from the command output

**Types Of Attack**

Choosing attack 1: port scan using nmap

A black background with white text

Description automatically generated

A close-up of a computer error

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

**The results of the scan as above**

for learning purposes, I am only executing a scan of the first 100 ports

A black background with white text

Description automatically generated

A black screen with white text

Description automatically generatedrunning the attacks.log file in the /var/log folder will show the logs registering the attack of the nmap port scan

**Choosing attack 2 : FTP Brute-force using Hydra**

A screenshot of a computer

Description automatically generated

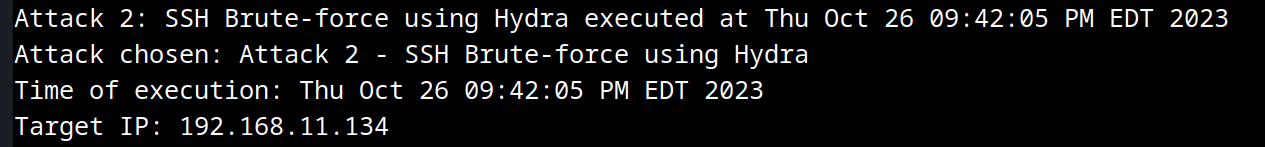
A computer screen shot of a program

Description automatically generated

For learning purposes, I will be using password and username: service which was previously cracked with john the ripper in Pentesting class

A screen shot of a computer code

Description automatically generated



Like attack1 , the logs for attack2 are registered and logged as shown

**Choosing attack 3: (Port Scanning using Masscan)**

A black screen with white text

Description automatically generated  
A screenshot of a computer error

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

The logs of the masscan attack are registered and logged in the var/log folder as well

Separately, I also saved the output of the massscan in the current folder where the script is run.

A black screen with white text

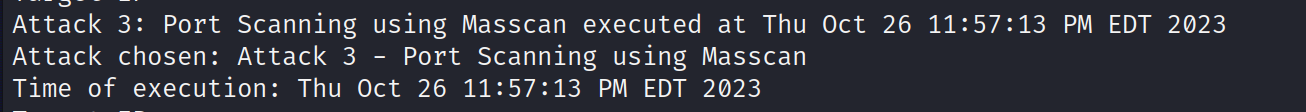
Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated



Above screenshot shows the results of the masscan saved in the current folder as well as a log saved in /var/loh/attacks.log

**Conclusion:**

This project provides a valuable learning experience in terms of possible attacks on remote machines.

This project focuses on scripting with functions; where it provides an option to make choices between the attacks that was offered to the user. Through this scripting, I am better equipped to understand the various forms of attacks carried on a host machine. Such an automatic system makes me realize the importance of staying alert during an attack.

The project opened my eyes to the possible vulnerabilities between network interactions between client and server in the real world and the crucial work done by SOC teams in protecting such critical infrastructure.

This hands-on experience had strengthened my understanding of network vulnerabilities and attacks and importance they played in the defense of our digital world today.