Table of Contents

Summary

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

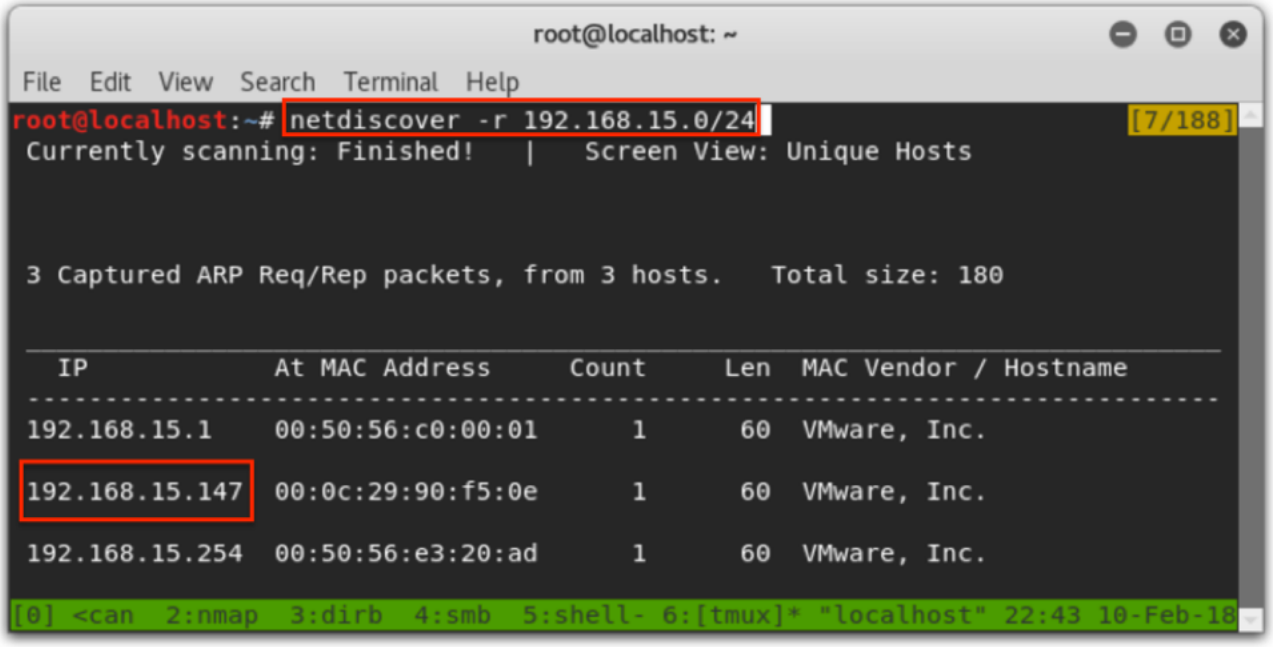
The primary vulnerability was simply recovered admin credentials in an open Samba share.

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

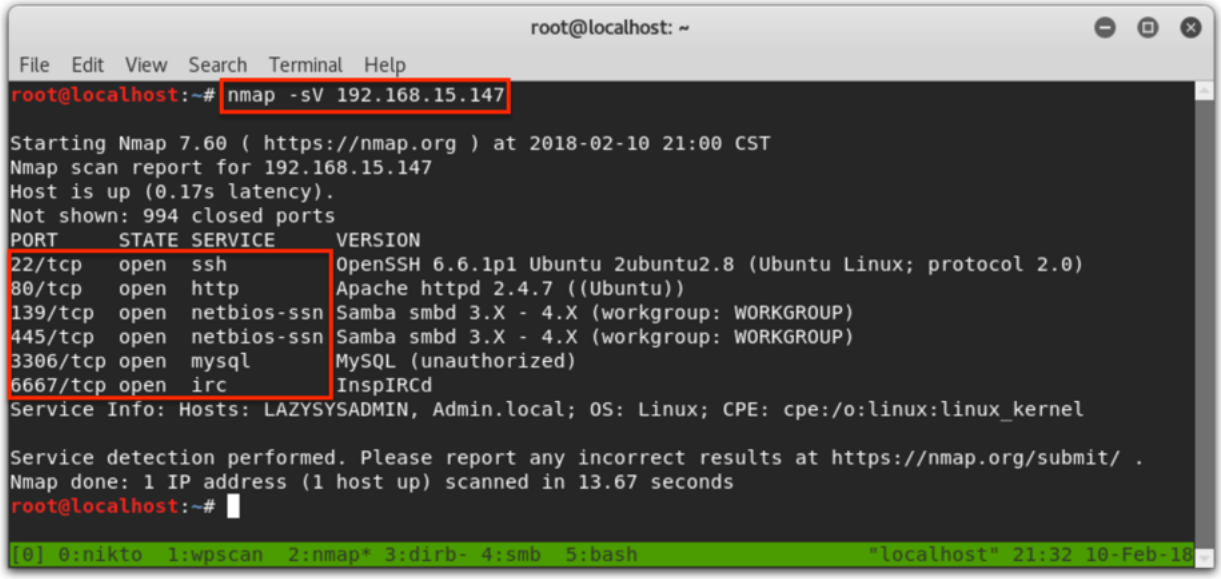
netdiscover

quickly scan my private range to find the host

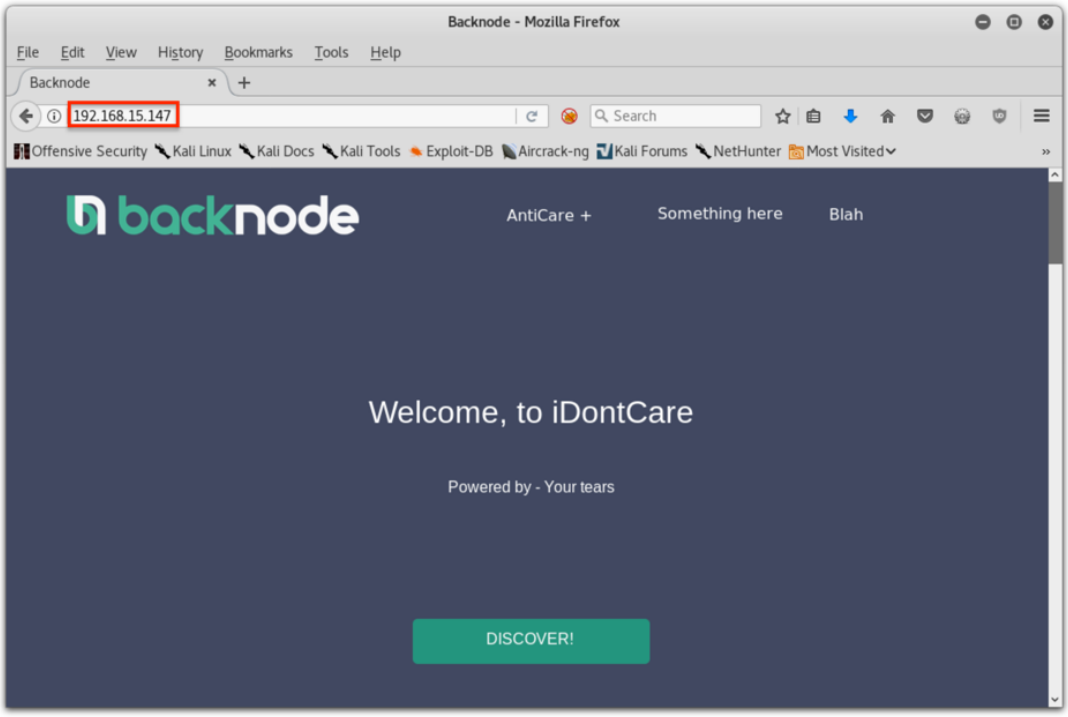


nmap

-sV to enumerate services

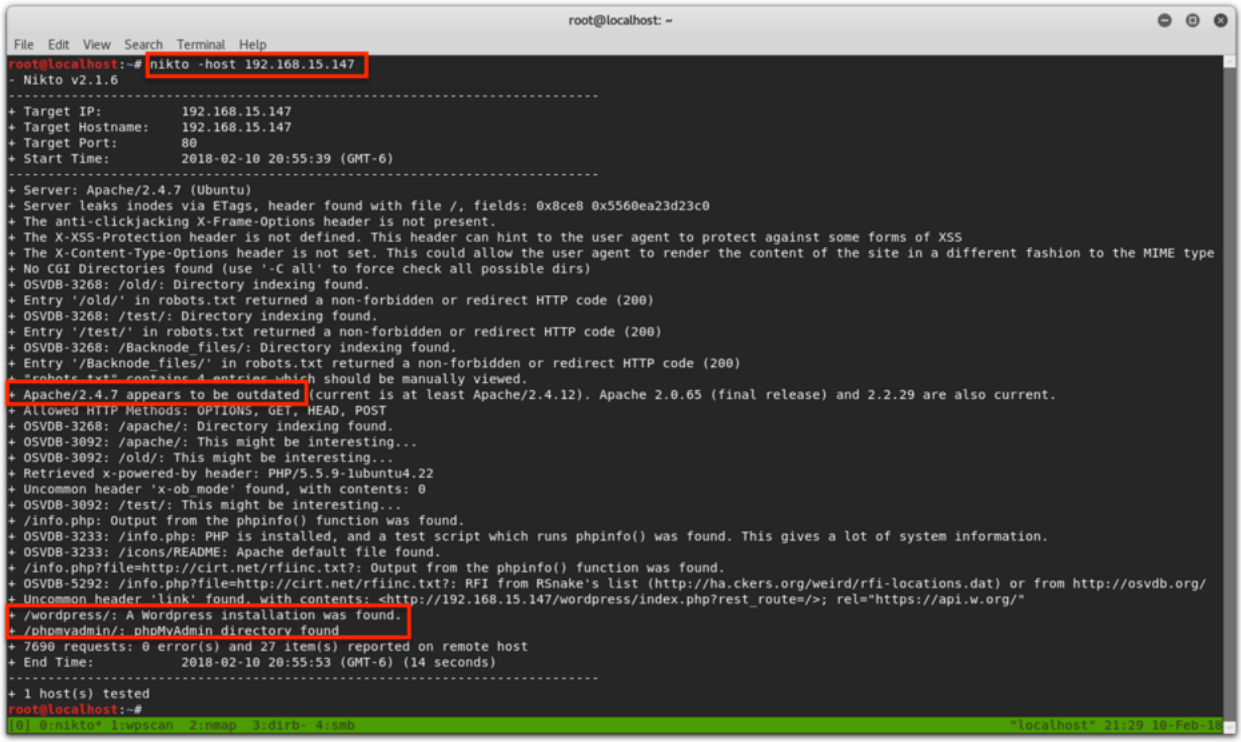


see what web service looks like



nikto

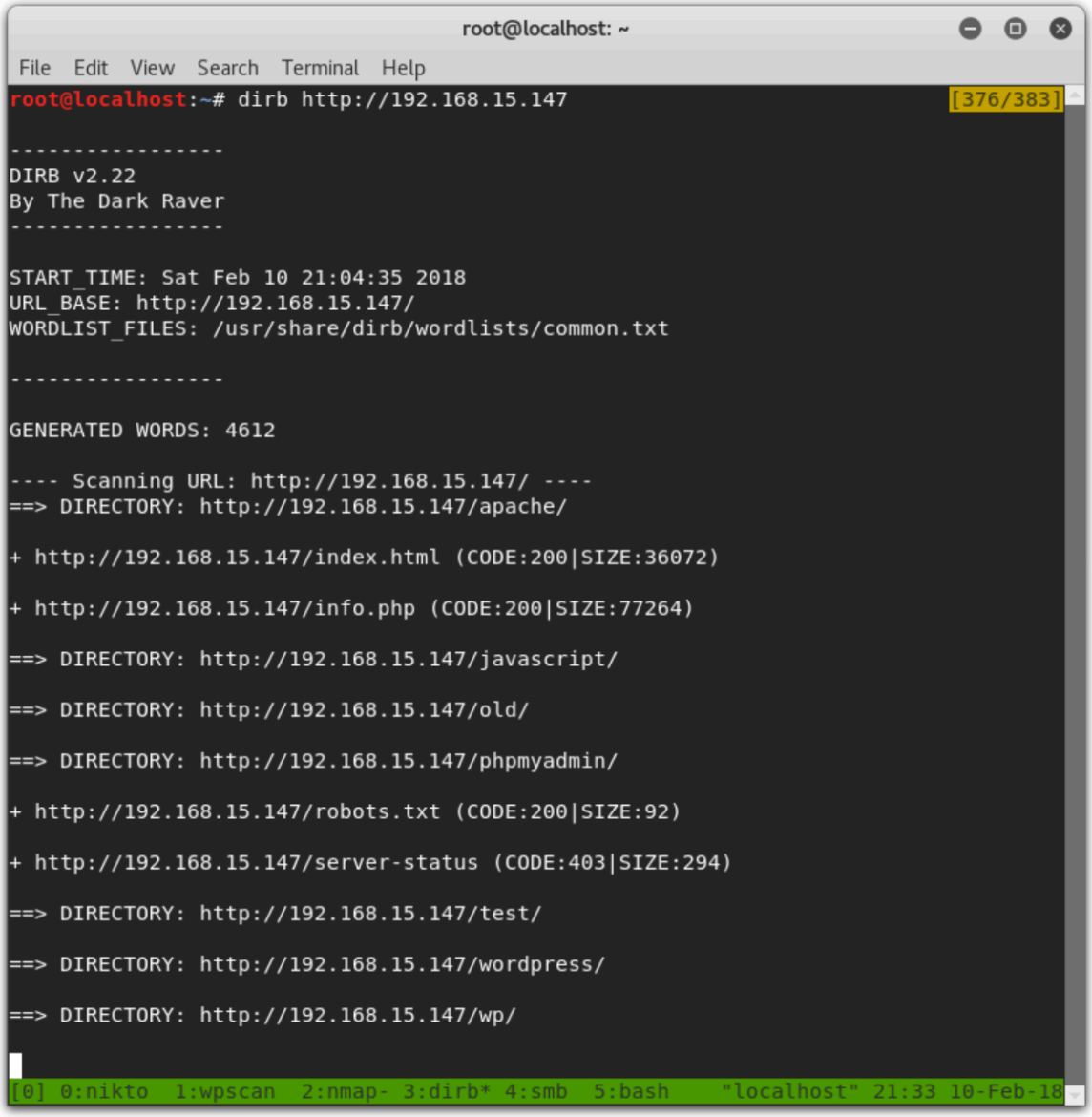
scan for immediate web vulnerabilities / attack vectors



- Outdated Apache
- Wordpress
- Phpmyadmin

dirb

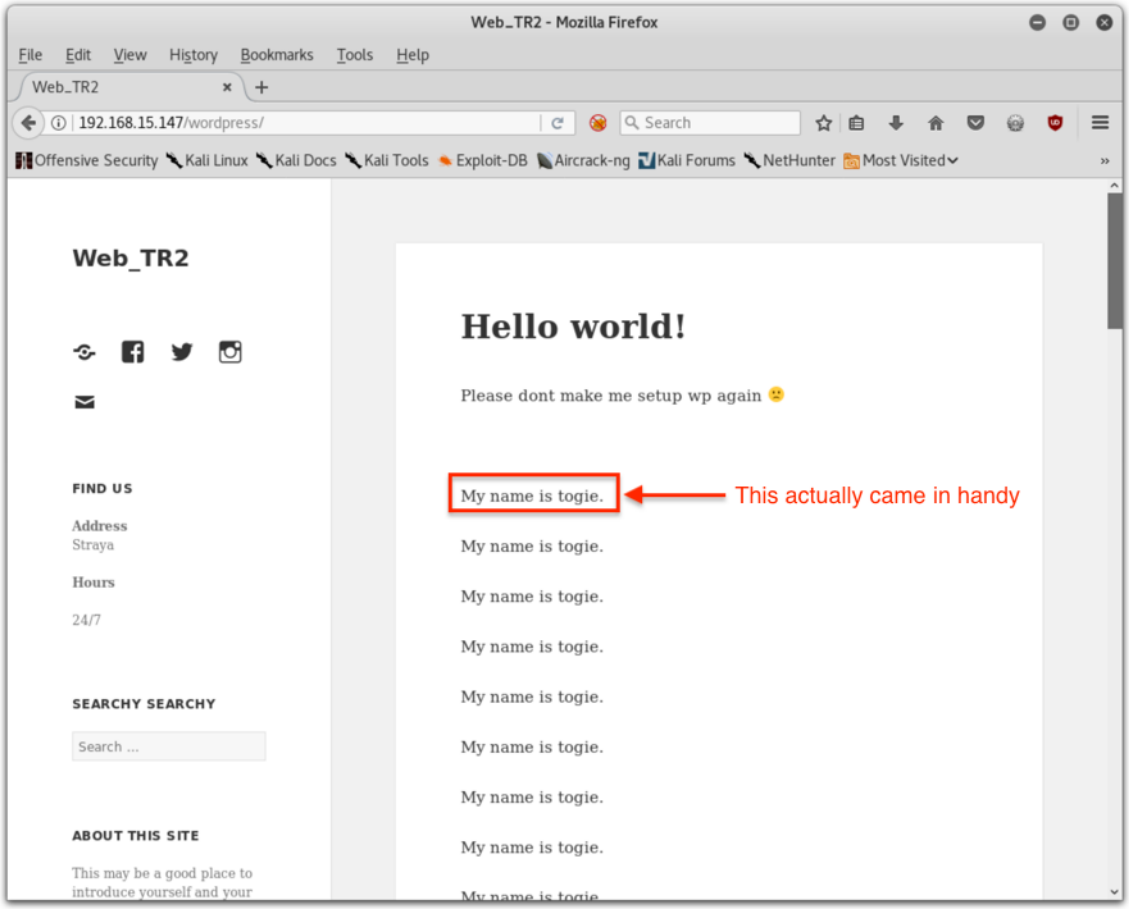
to enumerate web directories



soooooo many directories

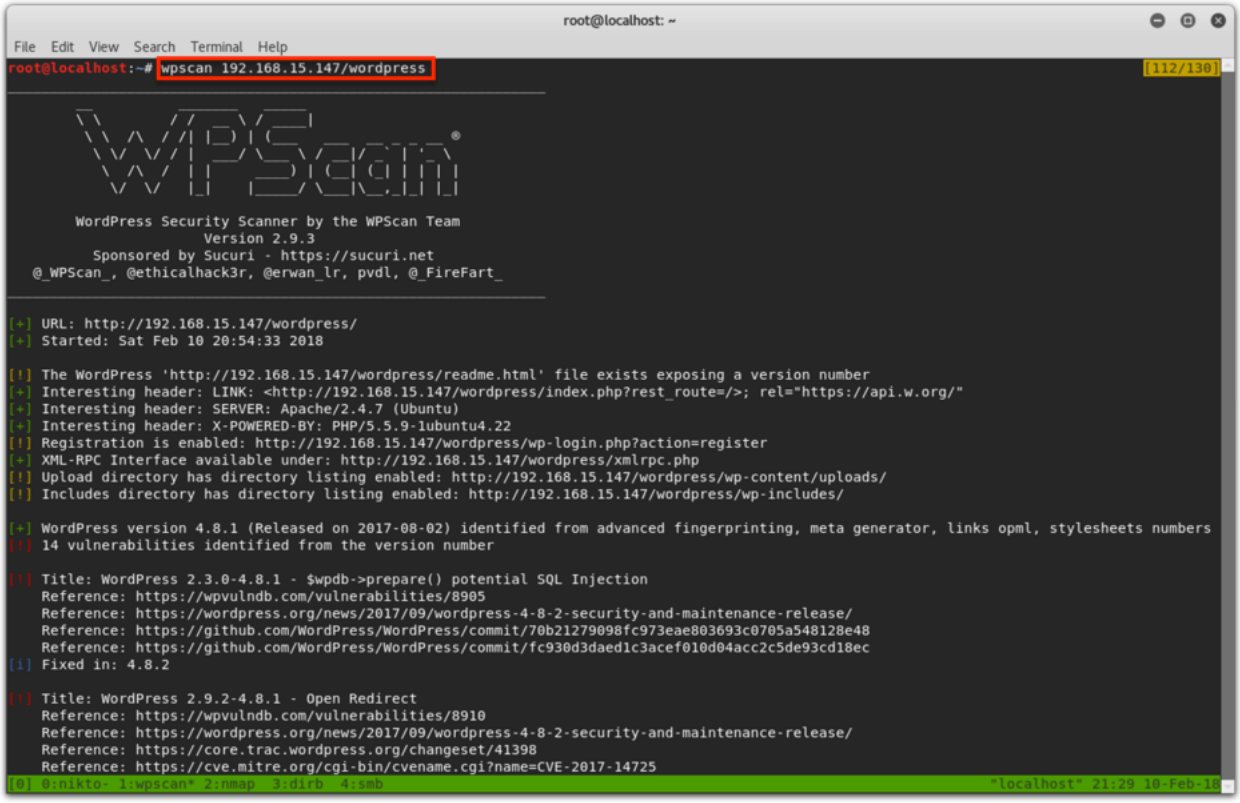
Some worth mentioning:

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



WPScan

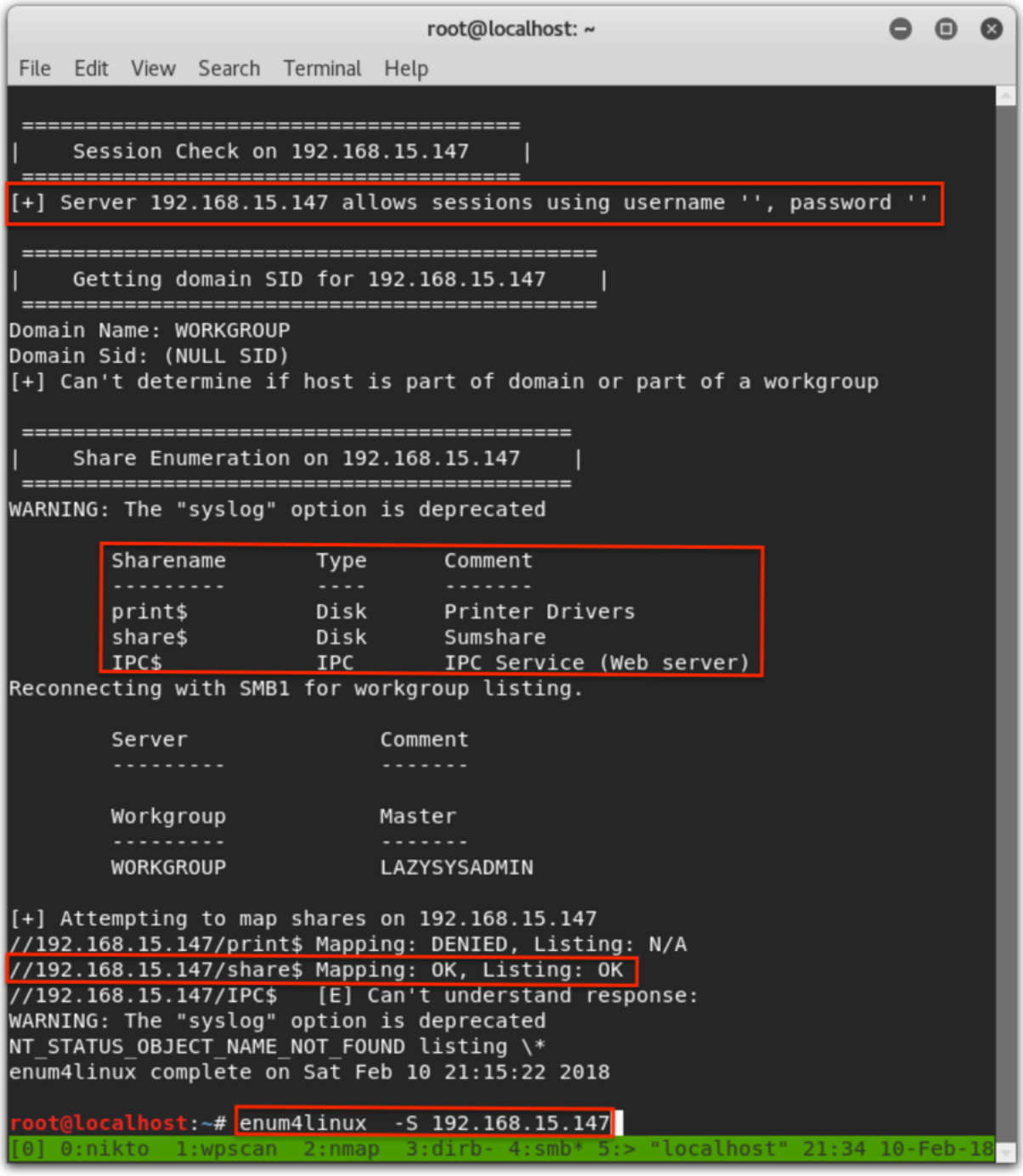
enumerate WordPress vulnerabilities



enum4linux

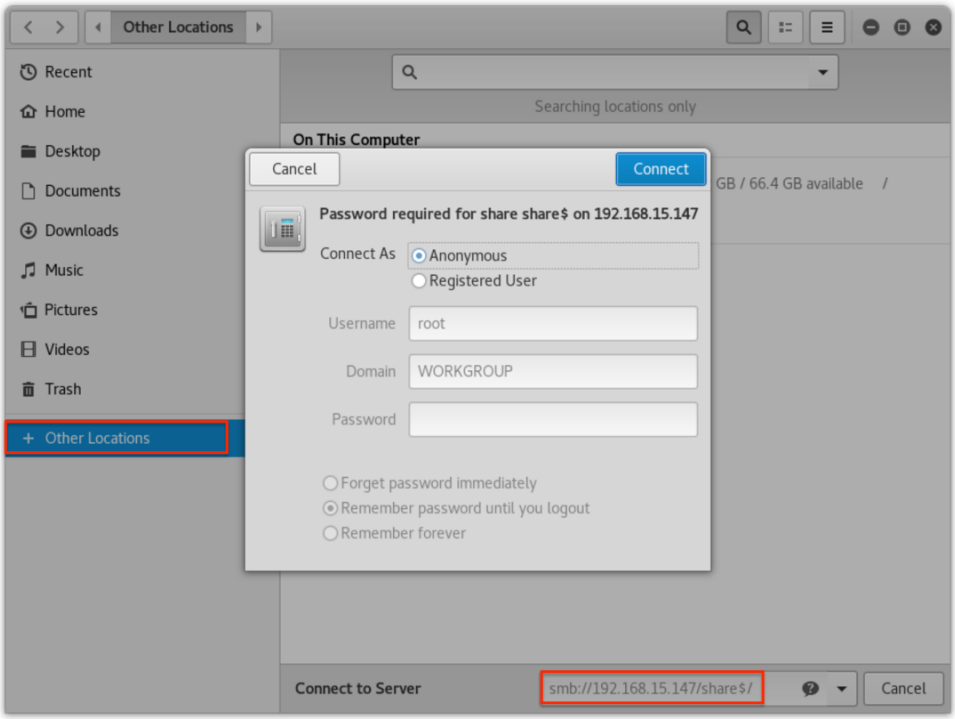
enumerate Samba shares

-S to get sharelist

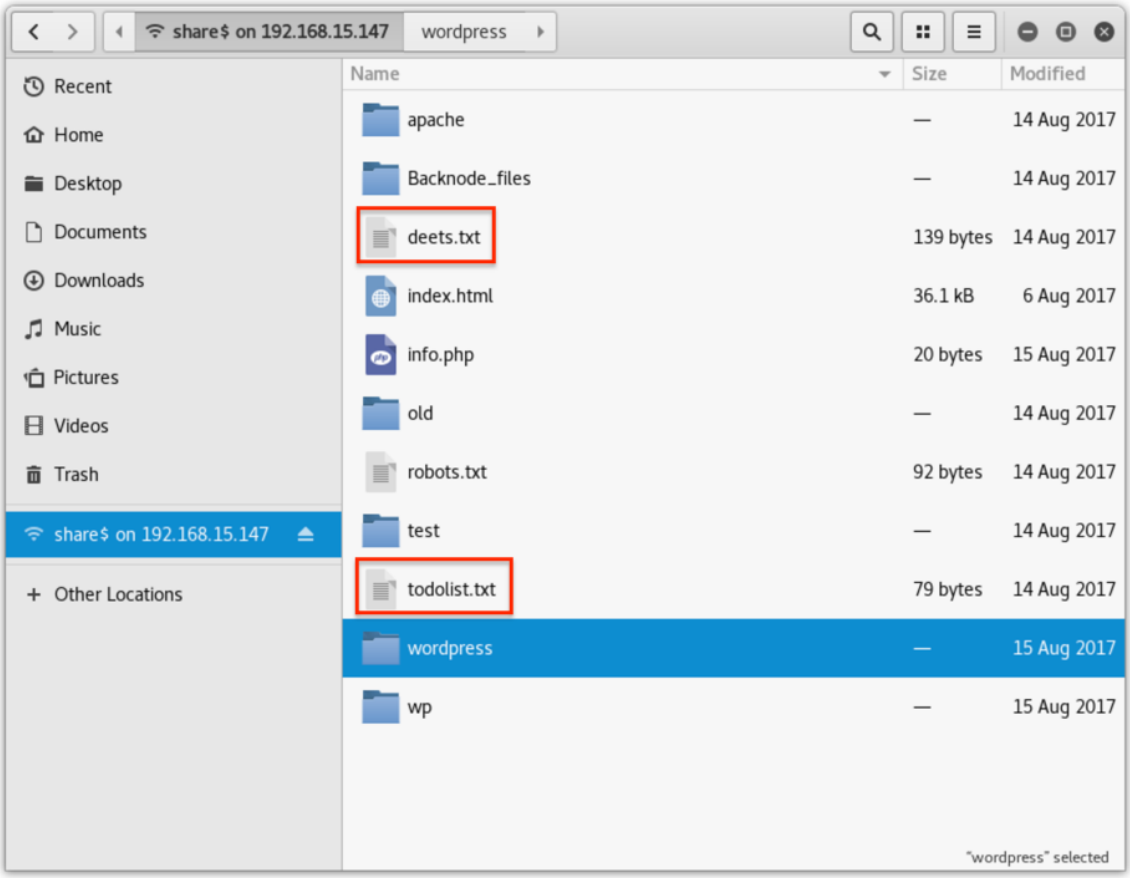


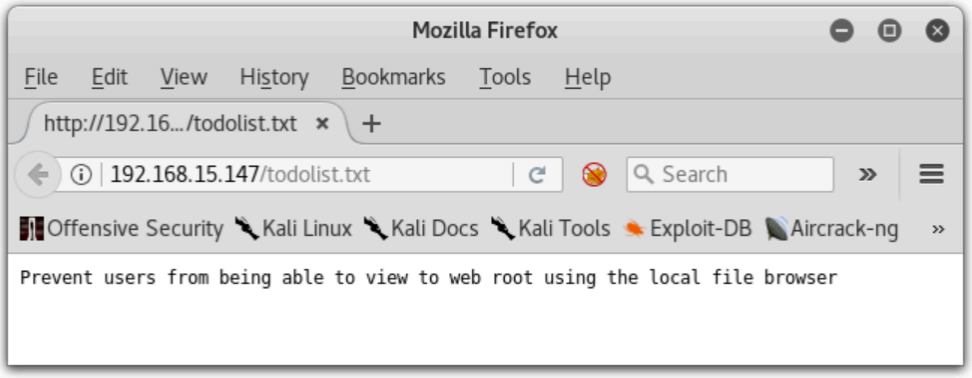
Found a share with anonymous access

Connecting to Samba

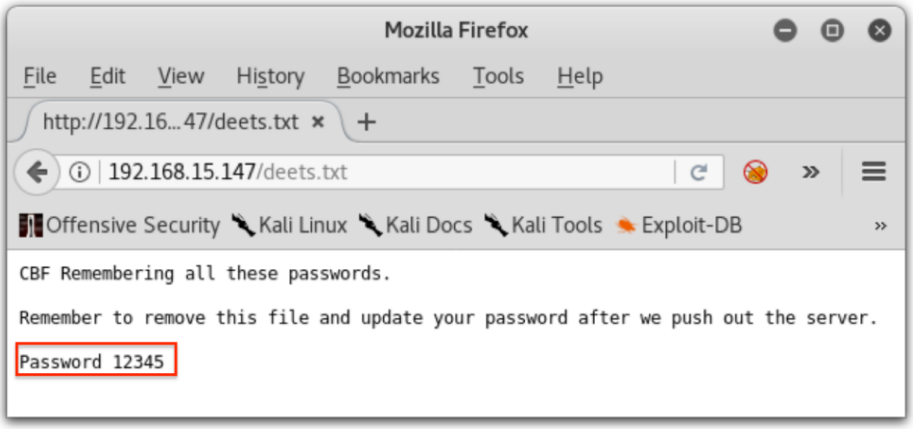


Found some interesting files on the share

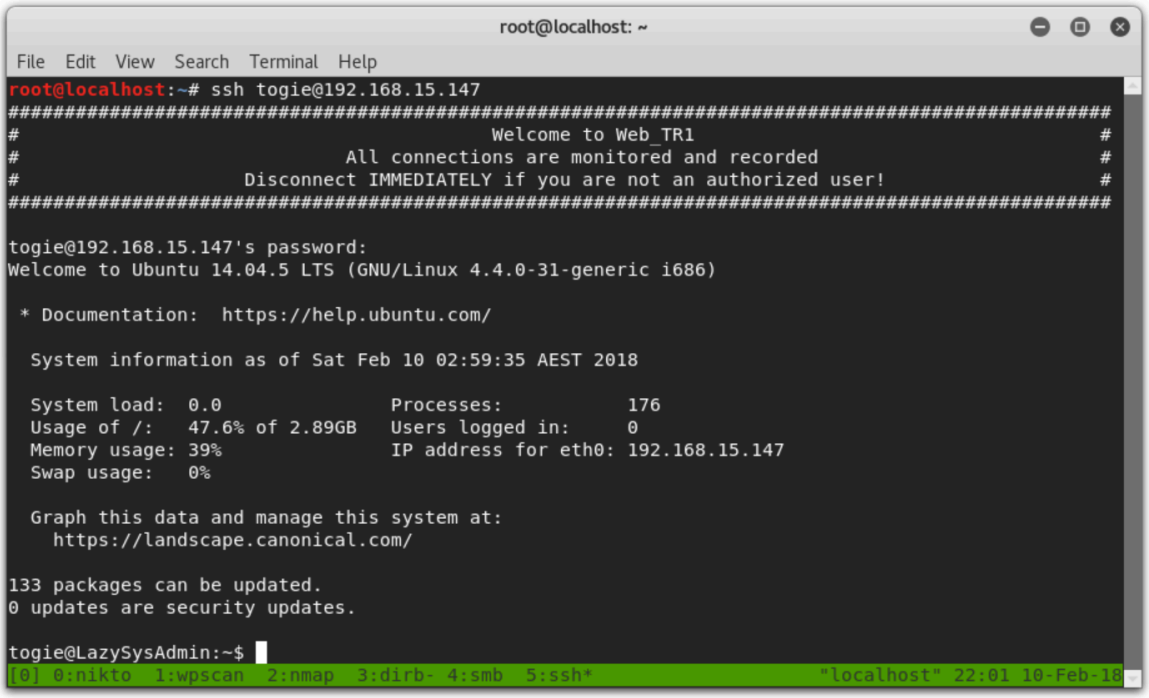




Recovered Credentials

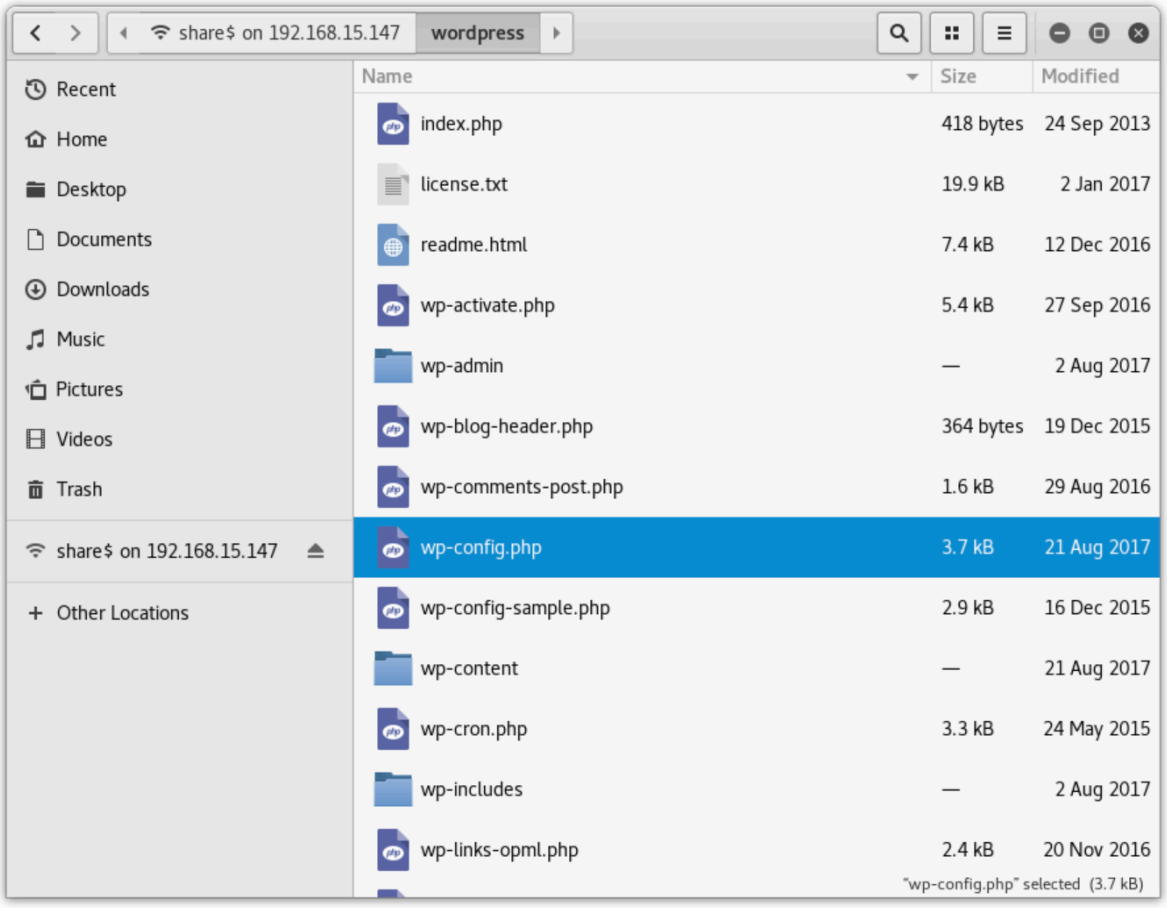


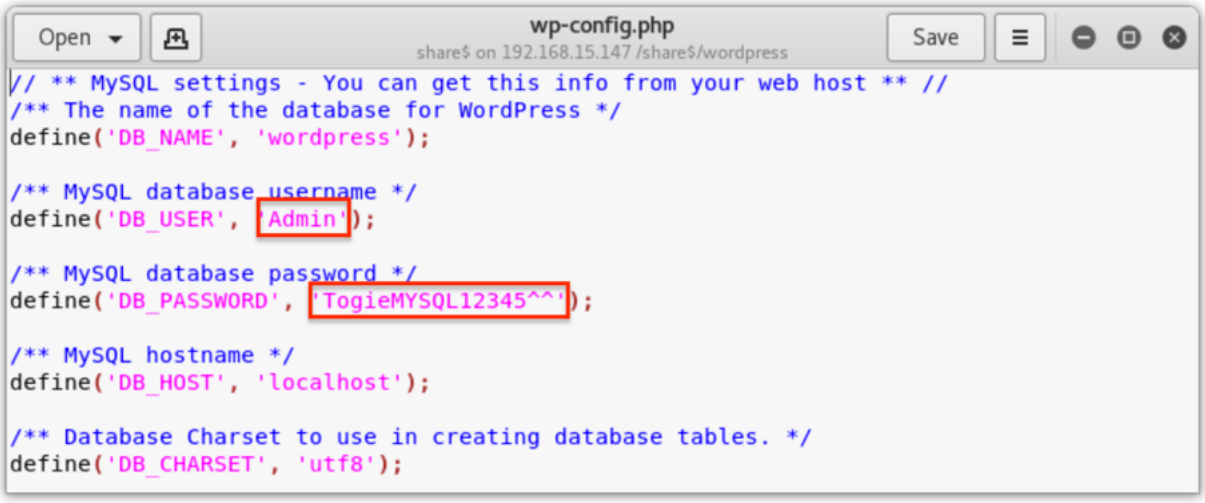
Validate SSH with credentials



User: togie
Password: 12345

Admin Panel Credentials

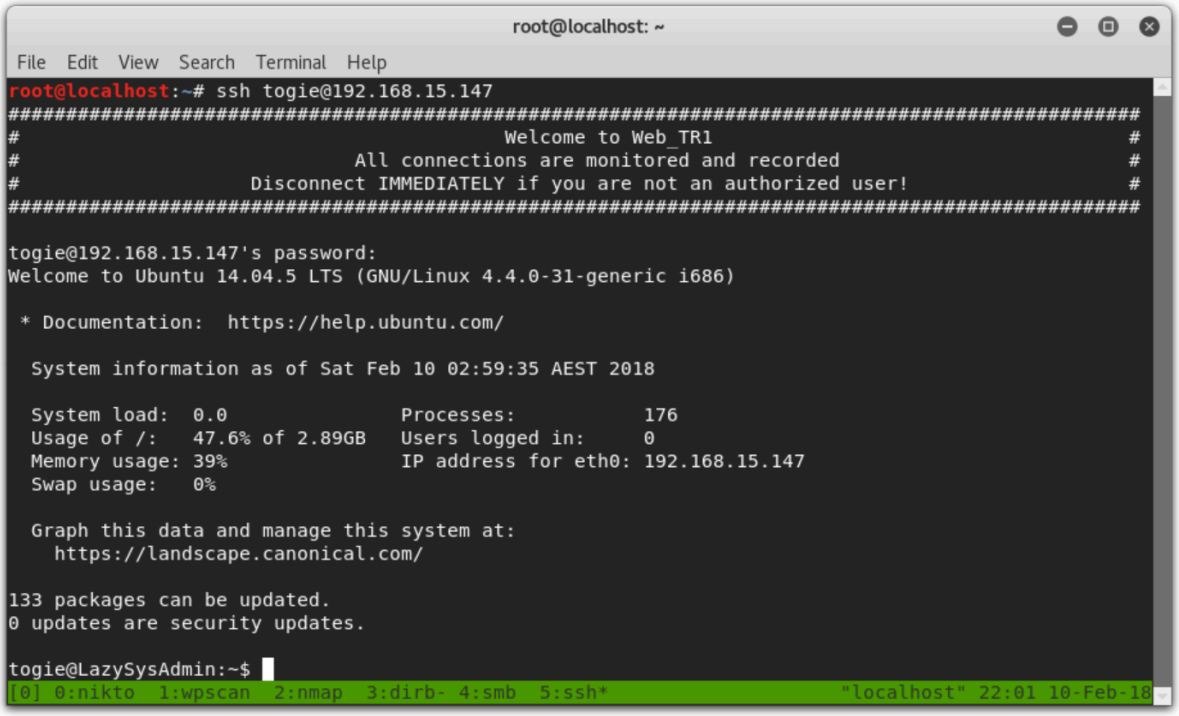




Worked for phpMyAdmin & WordPress admin panels

Getting a shell

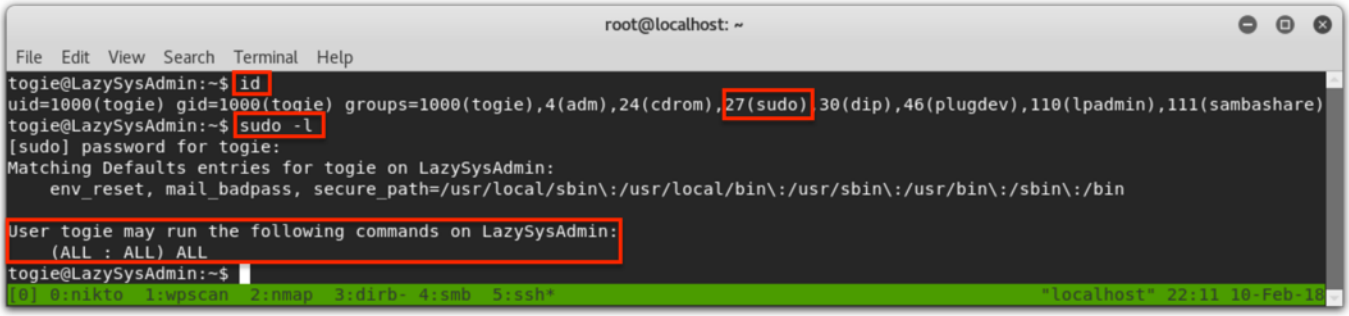
SSH w/ recovered creds



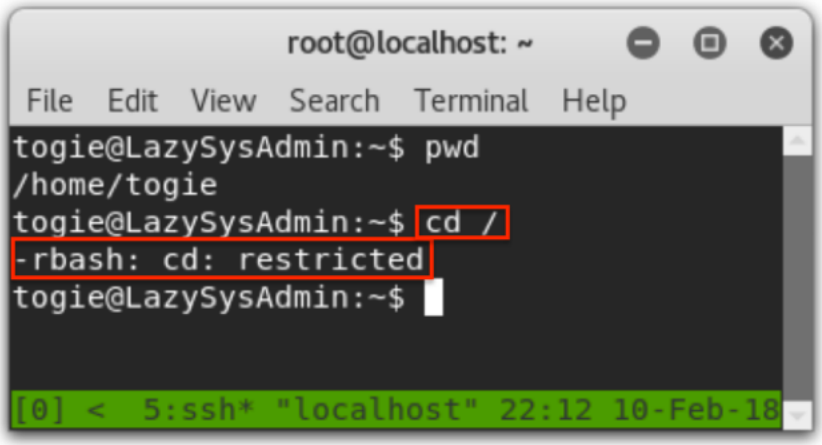
User: togie
Password: 12345

Enumerate privileges

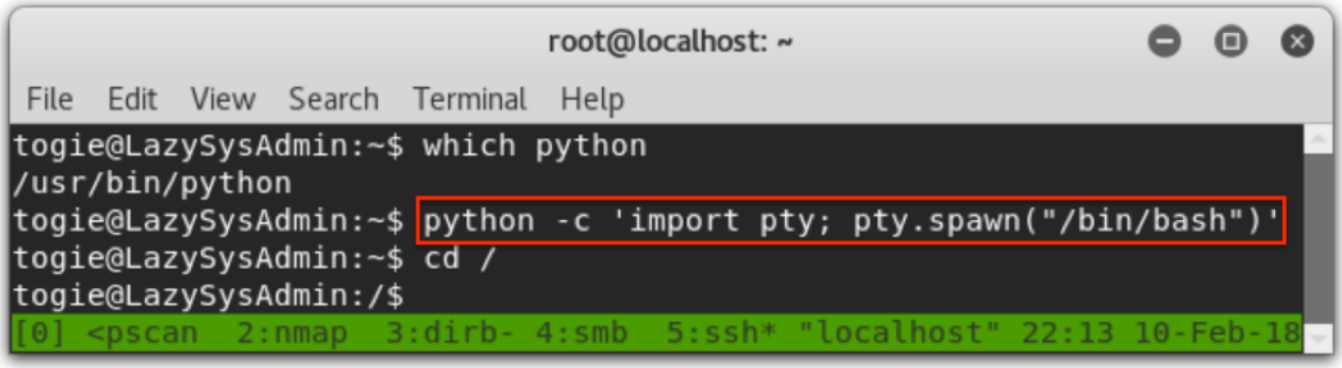
sudo -l

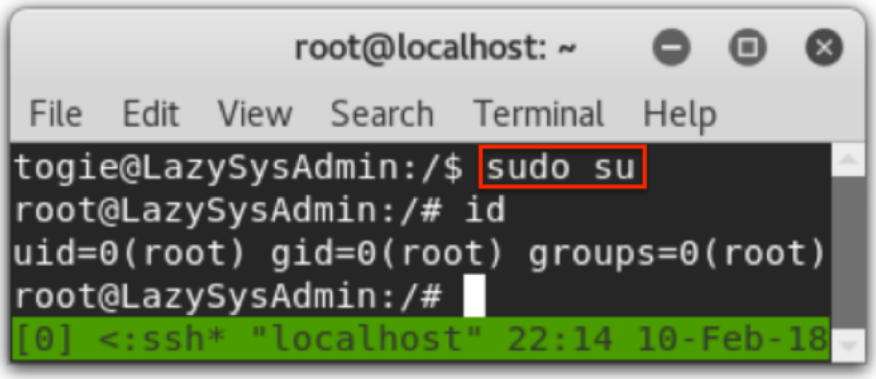


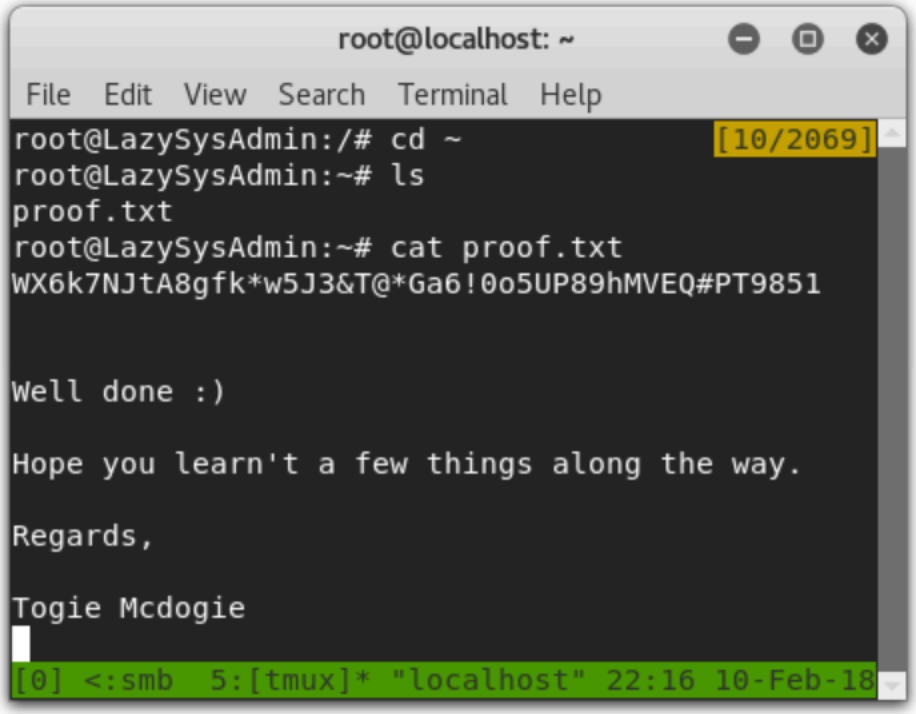
Breaking out of a locked down shell



Spawn a new bash process with python

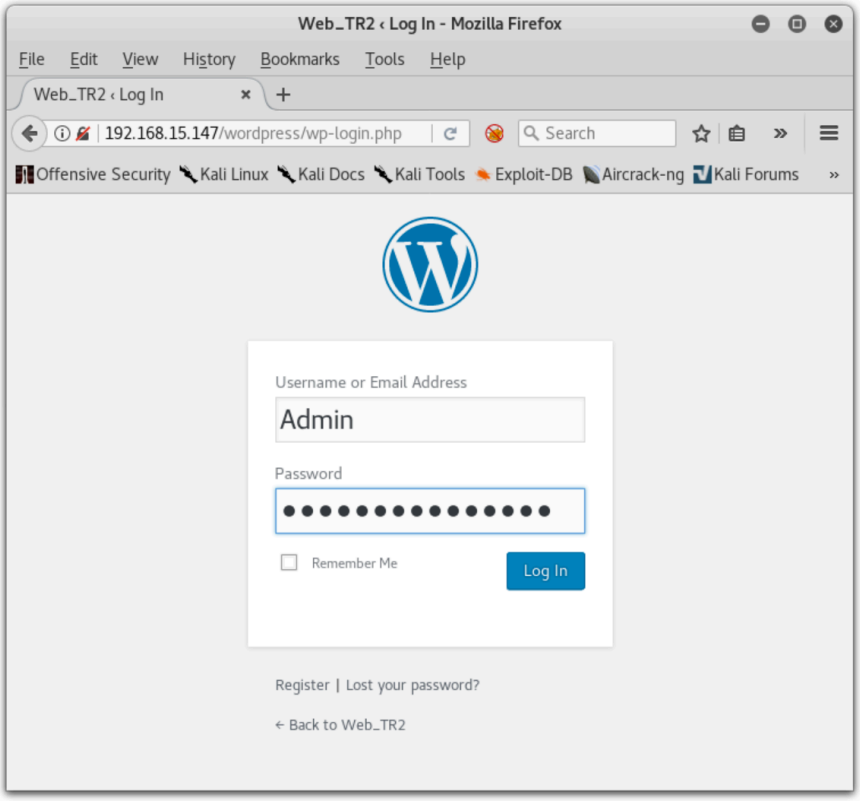


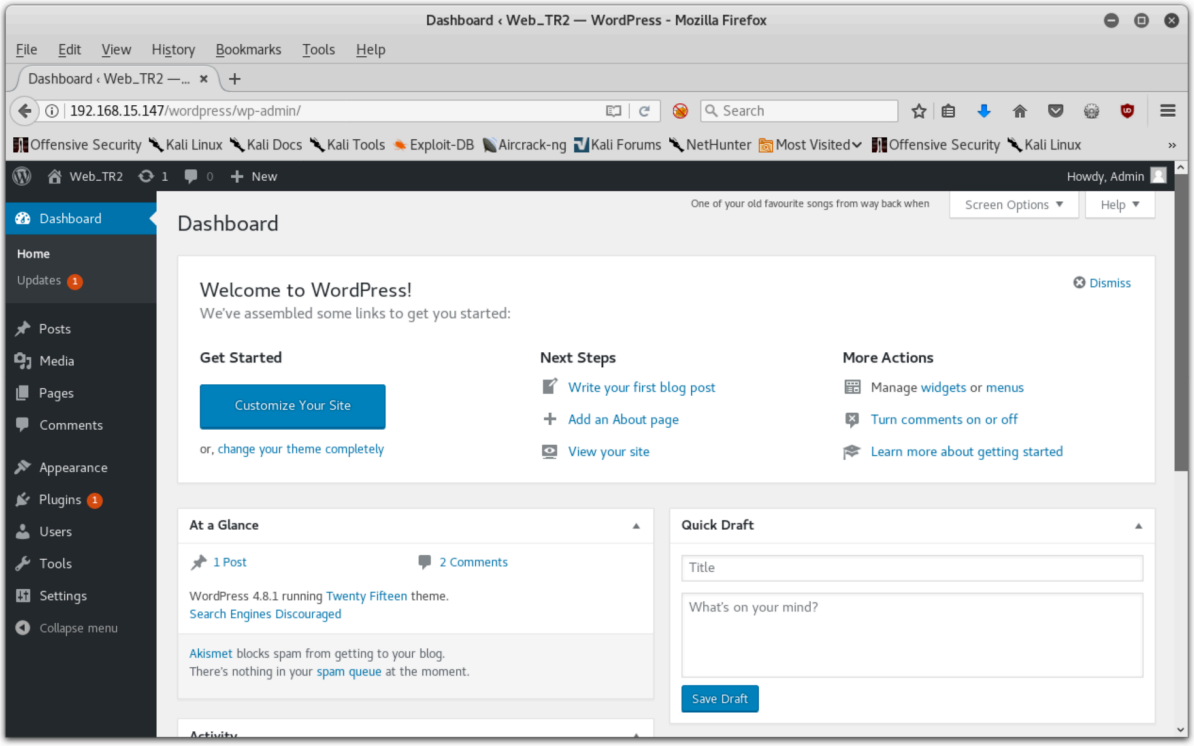



root@localhost: ~
File Edit View Search Terminal Help
root@LazySysAdmin:/# cd ~ [10/2069]
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
Well done :)
Hope you learn't a few things along the way.
Regards,
Togie Mcdogie
[0] <:smb 5:[tmux]* "localhost" 22:16 10-Feb-18

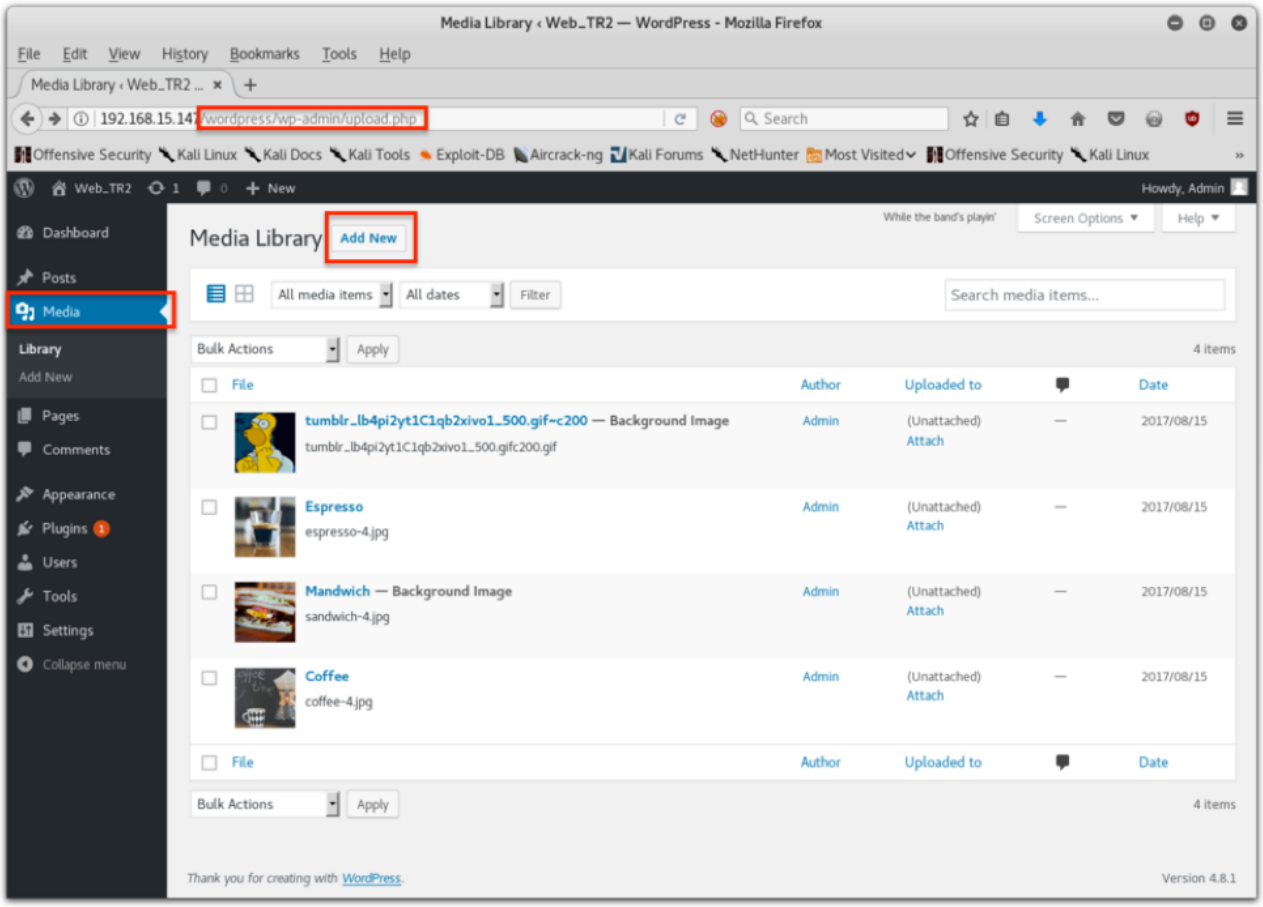
Persistence

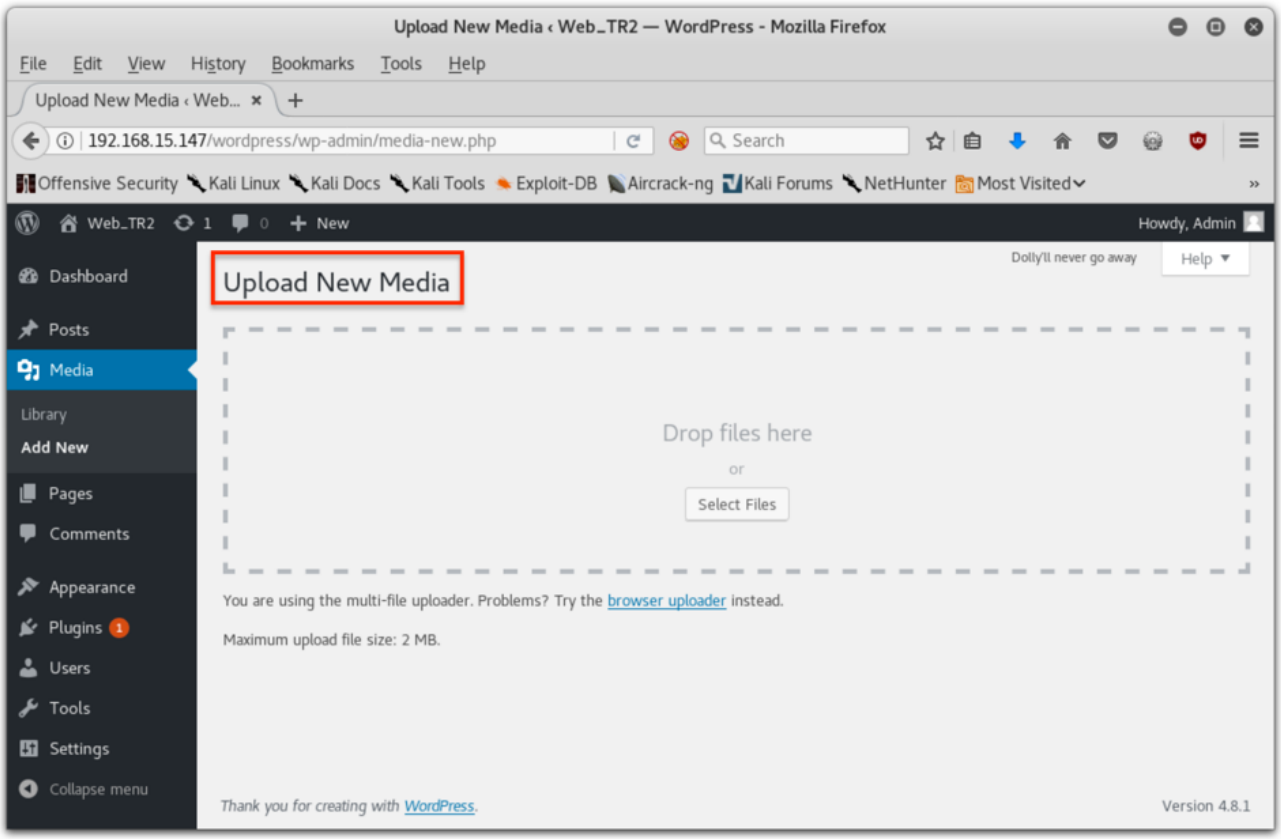
Sign into WordPress admin panel using recovered credentials.



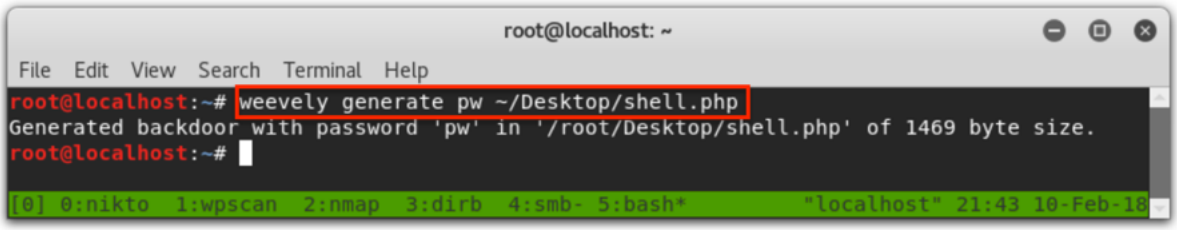


File Upload

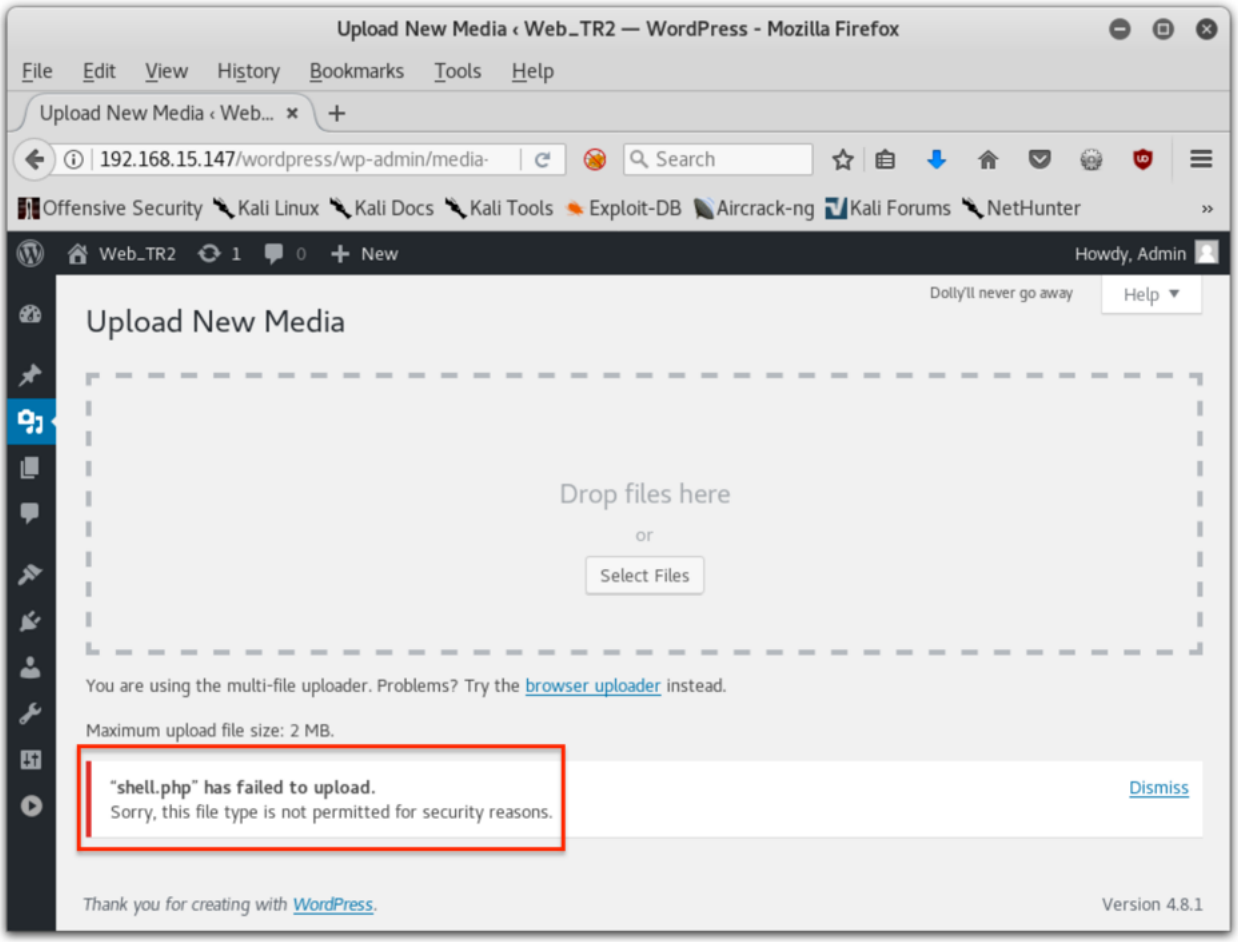

Media Library ‹ Web_TR2 — WordPress - Mozilla Firefox
File Edit View History Bookmarks Tools Help
192.168.15.147/wordpress/wp-admin/upload.php
Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security Kali Linux
Web_TR2 1 0 New
Howdy, Admin
Dashboard
Posts
Media
Library
Add New
Pages
Comments
Appearance
Plugins 1
Users
Tools
Settings
Collapse menu
Media Library
Add New
While the band's playin'
Screen Options
Help
All media items
All dates
Filter
Search media items...
Bulk Actions
Apply
4 items
File
Author
Uploaded to
Date
tumblr_lb4pi2yt1C1qb2xivo1_500.gif~c200 — Background Image
tumblr_lb4pi2yt1C1qb2xivo1_500.gifc200.gif
Admin
(Unattached)
Attach
2017/08/15
Espresso
espresso-4.jpg
Mandwich — Background Image
sandwich-4.jpg
Coffee
coffee-4.jpg
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
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
Pages
Comments
Appearance
Plugins 1
Users
Tools
Settings
Collapse menu
Upload New Media
Dolly'll never go away
Help
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

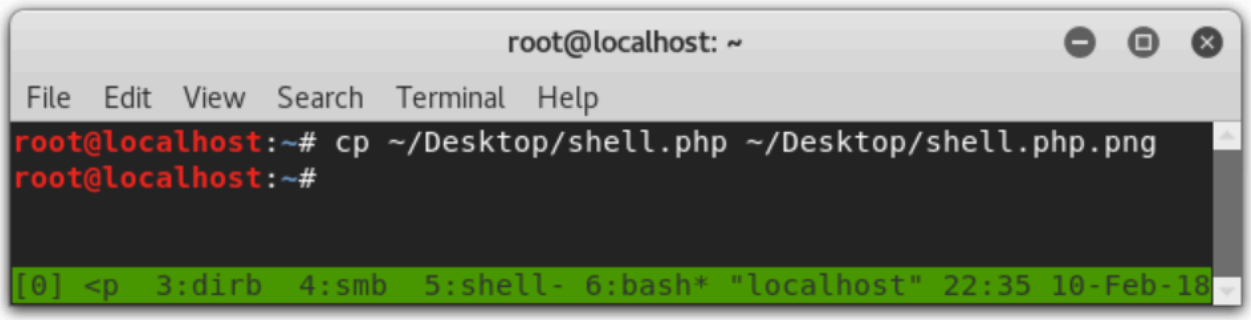
Weevely PHP webshell



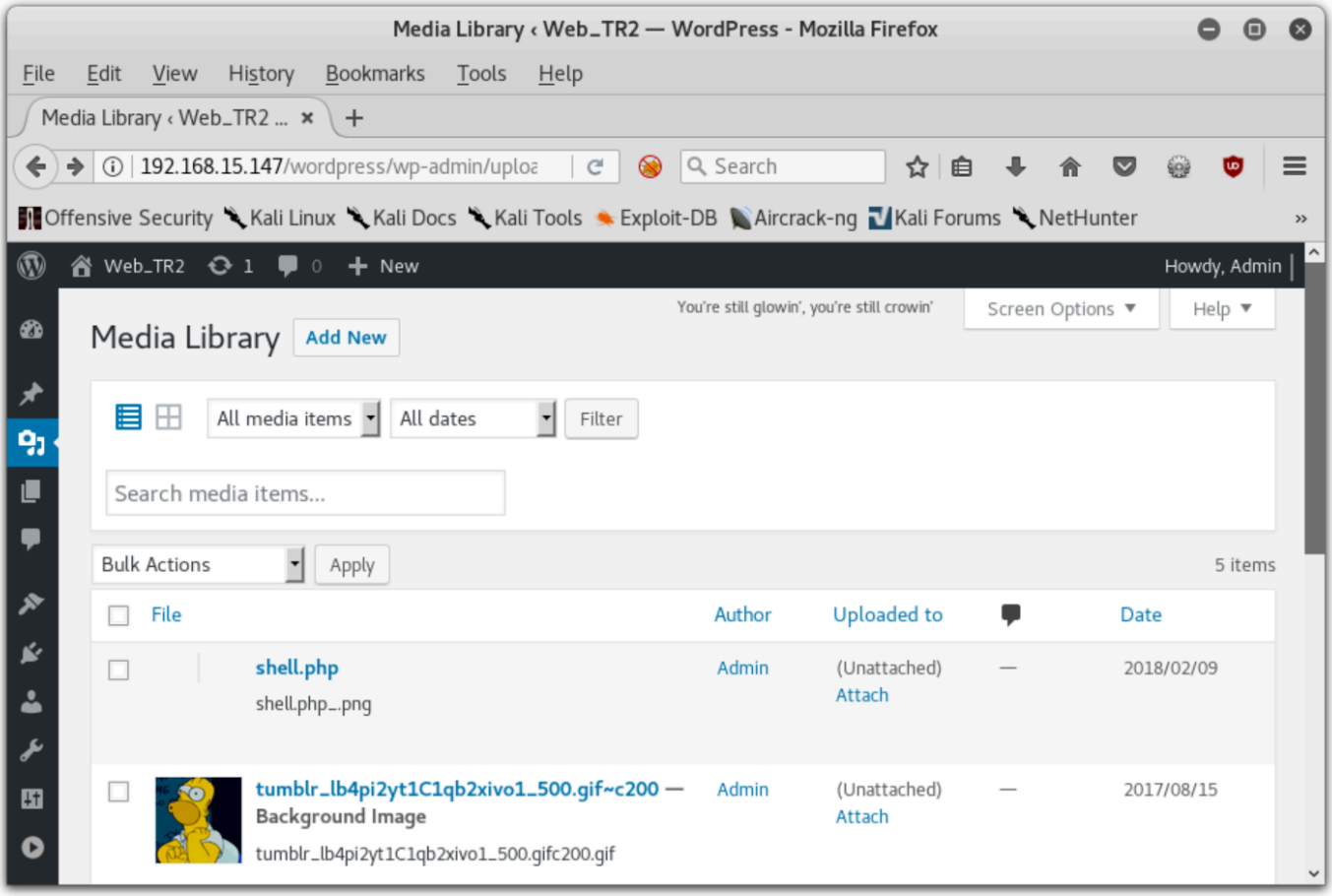
WordPress did not like my webshell for “security reasons”



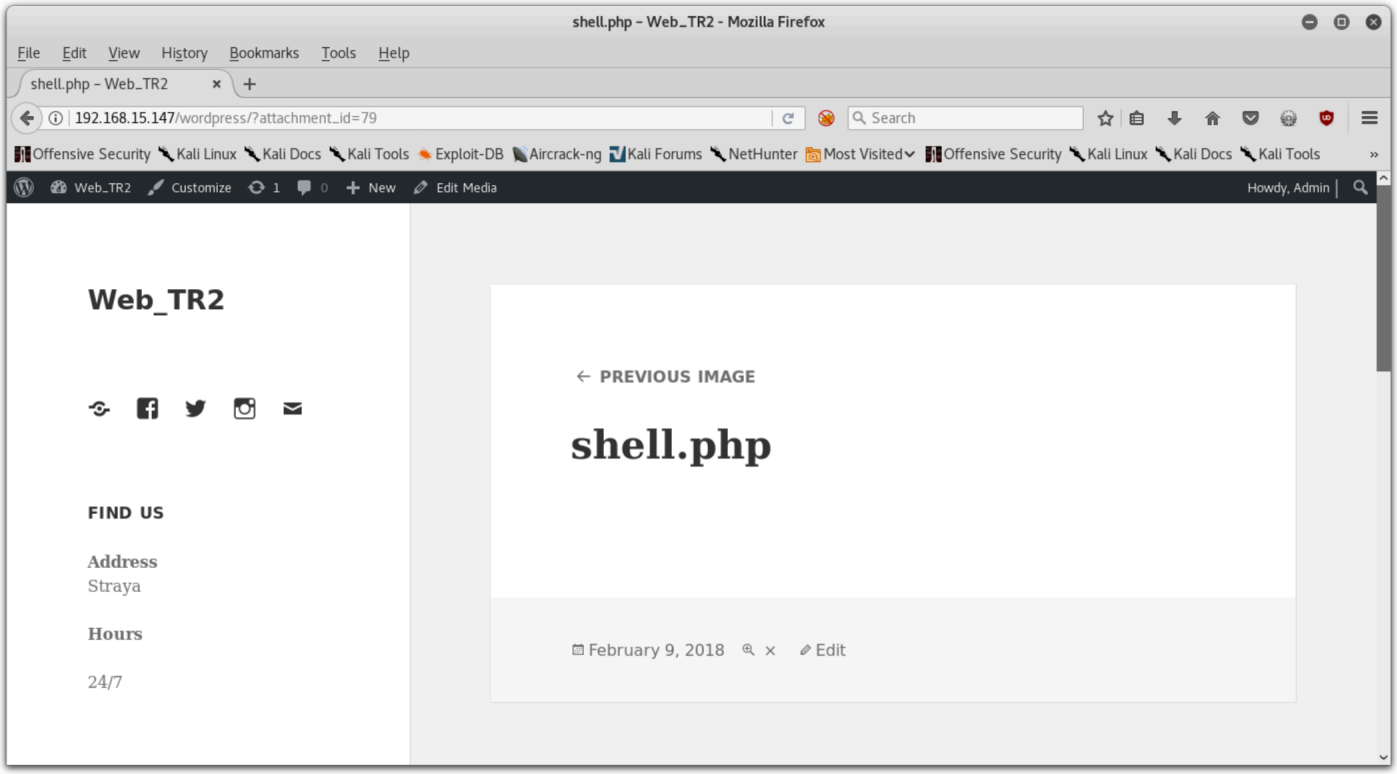
So I added .png to the file extention



. . . and that worked!



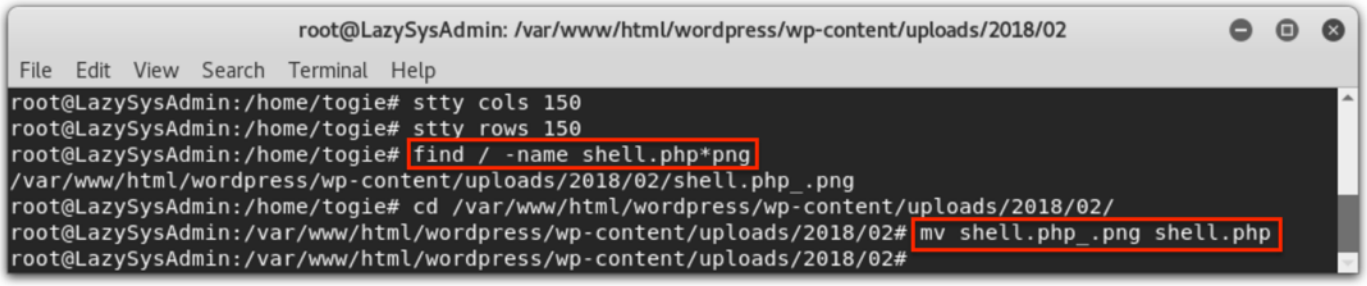
. . . very stealth . . . probably want to delete this post



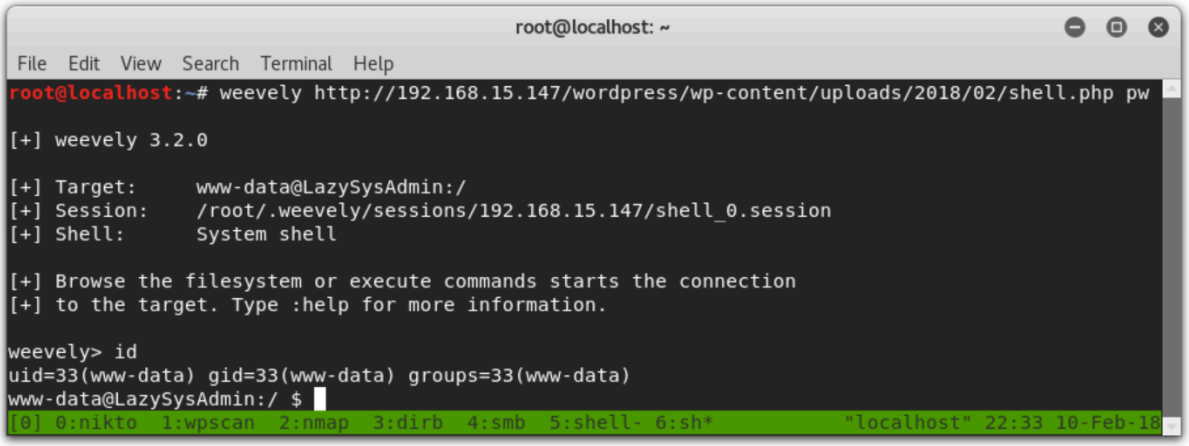
Edit the upload

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



Access the webshell



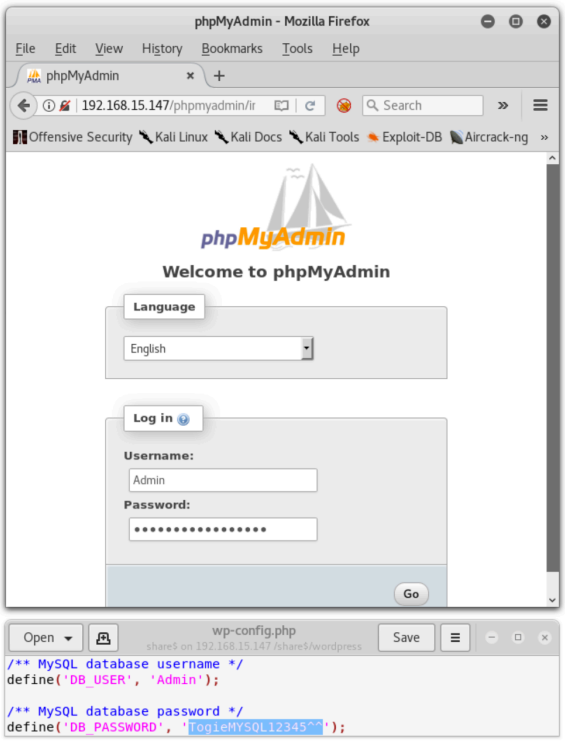
From here, there are a few things worth attempting:

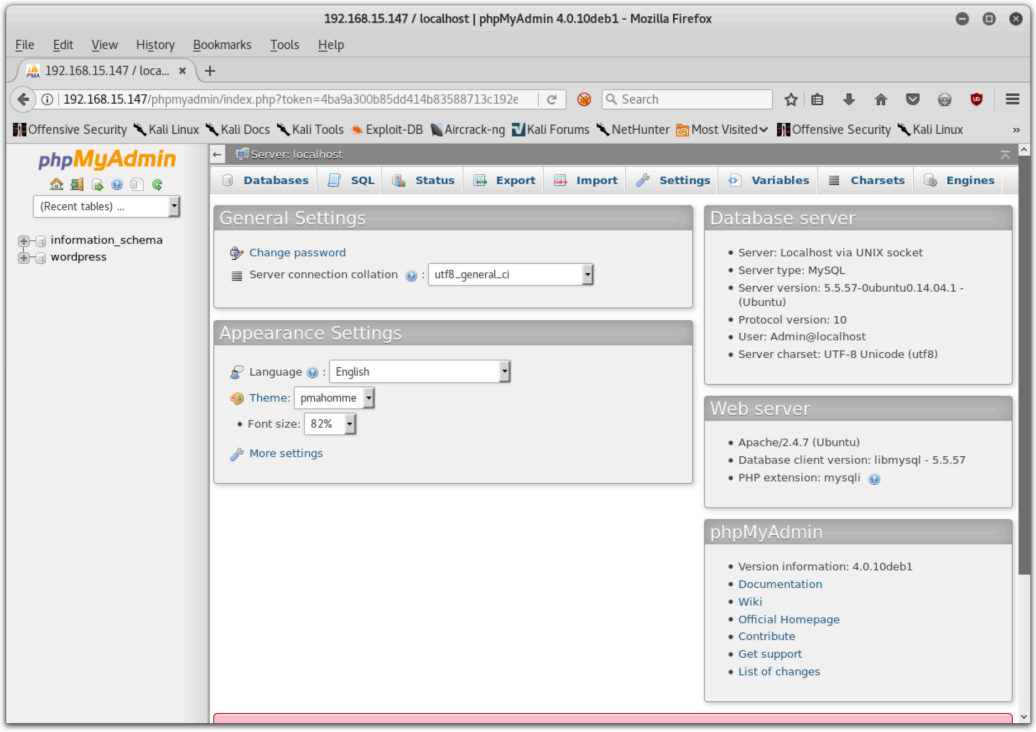
- give the www-data user elevated privileges
- assign another user with elevated privileges to execute this shell (i.e. togie or root)

Unattempted Attack Vectors

phpMyAdmin

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





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.