Cyborg_THM

Enumuration

# Got a admin directory consisting a website

# we get three users ,josh,alex

#we have a /etc dir having a passwd dile apparently having a hash and somename

# in website we get to download a archive.tar

# we untar it and it has many differnt conf files but its all gibberish

# we read the readme file which showed that this was all a backup made by using borgbackup utility

# we research and see that we can install these backups using borg binary

# the file we got in /etc dir had a name music_Archive which is apparently a directory as stated in website blog

# we decode the hash and get a password which is squidward\

# Now we can can install the backup by the command

```
./borgbinary extract  home/field/dev/final_archive::music_archive
```

the above given path is the path when we untar the tar archive a directory system wasinstalled. This directoy path is a repo in that borh backup system

we use the password to extract and get alex file system and get his ssh crreds

# Now login as alex

#

Nmap

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|   256 68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_  256 56:2c:79:92:ca:23:c3:91:49:35:fa:dd:69:7c:ca:ab (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   193.64 ms 10.4.0.1
2   ... 3
4   460.29 ms 10.10.104.110

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 36.73 seconds
```

22:ssh

http:80

Exploitation

Post Exploitation

# We see that we can run a backup.sh file as sudo

# its owned by us but we dont have write access so we chmod it

# Now e copied bash binary to /tmp and set it as suid bit

# now we run the backup.sh with sudo and then /tmp/root with -p for privileged mode and get a root shell

LOot

credentials

# We get a passwd file withh username an hash   music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.

we decode it and get squidward password

# ssh creds

alex:S3cretP@s3

FLAGS

# User flag

flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}

# Root Flag

flag{Than5s_f0r_play1ng_H0p£_y0u_enJ053d}