**SECURETECH INNOVATIONS**
***your partner in digital security***

# Penetration Testing Report

## Powerzio

## Expert auditor in charge of the assignment :

**Noé Jaïs, François Machere, Thomas Lamballais**

# Contents

# Audit Specifications

**Start date** : 14/01/2024

**End date** : 9/02/2024

**Duration** : 1 month

**Document Reference** : M-TRC-853 - Report

**Company** : POWERZIO

# Document Versions

| Version | Date | Description |
|---|---|---|
| 0.1 | 16/01/2024 | Initial version |
| 0.2 | 22/01/2024 | Add audit specifications |
| 0.3 | 25/01/2024 | Add pre-engagement information and summary |
| 0.4 | 30/01/2024 | Add vulnerabilities listing |
| 0.5 | 2/02/2024 | Add remediation advice |
| 0.6 | 04/02/2024 | Add description of the methodology |
| 0.7 | 06/02/2024 | Add audit details |
| 1.0 | 09/02/2024 | Delivery version |

# Summary

### Audit objectives

- To evaluate the security of POWERZIO's remote work infrastructure, including VPNs, remote access tools, and end-point security.
- To identify potential vulnerabilities that could be exploited in a remote working scenario.
- To assess the overall resilience of POWERZIO's IT infrastructure against cyber threats, considering the critical nature of their operations as an energy contractor.

### Scope of the audit

- Security assessment of remote access systems, including VPNs and remote desktop protocols.
- Evaluation of network security controls and firewall configurations.
- Analysis of end-point protection mechanisms on devices used for remote work.
- Review of policies and procedures related to remote work, including access controls and employee cybersecurity awareness.

### Reporting structure

- Detailed report including risk assessment, findings, and remediation advice to be provided to POWERZIO executive leadership team.

### Compliance standards

- Ensuring compliance with relevant cybersecurity standards and best practices, as well as legal requirements pertinent to the energy sector.

### Confidentiality statement

- All information gathered, processed, and reported in this audit will be treated with the utmost confidentiality.
- Adherence to POWERZIO's data protection policies and any relevant data protection legislation.

### Stakeholders

- POWERZIO executive leadership team

### Contact Information

- POWERZIO contact : executive.groups@powerzio.com
- Lead auditor contact : noe.jais@securetech.com

# Pre-engagement information

## Audit Team

- Cybersecurity auditor : Noé Jaïs
- Network security specialist : François Machere
- Security analyst : Thomas Lamballais

## Scope

- 10.10.11.0/24

## Methodology

- Black Box

# Vulnerabilities Listing

| Vulnerabilities | | | | | | Remediations | | | |
|---|---|---|---|---|---|---|---|---|---|
| Id | Vulnerability | Affected IP | Affected Port | Description | Severity | Id | Remediation | Difficulty | Priority |
| V01 | OpenSSH 7.6p1 | 10.10.10.9 | 22 | The system is running a vulnerable version of OpenSSH (7.6p1) allowing username enumeration | Medium | R01 | Update to the latest versions of OpenSSH apply security patches, and ensure network security configurations are up to date | Easy | Low |
| V02 | OpenSSH 7.2p2 | 10.10.10.10 | 22 | Outdated versions of OpenSSH detected (7.2p2) | Medium | R02 | Update to the latest versions of OpenSSH apply security patches, and ensure network security configurations are up to date | Medium | Medium |
| V03 | Dnsmasq 2.75 | 10.10.10.10 | 53 | dnsmasq version 2.75 is susceptible to a Denial of Service (DoS) | Medium | R03 | Update to the latest stable version of dnsmasq that includes a fix for the DoS vulnerability. Review dnsmasq configuration files to apply best security practices | Medium | High |
| V04 | OpenSSH 7.2p2 | 10.10.10.11 | 22 | Outdated versions of OpenSSH detected (7.2p2) | Medium | R04 | Update to the latest versions of OpenSSH apply security patches, and ensure network security configurations are up to date | Medium | Medium |
| V05 | Dnsmasq 2.75 | 10.10.10.11 | 53 | dnsmasq version 2.75 is susceptible to a Denial of Service (DoS) | High | R05 | Update to the latest stable version of dnsmasq that includes a fix for the DoS vulnerability. Review dnsmasq configuration files to apply best security practices | Medium | High |
| V06 | NLnet Labs NSD | 10.10.10.13 | 53 | The Name Server Daemon (NSD) is outdated, there is a missing PTR (Pointer) record, and a DNS enumeration issue | Medium | R06 | Update NSD to the latest version, add the missing PTR record, and secure DNS settings to prevent enumeration. Implement DNS security best practices | High | Low |
| V07 | Samba smbd 3.X - 4.X | 10.10.10.22 | 139, 445 | Outdated Samba version, anonymous connection, listing of confidential shared folder and connection to private shared folder of Myles | Critical | R07 | Update to the latest secure version of Samba, review configuration files for security best practices, and restrict access to the necessary minimum | Medium | High |
| V08 | CGI Camera surveillance Netwave IP camera | 10.10.10.24 | 23023 | Netwave IP Camera running vulnerable CGI who lead to a password vulnerability disclosure | High | R08 | Update camera firmware to the latest version, change default credentials, and ensure that cameras are not accessible from untrusted networks | Easy | High |
| V09 | Werkzeug/3.0.1 Python/ | 10.10.10.26 | 80 | The service is running outdated Werkzeug/Python versions | Medium | R09 | Update to the latest versions of Python and Werkzeug, check for compatibility issues, and perform a thorough code review | Medium | Low |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 3.8.17 | | | | | | to patch potential exploits | | |
| V10 | Mosquitto 2.0.15 | 10.10.10.34 | 1883 | MQTT broker running an outdated version of Mosquitto (2.0.15) | Medium | R10 | Update to the latest stable version of Mosquitto, ensure secure configuration of the broker, and implement strong authentication and encryption mechanisms | Medium | Low |
| V11 | Node.js Express framework | 10.10.10.48 | 80 | Detected vulnerable version of the Node.js Express Framework, which lead to DOS vunlnerability | Critical | R11 | Update Node.js and the Express Framework to the latest versions, review all dependencies for vulnerabilities and update them, and conduct a code review for potential security flaws | High | High |
| V12 | Vsftpd 2.3.4 | 10.10.10.53 | 21 | The service is running vulnerable versions of Vsftpd, which lead to unauthorized access and code execution | Critical | R12 | Update to the latest versions of Vsftpd, apply all security patches, and ensure secure configurations for both services. Regularly review logs for any unusual access patterns and verify there is no new member created | High | High |
| V13 | OpenSSH 7.2p2 | 10.10.10.53 | 22 | The service is running an outdated versions of OpenSSH (7.2p2), potentially leading to security vulnerabilities | Medium | R13 | Update to the latest versions of OpenSSH apply security patches, and ensure network security configurations are up to date | Medium | Medium |
| V15 | OpenSSH 7.2p2 | 10.10.10.84 | 22 | Detected OpenSSH version with known vulnerabilities that could lead to security breaches | Medium | R15 | Update to the latest versions of OpenSSH apply security patches, and ensure network security configurations are up to date | Medium | Medium |
| V16 | Redis key-value store 3.0.6 | 10.10.10.132 | 6379 | Outdated Redis version (3.0.6) with no credential requirement for access, posing a high risk of unauthorized data access | High | R16 | Update Redis to the latest stable release, configure password protection to secure access, and implement network-level security controls to restrict unauthorized access | High | High |
| V21 | Pop3 | 10.10.10.216 | 110 | The POP3 service on the server does not implement account lockout or strong password requirements, allowing for successful brute-force attacks | High | R21 | Enforce strong password policies, implement account lockouts, and monitor for unusual access patterns | High | High |
| V23 | Apache httpd 2.4.38 | 10.10.10.222 | 80 | The Apache HTTP server runs on an outdated version (2.4.38), exposing a vulnerability that allows users to be enumerated. This flaw can be exploited to carry out brute force attacks | Medium | R23 | Upgrade to the latest stable version of Apache HTTP Server. Review and apply security best practices in the server configuration. Enable only necessary modules and directives | Medium | Low |
| V24 | Mysql MariaDB 11.2.2 | 10.10.10.223 | 3306 | The service is running an outdated version of MariaDB (11.2.2), potentially leading to security vulnerabilities | Medium | R24 | Update MariaDB to the latest version to address known vulnerabilities and improve security. Ensure strong passwords are used and review user privileges | Medium | Low |

**Vulnerability ID**: V01
**Affected System IP**: 10.10.10.9
**Affected port**: 22
**Affected Component**: OpenSSH 7.6p1
**Operating System**: Ubuntu 4ubuntu0.7
**Description**: The system is running a vulnerable version of OpenSSH (7.6p1).
**Severity Rating**: **Medium**
**Potential Impact**: Allowing username enumeration who can lead to brute force attack.
**Discovery Date**: 16/01/2024
**Remediation Advice**: Update to the latest version of OpenSSH and apply relevant security patches.
**Evidence/Proof of Concept**:

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 10.10.10.9:22 - SSH - Using malformed packet technique
[*] 10.10.10.9:22 - SSH - Starting scan
[+] 10.10.10.9:22 - SSH - User 'pc9' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**References**:
[OpenSSH 2.3 < 7.7 - Username Enumeration]

**Vulnerability ID**: V02
**Affected System IP**: 10.10.10.10
**Affected port**: 22
**Affected Component**: OpenSSH 7.2p2
**Operating System**: Ubuntu 4ubuntu2.10
**Description**: The system is running OpenSSH version 7.2p2
**Severity Rating**: **Medium**
**Potential Impact**: While no immediate vulnerabilities were found, maintaining an outdated version of critical software like OpenSSH could potentially expose the system to future security threats and vulnerabilities as they are identified
**Discovery Date**: 16/01/2024
**Remediation Advice**: Update to the latest version of OpenSSH and apply relevant security patches
**Evidence/Proof of Concept**: Identified through version analysis

**Vulnerability ID**: V03
**Affected System IP**: 10.10.10.10
**Affected port**: 53
**Affected Component**: dnsmasq 2.75
**Description**: The system is running an outdated dnsmasq version
**Severity Rating**: **Medium**
**Potential Impact**: This outdated dnsmasq version could lead to DNS spoofing and cache poisoning, risking network security and disrupting service integrity
**Discovery Date**: 16/01/2024
**Remediation Advice**: Upgrade to the latest dnsmasq version
**Evidence/Proof of Concept**: Identified through version analysis

**Vulnerability ID**: V04
**Affected System IP**: 10.10.10.11
**Affected port**: 22
**Affected Component**: OpenSSH 7.2p2
**Operating System**: Ubuntu 4ubuntu2.10
**Description**: The system is running OpenSSH version 7.2p2
**Severity Rating**: **Medium**
**Potential Impact**: While no immediate vulnerabilities were found, maintaining an outdated version of critical software like OpenSSH could potentially expose the system to future security threats and vulnerabilities as they are identified
**Discovery Date**: 16/01/2024
**Remediation Advice**: Update to the latest version of OpenSSH and apply relevant security patches
**Evidence/Proof of Concept**: Identified through version analysis

**Vulnerability ID**: V05
**Affected System IP**: 10.10.10.11
**Affected port**: 53
**Affected Component**: dnsmasq 2.75
**Description**: The system is running an outdated dnsmasq version
**Severity Rating**: **Medium**
**Potential Impact**: This outdated dnsmasq version could lead to DNS spoofing and cache poisoning, risking network security and disrupting service integrity
**Discovery Date**: 16/01/2024
**Remediation Advice**: Upgrade to the latest dnsmasq version
**Evidence/Proof of Concept**: Identified through version analysis

**Vulnerability ID**: V06
**Affected System IP**: 10.10.10.13
**Affected port**: 53
**Affected Component**: NLnet Labs NSD
**Description**: The Name Server Daemon (NSD) is outdated, there is a missing PTR (Pointer) record, and a DNS enumeration issue
**Severity Rating**: **Medium**
**Potential Impact**:
The vulnerabilities may lead to DNS spoofing and unauthorized network mapping, risking data exposure and service disruptions
**Discovery Date**: 28/01/2024
**Remediation Advice**: Update NSD to the latest version, add the missing PTR record, and secure DNS settings to prevent enumeration. Implement DNS security best practices
**Evidence/Proof of Concept**:

```
[*] 10.10.10.13:53 - Querying DNS NS records for powerzio.com
[+] 10.10.10.13:53 - powerzio.com NS: dns1.registrar-servers.com
[+] 10.10.10.13:53 - powerzio.com NS: dns2.registrar-servers.com
[*] 10.10.10.13:53 - Attempting DNS AXFR for powerzio.com from 156.154.132.200
[*] 10.10.10.13:53 - Query powerzio.com DNS AXFR - no results were received
[*] 10.10.10.13:53 - Attempting DNS AXFR for powerzio.com from 156.154.133.200
[*] 10.10.10.13:53 - Query powerzio.com DNS AXFR - no results were received
[*] 10.10.10.13:53 - Querying DNS CNAME records for powerzio.com
[*] 10.10.10.13:53 - Querying DNS NS records for powerzio.com
[+] 10.10.10.13:53 - powerzio.com NS: dns1.registrar-servers.com
[+] 10.10.10.13:53 - powerzio.com NS: dns2.registrar-servers.com
[*] 10.10.10.13:53 - Querying DNS MX records for powerzio.com
[+] 10.10.10.13:53 - powerzio.com MX: eforward5.registrar-servers.com
[+] 10.10.10.13:53 - powerzio.com MX: eforward4.registrar-servers.com
[+] 10.10.10.13:53 - powerzio.com MX: eforward1.registrar-servers.com
[+] 10.10.10.13:53 - powerzio.com MX: eforward2.registrar-servers.com
[+] 10.10.10.13:53 - powerzio.com MX: eforward3.registrar-servers.com
[*] 10.10.10.13:53 - Querying DNS SOA records for powerzio.com
[+] 10.10.10.13:53 - powerzio.com SOA: dns1.registrar-servers.com
[*] 10.10.10.13:53 - Querying DNS TXT records for powerzio.com
[+] 10.10.10.13:53 - powerzio.com TXT: google-site-
verification=TYT_12MYYv9VBiPWcwHxcECB2sJkBT-qJ8otxBeuejI
[+] 10.10.10.13:53 - powerzio.com TXT: v=spf1 include:spf.efwd.registrar-
servers.com ~all
[*] 10.10.10.13:53 - Querying DNS SRV records for powerzio.com
[*] Auxiliary module execution completed
```

**Vulnerability ID**: V07
**Affected System IP**: 10.10.10.22
**Affected port**: 139,445
**Affected Component**: Samba smbd 3.X-4.X
**Description**: The system is running Samba versions 3.X to 4.X
**Severity Rating**: **Critical**
**Potential Impact**: This vulnerability allows unauthorized access to shared network resources, which can lead to the theft of private information.
**Discovery Date**: 16/01/2024
**Remediation Advice** : Update to the latest stable version of Samba and make sure to remove the anonymous connection in the smb.conf file
**Evidence/Proof of Concept**:

```
[→  ~ smbclient \\\\10.10.10.22\\myles -U Myles --password='<78P7,P'
 Can't load /usr/local/etc/smb.conf - run testparm to debug it
 Try "help" to get a list of possible commands.
[smb: \> ls
  .                                   D        0  Thu Jan 11 10:27:36 2024
  ..                                  D        0  Thu Jan 11 10:27:33 2024
  .profile                            H      655  Fri Jul 12 21:26:32 2019
  .bashrc                             H     3771  Tue Sep  1 01:27:45 2015
  .bash_logout                        H      220  Tue Sep  1 01:27:45 2015
  todo                                N      164  Thu Jan 11 10:12:31 2024

                23990808 blocks of size 1024. 1414216 blocks available
smb: \>
```

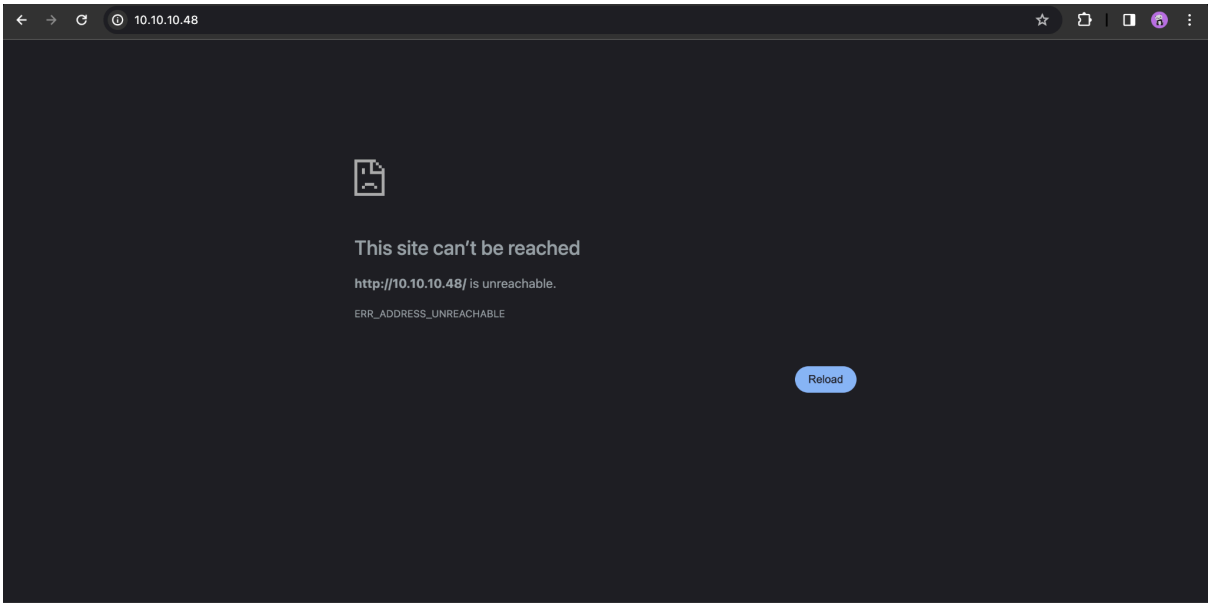
**Vulnerability ID**: V08
**Affected System IP**: 10.10.10.24
**Affected port**: 23023
**Affected Component**: Netwave IP camera
**Description**: Netwave IP Camera running vulnerable CGI that could allow unauthorized access or camera hijacking
**Severity Rating**: **Critical**
**Potential Impact**: Allows an unauthenticated attacker to exfiltrate sensitive information about the network configuration like the network SSID and password
**Discovery Date**: 28/01/2024
**Remediation Advice**: Update camera firmware to the latest version, change default credentials, and ensure that cameras are not accessible from untrusted networks
**Evidence/Proof of Concept**:

```
getting system information..10.10.10.24:23023
victims MAC-ADDRESS: 003E0502328A
getting wireless information..
victims wireless information..
                [Default]
                CountryRegion=0
                SSID=NuclearNetwork1
                NetworkType=Infra
                Channel=0
                WirelessMode=0
                AuthMode=WPA2PSK
                EncrypType=AES
                WPAPSK=Nucle@RPow3r

checking for memory dump vulnerability..
starting to read memory dump.. this could take a few minutes
hit CTRL+C to exit..
strings in binary data found.. password should be around line 10000
198488

mac address triggered.. printing the following dumps, could leak username and passwords..

firstline.. root

possible username: z448ehUgcQmoUw

possible password: MyGreatWifi

following line..

defaultPasswordPlzChangeMe

199559

mac address triggered.. printing the following dumps, could leak username and passwords..

firstline.. root

possible username: z448ehUgcQmoUw

possible password: MyGreatWifi

following line..

defaultPasswordPlzChangeMe
```

**References**:
[Information disclosure in Netwave IP camera]

**Vulnerability ID**: V10
**Affected System IP**: 10.10.10.34
**Affected port**: 1883
**Affected Component**: Mosquitto 2.0.15
**Description**: MQTT broker running an outdated version of Mosquitto
**Severity Rating**: **Medium**
**Potential Impact**: Unauthorized access and data manipulation could occur, compromising system integrity and confidentiality
**Discovery Date**: 28/01/2024
**Remediation Advice**: Update to the latest stable version of Mosquitto, ensure secure configuration of the broker, and implement strong authentication and encryption mechanisms
**Evidence/Proof of Concept**: Identified through version analysis

**Vulnerability ID**: V11
**Affected System IP**: 10.10.10.48
**Affected port**: 80
**Affected Component**: Node.js Express framework
**Description**: Detected vulnerable version of the Node.js Express Framework allowing DOS vulnerability
**Severity Rating**: **Critical**
**Potential Impact**: Impossibility to reach the site
**Discovery Date**: 28/01/2024
**Remediation Advice**: Update Node.js and the Express Framework to the latest versions, review all dependencies for vulnerabilities and update them, and conduct a code review for potential security flaws
**Evidence/Proof of Concept**:




**References**:
CVE-2013-4450

**Vulnerability ID**: V12
**Affected System IP**: 10.10.10.53
**Affected port**: 21 (FTP), 22 (SSH)
**Affected Component**: vsftpd 2.3.4, OpenSSH 7.2p2
**Description**: The system is running vsftpd version 2.3.4 and OpenSSH version 7.2p2, both of which are known to have critical vulnerabilities. vsftpd 2.3.4 is vulnerable to backdoor access (CVE-2011-2523), and OpenSSH 7.2p2 has user enumeration issues (CVE-2016-6210) among other potential.
**Severity Rating**: **Critical**
**Potential Impact**: Could allow an attacker to gain unauthorized access, escalate privileges, or execute arbitrary code on the server, leading to a full system compromise.
**Discovery Date**: 26/01/2024
**Remediation Advice**: Update to the latest versions of vsftpd and OpenSSH, ensuring that all relevant security patches are applied. Configure both services securely and conduct regular reviews of system and security logs for any unusual access patterns. Additionally, audit accounts periodically to confirm that no unauthorized users have been created.
**Evidence/Proof of Concept**:

```
adduser
adduser: Only one or two names allowed.
adduser john
Adding user `john' ...
Adding new group `john' (1002) ...
Adding new user `john' (1002) with group `john' ...
Creating home directory `/home/john' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: pass
Retype new UNIX password: pass
passwd: password updated successfully
Changing the user information for john
Enter the new value, or press ENTER for the default
        Full Name []: john travolta
        Room Number []: 0
        Work Phone []:
        Home Phone []:
        Other []:

Is the information correct? [Y/n] y
sh: 40: y: not found
Y
sh: 41: Y: not found
YES
sh: 42: YES: not found


ls
adduser.conf
whoams
sh: 46: whoams: not found
whoami
root
usermod -aG sudo john
ls
adduser.conf
id john
uid=1002(john) gid=1002(john) groups=1002(john),27(sudo)
```

**References**:
CVE-2011-2523
CVE-2016-6210

**Vulnerability ID**: V15
**Affected System IP**: 10.10.10.84
**Affected port**: 22
**Affected Component**: OpenSSH 7.6p1
**Operating System**: Ubuntu 4ubuntu0.7
**Description**: The system is running an outdated version of OpenSSH (7.6p1)
**Severity Rating**: **Medium**
**Potential Impact**: While no immediate vulnerabilities were found, maintaining an outdated version of critical software like OpenSSH could potentially expose the system to future security threats and vulnerabilities as they are identified
**Discovery Date**: 16/01/2024
**Remediation Advice**: Update to the latest version of OpenSSH and apply relevant security patches
**Evidence/Proof of Concept**: Identified through version analysis

**Vulnerability ID**: V16
**Affected System IP**: 10.10.10.132
**Affected port**: 6379
**Affected Component**: Redis key-value store 3.0.6
**Description**: Outdated Redis version with no password configuration allowing unauthorized data access
**Severity Rating**: **Medium**
**Potential Impact**: Attackers can gain unauthorized access to the Redis data store, allowing them to view, modify, or delete data held within the database. This access could lead to the compromise of sensitive information.
**Discovery Date**: 28/01/2024
**Remediation Advice**: Update Redis to the newest stable release, configure password protection, and implement network-level security controls to restrict access
**Evidence/Proof of Concept**:

```
msf6 auxiliary(gather/redis_extractor) > run

[+] 10.10.10.132:6379      - Connected to Redis version 3.0.6
[*] 10.10.10.132:6379      - Extracting about 849 keys from database 0

Data from 10.10.10.132:6379      database 0
==========================================

 Key       Value
 ---       -----
 1003774   mathis
 1034536   park
 1039442   wong
 1054483   hester
 1086204   brady
 1087108   lindsey
 1108630   cabrera
 1118115   osborne
 1129644   stafford
 1130438   zimmerman
 1143741   phelps
 1148403   prince
 1157520   mcfarland
 1177868   hopkins
 1190678   perez
 1230264   ward
 1272742   kirkland
 1275052   stephens
 1275132   wynn
 1280124   castillo
 1285001   jones
 1295481   conley
 1309541   vaughn
 1338115   zamora
 1350192   ross
 1350232   bond
 1356079   meyer
 1361310   patel
 1371561   dunn
 1373589   petersen
 1376003   joyner
 1380716   moss
 1388549   lang
 1412135   mcknight
 1430747   travis
 1439575   macias
 1445048   fleming
 1450840   serrano
 1452409   henderson
 1481870   peterson
 1483034   barker
 1524372   tyler
 1533911   melton
 1541533   burton
 1544385   guzman
 1544393   church
 1551530   castaneda
```

**Vulnerability ID**: V21
**Affected System IP**: 10.10.10.216
**Affected port**: 110
**Affected Component**: Pop3
**Description**: The POP3 service on the server is susceptible to brute-force attacks, as demonstrated by the successful acquisition of user 'Myles' credentials
**Severity Rating**: **High**
**Potential Impact**: An attacker could gain unauthorized access to private emails and sensitive information within the mailbox
**Discovery Date**: 28/01/2024
**Remediation Advice**: Enforce strong password policies, implement account lockouts after several failed attempts, and regularly monitor for suspicious access patterns
**Evidence/Proof of Concept**:

```
[→  ~ telnet 10.10.10.216 110
Trying 10.10.10.216...
Connected to 10.10.10.216.
Escape character is '^]'.
+OK Dovecot Ready.
USER Myles
+OK Accepted, password please
PASS admin
+OK Mailbox open, 2 messages
```

**References**:
[POP3 Login Utility - Metasploit]

**Vulnerability ID**: V23
**Affected System IP**: 10.10.10.222
**Affected port**: 80
**Affected Component**: Apache httpd 2.4.38
**Description**: The Apache HTTP server runs on an outdated version (2.4.38), exposing a vulnerability that allows users to be enumerated
**Severity Rating**: **Medium**
**Potential Impact**: Allowing users enumerations lead to brute force attacks and service compromission
**Discovery Date**: 28/01/2024
**Remediation Advice**: Upgrade to the latest stable version of Apache HTTP Server. Review and apply security patches. Enable only necessary modules and directives
**Evidence/Proof of Concept**:

```
[*] / - WordPress Version 5.2.4 detected
[*] 10.10.10.222:80 - / - WordPress User-Enumeration - Running User Enumeration
[+] / - Found user 'fraser' with id 1
[+] / - Found user 'warren' with id 2
[+] / - Usernames stored in: /Users/noejais/.msf4/loot/20240209163740_default_10.10.10.222_wordpress.users_194757.txt
[*] 10.10.10.222:80 - / - WordPress User-Validation - Running User Validation
[*] 10.10.10.222:80 - [1/0] - / - WordPress Brute Force - Running Bruteforce
[*] / - Brute-forcing previously found accounts...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**Vulnerability ID**: V24
**Affected System IP**: 10.10.10.223
**Affected port**: 3306
**Affected Component**: Mysql MariaDB 11.2.2
**Description**: Outdated MySQL version with known vulnerabilities
**Severity Rating**: **Medium**
**Potential Impact**: The service is running an outdated version of MariaDB, potentially leading to security vulnerabilities
**Discovery Date**: 28/01/2024
**Remediation Advice**: Update MariaDB to the latest version to address known vulnerabilities and improve security. Ensure strong passwords are used and review user privileges
**References**:
MariaDB Security

# Description of the methodology

The methodology for auditing POWERZIO's digital security is designed to systematically and ethically evaluate and enhance their cybersecurity. It focuses on identifying vulnerabilities, especially in remote work infrastructure, and gauging the resilience of IT systems against cyber threats. The approach ensures compliance with cybersecurity standards and safeguards system integrity and confidentiality. The primary aim is to provide actionable insights for strengthening POWERZIO's defenses against cyber attacks.

## Initial Assessment and Planning

Establishing the audit's scope, objectives, and communication protocols to align with POWERZIO's operational and compliance needs.

## Penetration Testing

Conducting focused tests on external and internal networks, particularly on remote access points like VPNs and RDP services.

## Vulnerability Assessment

Using automated tools for a comprehensive scan to identify and prioritize potential security weaknesses.

## Exploitation Techniques

Attempting controlled exploitation of identified vulnerabilities to assess potential impacts, ensuring non-disruptive methods to maintain system integrity.

## Standardized Frameworks

Adhering to established testing standards such as PTES and OWASP guidelines for ethical and legal compliance.

## Documentation and Reporting

Maintaining detailed documentation of the testing process, findings, and evidence, aimed at providing actionable insights in the final report.

# Audit Details

## Scanning

- **Objective:**

The initial step in our penetration testing methodology involves conducting a comprehensive scan of the target network to identify open ports, services, and their corresponding versions. This phase is crucial for mapping out the attack surface of POWERZIO's infrastructure and setting the stage for more targeted enumeration and exploitation efforts.

- **Tools Used:**

**Nmap**: A network scanning tool used to discover hosts and services on a computer network by sending packets and analyzing the responses.

- **Methodology:**

We utilized **Nmap**, employing the flags **-sV** to detect service versions, **-p-** to scan all 65535 ports, and **--open** to only show open ports, which significantly reduces the noise in the scan results. This comprehensive scan was aimed at uncovering as much information as possible about the underlying services and their configurations.

- **Execution:**

The scanning was conducted from a controlled environment to minimize the impact on POWERZIO's operational network. The command executed was as follows :

**nmap -sV -p- --open <target-IPs>**

<target-IPs> represents the range of IP addresses within the scope defined by POWERZIO, specifically the subnet 10.10.11.0/24.

- **Results:**

The scan results revealed several open ports across multiple systems within the target network, providing valuable insights into potential vectors for further investigation and exploitation. Key findings include, but are not limited to :

Multiple instances of OpenSSH on various versions, some of which are known to be vulnerable to exploits.
DNS service running dnsmasq with a version susceptible to a Denial of Service (DoS) attack.
Samba services indicating potential vulnerabilities in file sharing configurations.
Netwave IP camera services running on custom ports, hinting at outdated firmware with known vulnerabilities.

- **Analysis:**

The scanning phase allowed us to construct a detailed map of POWERZIO's network infrastructure, identifying critical services and potential vulnerabilities based on the version information gathered. This information is essential for prioritizing targets for deeper enumeration and exploitation in the subsequent phases of the audit.

- **Conclusion:**

The comprehensive scan using **Nmap** provided a solid foundation for our penetration testing efforts, revealing a diverse set of services and potential vulnerabilities across POWERZIO's network. These findings highlight the importance of regular and thorough scanning as a part of an effective cybersecurity strategy

## Enumeration

- **Objective:**

To methodically identify and document detailed information about live systems, services, and applications within POWERZIO's network, particularly those with potential vulnerabilities as identified in the scanning phase. The goal was to ascertain service configurations, operating systems, network structure, and potential security weaknesses.

- **Tools Used:**

**Nmap:** For more detailed scanning, including OS detection and service version identification.

**Searchsploit:** Utilized to search the Exploit Database for known vulnerabilities corresponding to the service versions identified by Nmap. This tool aids in mapping out potential exploits for the enumerated services.

**Dirb:** A web content scanner aimed at discovering hidden files and directories on web servers.

- **Methodology:**

The enumeration phase began with targeted scans against specific IPs and ports where vulnerabilities were suspected from the initial scan results. The team used a combination of automated tools and manual techniques to gather comprehensive data about each target, including:

- Operating system versions and patches.
- Service configurations and versions (SSH, DNS, HTTP/HTTPS, FTP, etc.).
- Presence of default or guessable credentials.
- Misconfigurations in web applications and databases.

- **Execution:**

**Service Enumeration:** Detailed scans were performed on services running on open ports to identify specific versions and configurations. For example, SSH and Samba services were thoroughly examined for version numbers to match them with known vulnerabilities.

**Web Application Enumeration:** Dirb was run against web servers using a command structure like dirb http://<target-IP>, along with common wordlists to uncover hidden files and directories.

**Credential Enumeration:** Attempts were made to identify valid usernames and passwords through brute-force or dictionary attacks on services such as FTP, SSH, and web applications, using customised word lists based on a number of criteria, such as the most frequently used references or recent password leaks.

- **Results:**

Enumeration provided a granular view of the target environment, revealing:

- Specific versions of operating systems and applications prone to exploitation.
- Misconfigured services and insecure software versions.
- Weak or default credentials that could be used for unauthorized access.
- Sensitive information exposed through misconfigured network shares and web directories.

- **Analysis:**

This phase highlighted the critical importance of maintaining up-to-date and properly configured systems. The detailed information gathered enabled the audit team to plan precise exploitation strategies, targeting the most vulnerable and high-value assets within POWERZIO's network.

- **Conclusion:**

The enumeration phase is vital for a successful penetration test, providing the depth of knowledge required to understand the target environment comprehensively. For POWERZIO, this phase underscored the need for rigorous configuration management, regular updates to software and systems, and strong password policies to mitigate the risks identified. Moving forward, these detailed findings will inform the exploitation phase, aiming to validate the identified vulnerabilities' impact in a controlled manner, thus demonstrating the real-world implications of these security weaknesses.

## Exploitation

- **Objective:**

The primary goal of the exploitation phase is to practically validate identified vulnerabilities and assess the impact of potential attacks on POWERZIO's infrastructure. This phase aims to exploit weaknesses found during the enumeration phase in a controlled and ethical manner, to demonstrate the real-world implications of these vulnerabilities without causing harm to the target systems.

- **Tools and Techniques Used:**

**Metasploit**: A comprehensive tool for developing and executing exploit code against a remote target machine.

**John the Ripper**: A powerful tool used for cracking passwords and testing the strength of passwords found during the enumeration phase.

**Custom Scripts**: Tailored scripts developed to exploit specific vulnerabilities identified in POWERZIO's systems, particularly where commercial tools were not applicable.

- **Methodology:**

Exploits were carefully selected and executed based on the vulnerabilities identified in the enumeration phase. The exploitation was conducted with the explicit consent of POWERZIO and under strict guidelines to ensure no disruption to business operations or data integrity.

**SSH and Samba Services**: Attempted to exploit known vulnerabilities in older versions of SSH and Samba services using Metasploit modules tailored for these purposes.

**Password Cracking**: Used John the Ripper to attempt cracking passwords, particularly focusing on weak passwords within the network's SSH and Samba services.

**Web Application Vulnerabilities**: Exploited known vulnerabilities in web applications using custom scripts and Metasploit modules designed for web exploits.

- **Execution:**

**SSH and Samba Exploitation**: Targeted exploitation using Metasploit was conducted against vulnerable SSH and Samba services to gain unauthorized access.

**Using John the Ripper**: Preparing a wordlist for most commonly used usernames and passwords. Configuring John the Ripper to use both dictionary and brute-force attacks to uncover weak passwords.

**Web Application Exploitation**: Deployed custom scripts and Metasploit modules against identified web application vulnerabilities, aiming to demonstrate the potential for data leakage or unauthorized access.

- **Results :**

The exploitation phase led to several key findings :

**Access Gained**: Managed to gain unauthorized access to systems through exploitation of SSH and Samba vulnerabilities, demonstrating the potential for internal network penetration.

**Passwords Cracked**: John the Ripper successfully cracked passwords, underscoring the need for a robust password policy.

**Vulnerability Validation**: Confirmed the existence and exploitability of multiple vulnerabilities in web applications, leading to potential unauthorized access and data exposure.

- **Analysis:**

This phase demonstrated the practical impact of vulnerabilities on POWERZIO's network. The successful exploitation of these vulnerabilities highlighted areas where security controls were either absent or ineffective, particularly in password management and service configuration.

- **Conclusion:**

The exploitation phase is crucial for demonstrating the real-world risks associated with identified vulnerabilities. The findings underscore the importance of regular vulnerability assessments, the implementation of strong password policies, and timely patching of software vulnerabilities. Recommendations for mitigating these risks include enhancing password complexity requirements, applying patches and updates to vulnerable services, and conducting regular security awareness training for employees.

## Cleaning Tracks

- **Objective:**

The objective of the cleaning tracks phase is to remove any evidence of the penetration testing activities from POWERZIO's systems and network. This ensures that the security and operational integrity of the network are maintained, and no backdoors or unintended vulnerabilities are left as a result of the testing.

- **Methodology:**

The cleaning process involves systematically retracing the steps taken during the penetration testing to identify and remove any changes made. This includes deleting any files uploaded, reversing any configuration changes, and ensuring that any accounts created for testing purposes are removed.

- **Techniques Used:**

**Manual Review**: Careful examination of system logs, temporary directories, and modified files to identify any artifacts of the penetration testing.

- **Execution:**

**File and Artifact Removal**: Deleted any files uploaded as part of the testing process, including tools, scripts, or data files used for exploitation or enumeration.

- **Verification:**

Conducted a thorough review of the systems and network to ensure that all artifacts of the penetration test were removed and that no unintended changes were left in place.

- **Conclusion:**

The cleaning tracks phase is a critical component of ethical penetration testing, ensuring that the target environment is left secure and unaltered.