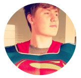

Jean-Francois Maes

Young Graduate at Dimension Data with special interest in Security and Automation & Co-Founder of Joy-Time

Follow

Pentest: Lazy Sys Admin

6 minute read

ON THIS PAGE

Another day another lab, this is going to be the last linux VM for a while, I'll do more of them at some point but for now I'll have to study for CCNA and after that I'd like to take a look at some windows machines. On todays menu is a vulnhub box called LazySysAdmin, it can be found here

Nmap recon

As always we start off with doing some basic nmap recon, first we start off with `nmap -sP` The output of this command let me know that the target ip is 10.0.2.12, please not, this can be different for you.

Next is to check what is running on that machine, we do it using `nmap -p- 10.0.2.12`

```
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6667/tcp open  irc
```

Spider the webpage

```
root@clueless:~# dirb http://10.0.2.12

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

```

START_TIME: Fri Dec  8 07:25:54 2017
URL_BASE: http://10.0.2.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.12/ ----
==> DIRECTORY: http://10.0.2.12/apache/
+ http://10.0.2.12/index.html (CODE:200|SIZE:36072)
+ http://10.0.2.12/info.php (CODE:200|SIZE:77201)
==> DIRECTORY: http://10.0.2.12/javascript/
==> DIRECTORY: http://10.0.2.12/old/
==> DIRECTORY: http://10.0.2.12/phpmyadmin/
+ http://10.0.2.12/robots.txt (CODE:200|SIZE:92)
+ http://10.0.2.12/server-status (CODE:403|SIZE:289)
==> DIRECTORY: http://10.0.2.12/test/
==> DIRECTORY: http://10.0.2.12/wordpress/
==> DIRECTORY: http://10.0.2.12/wp/
```

I see wordpress and phpmyadmin, it’s also worth checking out robots.txt Since we have no valid credentials yet, we should probably focus on wordpress first.

wordpress

http://10.0.2.12/wordpress/wp-login.php is the url to go to the wordpress login page, the first thing you should try is type in username a password a to see the error message. this gave me an invalid username message, which is great, because this means that we can bruteforce the username if it’s necessary.

let’s first run wpscan

this gave us some nice exploits..

```
root@clueless:~# wpscan --url http://10.0.2.12/wordpress/

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

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://10.0.2.12/wordpress/
[+] Started: Fri Dec  8 07:36:19 2017

[!] The WordPress 'http://10.0.2.12/wordpress/readme.html' file exists exposing a version number
[+] Interesting header: LINK: <http://10.0.2.12/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://10.0.2.12/wordpress/wp-login.php?action=register
[+] XML-RPC Interface available under: http://10.0.2.12/wordpress/xmlrpc.php
[!] Upload directory has directory listing enabled: http://10.0.2.12/wordpress/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://10.0.2.12/wordpress/wp-includes/

[+] WordPress version 4.8.1 (Released on 2017-08-02) identified from meta generator, links opml, stylesheets numbers
[!] 12 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/70b21279098fc973eae803693c0705a548128e48
    Reference: https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2c5de93cd18ec
[i] 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
[i] Fixed in: 4.8.2
```

```
[!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping
    Reference: https://wpvulndb.com/vulnerabilities/8911
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/41457
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14719
[i] Fixed in: 4.8.2

[!] Title: WordPress 4.4-4.8.1 - Path Traversal in Customizer
    Reference: https://wpvulndb.com/vulnerabilities/8912
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/41397
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14722
[i] Fixed in: 4.8.2

[!] Title: WordPress 4.4-4.8.1 - Cross-Site Scripting (XSS) in oEmbed
    Reference: https://wpvulndb.com/vulnerabilities/8913
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/41448
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14724
[i] Fixed in: 4.8.2

[!] Title: WordPress 4.2.3-4.8.1 - Authenticated Cross-Site Scripting (XSS) in Visual Editor
    Reference: https://wpvulndb.com/vulnerabilities/8914
    Reference: https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
    Reference: https://core.trac.wordpress.org/changeset/41395
    Reference: https://blog.sucuri.net/2017/09/stored-cross-site-scripting-vulnerability-in-wordpress-4-8-1.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14726
[i] Fixed in: 4.8.2
```

```
[!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset
    Reference: https://wpvulndb.com/vulnerabilities/8807
    Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html
    Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html
    Reference: https://core.trac.wordpress.org/ticket/25239
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295

[!] Title: WordPress <= 4.8.2 - $wpdb->prepare() Weakness
    Reference: https://wpvulndb.com/vulnerabilities/8941
    Reference: https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/
    Reference: https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799ddd577202167d
    Reference: https://twitter.com/ircmaxell/status/923662170092638208
    Reference: https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-technical.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16510
[i] Fixed in: 4.8.3

[!] Title: WordPress 2.8.6-4.9 - Authenticated JavaScript File Upload
    Reference: https://wpvulndb.com/vulnerabilities/8966
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206adde299b0509
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17092
[i] Fixed in: 4.8.4

[!] Title: WordPress 1.5.0-4.9 - RSS and Atom Feed Escaping
    Reference: https://wpvulndb.com/vulnerabilities/8967
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3d1f4f90541de
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17094
[i] Fixed in: 4.8.4

[!] Title: WordPress 4.3.0-4.9 - HTML Language Attribute Escaping
    Reference: https://wpvulndb.com/vulnerabilities/8968
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd691420f43da6c09a
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17093
[i] Fixed in: 4.8.4

[!] Title: WordPress 3.7-4.9 - 'newbloguser' Key Weak Hashing
    Reference: https://wpvulndb.com/vulnerabilities/8969
    Reference: https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591b864d833326c
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17091
[i] Fixed in: 4.8.4

[+] WordPress theme in use: twentyfifteen - v1.8

[+] Name: twentyfifteen - v1.8
 |  Last updated: 2017-11-16T00:00:00.000Z
 |  Location: http://10.0.2.12/wordpress/wp-content/themes/twentyfifteen/
 |  Readme: http://10.0.2.12/wordpress/wp-content/themes/twentyfifteen/readme.txt
[!] The version is out of date, the latest version is 1.9
 |  Style URL: http://10.0.2.12/wordpress/wp-content/themes/twentyfifteen/style.css
 |  Theme Name: Twenty Fifteen
 |  Theme URI: https://wordpress.org/themes/twentyfifteen/
 |  Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple,...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Fri Dec  8 07:36:24 2017
[+] Requests Done: 351
[+] Memory used: 35.18 MB
[+] Elapsed time: 00:00:04
```

I've tried bruteforcing with some wordlists, but was not able to crack the admin password, so It's time to go back and see what other services are running on the machine..

nmap service discovery

`nmap -sC 10.0.2.12`

```
Host script results:
|_nbstat: NetBIOS name: LAZYSYSADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: lazysysadmin
|   NetBIOS computer name: LAZYSYSADMIN\x00
|   Domain name: \x00
|   FQDN: lazysysadmin
|_  System time: 2017-12-08T16:58:01+10:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2017-12-08 07:58:01
|_  start_date: 1601-01-01 00:17:30
```

Samba

We see that there is a Samba Ubuntu running so we can try to connect to it with `smbclient -L 10.0.2.12` this will prompt us for a password, we don't know this password so just press enter (so you use anonymous mode), and you'll see the following output:

```
root@clueless:~# smbclient -L 10.0.2.12
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:

        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
```

two options now, use CLI or GUI, I recommend GUI, open your explorer and go to “other locations” type in the following server address: `smb://10.0.2.12` and you can browse freely

alternatively, using CLI

`smbclient //LAZYSYSADMIN/share$`

Will grant you access to an smb shell in the share folder

`get` will download files from the samba server into your home dir.

I used the GUI approach.

in the samba share you will find a document called “deets.txt”

when you open it it will contain this:

```
CBF Remembering all these passwords.

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

Password 12345
```

in the”wp-config.php” file there was the following interesting line `DB_PASSWORD,TogieMYSQL12345^^'` ——

Root

I tried to SSH `ssh togie@10.0.2.12` togie because on wordpress he has a post saying my name is togie, and in the password of the wpdb there is also Togie in there and used the password 12345 it worked.

`sudo -l` showed me that togie can run all commands

so all we have to do is `sudo -i` and we are Root

Tags: ctf exploits Pentest

Categories: Penetration-Testing

Updated: December 08, 2017

SHARE ON

Twitter Facebook G+ Google+ in LinkedIn

Previous Next

YOU MAY ALSO ENJOY

Pentest: Domo arigato mr. Roboto

9 minute read

Since I want to do the OSCP certifcation next year, I figured it's time to try and tackle a machine that is listed under "OSCP like" in some forums I scoured...

Pentest: owning Zico2

8 minute read

Another day, another VM to get owned! This time I'm doing an intermediate one called Zico2, as always this VM is available on Vulnhub here. —-

Pentest: owning a docker host

10 minute read

As I did my bachelorthesis around Docker and best practices around Docker, I found it interesting and challenging for myself to break a Docker host. Vulnhub ...

Pentest: owning rick and morty VM

6 minute read

My collegues told me about vulnhub, a website for peneteration tester to test their skills on boot2root VM's. On the site you'll find multiple boxes, with va...

FOLLOW: GITHUB FEED