REPORT ASSIGNMENT 2 – GROUP 51

Name of students:

- *Kambakhsh Jafari*
- *Ngoc Xuân Thu Dinh*

Programme: Health Informatics

Contents

Introduction

This report is comprised of a few chapters. Chapter 1 declares the main framework we will follow for penetration testing and the strategies used for gaining access to the system. Chapter 2 reports detailed steps in texts and screenshots of each strategies and its results. Chapter 3 demonstrates steps for obtaining the flags in the Metasploitable system and cracking passwords of Super Users. In Chapter 4, we will discuss our conclusions of the assignment.

Chapter 1: Design

Since we know that the system exists (with provided IP address) and some minimal information (Metasploitable), we assumed that this exercise is the first level – "External attacker with no knowledge of the system" (1, p. 828). Our goal for this penetration test is to gain access to the target system and to collect secret information (four flags), username and password of SuperUsers.

Here are our design plan adapted from Bishop (1, p.830) and Kenedy et al. (2, p.3):

1. **Intelligence gathering:** We will run scans of the targeted system to collect more information about it, such as ports, protocols, OS , services and their versions. In this assignment we will use Nmap because we have familiarized ourselves with it during the Assignment 1. This step is the crucial for all strategies (2, p. 18).
2. **Hypothesis**: We will use information collected from the scan results to identify vulnerabilities and to plan for different approaches. We will research the vulnerabilities through various sources such as books, blog posts and exploit database. Each approach will be reported with details in Chapter 2. Our potential approaches are:
    a. Finding a vulnerable services that can help enabling us to initiate a backdoor
    b. Finding vulnerable services that allow us to execute remote arbitrary commands to gain access to the system
3. **Exploitation**: Testing the approaches on Armitage to see if the vulnerabilities can be exploited
4. **Post Exploitation**: During this phase, by interacting with the target system through Shell, we will try to escalate privilege if we have not during the previous phase. With Super User privileges, we will explore the system and find as many flags as possible. We will also look into etc/shadow where the hashes values of passwords located, and use John the Ripper to find these passwords.

Chapter 2: Experiment results

1. Intelligence gathering

In Kali Linux terminal, we ran several scans with different options, one of them was `sudo nmap -sS -sV -A` on our target `10.11.203.107` to know more about TCP connection, service version detection, operating system detection and version detection on the IP address of our target. We specified `-A` for a more detailed and comprehensive result, `-sS` for a stealthier and less likely to be detected by the system, and `-sV` to determine the versions of services (3).

```
# Nmap 7.94 scan initiated Sun Dec 10 15:18:13 2023 as: nmap -sS -sV -A -oN nmap0612.txt 10.11.203.107
Nmap scan report for 10.11.203.107
Host is up (0.00054s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.11.202.234
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-12-10T20:25:46+00:00; +7m12s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

Figure 1: One of our nmap scan results

2. Hypothesis – Exploitation

Strategy 1: Vsftpd 2.3.4 backdoor

After scanning the system, Nmap showed us that TCP port 21 uses the vsftpd 2.3.4 service. This is a known vulnerability for UNIX operating systems in the "Exploit Database" (7). It can be used for exploiting through backdoor. Our hypothesis is that we can exploit our target using this exploit.

On Armitage, we used the exploit `unix/ftp/vsftpd_234_backdoor` with `RHOSTS` as `10.11.203.107` and successfully initiated a backdoor, resulting an interacting Shell on the target. With this exploitation, we directly gained root access on the target, so there was no need for a privilege escalation step. Using the command window, we could be able to explore all files and directory in the target system, which helped us obtain all the flags in Chapter 3 and read the `etc/shadow` file.

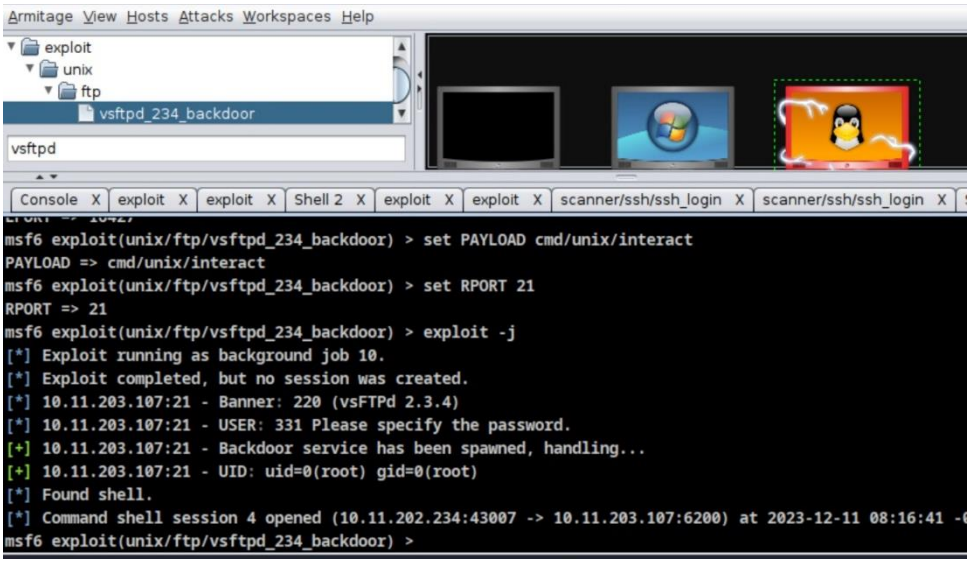

Figure 2: Using vsftpd 2.3.4 backdoor

Strategy 2: Samba usernamemap_script

Nmap also showed that the target was using Samba version 3.0.20, which is vulnerable to remote arbitrary commands with root privileges (4).

On Armitage, we searched for exploit `multi/samba/usermap_script` and with this exploit, we successfully gained a shell on the target with root privilege. Similarly to Strategy 1, we could obtain all flags and shadow file.

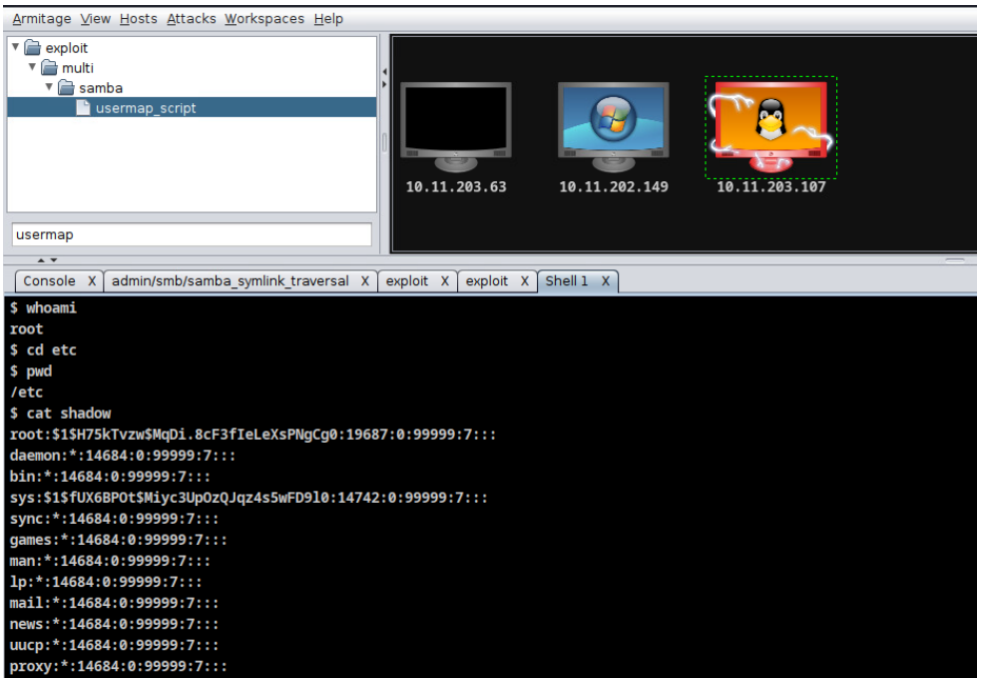

Figure 3: Using Samba usermap_script exploit to gain root access

Strategy 3: DistCC_exec

This strategy came up after another scan with `nmap -Pn -n -p- 10.11.203.107` to see if we missed something in previous scans. And we could see that the port 3632 was open and running `distccd` service.

```
1 # Nmap 7.94 scan initiated Sun Dec 10 16:38:26 2023 as: nmap -Pn -n -p- -oN nmap0712.txt 10.11.203.107
2 Nmap scan report for 10.11.203.107
3 Host is up (0.00058s latency).
4 Not shown: 65506 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE
6 21/tcp    open  ftp
7 22/tcp    open  ssh
8 23/tcp    open  telnet
9 25/tcp    open  smtp
10 80/tcp   open  http
11 111/tcp  open  rpcbind
12 139/tcp  open  netbios-ssn
13 445/tcp  open  microsoft-ds
14 512/tcp  open  exec
15 513/tcp  open  login
16 514/tcp  open  shell
17 1099/tcp open  rmiregistry
18 1524/tcp open  ingreslock
19 2049/tcp open  nfs
20 2121/tcp open  ccproxy-ftp
21 3306/tcp open  mysql
22 3632/tcp open  distccd
23 5432/tcp open  postgresql
24 5900/tcp open  vnc
25 6000/tcp open  X11
26 6667/tcp open  irc
27 6697/tcp open  ircs-u
28 8009/tcp open  ajp13
29 8180/tcp open  unknown
30 8787/tcp open  msgsrvr
```

Figure 4: Nmap scan reveal distccd

Then, we tried the exploit `unix/misc/distcc_exec` on Armitage and gained a Shell as user `daemon`. We are aware that a privilege escalation has to be perfomed at this point. However, due to the limited time and instruction to not modify the system, we decided to not go for privilege escalation. During our exploitation, using the command `uname -a`, we discovered this server was running an old version of Linux kernel (2.6.24). This version is vulnerable to exploit such as DirtyCow (6) which would allow us to escalate privilege if we were allowed to download and execute code to the system and modify the access control.

With daemon privilege, we were able to access the etc folder and open all the files that contain our flags (`SuperSecretInformatiom`, `.HiddenSecretInformation`, `motd` and `passwd`). However, daemon cannot read `etc/shadow`. Therefore, with this strategy we could obtain all flags, but not the passwords.

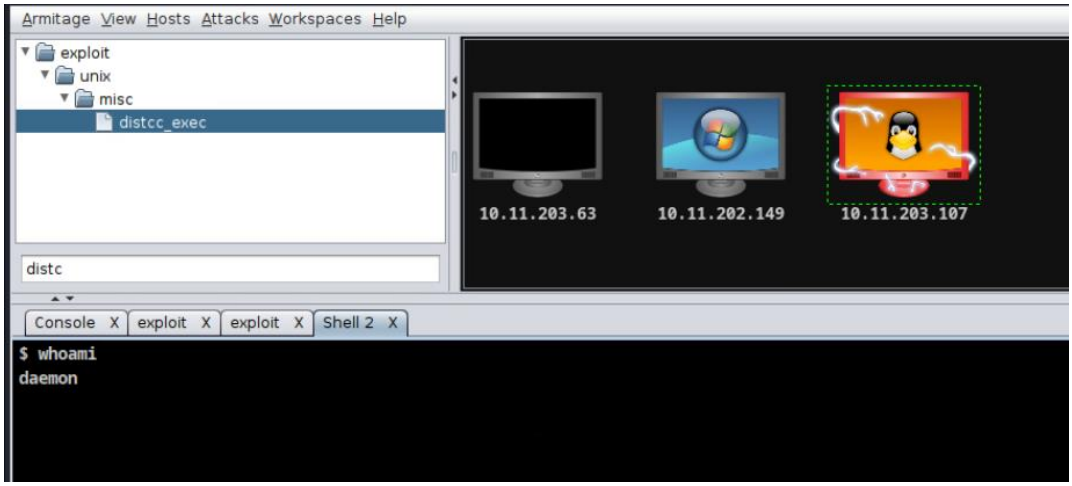

Figure 5: Gaining Shell as daemon

Chapter 3: Capture the flags

After locating to `etc` folder, we used the command `ls -lsa` to see information detailed information about each file and directory, including permissions, number of links, owner, group, size, and the timestamp of the last modification, and especially the file with "." in front of it. We immediately spot the files `SuperSecretInformation` and `.HiddenSecretInformation`.

Flag 1

The file `SuperSecretInformation` contains the following information:

```
$ cat SuperSecretInformation
Rot13

Wrfcre'f snibhevgr guvatf va gur jbeyq vf Jvaqbjf naq erq jvar
$
```

Figure 6: Inside SuperSecretInformation file

We recognized that the message was encrypted with monoalphabetic rotation cipher with rotation of 13. Using simple Python script, we were able to decipher the text as follow:

`Jesper's favourite things in the world is Windows and red wine`

```python
def decipher_rotate_cipher(text, shift):
    result = ""

    for i in range(len(text)):
        char = text[i]

        if char.isupper():
            result += chr((ord(char) - shift - 65) % 26 + 65)

        elif char.islower():
            result += chr((ord(char) - shift - 97) % 26 + 97)

        else:
            result += char

    return result

encrypted_text = "Wrfcre'f snibhevgr guvatf va gur jbeyq vf Jvaqbjf naq erq jvar"
shift = 13

decrypted_text = decipher_rotate_cipher(encrypted_text, shift)
print("Encrypted text: ", encrypted_text)
print("Decrypted text: ", decrypted_text)
```

✓ 0.0s

```
Encrypted text:  Wrfcre'f snibhevgr guvatf va gur jbeyq vf Jvaqbjf naq erq jvar
Decrypted text:  Jesper's favourite things in the world is Windows and red wine
```

Figure 7: Decipher the message

Flag 2

In the file `.HiddenSecretInformation` we found the following message in clear:

`Ulf has sailed all of the seven seas`

```
$ cat .HiddenSecretInformation
Ulf has sailed all of the seven seas
$
```

Figure 8: Inside .HiddenSecretInformation file

Flag 3

Following the instruction, we used the code `cat /etc/motd` to open the file.

We observed a long text hinted that there is a secret message hidden in plain text, we assumed that this is some kind of steganography.

```
Others might have said that you need encryption to protect a secret
Later, or now, you might see that this may not be true
Demented as i am, i hide without a code, visible to you

Glass, thin as glass, transparent, visible, yet blurry
Rodents! stealing my secrets? no, they will stay hidden, so don't be in a hurry
Away from the public eye
Very secret, yes, search low and high
Every day, every night, i dread the day when it comes out
You, my dear reader, will you be the one
And find my secret, try, it will be fun.
Read again, and read in a new way
Definitely, let your eyes to the left sway.
```

Figure 9: Some hints from the message

We took hint from last line of the text and try take the first characters of each line, and then we got the following message:

`NOD BUILDING IS BUILT ON AN OLD GRAVEYARD`

Flag 4

We used `cat etc/passwd` to open the file passwd. This file is supposed to contain usernames, encrypted passwords, user ID, group ID, name of users, user home directory and login shell (8). However, upon careful inspection, the last line of the file does not look like others, because it contains a message:

`Eric is afraid of frogs`

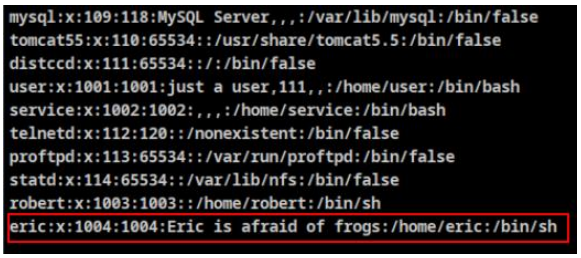

Figure 10: Secret message in passwd file

cat /etc/shadow > acc_pass

Chapter 4: Cracking the passwords

With root privilege we can easily access the `etc/shadow` that other normal users cannot. We then copy the content into a txt file in our Kali machine, called `acc_pass`.

In a command shell, we run `sudo john –incremental acc_pass` with the aim of trying a brute force attack (5). After some time, we stopped the command and only achieved seven out of nine passwords.

Figure 11: First brute force attack

Among these seven cracked passwords, msfadmin is a SuperUser, highlighted with red text by john. We also tested usernames and passwords obtained from `john` with `ssh_login` on Armitage to check if they are valid.

We tried running john again with the last two hashes of user `root` and `robert` in a file called `acc_pass2`. Brute force might take a long time to crack all passwords, since it tries every possible combination. Therefore, we decided to change our strategy to dictionary attack (5). During investigating our Kali VM, we found that a zipped `rockyou.txt` wordlist at this location: `/usr/share/wordlists/rockyou.txt.gz` in our VM. Therefore we unzip this rockyou.txt and used it for our dictionary attack with `sudo john –w=rockyou.txt acc_pass2`.

After some more time, we achieved the last two passwords, and one of them is a SuperUser – **root**.

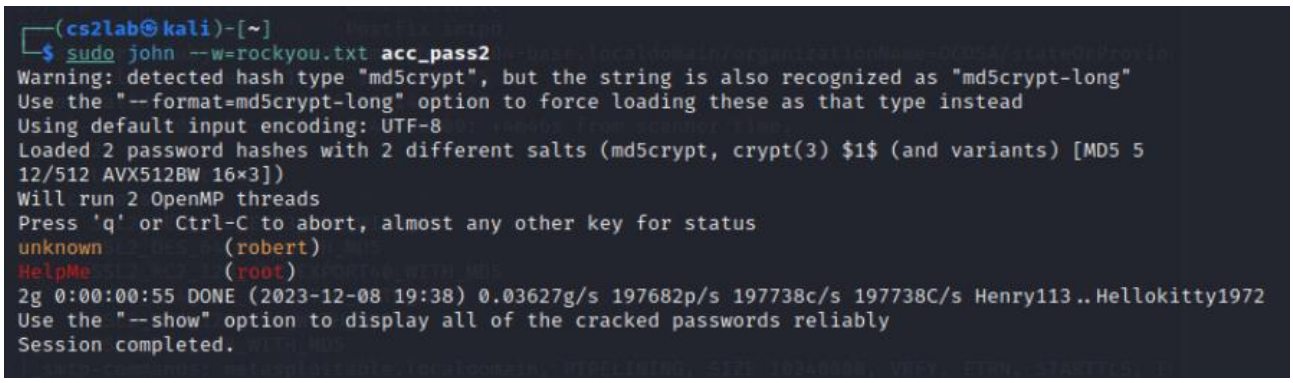

Figure 12: Dictionary attack with rockyou wordlist

In the end, we successfully cracked all the passwords, with msfadmin and root as super users.

Conclusion

With this assignment, we gained a deeper insight into various aspects of cybersecurity, such as:

- Through this penetration test, we understood different stages of an attack, from initial information gathering to gaining access and potentially to privilege escalation.
- When learning how to take advantage of the vulnerabilities, we could see how a minor misconfigurations or outdated software can lead to a serious security breach. Therefore, we understand more why regular updates are crucial for security.
- In hindsight, there are many different ways to gain access into a system, but some vulnerabilities are more serious than others. For example, with `distccd` vulnerability, we only gained access as normal user, and it could have taken more work to escalate privilege; while with `vsftpd` backdoor, we gained root access right away.

Reference:

1. Bishop, M., Sullivan, E. and Ruppel, M., 2019. *Computer Security: Art and Science*. Second edition ed. Boston: Addison-Wesley.
2. Kennedy D, O'Gorman J, Kearns D, Aharoni M. Metasploit: The Penetration Tester's Guide. No Starch Press; 2011.
3. Nmap Project. Port Scanning Techniques [Internet]. Nmap: the Network Mapper - Free Security Scanner. [cited 2023 Dec 11]. Available from: https://nmap.org/book/port-scanning-options.html
4. InfoSec Matter. Metasploit Module Library: exploit/multi/samba/usermap_script [Internet]. InfoSec Matter. [cited 2023 Dec 11]. Available from: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/samba/usermap_script
5. StationX. How to Use John the Ripper [Internet]. StationX. [cited 2023 Dec 11]. Available from: https://www.stationx.net/how-to-use-john-the-ripper/
6. Exploit Database. Dirty Cow [Internet]. Exploit Database. [cited 2023 Dec 11]. Available from: https://www.exploit-db.com/exploits/40839
7. Exploit Database. Vsftpd 2.3.4 – Backdoor Command Execution [Internet]. Exploit Database. [cited 2023 Dec 11]. Available from: https://www.exploit-db.com/exploits/17491
8. IBM. Using the /etc/passwd file [Internet]. [cited 2023 Dec 12]. Available from: https://www.ibm.com/docs/fi/aix/7.1?topic=passwords-using-etcpasswd-file