Security Audit

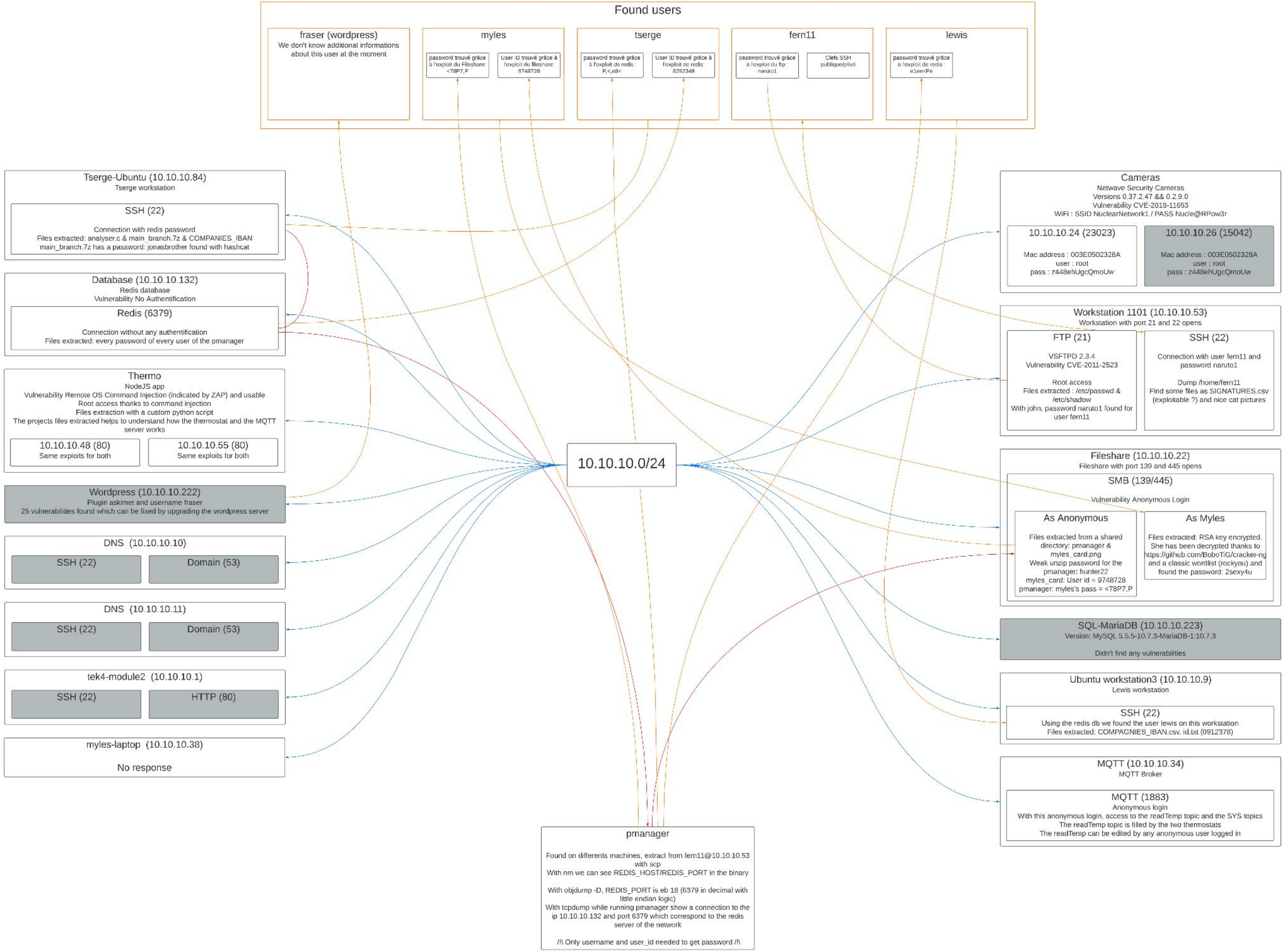
Our Team

Alexandre Ohayon

Thibault Le Guelinel De Lignerolles

William Petitprez

Emilien Delevoye



Found users

fraser (wordpress)
We don't know additional informations about this user at the moment

myles
password trouvé grâce à l'exploit du Fileshare: <78P7,P
User ID trouvé grâce à l'exploit du fileshare: 9748728

tserge
password trouvé grâce à l'exploit de redis: P,<,e8<
User ID trouvé grâce à l'exploit de redis: 8292349

fern11
password trouvé grâce à l'exploit du ftp : naruto1
Clefs SSH publique/privé

lewis
password trouvé grâce à l'exploit de redis : e1ee<Pe

Tserge-Ubuntu (10.10.10.84)
Tserge workstation
SSH (22)
Connection with redis password
Files extracted: analyser.c & main_branch.7z & COMPANIES_IBAN
main_branch.7z has a password: jonasbrother found with hashcat

Database (10.10.10.132)
Redis database
Vulnerability No Authentification
Redis (6379)
Connection without any authentification
Files extracted: every password of every user of the pmanager

Thermo
NodeJS app
Vulnerability Remote OS Command Injection (indicated by ZAP) and usable
Root access thanks to command injection
Files extraction with a custom python script
The projects files extracted helps to understand how the thermostat and the MQTT server works
10.10.10.48 (80)
Same exploits for both
10.10.10.55 (80)
Same exploits for both

Wordpress (10.10.10.222)
Plugin askimet and username fraser
25 vulnerabilities found which can be fixed by upgrading the wordpress server

DNS (10.10.10.10)
SSH (22)
Domain (53)

DNS (10.10.10.11)
SSH (22)
Domain (53)

tek4-module2 (10.10.10.1)
SSH (22)
HTTP (80)

myles-laptop (10.10.10.38)
No response

10.10.10.0/24

Cameras
Netwave Security Cameras
Versions 0.37.2.47 && 0.2.9.0
Vulnerability CVE-2018-11653
WiFi : SSID NuclearNetwork1 / PASS Nucle@RPow3r
10.10.10.24 (23023)
Mac address : 003E0502328A
user : root
pass : z448ehUgcQmoUw
10.10.10.26 (15042)
Mac address : 003E0502328A
user : root
pass : z448ehUgcQmoUw

Workstation 1101 (10.10.10.53)
Workstation with port 21 and 22 opens
FTP (21)
VSFTPD 2.3.4
Vulnerability CVE-2011-2523

Root access
Files extracted : /etc/passwd & /etc/shadow
With john, password naruto1 found for user fern11
SSH (22)
Connection with user fern11 and password naruto1

Dump /home/fern11
Find some files as SIGNATURES.csv (exploitable ?) and nice cat pictures

Fileshare (10.10.10.22)
Fileshare with port 139 and 445 opens
SMB (139/445)
Vulnerability Anonymous Login
As Anonymous
Files extracted from a shared directory: pmanager & myles_card.png
Weak unzip password for the pmanager: hunter22
myles_card: User id = 9748728
pmanager: myles's pass = <78P7,P
As Myles
Files extracted: RSA key encrypted.
She has been decrypted thanks to https://github.com/BoboTiG/cracker-ng and a classic wordlist (rockyou) and found the password: 2sexy4u

SQL-MariaDB (10.10.10.223)
Version: MySQL 5.5.5-10.7.3-MariaDB-1:10.7.3

Didn't find any vulnerabilities

Ubuntu workstation3 (10.10.10.9)
Lewis workstation
SSH (22)
Using the redis db we found the user lewis on this workstation
Files extracted: COMPAGNIES_IBAN.csv, id.txt (0912378)

MQTT (10.10.10.34)
MQTT Broker
MQTT (1883)
Anonymous login
With this anonymous login, access to the readTemp topic and the SYS topics
The readTemp topic is filled by the two thermostats
The readTemp can be edited by any anonymous user logged in

pmanager

Found on differents machines, extract from fern11@10.10.10.53 with scp
With nm we can see REDIS_HOST/REDIS_PORT in the binary

With objdump -D, REDIS_PORT is eb 18 (6379 in decimal with little endian logic)
With tcpdump while running pmanager show a connection to the ip 10.10.10.132 and port 6379 which correspond to the redis server of the network

/!\ Only username and user_id needed to get password /!\

Exploits

10.10.10.22 (fileshare.powerzio.lan) #1

Found port 139 and 445 open

Network Scanning

Found SMB Service on a Windows machine

Services identification

Some critical files are public and can be accessed with an anonymous account

Services issues

Fix access to the server or move the critical files to a private directory

Fix vulnerabilities

10.10.10.22 (fileshare.powerzio.lan) #2

Found Myles' identifiant is in the public files

Found identifiant

The password manager has a common password

Found password

With these informations we can access to Myles' private data

Access to private data

Myles should change his password and store it in a secure password manager

Fix vulnerabilities

10.10.10.132 (database.powerzio.lan)

Found port 6379 open

Network Scanning

We found that it was a redis service

Service identification

We successfully get access to the redis db without password

Service issues

Put a login password to your redis access

Fix vulnerabilities

10.10.10.84 (tserge-ubuntu.powerzio.lan)

Found port 22 open

Network scanning

We thought that maybe the user “tserge”using this machine in ssh is in the redis db

Potential exploit

Using the user found in the redis db we could connect as tserge in is session

Access to private data

Fix the redis vulnerability and change every password

Fix vulnerabilities

10.10.10.9 (Ubuntu workstation3)

Found port 22 open

Network scanning

We thought that maybe the user using this machine in ssh is in the redis db

Potential exploit

Using the user found in the redis db we could connect as lewis in is session

Access to private data

Fix the redis vulnerability and change every password

Fix vulnerabilities

10.10.10.53 (workstation1101.powerzio.lan)

Found ports 21 and 22 open

Network Scanning

VSFTPD 2.3.4

Services Identification

Using the vulnerability CVE-2011-2523 we got root access to the FTP

Access to private data

Close the port 6200

Fix vulnerabilities

10.10.10.(48,55) (thermo2/7.powerzio.lan)

Found port 80 open

Network Scanning

We used ZAP to find potential exploit: remote OS command injection

Found Potential Exploit

We successfully injected OS command and get root access to the host

Access to private data

Add a back-end process which parse the data from the client and reject injections

Fix vulnerabilities

10.10.10.34 (MQTT)

Found port 1883 open

Network scanning

We logged in as an anonymous user

Potential exploit

We can read and write data on the mqtt server as anonymous

Access to private data

Add a required login to access the mqtt server

Fix vulnerabilities

10.10.10.(24,26) (cam)

Found port 23023 for 10.10.10.24 and port 15042 for 10.10.10.26 open

Network Scanning

We found that it was a camera working with netwave service

Service identification

The versions of the camera permit to extract WiFi SSID/PASS and camera logins

Service issues

Update the cameras or change them

Fix vulnerabilities

10.10.10.222 (web.powerzio.lan)

Found port 80 open

Network Scanning

We used WPScan to have an overview of the server

Found Potential Exploit

We found some updates to apply

Access to private data

Update the WordPress version and the plugins

Fix vulnerabilities

Ignore or didn’t find anything

DNS

10.10.10.10
10.10.10.11

myles-laptop

10.10.10.38

tek4-module2

10.10.10.1

SQL-MariaDB

10.10.10.223