

Report

Task 1: Network Configuration

Figure 1

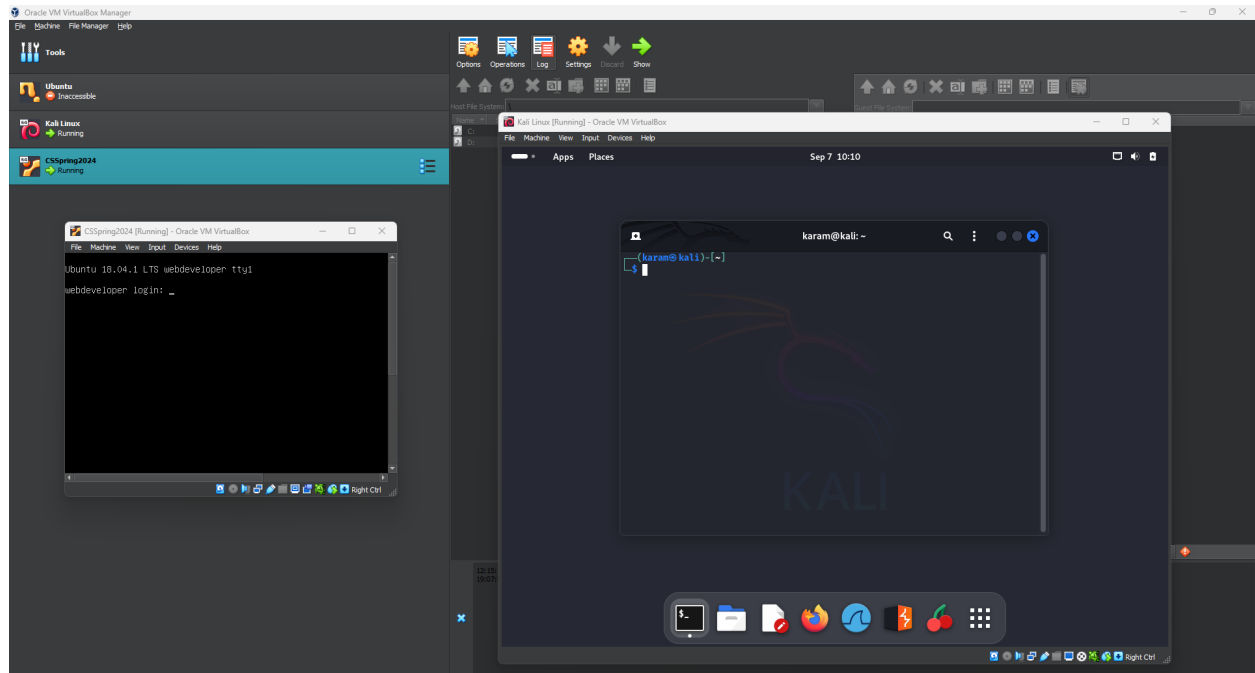


Table 1

VM	IP Address	Subnet mask	Default Gateway	Network Adapter
Kali Linux	192.168.100.35	255.255.255.0	192.168.100.1	Brigid Adapter
Target	192.168.100.37	255.255.255.0	192.168.100.1	Brigid Adapter

Task 2: Reconnaissance and Vulnerability Analysis

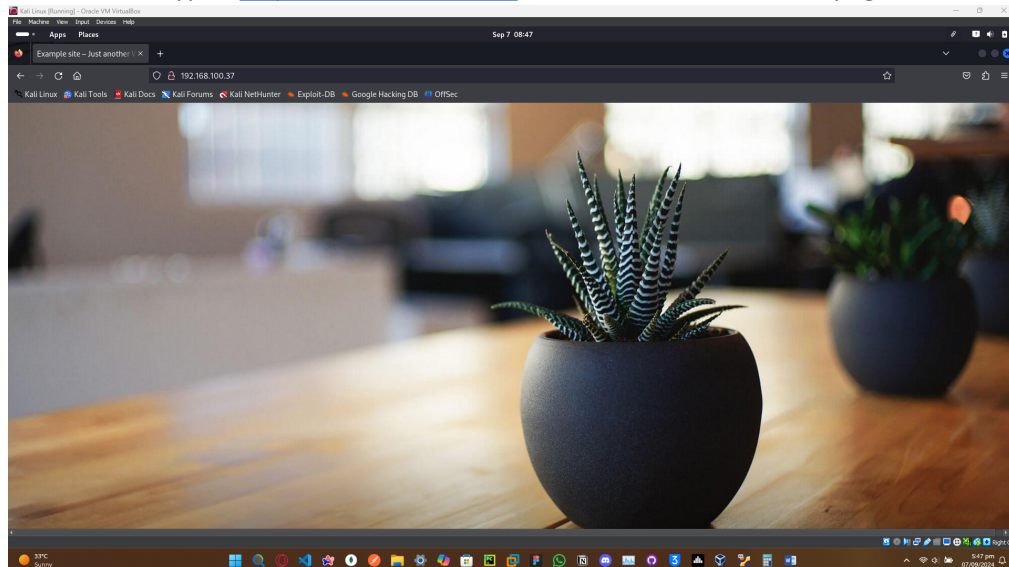
1. Identify the target machine's IP address
 - a. I used the `"sudo netdiscover"` on my home Wi-Fi but there were way too many devices that I was unable to find the target device so I used my mobile hotspot and then again ran the command but it was way too slow so I used the `"ifconfig"` command to get the info related to the adaptor and then used the command with a specific IP range and device adaptor `"sudo netdiscover -i eth0 -r 192.168.100.0/24"` then easily, I got the device, it was only one device named `"PCS Systemtechnik GmbH"` with an IP of `"192.168.100.37"`.
2. Determine the open ports and running services

```
karam@kali: ~  
  
(karam@kali)-[~]  
$ sudo nmap 192.168.100.37  
[sudo] password for karam:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 08:19 EDT  
Nmap scan report for 192.168.100.37  
Host is up (0.00050s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:CC:54:C9 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

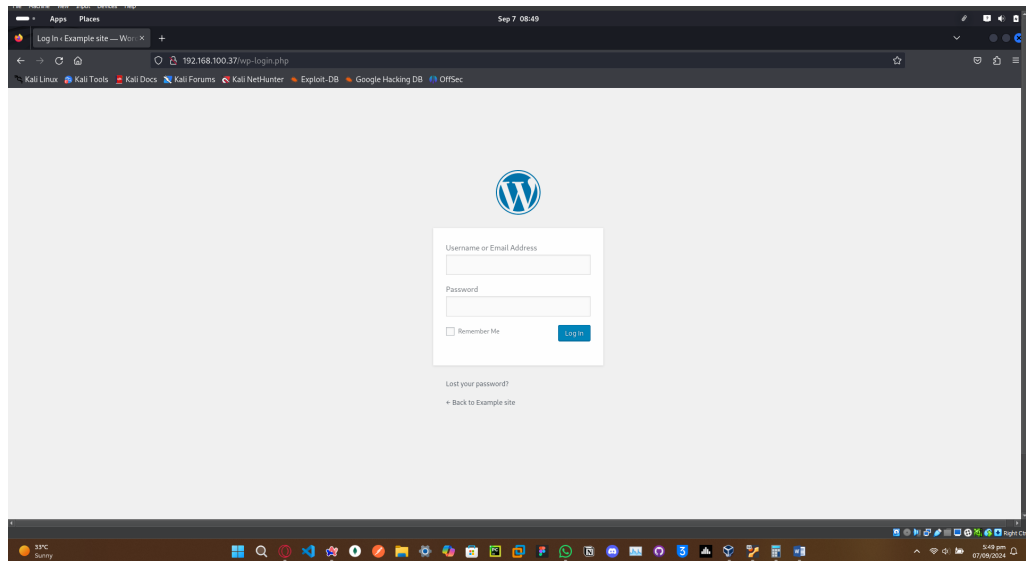
- a.
- b. I used the command “`sudo nmap 192.168.100.37`” to find the open ports which is port 80 aka http port running http service and port 22 the port running TCP service.

3. Identify Vulnerabilities in Web Application

- a. As I find out that the service is http and the IP is 192.168.100.37 so I went to the browser and typed <http://192.168.100.37/> and it took me to the webpage .



- b.
- c. There I found out a login page on the link <http://192.168.100.37/wp-login.php>.



- d.
- e. I tried to use the common username and password combos like admin/admin, admin/password etc but failed.

4. Directory Enumeration Using Dirb

```
karam@kali: ~/Desktop
File Actions Edit View Help
karam@kali) [~/Desktop]
$ dirb http://192.168.100.37/

DIRB v2.22
By The Dark Raver

START_TIME: Sat Sep 7 06:36:37 2024
URL_BASE: http://192.168.100.37/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.100.37/ ---
+ http://192.168.100.37/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.100.37/ipdata/
+ http://192.168.100.37/server-status (CODE:403|SIZE:302)
=> DIRECTORY: http://192.168.100.37/wp-admin/
=> DIRECTORY: http://192.168.100.37/wp-content/
=> DIRECTORY: http://192.168.100.37/wp-includes/
+ http://192.168.100.37/xmlrpc.php (CODE:405|SIZE:42)

--- Entering directory: http://192.168.100.37/ipdata/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.100.37/wp-admin/ ---
```

- a.
- b. I used the command “dirb <http://192.168.100.37/>” to search for hidden directories or files that may contain sensitive information.
- c. I didn’t understand what this info is representing so I asked GPT about it.

1. Directories and Files Found:

- <http://192.168.100.37/index.php> : This is a page that redirects (HTTP status 301) but doesn't display content.
- <http://192.168.100.37/ipdata/> : This directory is found and is listable.
- <http://192.168.100.37/server-status> : Access is forbidden (HTTP status 403).
- <http://192.168.100.37/wp-admin/> : This is a WordPress admin directory.
- <http://192.168.100.37/wp-content/> : This is where WordPress stores content like themes and plugins.
- <http://192.168.100.37/wp-includes/> : Contains WordPress core files, and it is listable.
- <http://192.168.100.37/xmlrpc.php> : This file is present but returns a method not allowed status (HTTP status 405).

d.

- e. By this I get to know that I Dirb has found three list able directories (wp-admin ,wp-includes ,ipdata) out of which two (wp-includes ,ipdata) are discoverable and one (wp-admin) requires login credentials.

The screenshot shows two browser windows. The left window displays the 'Index of /wp-includes' directory, listing various files and folders such as 'ID3/', 'IXR/', 'Requests/', 'SimplePie/', 'Text/', 'admin-bar.php', 'atomlib.php', 'author-template.php', 'bookmark-template.php', 'bookmark.php', 'cache.php', 'canonical.php', 'capabilities.php', 'category-template.php', 'category.php', 'certificates/', 'class-IXR.php', 'class-feed.php', 'class-http.php', 'class-json.php', 'class-oembed.php', 'class-phpass.php', 'class-phpmailer.php', 'class-pop3.php', 'class-requests.php', and 'class-simpleninja.php'. The right window displays the 'Index of /ipdata' directory, showing a 'Parent Directory' link and a file named 'analyze.cap' with a size of 2.8M. Below the file list, it indicates 'Apache/2.4.29 (Ubuntu) Server at 192.168.100.37 Port 80'.

f.

- g. There was nothing in the wp-include as it contained all the static files that doesn't give any info generally.

h. In ipdata I found a Wireshark file named as [analyze.cap](#) and opened it.

- i. Then I checked the [http:post methods](#) because usually forms are submit using this type of request.

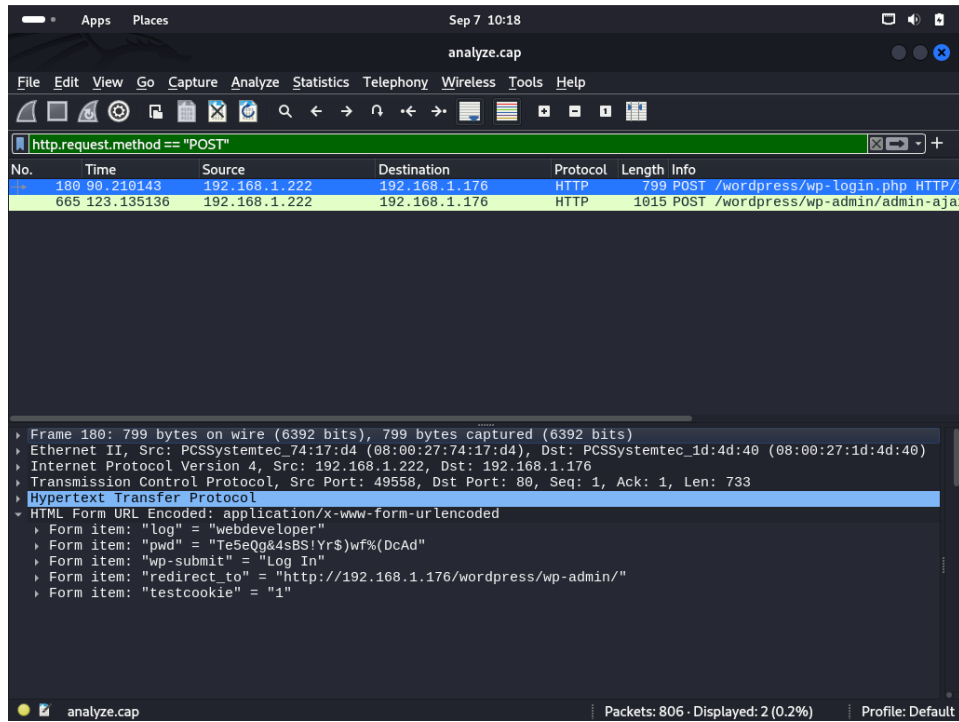
j. I used the Wireshark filter and used the command [http.request.method == "POST"](#).

The screenshot shows the Wireshark interface with the filter 'http.request.method == "POST"' applied. The packet list shows two packets. The first packet is an HTTP POST request to '/wordpress/wp-login.php' with a length of 799 bytes. The second packet is an HTTP POST request to '/wordpress/wp-admin/admin-ajax.php' with a length of 1015 bytes. The details pane for the second packet is visible, showing the 'HTTP' section with 'POST' method and 'application/x-www-form-urlencoded' content type.

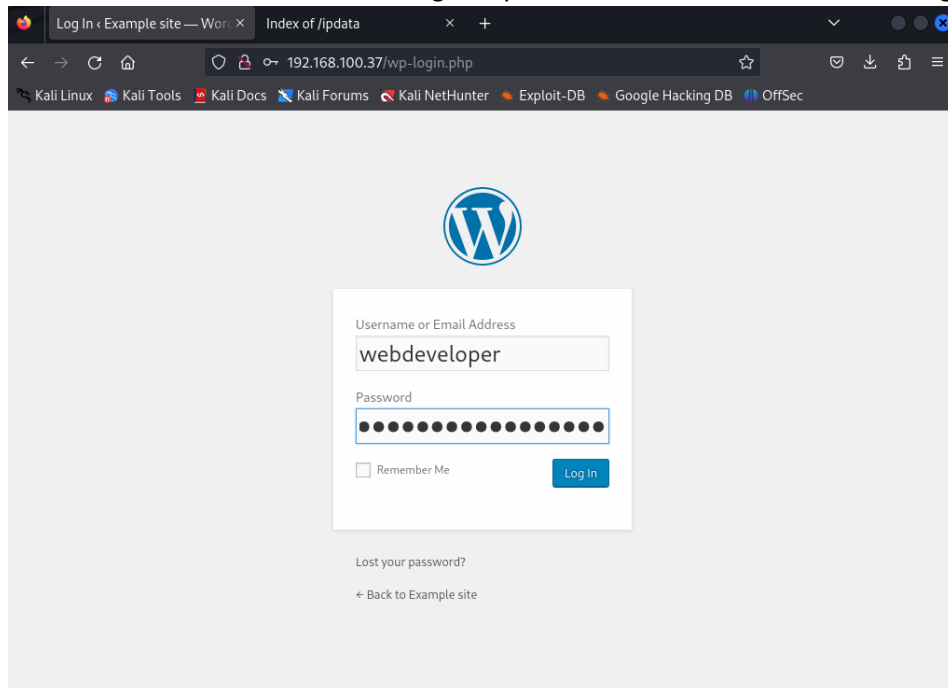
k.

- l. As by the length info it was obvious the second packet had something to do with the "[admin-ajax.php](#)" so I clicked it and opened its details.

m. After searching around under the heading HTML Form URL-encoded, I found some info as shown in the pic below.

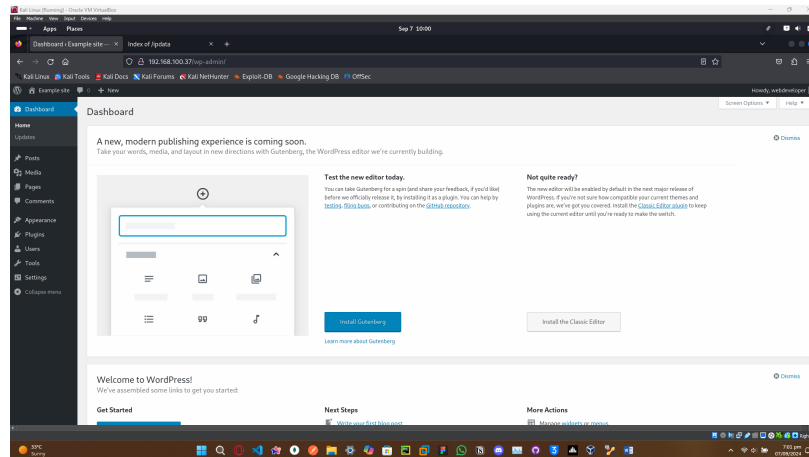


- n. analyze.cap Packets: 806 · Displayed: 2 (0.2%) Profile: Default
- o. There were form items named as log and pwd and when I used them on the login page.



- p.
- q. After using it as login credentials, I was on the dashboard as shown below.

r.



Conclusion

- **Login:** webdeveloper
- **Password:** Te5eQg&4sBS!Yr\$)wf%(DcAd

This concludes the analysis and demonstrates the process of identifying a target machine, discovering vulnerabilities, and successfully exploiting them to gain access.