CYBERIUM ARENA

SIMULATOR

PROJECT

PENETRATION TESTING

VULNER

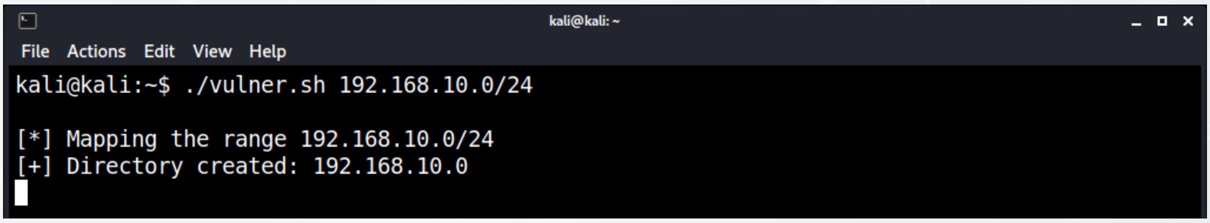
Objective

Create a script that maps network devices for ports, services, and vulnerabilities.

Functions

1. Getting the user input

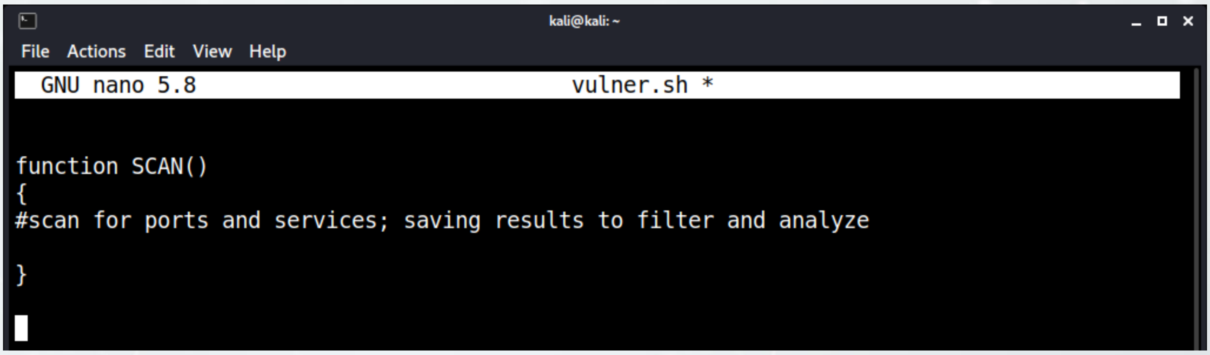
The user enters the network range, and a new directory should be created.



```
kali@kali:~$ ./vulner.sh 192.168.10.0/24

[*] Mapping the range 192.168.10.0/24
[+] Directory created: 192.168.10.0
```

2. Mapping ports and services

The script scans and maps the network, saving information into the directory.
Available tools: nmap, masscan

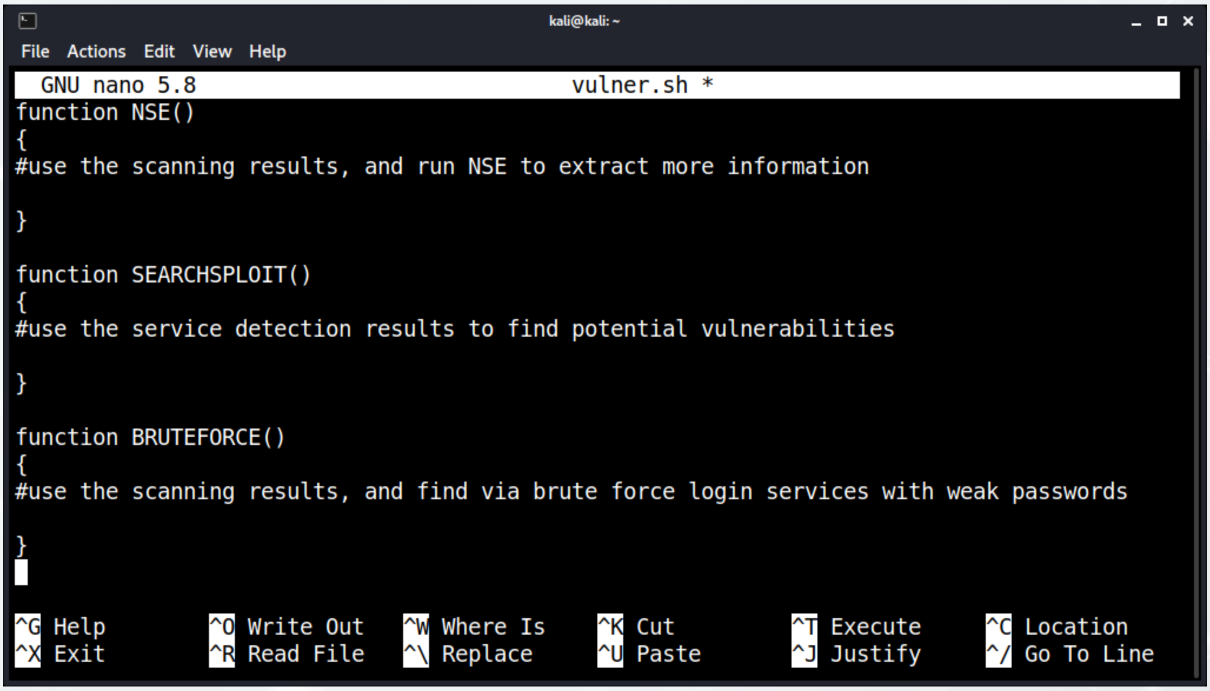


```
  GNU nano 5.8                          vulner.sh *


function SCAN()
{
#scan for ports and services; saving results to filter and analyze

}
```

3. Mapping vulnerabilities

The script will look for vulnerabilities using the **nmap scripting engine**, **searchsploit**, and **finding weak passwords** used in the network.

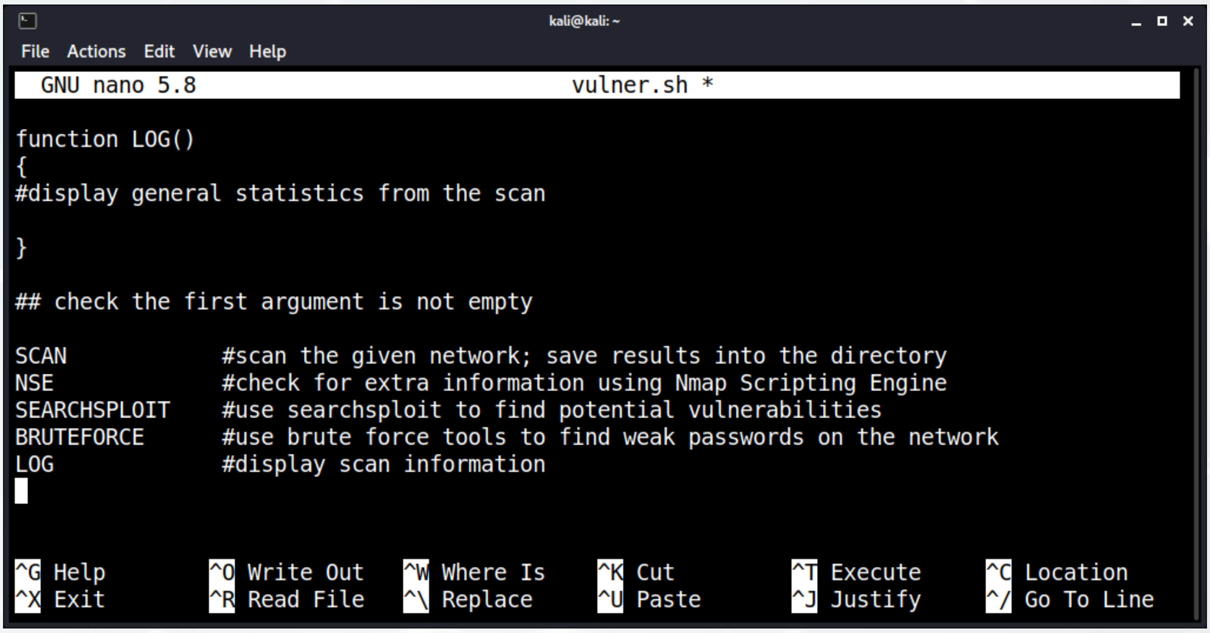
Available tools: nmap, searchsploit, hydra, medusa



```
  GNU nano 5.8                              vulner.sh *
function NSE()
{
#use the scanning results, and run NSE to extract more information

}

function SEARCHSPLOIT()
{
#use the service detection results to find potential vulnerabilities

}

function BRUTEFORCE()
{
#use the scanning results, and find via brute force login services with weak passwords

}

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

4. Displaying results

At the end of the scan, show the user the general scanning statistics.



```
 GNU nano 5.8                          vulner.sh *

function LOG()
{
#display general statistics from the scan

}

## check the first argument is not empty

SCAN            #scan the given network; save results into the directory
NSE             #check for extra information using Nmap Scripting Engine
SEARCHSPLOIT    #use searchsploit to find potential vulnerabilities
BRUTEFORCE      #use brute force tools to find weak passwords on the network
LOG             #display scan information


^G Help       ^O Write Out   ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File   ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

Comments

1. Use comments in your code to explain.
2. If you are using code from the internet, add credit and links.

Submitting

1. Submit the source code (.sh) and a pdf file with the screenshots proving the functions work.
2. Send the project to the trainer email.
3. In the email subject type **project: Vulner <student name>**.