Powerzio penetration test

Leo Smith; Baudouin Vanhoffelen; Alexandre Chetafi; Guillaume Djaider-fornari

Summary

01

Our methodology

Discovery

Searching for machines inside of the network and started creating a small map of the network.

Scanning

Scan each machine for different vulnerabilities and known exploits.

Footprinting

Determine each service and the operating system running on the machines.

Exploitation

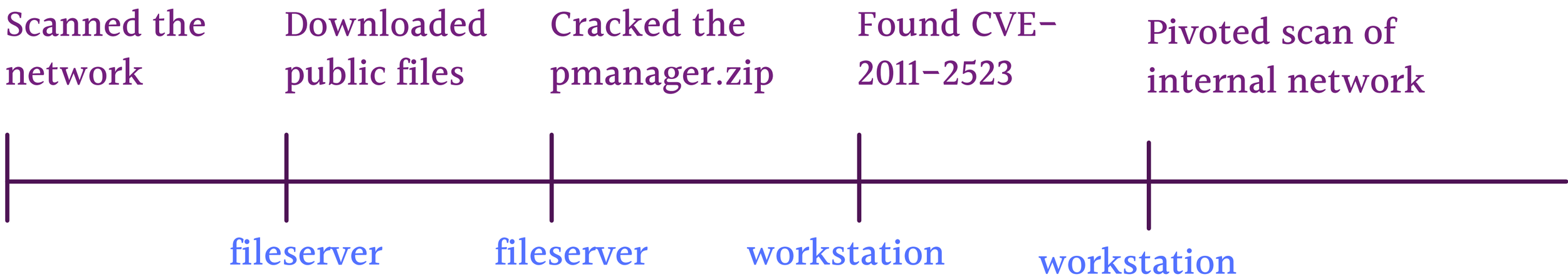
Exploit the machine and gain access to potentially sensitive or trivial information.

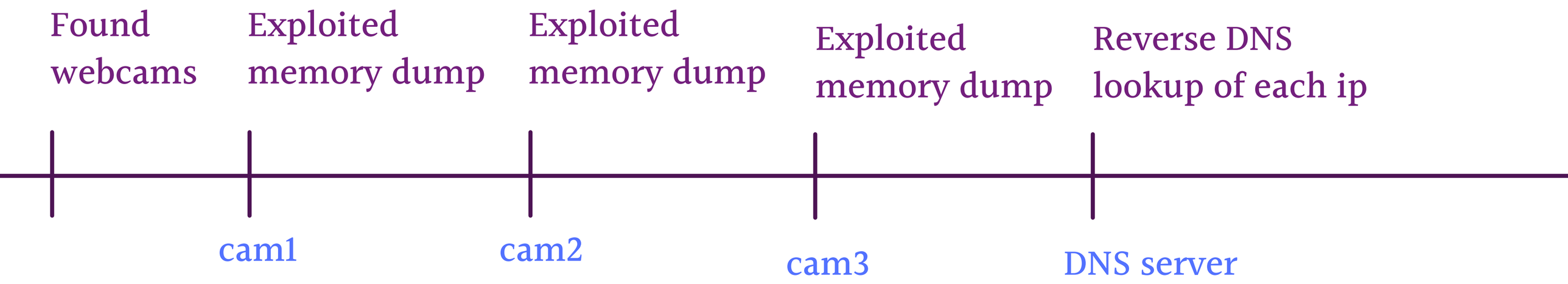
Reporting

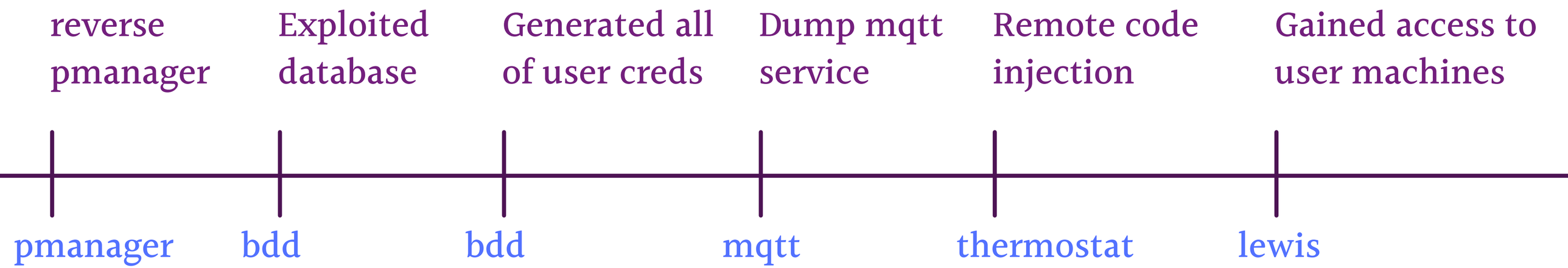
Report the vulnerability found and how we where able to penetrate the machine and what knowledge we gained from the attack.

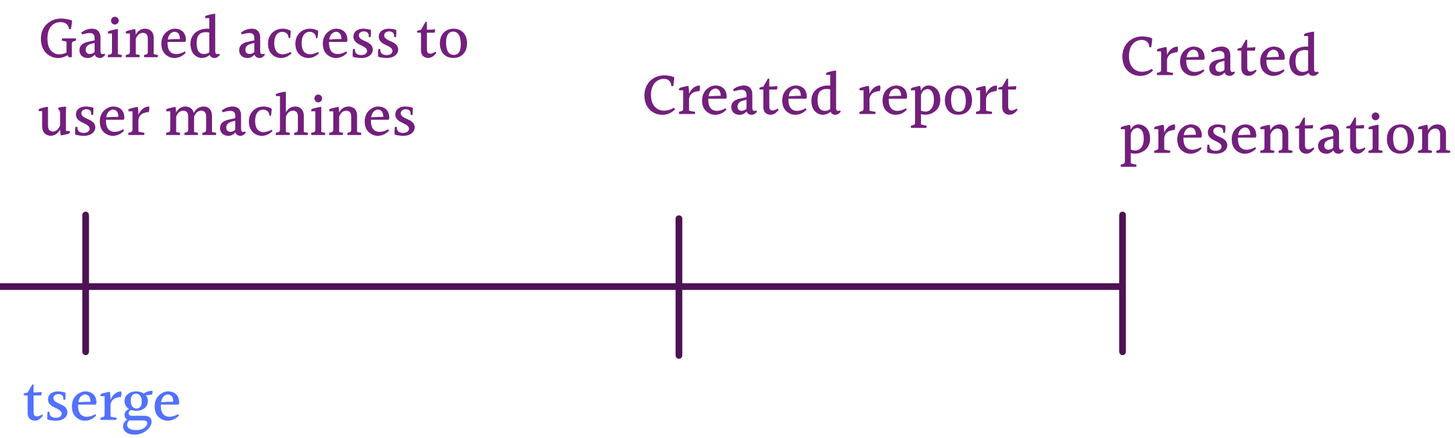
02

Timeline of the engagement


Scanned the network
Downloaded public files
Cracked the pmanager.zip
Found CVE-2011-2523
Pivoted scan of internal network
fileserver
fileserver
workstation
workstation


Found webcams
Exploited memory dump
Exploited memory dump
Exploited memory dump
Reverse DNS lookup of each ip
cam1
cam2
cam3
DNS server


reverse pmanager
Exploited database
Generated all of user creds
Dump mqtt service
Remote code injection
Gained access to user machines
pmanager
bdd
bdd
mqtt
thermostat
lewis


Gained access to user machines
Created report
Created presentation
tserge

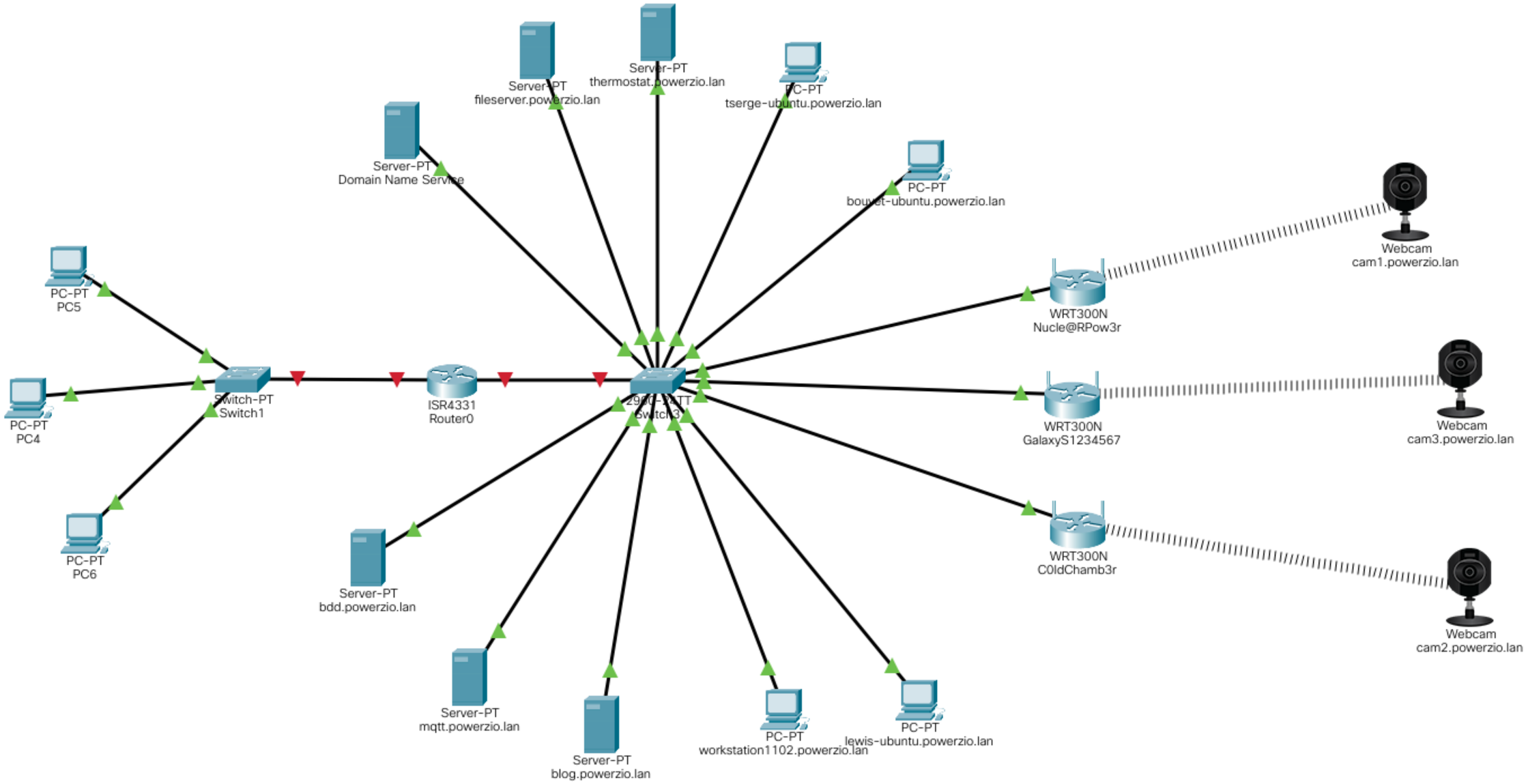
03

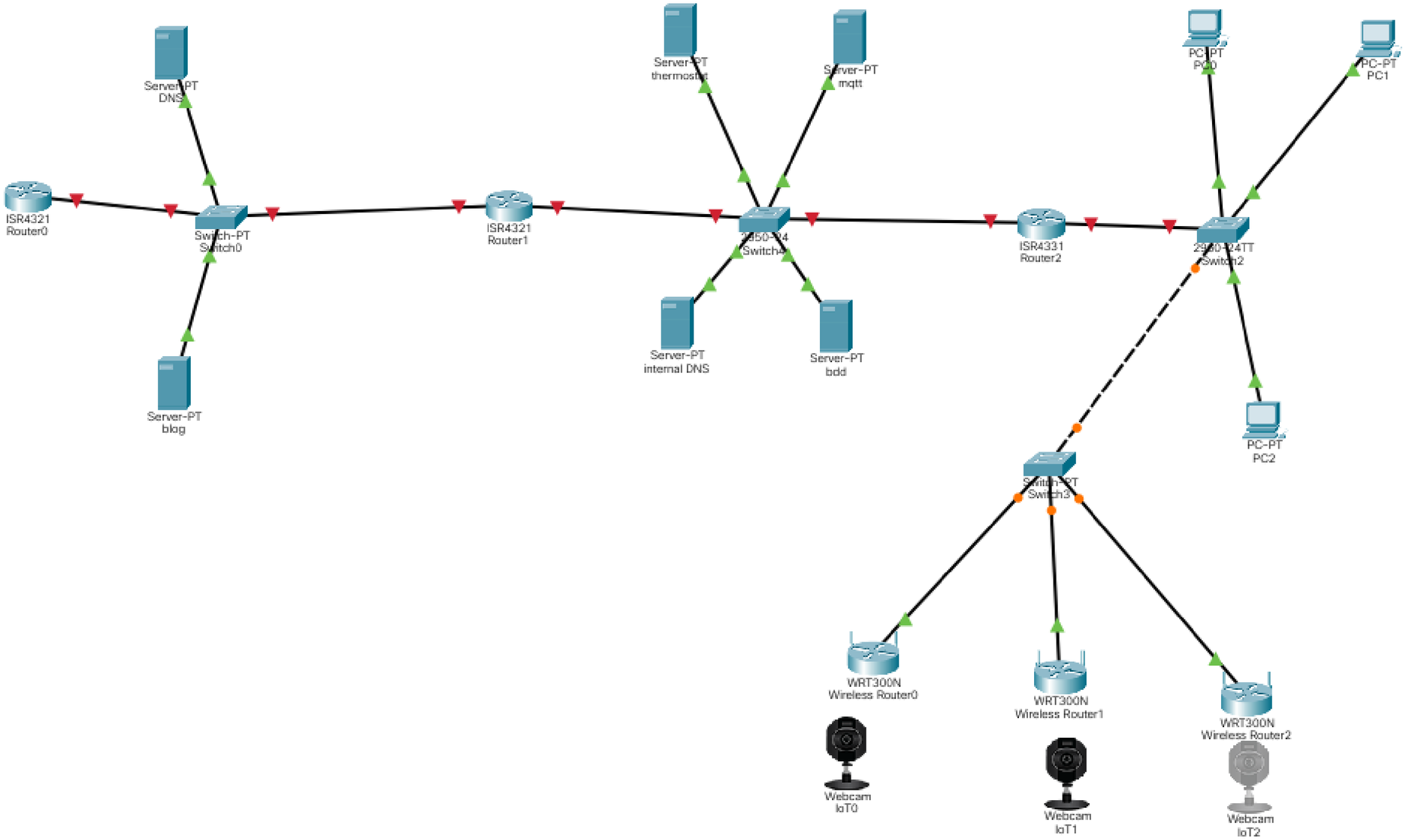
Our findings

Vulnerability	Severity	Location
Reverse DNS lookup	Informational	Page 9
CVE-2011-2523	Critical	Page 11
Anonymous Loggin	Moderate	Page 14
EDB-ID 41236	High	Page 18
Remote Code Execution	Critical	Page 21
No Authentification	High	Page 23
Insecure password generation	High	Page 26
No Authentification	High	Page 30
CVE-2021-3156	High	Page 33

04

Remediations


Server-PT
fileserver.powerzio.lan
Server-PT
thermostat.powerzio.lan
PC-PT
tserge-ubuntu.powerzio.lan
Server-PT
Domain Name Service
PC-PT
bouvet-ubuntu.powerzio.lan
Webcam
cam1.powerzio.lan
PC-PT
PC5
WRT300N
Nucle@RPow3r
Switch-PT
Switch1
ISR4331
Router0
2960-24TT
Switch0
WRT300N
GalaxyS1234567
Webcam
cam3.powerzio.lan
PC-PT
PC4
PC-PT
PC6
WRT300N
C0ldChamb3r
Webcam
cam2.powerzio.lan
Server-PT
bdd.powerzio.lan
Server-PT
mqtt.powerzio.lan
Server-PT
blog.powerzio.lan
PC-PT
workstation1102.powerzio.lan
PC-PT
lewis-ubuntu.powerzio.lan


Server-PT
DNS
ISR4321
Router0
Switch-PT
Switch0
Server-PT
blog
ISR4321
Router1
Server-PT
thermostat
Server-PT
mqtt
Switch4
Server-PT
internal DNS
Server-PT
bdd
ISR4331
Router2
PC-PT
PC0
PC-PT
PC1
Switch2
PC-PT
PC2
Switch3
WRT300N
Wireless Router0
WRT300N
Wireless Router1
WRT300N
Wireless Router2
Webcam
IoT0
Webcam
IoT1
Webcam
IoT2

THANK YOU FOR LISTENING