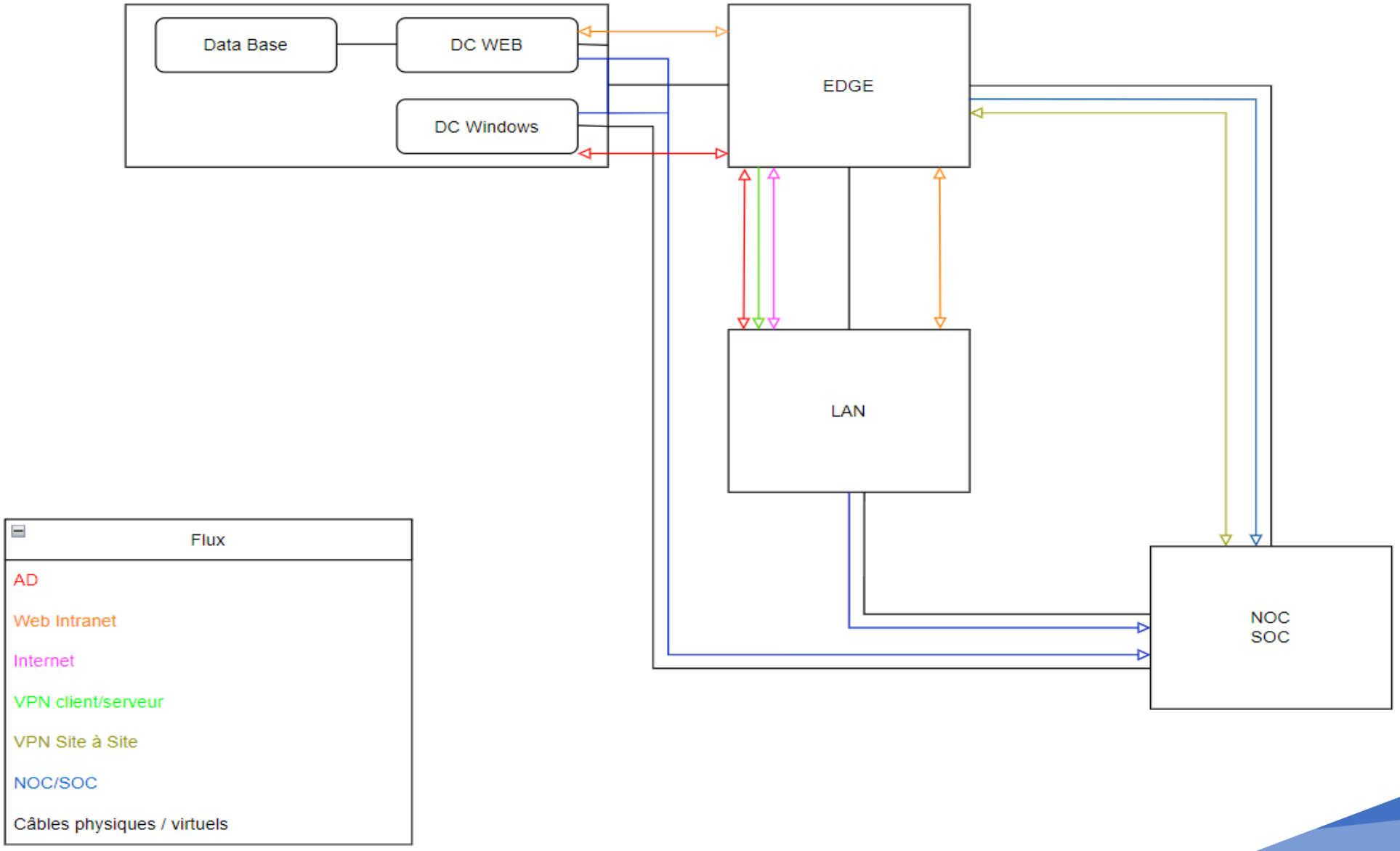
Documentation Technique

Equipe Cybersécurité Technobel

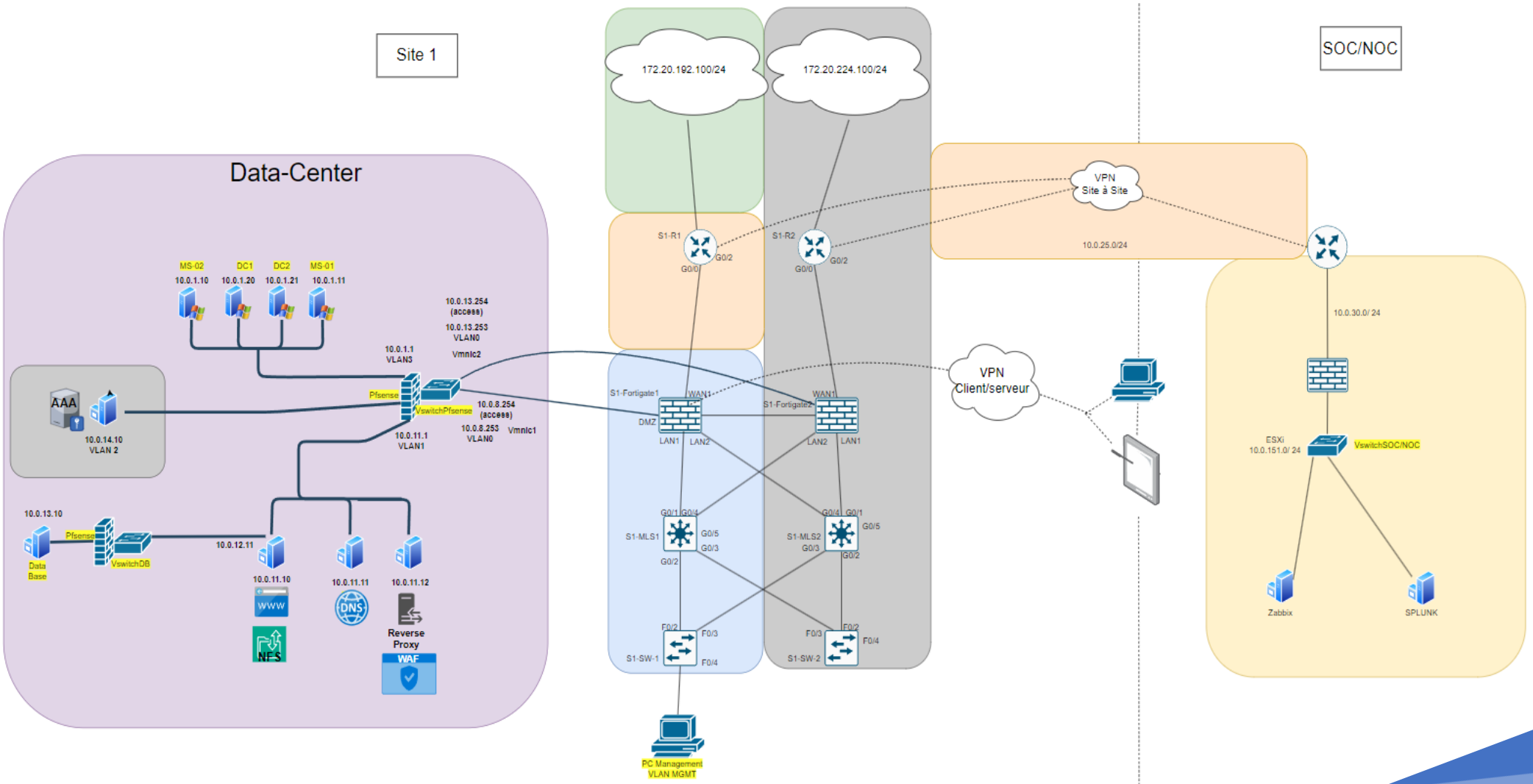
HLD


Data Base
DC WEB
DC Windows
EDGE
LAN
NOC
SOC
Flux
AD
Web Intranet
Internet
VPN client/serveur
VPN Site à Site
NOC/SOC
Câbles physiques / virtuels

Description

- Le flux AD (Rouge) sort du data center et rejoint le LAN pour permettre aux hôtes de rejoindre le domaine et de communiquer en sens inverse, il traverse également le EDGE pour permettre aux clients du VPN en télétravail de faire de même.
- Le flux web intranet (Orange) sort du data center et rejoint le LAN pour permettre aux hôtes de se connecter aux serveur web et de communiquer en sens inverse, il traverse également le EDGE pour permettre aux clients du VPN en télétravail de faire de même.
- Le flux Internet (Violet) sort du LAN vers le EDGE pour sortir par un PAT afin de créer une connexion internet lorsque le flux revient à l'hôte.
- Le flux VPN client/serveur (Vert) traverse le EDGE pour rejoindre son point de sortie sur l'interface WAN du Fortigate dans le LAN.
- Le flux VPN Site à Site (Doré) part du routeur core dans le EDGE pour rejoindre le routeur du SOC/NOC et inversement.
- Le flux NOC/SOC (Bleu) tous les modules envois leurs logs (SNMP, agent Zabbix, agent SPLUNK) vers la Zabbix et la SPLUNK du module SOC/NOC.

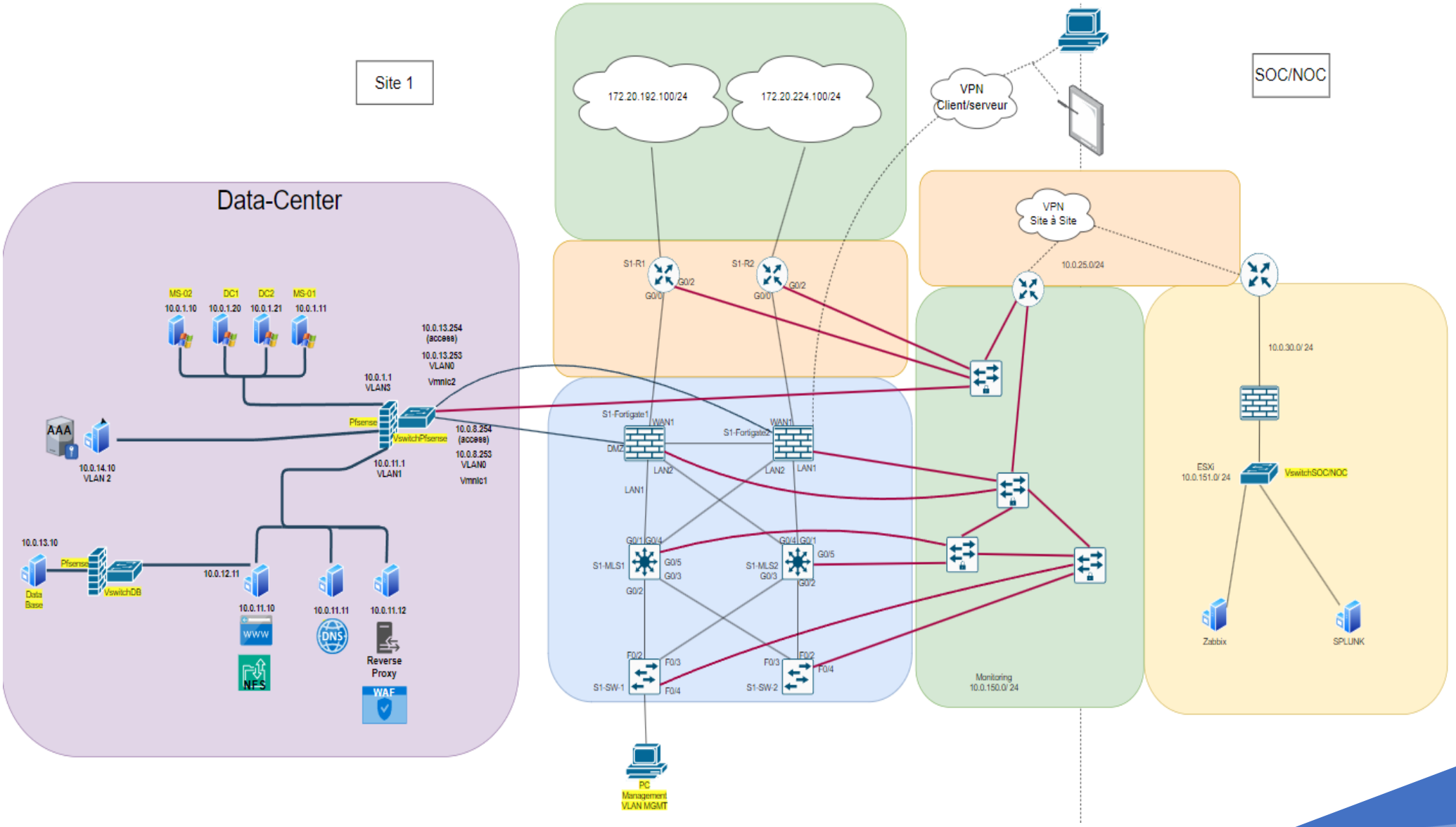
LLD solution client



Description

- Infrastructure modulaire : LAN, EDGE, Data-Center, NOC/SOC
- Module LAN :
  - Switch d’accès Cisco 2960
  - Switch MLS Cisco WS-C3560CG-8PC-S
  - Firewall fortigate 60F (VPN client/serveur)
- Module EDGE :
  - Routeur Core Cisco 2911 (PAT, ACL, VPN Site à Site)
- Module Data-Center :
  - AD windows server 2019 (DC, MS, DNS, DHCP, SMB, DFS, DFSR, OU, GPO)
  - Serveur web sur Rocky Linux (page d’index)
  - Serveur DNS sur Rocky Linux (BIND)
  - Data base sur Rocky Linux (MySQL)
- Module NOC/SOC :
  - Zabbix sur Alma Linux
  - SPLUNK

Description solution alternative



Description

- Switch IE 2000 :
  - Séparation du réseau de monitoring pour éviter un mélange des flux.
  - Alimentation séparée pour conserver l'envois des logs en cas de coupure de courant.
  - Protocol spécifique au réseau de monitoring
  - Besoin plus important en matériel
  - Solution plus sécurisée et préconisée en entreprise.

PENTEST RCOMMUNE

Équipe Cybersécurité Technobel

Table des matières

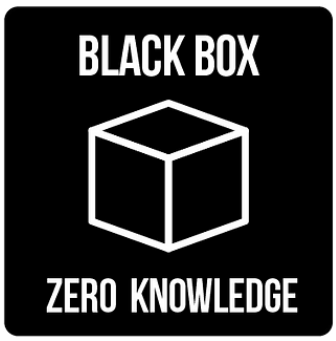
Description du Pentest

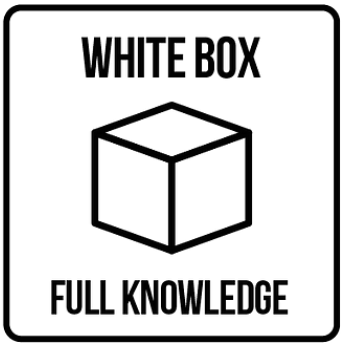
Un « Pentest » ou également appelé test de pénétration est une méthode d'évaluation de la sécurité d'un système informatique par la démonstration, par simulation des actions d'attaquants. Son objectif est de détecter des vulnérabilités exploitables à des fins malveillantes, afin de pouvoir enclencher leur correction.

Contexte et Objectif

Dans le cadre de ce PoC (Proof of Concept), l'équipe Cyber de Technobel a réalisé un test de pénétration sur l'infrastructure test qu'elle a mise en place à la suite d'une demande cliente de la Rcommune située en Belgique. Cette demande visait la mise en place d'une infrastructure sécurisée et modulaire pour le service des eaux de l'administration communale de la rcommune. L'objectif de ce Pentest étant d'en récolter ses vulnérabilités exploitables et d'en émettre des recommandations pour les corriger.

Scope et conditions du Pentest





Pour la réalisation du test de pénétration, l'équipe cyber Technobel s'est fixée un scope limité, où le pentesteur qui a réalisé les tests possède un niveau de connaissance défini par rapport à ce qui compose physiquement et logiquement l'infrastructure mise en place.

Ce test de pénétration a été réalisé dans des conditions de **GREY BOX**, c'est-à-dire que le pentesteur possède quelques connaissances concernant l'infrastructure testée ; notamment l'existence d'un Active Directory, d'un data Center ainsi que du nom de domaine du site Web de la rcommune. Le pentesteur a eu également quelques accès afin de réaliser ses tests : **une machine virtuelle Linux** ayant un accès au réseau de données et **une machine Windows 10** faisant partie de l'Active Directory de l'infrastructure.

Le pentest a été segmenté en plusieurs étapes distinctes ci-dessous :

- Reconnaissance passive ;
- Port scanning ;
- Enumération ;
- Scan et analyse de vulnérabilités ;
- Exploitation des vulnérabilités

Ces étapes seront détaillées et décrites dans les sections ultérieures de ce rapport qui leur sont dédiées.

Bien que les résultats des tests aient apporté des vulnérabilités ainsi que des recommandations liées à ces dernières, ce pentest a été réalisé dans une infrastructure créée par l'équipe cyber Technobel en 25 jours. Le projet étant un PoC (Proof of Concept), certaines parties et/ou fonctionnalités du projet n'ont pas pu être mises en place dans le temps imparti par faute de ressources, de temps ou de connaissances. Le contexte de ce PoC implique également les limitations techniques de Pentest qui ne pourra opérer uniquement sur ce qui a été mis en place par l'équipe pour en déduire des résultats sur lesquels s'appuyer.

Ce PoC est effectué dans un cadre pédagogique au cours d'un cursus qualifiant au sein de l'ASBL Technobel impliquant les onze stagiaires ayant participé à ce projet, justifiant la présence ou non de schémas, graphes et sections d'informations présents dans ce rapport.

Reconnaissance Passive

Description

Cette phase consiste à collecter des informations sur la cible sans interagir directement avec elle, afin de ne pas attirer l'attention. Elle repose sur l'examen de sources publiques et accessibles.

Outils utilisés

Dig

Dig (Domain Information Groper) est un outil puissant ayant pour but d'interroger les serveurs DNS et obtenir les informations détaillées sur un domaine, il ne génère aucun trafic détectable.

L'analyse Dig révèle plusieurs informations :

- L'adresse IP liée au nom de domaine du site Web rcommune.lux.pz qui est celle du serveur Web ou d'un Reverse Proxy : **10.0.11.12**
- Le nom de domaine du serveur DNS utilisé par le serveur Web ainsi que son adresse ip qui lui est associée : **ns1.lux.pz 10.0.11.11**
- Le nom de la zone DNS : **lux.pz**

Traceroute

Traceroute est un outil utilisé pour cartographier le chemin probable que peut prendre un paquet de données entre un hôte local et un hôte distant à travers le réseau (Routeurs/ Routeurs Capabilities)

L'analyse Traceroute révèle plusieurs informations :

- Le chemin emprunté par les hôtes de l'infrastructure pour atteindre Internet ainsi que le chemin pour atteindre le serveur Web local
- Le nombre de sauts parmi les appareils couche 3 au sein de l'infrastructure, ce qui permet à l'attaquant de réaliser un début de cartographie de l'infrastructure.

10.0.0.1->10.0.2.1->10.0.6.1->194.78.154.145 (static.isp.belgacom) pour le cheminement vers Internet.

10.0.0.1->10.0.2.1->10.0.8.253->10.0.11.12 (Server Web ou Reverse Proxy) pour le cheminement vers le serveur Web www.rcommune.lux.pz

Dans le cadre du PoC (Proof of Concept), nombres d'outils utilisés pour de la reconnaissance passive se basent sur des informations fournies dans des bases de données publiques sur Internet. De ce fait, il est impossible pour le Pentesteur de les utiliser dans le cadre de ce Projet, les serveurs Web et DNS étant hébergés en local. Voici une liste non exhaustive de ces outils recommandés :

Dnsenum/Whois – Enumération DNS, **theharvester** – Adresses mail liée à un DNS server, **shodan** – Enumeration IoT, **maltego** – Datamining tool.

Reconnaissance Active

Description

Cette phase consiste à interagir directement avec la cible pour collecter des informations, elle implique des techniques comme le scan de port, l'interrogation de services ou l'envoi de paquets spécifiques pour évaluer la réponse du système.

Port Scanning

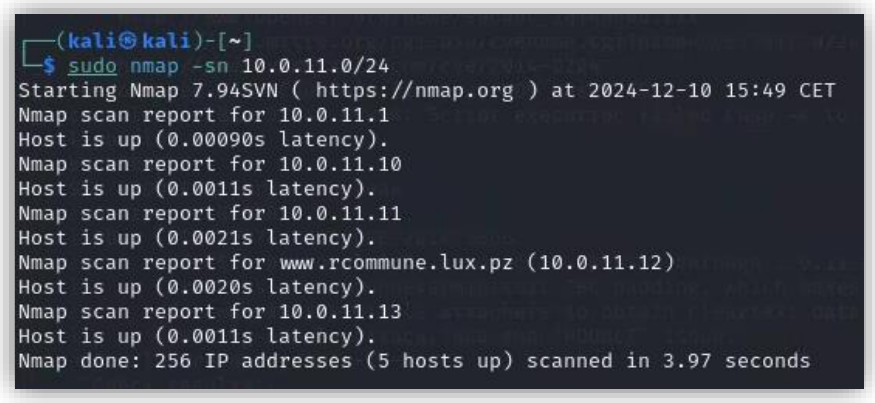
Le Port Scanning est une technique utilisée lors de la phase de reconnaissance active qui vise à envoyer des paquets à différents ports sur une machine distante afin de déterminer quels ports sont ouverts, fermés ou filtrés, et quels services ou applications y sont associés.

Outils utilisés

Nmap

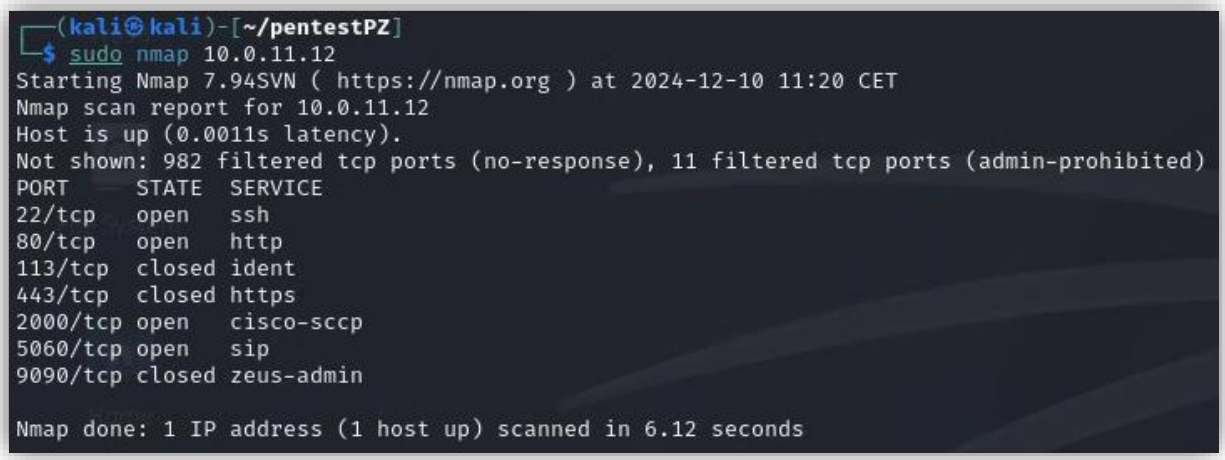
Nmap (Network Mapper) est un outil de reconnaissance active largement utilisé lors d'un pentest, il permet de découvrir les hôtes actifs sur un réseau, d'identifier les ports ouverts, de déterminer les services qui y tournent et d'en apprendre davantage sur la configuration de ces services.

Le pentesteur a effectué des scans nmap sur les adresses IP récoltées lors de la reconnaissance passive. Il a ensuite analysé les machines des réseaux du Data Center grâce à l'outil Nmap, et a découvert dans ses recherches la véritable adresse IP du serveur Web ainsi que les machines du réseau de l'Active Directory.



Découverte de la présence d'un **Reverse Proxy** ainsi que de la véritable adresse IP du serveur Web.

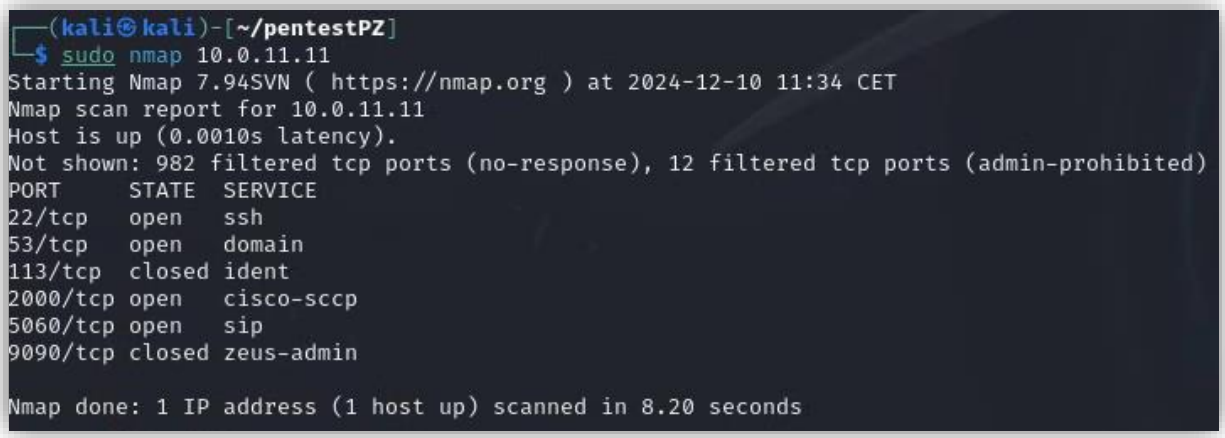
- Scan des 1000 ports les plus connus sur la machine **10.0.11.12**, soit la machine **Reverse Proxy**



Ports Ouverts- Reverse Proxy

TCP	UDP
22/tcp SSH	5060/udp SIP
80/tcp http	
2000/tcp cisco-sccp	
5060/tcp SIP	

- Scan des 1000 ports les plus connus sur la machine **10.0.11.11**, la machine faisant office de **serveur DNS**



Ports ouverts – Serveur DNS

TCP	UDP
22/tcp SSH	5060/tcp SIP
53/tcp DNS	
2000/tcp cisco-sccp	
5060/tcp SIP	

- Scan de l'intégralité des ports de la machine 10.0.6.1 représentants le dernier saut IP avant le passage aux IP publiques qui devrait logiquement être associée à un **routeur.**

```
┌──(kali㉿kali)-[~/pentestPZ]
└─$ sudo nmap -p1-65535 10.0.6.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 11:36 CET
Nmap scan report for 10.0.6.1
Host is up (0.0027s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
2000/tcp open  cisco-sccp
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 54.51 seconds
```

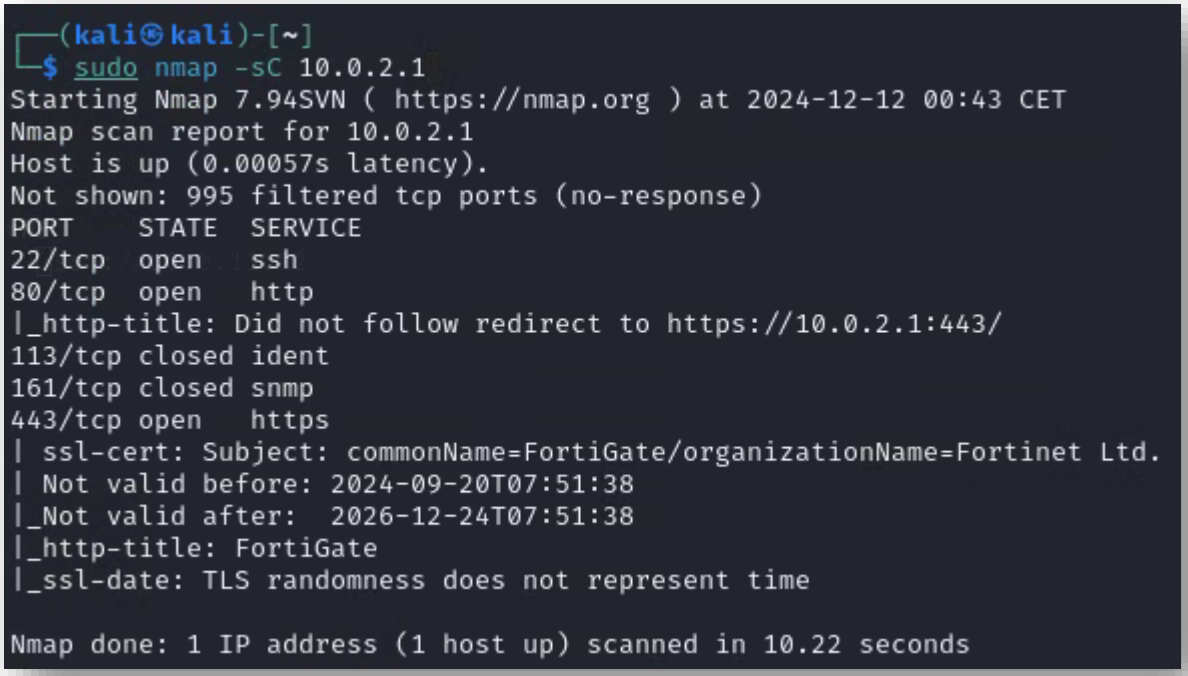
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -T4 -F -sV 10.0.6.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 01:02 CET
Warning: 10.0.6.1 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.0.6.1
Host is up (0.0013s latency).
Not shown: 92 closed udp ports (port-unreach)
PORT      STATE         SERVICE       VERSION
123/udp   open          ntp           NTP v4 (secondary server)
161/udp   open          snmp          Cisco SNMP service; ciscoSystems SNMPv3 server
162/udp   open|filtered snmptrap
500/udp   open          isakmp?
3703/udp  open|filtered adobeserver-3
4500/udp  open|filtered nat-t-ike
5060/udp  open|filtered sip
49185/udp open|filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 207.96 seconds
```

Ports ouverts - Router

TCP	UDP
2000/tcp cisco-sccp	123/udp NTP
5060/tcp SIP	161/udp SNMP
	162/udp SNMPtrap
	500/udp ISAKMP
	4500/udp NAT-T-IKE
	5060/udp SIP
	49262/udp Unknown

Le Pentesteur établit des conclusions suite aux résultats de ces scans :

- L'infrastructure a mis en place la possibilité d'un établissement d'une connexion de type **VPN** qui se base sur le **framework IPSEC**, qui authentifie et encrypte les données traversant le tunnel VPN
- Les paquets traversent un **NAT** pour sortir de l'infrastructure
- Le routeur est monitoré via le protocole SNMP et est un modèle du constructeur **Cisco**



Ports ouverts – Pare-feu

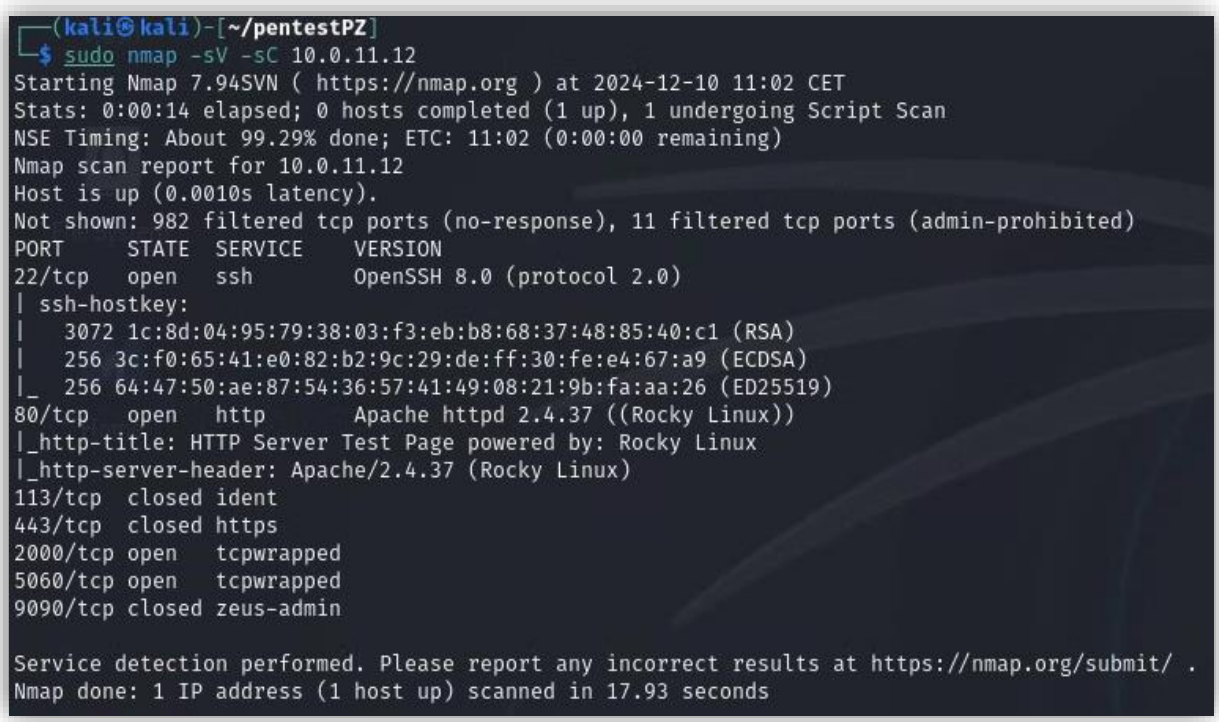
TCP	UDP
22/tcp SSH	
80/tcp http	
443/tcp https	

Le Pentesteur établit des conclusions suite aux résultats de ce scan :

- La machine scannée est un **pare-feu**, plus spécifiquement de la marque Fortinet. C'est donc un **Fortigate** comme montré ci-dessus dans les résultats.
- Le Pare-feu peut être paramétré via une **interface GUI**, comme le prouvent les informations http remontées ainsi que la date de validité du certificat SSL pour le procotole https.

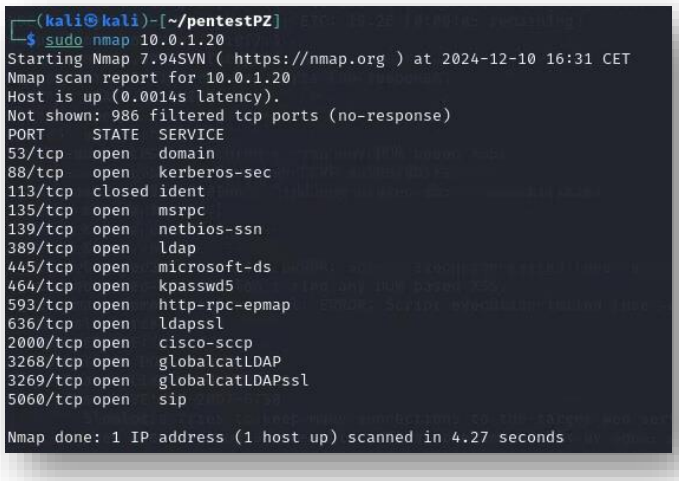
Enumération

L'énumération est l'étape clé de la phase de reconnaissance active, elle consiste à interroger plus en profondeurs les services pour en apprendre davantage sur leurs configurations, les versions de logiciels, les utilisateurs et mots de passe ou d'autres informations sensibles.

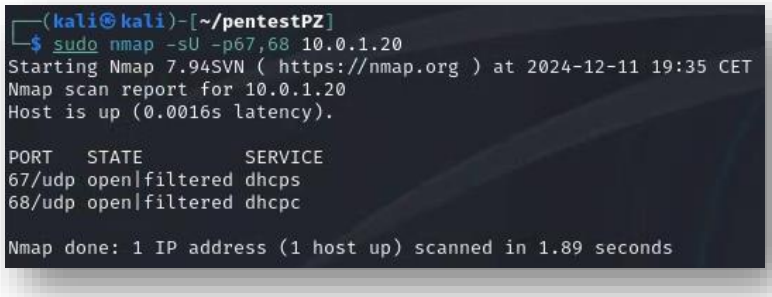


En approfondissant les scans Nmap, le Pentesteur a pu récolter davantage d'informations :

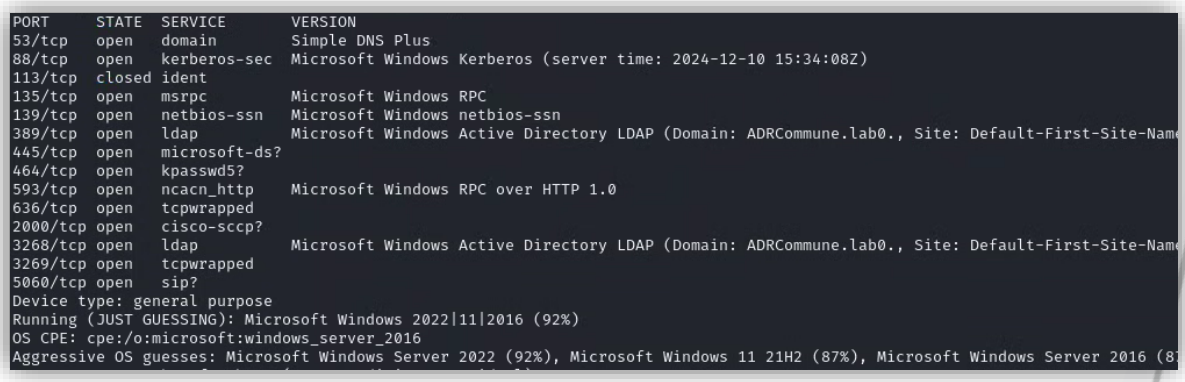
- Le serveur Web utilise Apache en version 2.4.37 et est hébergée sur une **machine Rocky Linux**
- Le protocole SSH utilisé avec l'outil OpenSSH 8.0 en version SSH 2.0 et qu'il utilise comme modèle de cryptage **R**



```
┌──(kali㉿kali)-[~/pentestPZ]
└─$ sudo nmap 10.0.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 16:31 CET
Nmap scan report for 10.0.1.20
Host is up (0.0014s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE  SERVICE
53/tcp   open   domain
88/tcp   open   kerberos-sec
113/tcp  closed ident
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
389/tcp  open   ldap
445/tcp  open   microsoft-ds
464/tcp  open   kpasswd5
593/tcp  open   http-rpc-epmap
636/tcp  open   ldapssl
2000/tcp open   cisco-sccp
3268/tcp open   globalcatLDAP
3269/tcp open   globalcatLDAPssl
5060/tcp open   sip

Nmap done: 1 IP address (1 host up) scanned in 4.27 seconds
```



```
┌──(kali㉿kali)-[~/pentestPZ]
└─$ sudo nmap -sU -p67,68 10.0.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 19:35 CET
Nmap scan report for 10.0.1.20
Host is up (0.0016s latency).

PORT   STATE         SERVICE
67/udp open|filtered dhcps
68/udp open|filtered dhcpc

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```



```
PORT     STATE  SERVICE       VERSION
53/tcp   open   domain        Simple DNS Plus
88/tcp   open   kerberos-sec  Microsoft Windows Kerberos (server time: 2024-12-10 15:34:08Z)
113/tcp  closed ident
135/tcp  open   msrpc         Microsoft Windows RPC
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open   ldap          Microsoft Windows Active Directory LDAP (Domain: ADRCommune.lab0., Site: Default-First-Site-Name
445/tcp  open   microsoft-ds?
464/tcp  open   kpasswd5?
593/tcp  open   ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open   tcpwrapped
2000/tcp open   cisco-sccp?
3268/tcp open   ldap          Microsoft Windows Active Directory LDAP (Domain: ADRCommune.lab0., Site: Default-First-Site-Name
3269/tcp open   tcpwrapped
5060/tcp open   sip?
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (92%), Microsoft Windows 11 21H2 (87%), Microsoft Windows Server 2016 (8
```

Le Pentesteur a donc découvert les plages d'adresses IP utilisées pour l'Active Directory et en a déduit :

- Les noms de domaine des contrôleurs de domaine et leurs adresses IP : **10.0.1.20 et 10.0.1.21**
- Les services installés et utilisés : Ldap, DNS, DHCP
- 92% de probabilité qu'il s'agisse d'un Windows server 2022

Scan et Analyse de vulnérabilités

Description

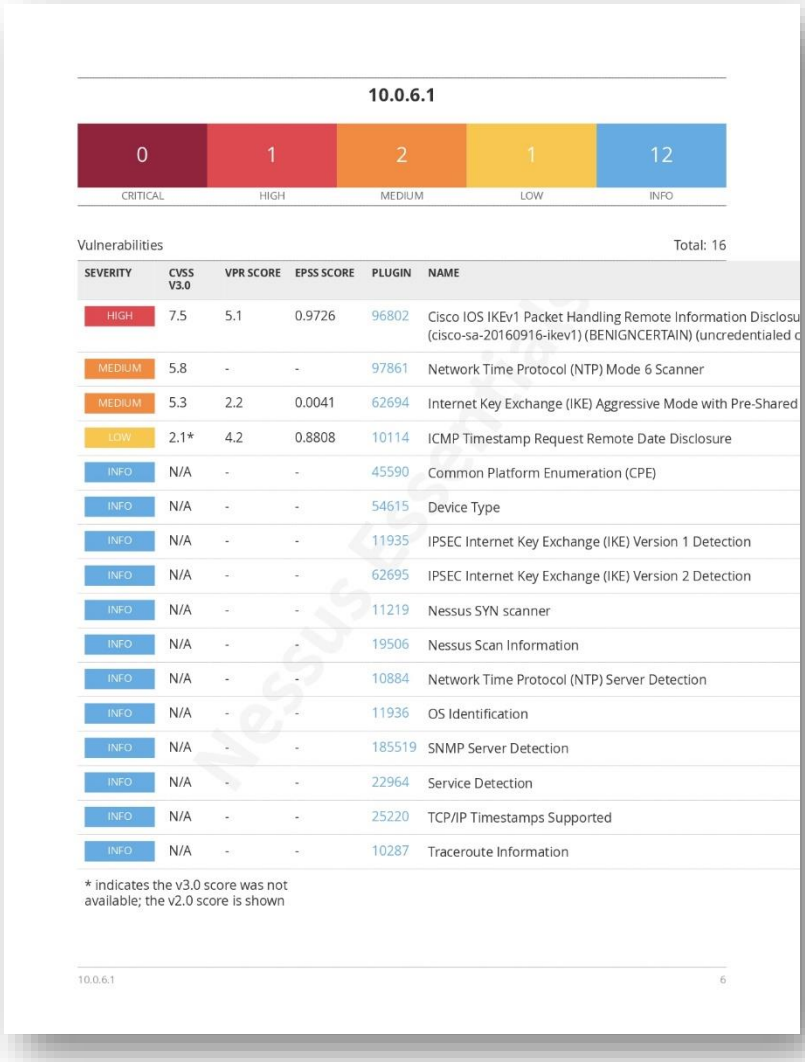
La phase de Scan et Analyse de vulnérabilités consiste à identifier les faiblesses dans un système cible, telles que les failles de sécurité dans les logiciels, les configurations ou les services. Elle implique l'utilisation d'outils pour scanner le réseau, les applications et les serveurs à la recherche de vulnérabilités connues, de mauvaises configurations ou d'autres points d'entrée exploitables par un attaquant.

Outils utilisés

Nessus

Nessus est un outil de scan de vulnérabilités largement utilisé dans les tests d'intrusion et l'audit de sécurité. Il permet de détecter des failles de sécurité dans les systèmes, réseaux, applications et configurations. Il analyse les hôtes à la recherche de vulnérabilités connues, telles que des logiciels obsolètes, des erreurs de configuration ou des failles exploitables. Il génère des rapports détaillés afin d'évaluer les risques et prioriser les corrections.

- Rapport de Scan de vulnérabilités sur le **routeur**



10.0.6.1

0	1	2	1	12
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 16

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	5.1	0.9726	96802	Cisco IOS IKEv1 Packet Handling Remote Information Disclosu (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed c
MEDIUM	5.8	-	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.3	2.2	0.0041	62694	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
INFO	N/A	-	-	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

10.0.6.1 6

➢ Rapport de Scan de vulnérabilités sur le **serveur Web**

10.0.11.10

14	10	4	1	30
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 59

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0108	139574	Apache 2.4.x < 2.4.46 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.6847	150280	Apache 2.4.x < 2.4.47 Multiple Vulnerabilities
CRITICAL	9.8	7.4	0.1305	161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow
CRITICAL	9.8	6.7	0.3791	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0104	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	0.0135	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	7.4	0.2048	156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF
CRITICAL	9.8	6.7	0.0087	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.1	5.9	0.8108	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities
CRITICAL	9.1	5.2	0.0147	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.0	6.5	0.0235	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	0.967	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	-	58987	PHP Unsupported Version Detection
HIGH	7.8	8.4	0.9607	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
HIGH	7.5	4.4	0.008	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0064	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	0.2877	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0243	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)

10.0.11.10 7

HIGH	7.5	4.4	0.0012	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0239	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0013	153585	Apache >= 2.4.17 < 2.4.49 mod_http2
HIGH	7.5	3.6	0.0016	153586	Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi
MEDIUM	6.1	3.0	0.0026	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities
MEDIUM	5.3	1.4	0.0016	193420	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestor HTTP Response Header
INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Head
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available

Nmap

┌──(kali㉿kali)-[~/pentestPZ]
└─$ sudo nmap --script vuln 10.0.0.1
Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-12 01:40 CET
Stats: 0:04:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.67% done; ETC: 01:44 (0:00:01 remaining)
Nmap scan report for 10.0.0.1
Host is up (0.0021s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-method-tamper:
| VULNERABLE:
| Authentication bypass by HTTP verb tampering
|State: VULNERABLE (Exploitable)
| This web server contains password protected resources vulnerable to authentication bypass
| vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the
| common HTTP methods and in misconfigured .htaccess files.
|
| Extra information:
|
| URIs suspected to be vulnerable to HTTP verb tampering:
| / [POST]
|
| References:
| http://www.imperva.com/resources/glossary/http_verb_tampering.html

```
|       https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
|       http://www.mkit.com.ar/labs/htexploit/
|_      http://capec.mitre.org/data/definitions/274.html
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-method-tamper:
|   VULNERABLE:
|   Authentication bypass by HTTP verb tampering
|     State: VULNERABLE (Exploitable)
|       This web server contains password protected resources vulnerable to authentication bypass
|       vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the
|       common HTTP methods and in misconfigured .htaccess files.
|
|     Extra information:
|
|   URIs suspected to be vulnerable to HTTP verb tampering:
|     / [POST]
|
|     References:
|       http://www.imperva.com/resources/glossary/http_verb_tampering.html
|       https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
|       http://www.mkit.com.ar/labs/htexploit/
|_      http://capec.mitre.org/data/definitions/274.html
```

```
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: BC:F1:F2:C6:F6:44 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 259.81 seconds
```

- Tests de vulnérabilités réalisés avec l'outil Nmap dévoile des vulnérabilités exploitables, ces tests ont été réalisé sur le serveur Web et sur une machine intermédiaire Cisco réalisant de la couche 3, probablement un multi-layer-Switch.

Exploitation des vulnérabilités

Description

Cette phase consiste à tester les exploitations possibles des vulnérabilités identifiées. Elle permet aux pentesteurs de tirer profit de certaines failles pour en découvrir de nouvelles.

Vulnérabilité SSH Rocky Linux

Le Port 22/tcp SSH est ouvert par défaut sur les machines Rocky Linux

Outil utilisé

Hydra

Outil puissant pour le pentesting, aussi appelé « cracker de mots de passe », qui permet de performer des attaques en brute force.

- Attaque Brute Force SSH sur les machines Rocky Linux

```
┌──(kali㉿kali)-[~/pentestPZ]
└─$ sudo hydra -l patrick -P wordlistpassword.txt ssh://10.0.11.12
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-12 00:51:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting ./hydra.restore
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per task
[DATA] attacking ssh://10.0.11.12:22/
[22][ssh] host: 10.0.11.12   login: patrick   password: starwars
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-12 00:51:29
```

- Détection de l'attaque sur le SIEM externalisé, **Splunk**

i	Time	Event
>	12/12/24 12:51:28.417 AM	type=USER_LOGIN msg=audit(1733961088.417:13669): pid=56869 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.416 AM	type=USER_LOGIN msg=audit(1733961088.416:13664): pid=56874 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.412 AM	type=USER_LOGIN msg=audit(1733961088.412:13657): pid=56876 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.412 AM	type=USER_LOGIN msg=audit(1733961088.412:13653): pid=56870 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.407 AM	type=USER_LOGIN msg=audit(1733961088.407:13645): pid=56872 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.407 AM	type=USER_LOGIN msg=audit(1733961088.407:13641): pid=56868 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.403 AM	type=USER_LOGIN msg=audit(1733961088.403:13633): pid=56875 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit
>	12/12/24 12:51:28.402 AM	type=USER_LOGIN msg=audit(1733961088.402:13629): pid=56873 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct="patrick" exe="/usr/sbin/sshd" hostname=? addr=10.0.0.43 terminal=ssh res=failed'UID="root" AUID="unset" host = rcommune.lux.pz source = /var/log/audit/audit.log sourcetype = linux_audit

Les analystes du SOC externalisé constatent un nombre de tentatives échouées répétées sur une très courte durée qui s'assimile à une attaque.

Injection SQL

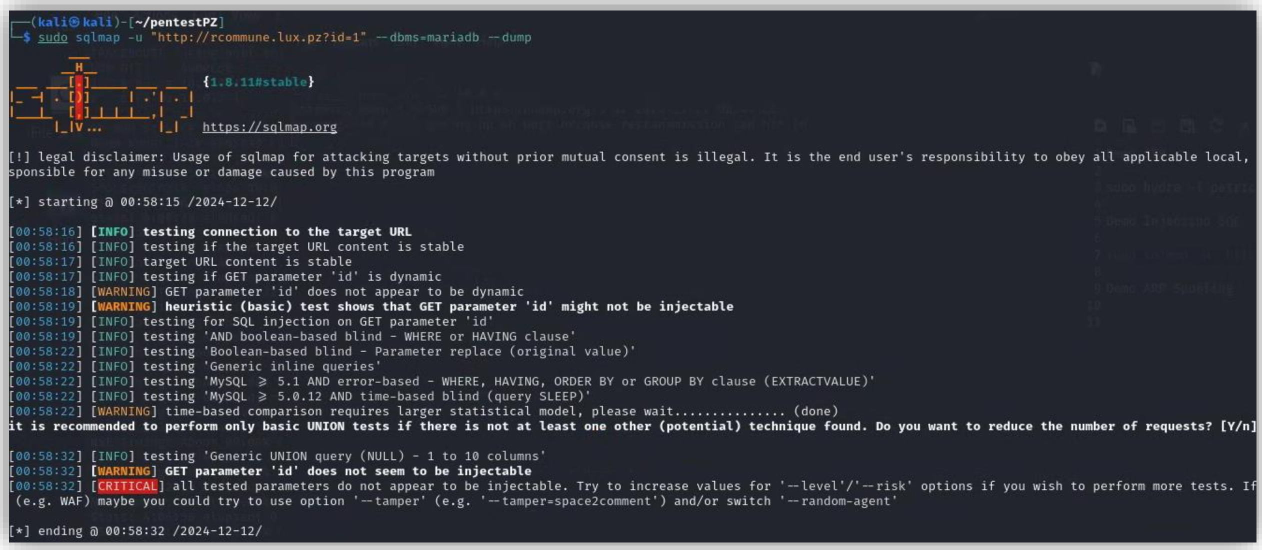
Une injection SQL est un groupe de méthodes d'exploitation de faille de sécurité d'une application interagissant avec une base de données. Elle permet d'injecter dans la requête SQL en cours un morceau de requête non prévu par le système et pouvant en compromettre la sécurité.

Outil utilisé

SQLMAP

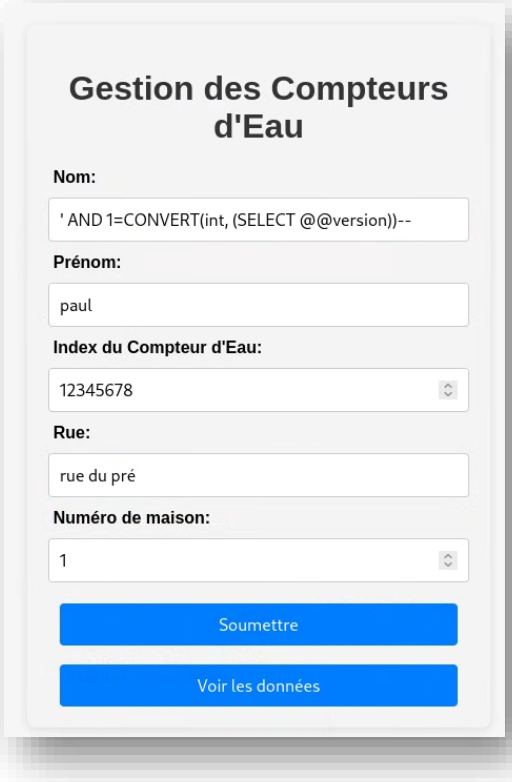
Outil de Pentest qui automatise la détection et l'exploitation de vulnérabilités d'injection SQL dans les applications Web.

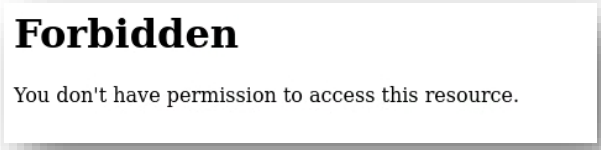
- ➢ Injection SQL automatisée sur le Reverse Proxy



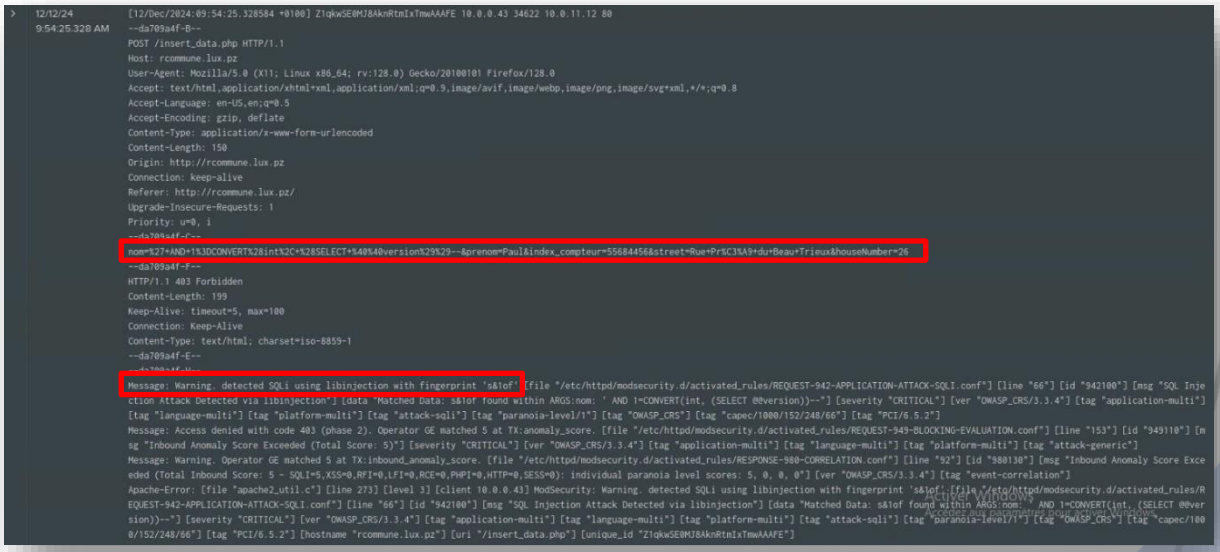
- ➢ Détection de l'attaque bloquée sur le SIEM externalisé, **Splunk**

- Injection SQL réalisée sur le site Web, accessible depuis l'hôte du Pentesteur





- Détection de l'attaque bloquée sur le SIEM externalisé, **Splunk**



Le WAF (Web Application Firewall) bloque les tentatives d'injection SQL, qu'elle soit automatisée ou manuelle, comme le montrent les nombreux logs remontés au SIEM externalisé.

ARP Spoofing

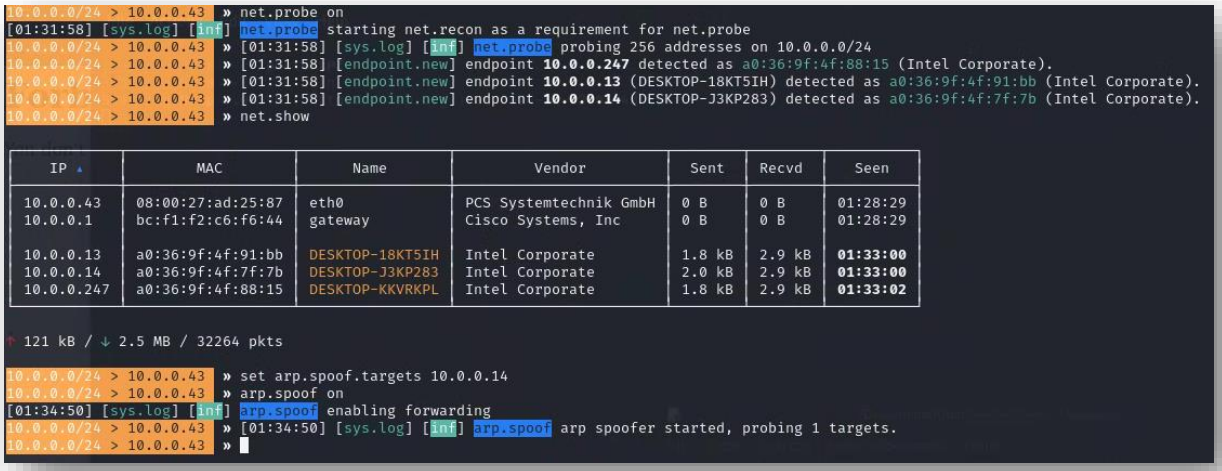
L'ARP spoofing (ou empoisonnement ARP) est une technique d'attaque réseau ou un attaquant envoie de fausses informations ARP (Address Resolution Protocol) sur un réseau local. L'ARP est utilisé pour associer des adresses IP aux adresses MAC (physiques) des appareils d'un réseau.

Outil utilisé

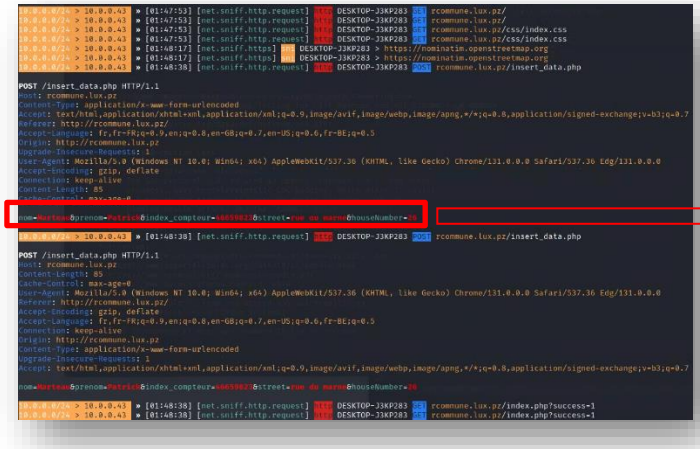
Bettercap

Bettercap est un outil de surveillance et d'attaque réseau, principalement utilisé pour les tests de pénétration et les audits de sécurité. Il permet de réaliser diverses attaques, telles que l'ARP spoofing, les attaques « Man-in-the-Middle », l'interception de trafic, la capture de paquets, et l'analyse de réseau en temps réel.

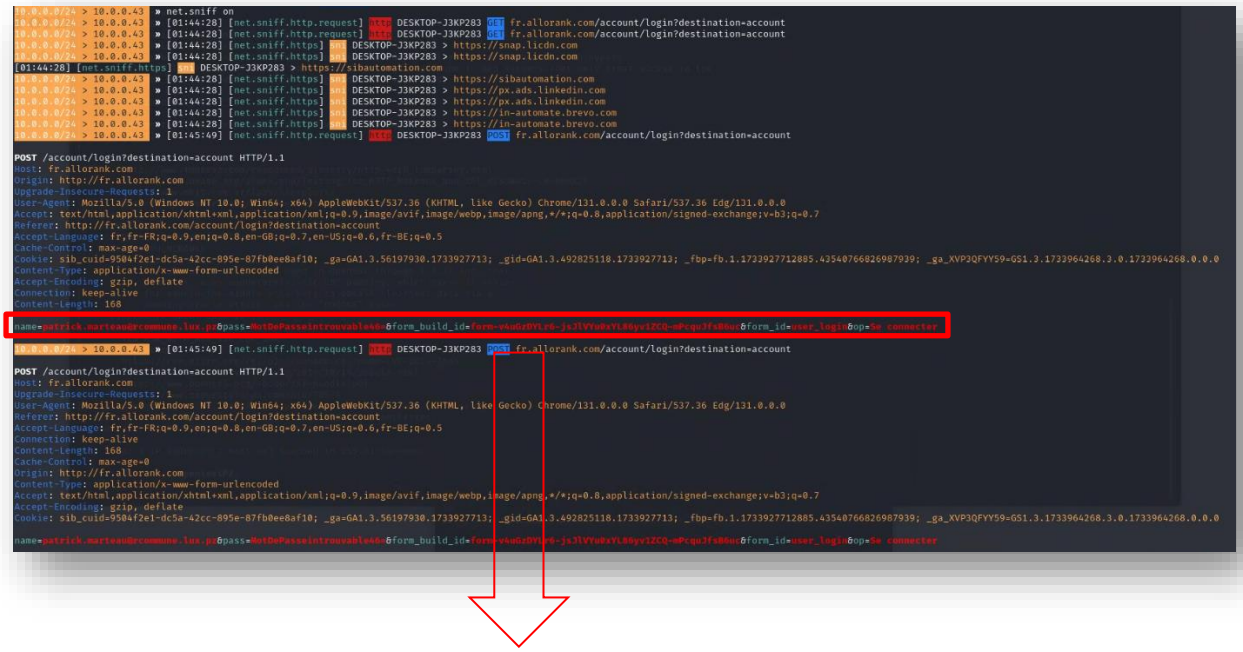
- Modification de la table ARP de la machine dite « victime »



- Surveillance de l'activité réseau de l'utilisateur de la machine victime



Informations rentrées par l'utilisateur sur le site Web Rcommune pour le service des eaux



Informations sensibles (Mots de passe) rentrées par l'utilisateur

- Table ARP de la machine « victime » modifiée, redirigeant le trafic vers l'attaquant

Avant l'attaque

```
Interface : 10.0.0.14 --- 0x10
  Adresse Internet      Adresse physique      Type
  10.0.0.1              bc-f1-f2-c6-f6-44     dynamique
  10.0.0.13             a0-36-9f-4f-91-bb     dynamique
  10.0.0.15             08-00-27-ad-25-87     dynamique
  10.0.0.43             08-00-27-ad-25-87     dynamique
  10.0.0.247            a0-36-9f-4f-88-15     dynamique
  10.0.0.255            ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
```

Après l'attaque

```
Interface : 10.0.0.14 --- 0x10
  Adresse Internet      Adresse physique      Type
  10.0.0.1              08-00-27-ad-25-87     dynamique
  10.0.0.13             a0-36-9f-4f-91-bb     dynamique
  10.0.0.15             08-00-27-ad-25-87     dynamique
  10.0.0.43             08-00-27-ad-25-87     dynamique
  10.0.0.247            a0-36-9f-4f-88-15     dynamique
  10.0.0.255            ff-ff-ff-ff-ff-ff     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.251           01-00-5e-00-00-fb     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
```

Router	Router 1	Router 2 SOC/NOC	NIS2 Compliance	Recommandations
Politique de sécurité				
Avez-vous une politique des sécurité pour le routeur ?	**?**	**?**		
Services inutilisés				
Les interfaces inutilisés sont-ils fermés ?	**Oui**	**Oui**		Unused interfaces on the router should be disabled.
Le DNS Lookup est-il désactivé pour le routeur ?	**Non**	**Non**		Accés au DNS Bind pour le WebServer.
Les TCP et UDP small servers sont-ils désactivés ?	**?**	?		
Le Cisco Discovery Protocol est-il désactivé ?	**?**	**?**		CDP which is used to obtain information such as the ip address, platform type of the neighboring Ciscodevices should be disabled on the router if not used by any application.
Le finger service est-il désactivé ?	**?**	**?**		Unauthorized persons can use the information obtained through this command for reconnaissance attacks. This service should be disabled.
Le serveur Bootp est-il désactivé ?	**?**	**?**		
Le directed broadcast est-il désactivé sur tous les interfaces ?	**?**	**?**		Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This feature should be disabled on the router as it could be used in denial-of-service attacks.
Le source routing est-il désactivé ?	**?**	**?**		Source routing is a feature that allows individual packets to specify routes. This is used in various attacks.
Le proxy ARP est-il désactivé ?	**?**	**?**		Proxy ARP helps in extending a LAN at layer 2 across multiple segments thereby breaking the LAN security perimeter.
L'ICMP redirect est-il désactivé ?	**Non**	**Non**		
Cryptage des mots de passe				
Les mots de passe sont-il cryptés dans le fichier de configuration ?	**Oui**	**Oui**		
Paramètres d'identification				
Le mot de passe enable secret est-il configuré?	**Oui**	**Oui**	PR.AC-1	
Le mot de passe enable secret est-il identique à un nom d'hôte, d'utilisateur ou autre mot de passe du réseau ?	**non**	**non**	PR.AC-1	
Le MOTD est-il défini ?	**Oui**	**Oui**	PR.AC-1	
Le mot de passe et le timeout de la console ont-il été défini ?	**Oui**	**Oui**	PR.AC-1	
Aux port est-il désactivé ?	**Oui**	**Oui**	PR.AC-1	
Les mots de passe et les timeout ont-il été défini sur les lignes VTY ?	**Oui**	**Oui**	PR.AC-1	
Les lignes VTY sont-elles restraintes à certaines adresses IP ?	**?**	**?**	PR.AC-1	
Votre politique de sécurité prévoit-elle une fréquence de changement des mots de passe ?	**Oui**	**Oui**	PR.AC-1	Router passwords need to be changed periodically, typically once every 4-6 months depending on the functionality of the router.
Les mots de passe répondent-ils aux critères définis dans votre politique de sécurité ?	**Oui**	**Oui**	PR.AC-1	All password defined on the router should meet the following criteria: Minimum 8 characters in length ; Should be alphanumeric along with special characters (@#$%) ; Should not include organization’s name in it
Les lignes Vty utilisent-elles SSH ?	**Non**	**Non**	PR.AC-1	

Router	Router 1	Router 2 SOC/NOC	NIS2 Compliance	Recommandations
Utilisez-vous Telnet ? (pour faire des sauvegarder des configuration par exemple ?)	**Non**	**Non**	PR.AC-1	The Telnet protocol transfers data in clear text thereby allowing an intruder to sniff valuable data such as passwords.
Identification de l'administrateur				
Existe-t-il une procédure documentée pour la création de nouveau utilisateur ?	**Oui**	**Oui**		
L'identification se fait-elle par un serveur Radius?	**Non**	**Non**		
L'administrateur a-t-il un compte réservé ?	**Oui**	**Oui**	PR.AC-4	
Les utilisateurs ont-ils le niveau de privilège le plus bas possible ? (Least Privilege)	**?**	**?**	PR.AC-4	Nous recommandons d'opter pour la règle du "least privilege" qui prévoit de donner l'accès minimum possible aux utilisateurs pour la réalisation de leur tâche.
MGMT Access				
Utilisez-vous un serveur HTTP/HTTPS pour gérer le routeur ?	**Non**	**Non**		This service allows the router to be monitored or have its configuration modified from the web browser. If not used, this service should be disabled.
Utilisez-vous SNMPv3 pour gérer le routeur ?	**Non**	**Non**		Ideally SNMP version 3 should be used on the router since it introduces authentication in the form of a username and password and offers encryption as well.
La community string par défaut a-t-elle été changée (private-public) ?	**?**	**?**		Default community strings such as ‘public’ and ‘private’ should be changed immediately before bring the router on the network.
A quelle fréquence est-elle changée ?	**?**	**?**		
NTP est-il utilisé pour synchroniser les routeurs ?	**Oui**	**Oui**		
Filtres				
Avez-vous des filtres RFC1918?	**Oui**	**Oui**		RFC 1918 addresses are meant to be used for internal networks only and have no reason to be seen on the Internet (the following addresses should be denied : 10.0.0.0. 172.16.0.0 192.168.0.0).
Route Protocol Security				
Le message d'authentification du protocol de routing est-il activé ?	**?**	**?**		
Maintenance de la configuration				
A quelle fréquence sauvegardez-vous la configuration ?	**?**	**?**	PR.IP-4	Il est conseillé de faire une sauvegarde "régulière" (à définir).
le back up se trouve-t-il dans une zone isolée ?	**?**	**?**	PR.IP-4	La sauvegarde doit se trouver sur un réseau différent du système que l'on sauvegarde et si possible sur un dispositif hors-ligne.
La sécurité de l'appareil où sont conservés les backups est-elle assurée ?	**?**	**?**	PR.IP-4	
Il y a-t-il une procédure documentée pour les backups ?	**?**	**?**	PR.IP-4	
Les changements apportés au routeur sont-ils documentés ?	**Oui**	**Oui**	PR.IP-4	
Redondance				
Il y a-t-il une redondance prévue pour les routeurs ?	**Oui**	**Oui**	ID.BE-5/PR.DS-4	Une redondance est prévue comme démontrer dans le LLD mais n'est actuellement pas mis en place.
Les procédures de récupération sont-elles documentées et testées ?	**?**	**?**	ID.BE-5/PR.DS-4	
Logs				

Router	Router 1	Router 2 SOC/NOC	NIS2 Compliance	Recommandations
Les accès refusés aux ports, services et protocoles sont-ils logués?			DE.AE-2/3	
Les procédures pour l'audit des logs sont-elles documentées et suivies ?	**Oui**	**Oui**	DE.AE-2/3	
Les logs sont-elles analysées ? A quelle fréquence ?	**Oui, 24/24**	**Oui, 24/24**	DE.AE-2/3	
Quelles sont les étapes définies en cas d'incident malicieux ?	**Voir DOC**	**Voir DOC**	DE.AE-2/3	

Server Web	RCommune	NIS2 Compliance	Recommandations
Général			
Toujours adhéré au principe du moindre privilège	Seul l'administrateur IT à accès au serveur WEB	PR-AC-4	Principe du moindre privilege.
Version Management			
Installer les updates de sécurités	Le serveur n'est pas à jour	PR.MA-1	Faire les dernières mise à jour en date.
Ne jamais installer de logiciels non supporté ou en fin de vie	Rocky Linux (RHEL) / Apache	PR.MA-1	Installer des logiciels étant mis à jour régulierement.
Installer des logiciels depuis des sources vérifiées	Logiciel téléchargé depuis le site officiel	ID.AM-2	
Vérifier l'intégrité des logiciels à installer	MD5 vérifié	ID.AM-2	Utilisé un logiciel qui permet de faire une verification totale.
Securité réseau			
Désactiver tous les services étranger	N'est installé sur le serveur web que ce qui est nécessaire à son bon fonctionnement et à l'indexisation des informations dans la database	PR.AC-4	Les permissions et autorisations d'accès sont gérées en intégrant les principes du moindre privilége.
Désactiver toutes les fonctions ICMP	Non		
Installer un pare-feu avec une politique de déni par défaut	Un WAF ainsi que PFSense est en place	PR.AC-5	Utilisé un pare-feu et placez le devant le server web dans votre infrastructure pour plus de sécurité.
Faire traverser un pare-feu les communications entrentes et sortantes	Un WAF ainsi que PFSense est en place	PR.AC-5	Utilisé un WAF (mode security) et placez le devant le server web dans votre infrastructure pour plus de sécurité.
Désactiver le routage sauf si explicitement demandé	Le routage est désactivé	PR.AC-4	Désactiver tout services non utilisé.
Séparer les serveurs publiques du réseau privé	Non	ISO27001	Mettre le serveur dans une DMZ pour isolé le publique trafique et privé.
Activer la signature des enregistrements DNS	Non	ISO27001	Confirme que le nom de domaine est lié à la bonne adresse IP. A mettre en place.
Authentification et autorisation			
Configurer l'authentification pour l'accès au mode monoposte	Non	PR.AC-3	Activé l'authentification pour les accès neccessaires.
Configurer l'authentification obligatoire pour tous les services non publics	?	PR.AC-3	Activé l'authentification pour les accès neccessaires.
Configurer l'autorisation obligatoire pour tous les services non publics	?	PR.AC-4	Autorisation oblgatoire pour tout les services non publiques.
Configurer l'authentification obligatoire pour tous les utilisateurs	Oui	PR.AC-3	Activé l'authentification pour les accès neccessaires.
Imposer l'utilisation de mots de passe forts	Oui	ISO27001	Utilisé des GPO pour les users de l'AD.
Supprimer tous les comptes par défaut, de test, invité et obsolètes	Il existe 2 comptes login "root" et celui de l'administrateur	PR.AC-4	Envisagez d'identifier séparément chaque personne ayant accès aux systèmes critiques de l'organisation avec un nom d'utilisateur afin de supprimer les comptes et les accès génériques et anonymes
Désactiver la connexion à distance pour les comptes administrateur	Non	ISO27001	Exige des contrôles d'accès stricts, y compris la limitation des accès distants pour les comptes privilégiés.
Protection de la vie privée et confidentialité			
Configurer les services pour qu'ils divulguent un minimum d'informations	?	PR.AC-4	Principe du moindre privilege.

Server Web	RCommune	NIS2 Compliance	Recommandations
Transmettre des informations sensibles via des connexions sécurisées	Les informations arrive via un VPN	PR.AC-4	Principe du moindre privilege.
Refuser l'accès aux informations sensibles via des connexions non sécurisées	?	PR.AC-4	Principe du moindre privilege.
N'utilisez jamais de certificats SSL non fiables ou expirés	Non	PR.AC-4	Passer par une autorité certifiée et ne pas passer par un certificat auto-signé
Ne jamais permettre au public d'accéder aux systèmes de test, de développement et d' acceptation	Oui	PR.AC-4	Principe du moindre privilege.
Configurer les autorisations de fichiers de manière aussi restrictive que possible	Oui	PR.AC-4	Utilisé des groupe d'utilisateur dans un AD et ajusté les accés.
Journalisation			
Restreindre l'accès aux informations de journalisation	SOC/NOC externe 24/7	DE.AE-2/3	Utilisé des GPO dans l'AD pour les restrictions.
Configurer la journalisation pour tous les services pertinents	SOC/NOC externe 24/7	DE.AE-2/3	Configuration interne au site SOC/NOC.
Configurer la journalisation pour tous les échecs d' authentification et d'autorisation	SOC/NOC externe 24/7	DE.AE-2/3	Configuration interne au site SOC/NOC.
Configurer la journalisation à distance pour tous les événements liés à la sécurité	SOC/NOC externe 24/7	DE.AE-2/3	Configuration interne au site SOC/NOC.
Surveillez et affichez régulièrement les journaux	SOC/NOC externe 24/7	DE.AE-2/3	Configuration interne au site SOC/NOC.
Spécifique au service			
Remplissez la liste de contrôle du développement sécurisé pour les applications Web	Non	PR.AC-4	Principe du moindre privilege.
Désactiver le téléchargement anonyme pour les services FTP	Non	PR.AC-4	Principe du moindre privilege.
Désactiver les transferts AXFR non autorisés dans le DNS	Non	PR.AC-4	Principe du moindre privilege.

Switch	Switch 1	NIS2 Compliance	Recommandations
Politique de sécurité			
Avez-vous une politique des sécurité pour les switches ?	Elles ne sont pas mise en place		Prévoir une configuration supplémentaire (DAI, port-security, storm-control,...)
Services inutilisés			
Les interfaces inutilisés sont-ils fermés ?	Elles sont shutdown et mise dans un vlan inuti		
Les TCP et UDP small servers sont-ils désactivés ?	Il est toujours actif.		Le TCP/UDP small server est utilisé pour faire des diagnostics. Il est préférable de le désactiver.
Le Cisco Discovery Protocol est-il désactivé ?	Le CDP a été désactivé et LLDP a été mis en pl		
L'ICMP redirect est-il désactivé ?	L'ICMP redirect est toujours actif.		Les messages ICMP peuvent être utilisés lors des phases de reconnaissance. Il est préférable de les désactiver.
Cryptage des mots de passe			
Les mots de passe sont-il cryptés dans le fichier de configuration ?	Le password encryption à été configuré.	PR.AC-1	
Paramètres d'identification			
Le mot de passe enable secret est-il configuré?	Le mot de passe enable est configuré.	PR.AC-1	
Le mot de passe enable secret est-il identique à un nom d'hôte, d'utilisateur ou autre mot de passe du réseau ?	Oui, le mot de passe est identique sur toutes le	PR.AC-1	Changer le mot de passe pour qu'il soit différent sur chaque machine afin d'éviter de pouvoir entrer partout avec les même credentials ?
Le MOTD est-il défini ?	Il est défini comme suit : "Accès non autorisé"	PR.AC-1	
Le mot de passe et le timeout de la console ont-il été défini ?	Le mdp est défini mais pas le timeout.	PR.AC-1	Le timeout permet de mettre un temps d'attente après x tentative ratée.
Aux port est-il désactivé ?	Tous les ports secondaires ont été désactiver.	PR.AC-1	
Les mots de passe et les timeout ont-il été défini sur les lignes VTY ?	Les mots de pasee sont en place mais le timeo	PR.AC-1	Ceci permet de réduire les chances d'accès inautorisé à la machine. Il est indispensable de configurer le timeout pour réduire les attaques brute force.
Votre politique de sécurité prévoit-elle une fréquence de changement des mots de passe ?	Oui, tous les 6 mois.	PR.AC-1	
Les mots de passe répondent-ils aux critères définis dans votre politique de sécurité ?	Oui, 16 caractères minimum avec majuscule, c	PR.AC-1	
Les lignes Vty utilisent-elles SSH ?	Oui	PR.AC-1	
Utilisez-vous Telnet ? (pour faire des sauvegarder des configuration par exemple ?)	Non	PR.AC-1	Il faudrait prévoir pour la politique de backup un serveur TFTP ?
Identification de l'administrateur			
Existe-t-il une procédure documentée pour la création de nouveau utilisateur ?	Oui, la commune a effectivement une docume		Elle existe mais est incomplète. Il faudrait ajouter l'approbation du
L'identification se fait-elle par un serveur Radius?	Non		Un serveur AAA devrait être installé pour gérer les identifiants.
Les utilisateurs ont-ils le niveau de privilège le plus bas possible ? (Least Privilege)	Chaque utilisateur est lié à son département et n'ont accès à rien qui ne concerne pas leur tâche.	PR.AC-4	Nous recommandons d'opter pour la règle du "least privilege" qui prévoit de donner l'accès minimum possible aux utilisateurs pour la réalisation de leur tâche.
L'administrateur a-t-il un compte réservé ?	Un compte est mis en place pour administrer l	PR.AC-4	

Switch	Switch 1	NIS2 Compliance	Recommandations
MGMT Access			
Utilisez-vous SNMPv3 pour gérer le routeur ?	Non, est actuellement en place SNMP v2c		
La community string par défaut a-t-elle été changée (private-public) ?	La community string a été changée.		
NTP est-il utilisé pour synchroniser les routeurs ?	Oui, le switch est actuellement strate 4 et le se		
Filtres			
Avez-vous des filtres RFC1918?	Des ACL sont en place au niveau du MLS et du		Principe du moindre privilege.
Maintenance de la configuration			
A quelle fréquence sauvegardez-vous la configuration ?		PR.IP-4	Des sauvegardes doivent être éffectué régulièrement
le back up se trouve-t-il dans une zone isolée ?		PR.IP-4	Les sauvegardes doivent être sur un réseau différent de la machine et/ou sur un support physique externe.
La sécurité de l'appareil où sont conservés les backups est-elle assurée ?		PR.IP-4	A mettre dans un endroit fermé avec une restriction maximum d'accès.
Il y a-t-il une procédure documentée pour les backups ?		PR.IP-4	
Les changements apportés au routeur sont-ils documentés ?	Un document de log pour les changements est	PR.IP-4	
Redondance			
Il y a-t-il une redondance prévue pour les switches ?	Une redondance est prévue comme démontrer dans le LLD mais n'est actuellement pas mis en	ID.BE-5/PR.DS-4	
Les procédures de récupération sont-elles documentées et testées ?	Non	ID.BE-5/PR.DS-4	
Logs			
Les accès refusés aux ports, services et protocoles sont-ils logués?	Les logs sont récupérés par le SOC/NOC	DE.AE-2/3	
Les logs sont-elles analysées ? A quelle fréquence ?	Elles sont analysées via le sous-traitant SOC/N	DE.AE-2/3	
Quelles sont les étapes définies en cas d'incident malicieux ?		PR.IP-9	

Tests de Vulnérabilités

Ces tests sont basés sur une multitude de base de données regroupant des Common Vulnerabilities. Des scripts dits NSE ainsi que l'utilisation de BETTERCAP sont utilisés afin de passer cette panoplie de tests de vulnérabilités en une commande et nous retourne des résultats très intuitifs.

BETTERCAP

1. Automatisation de l'ARP Spoofing

Découverte des hôtes sur le réseau
Choix de l'hôte cible
Lancement de l'attaque
Elle modifie la table ARP de la victime afin que l'adresse MAC de sa gateaway soit celle de la machine attaquante.
Activation du sniffing

2. L'attaque est fonctionnelle suite à un manque de configuration sur les appareils

Voici la configuration recommandée

Concernant les switch Cisco en place. Il est nécessaire d'avoir un serveur DHCP (de préférence IEEE) en place car le switch remplit la table "trust" ARP dynamiquement. Ensuite mettre en place le DAI

Active le DHCP Snooping sur les vlans spécifiées

Sélectionne l'interface trust

Définir cette interface comme trusted

Active le DAI sur les vlan spécifiées

Configurer la limite de taux sur une interface non trustée. Pour bien délimiter la limite il faut faire une baseline des pacquets arp qui doivent transité à travers l'interface trustée.

Si le port passe en mode "error-disable" c'est qu'il reçoit trop de requête ARP. Soit suite à une attaque ou alors un erreur dans la définition de la baseline.

Common Vulnerabilities and Exposures

Concerne l'ID.RA-1 du NIS2	Colonne 1	Colonne 2
Appareil	**CVE**	Description
HP (BIOS L01 v02.53)	CVE-2022-37018	A potential vulnerability has been identified in the system BIOS for certain HP PC products which may allow escalation of privileges and code execution. HP is releasing firmware updates to mitigate the potential vulnerability.
	CVE-2022-23958	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.
	CVE-2022-23957	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.
	CVE-2022-23956	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.
	CVE-2022-23955	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.
	CVE-2022-23954	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.
	CVE-2022-23953	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.
	CVE-2022-23934	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23933	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23932	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23931	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23930	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23929	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.

	CVE-2022-23928	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23927	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23927	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23926	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23925	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2022-23924	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.
	CVE-2021-3661	A potential security vulnerability has been identified in certain HP Workstation BIOS (UEFI firmware) which may allow arbitrary code execution. HP is releasing firmware mitigations for the potential vulnerability.
	CVE-2019-6322	HP has identified a security vulnerability with some versions of Workstation BIOS (UEFI Firmware) where the runtime BIOS code could be tampered with if the TPM is disabled. This vulnerability relates to Workstations whose TPM is enabled by default.
	CVE-2019-6321	HP has identified a security vulnerability with some versions of Workstation BIOS (UEFI Firmware) where the runtime BIOS code could be tampered with if the TPM is disabled. This vulnerability relates to Workstations whose TPM is disabled by default.
	CVE-2017-2751	A BIOS password extraction vulnerability has been reported on certain consumer notebooks with firmware F.22 and others. The BIOS password was stored in CMOS in a way that allowed it to be extracted. This applies to consumer notebooks launched in early 2014.
	CVE-2016-2243	Sure Start on HP Commercial PCs 2015 allows local users to cause a denial of service (BIOS recovery failure) by leveraging administrative access.

	CVE-2015-0949	The System Management Mode (SMM) implementation in Dell Latitude E6430 BIOS Revision A09, HP EliteBook 850 G1 BIOS revision L71 Ver. 01.09, and possibly other BIOS implementations does not ensure that function calls operate on SMRAM memory locations, which allows local users to bypass the Secure Boot protection mechanism and gain privileges by leveraging write access to physical memory.
	CVE-2012-5218	HP ElitePad 900 PCs with BIOS F.0x before F.01 Update 1.0.0.8 do not enable the Secure Boot feature, which allows local users to bypass intended BIOS restrictions and boot unintended operating systems via unspecified vectors.
	CVE-2008-3902	HP firmware 68DTT F.0D stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer, aka SSRT080104.
	CVE-2008-0706	Unspecified vulnerability in the BIOS F.26 and earlier for the HP Compaq Notebook PC allows physically proximate attackers to obtain privileged access via unspecified vectors, possibly involving an authentication bypass of the power-on password.
	CVE-2008-0211	Unspecified vulnerability in the BIOS F.04 through F.11 for the HP Compaq Business Notebook PC allows local users to cause a denial of service via unspecified vectors.
Rocky Linux 8.7	CVE-2022-32893	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6.1 and iPadOS 15.6.1, macOS Monterey 12.5.1, Safari 15.6.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.
Cisco Routeur 2911	CVE-2018-0163	A vulnerability in the 802.1x multiple-authentication (multi-auth) feature of Cisco IOS Software could allow an unauthenticated, adjacent attacker to bypass the authentication phase on an 802.1x multi-auth port. The vulnerability is due to a logic change error introduced into the code. An attacker could exploit this vulnerability by trying to access an 802.1x multi-auth port after a successful supplicant has authenticated. An exploit could allow the attacker to bypass the 802.1x access controls and obtain access to the network. Cisco Bug IDs: CSCvg69701.
	CVE-2013-1241	The ISM module in Cisco IOS on ISR G2 routers does not properly handle authentication-header packets, which allows remote authenticated users to cause a denial of service (module reload) via a series of malformed packets, aka Bug ID CSCub92025.
Fortigate60F	CVE-2021-36173	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6.4.6, 6.2.0 through 6.2.9, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images.

	CVE-2020-12818	An insufficient logging vulnerability in FortiGate before 6.4.1 may allow the traffic from an unauthenticated attacker to Fortinet owned IP addresses to go unnoticed.
Cisco Switch2960	CVE-2017-3881	A vulnerability in the Cisco Cluster Management Protocol (CMP) processing code in Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a reload of an affected device or remotely execute code with elevated privileges. The Cluster Management Protocol utilizes Telnet internally as a signaling and command protocol between cluster members. The vulnerability is due to the combination of two factors: (1) the failure to restrict the use of CMP-specific Telnet options only to internal, local communications between cluster members and instead accept and process such options over any Telnet connection to an affected device; and (2) the incorrect processing of malformed CMP-specific Telnet options. An attacker could exploit this vulnerability by sending malformed CMP-specific Telnet options while establishing a Telnet session with an affected Cisco device configured to accept Telnet connections. An exploit could allow an attacker to execute arbitrary code and obtain full control of the device or cause a reload of the affected device. This affects Catalyst switches, Embedded Service 2020 switches, Enhanced Layer 2 EtherSwitch Service Module, Enhanced Layer 2/3 EtherSwitch Service Module, Gigabit Ethernet Switch Module (CGESM) for HP, IE Industrial Ethernet switches, ME 4924-10GE switch, RF Gateway 10, and SM-X Layer 2/3 EtherSwitch Service Module. Cisco Bug IDs: CSCvd48893.
Server ESXI 8.0	CVE-2024-22253	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the UHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.
	CVE-2024-22252	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.
	CVE-2020-3999	VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition.
	CVE-2024-22273	The storage controllers on VMware ESXi, Workstation, and Fusion have out-of-bounds read/write vulnerability. A malicious actor with access to a virtual machine with storage controllers enabled may exploit this issue to create a denial of service condition or execute code on the hypervisor from a virtual machine in conjunction with other issues.
	CVE-2024-37087	The vCenter Server contains a denial-of-service vulnerability. A malicious actor with network access to vCenter Server may create a denial-of-service condition.

	CVE-2024-37086	VMware ESXi contains an out-of-bounds read vulnerability. A malicious actor with local administrative privileges on a virtual machine with an existing snapshot may trigger an out-of-bounds read leading to a denial-of-service condition of the host.
	CVE-2024-22255	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability in the UHCI USB controller. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process.
Windows10 (Pro) 22h2	CVE-2024-49074	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
	CVE-2024-49073	Windows Mobile Broadband Driver Elevation of Privilege Vulnerability
	CVE-2024-49046	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability
	CVE-2024-49039	Windows Task Scheduler Elevation of Privilege Vulnerability
	CVE-2024-43646	Windows Secure Kernel Mode Elevation of Privilege Vulnerability
	CVE-2024-43644	Windows Client-Side Caching Elevation of Privilege Vulnerability
	CVE-2024-43643	Windows USB Video Class System Driver Elevation of Privilege Vulnerability
	CVE-2024-43641	Windows Registry Elevation of Privilege Vulnerability
	CVE-2024-43640	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
	CVE-2024-43638	Windows USB Video Class System Driver Elevation of Privilege Vulnerability
	CVE-2024-43637	Windows USB Video Class System Driver Elevation of Privilege Vulnerability
	CVE-2024-43636	Win32k Elevation of Privilege Vulnerability
	CVE-2024-43634	Windows USB Video Class System Driver Elevation of Privilege Vulnerability
	CVE-2024-43631	Windows Secure Kernel Mode Elevation of Privilege Vulnerability
	CVE-2024-43630	Windows Kernel Elevation of Privilege Vulnerability
	CVE-2024-43629	Windows DWM Core Library Elevation of Privilege Vulnerability
	CVE-2024-43626	Windows Telephony Service Elevation of Privilege Vulnerability
	CVE-2024-43624	Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability
	CVE-2024-43623	Windows NT OS Kernel Elevation of Privilege Vulnerability
	CVE-2024-43530	Windows Update Stack Elevation of Privilege Vulnerability
	CVE-2024-43452	Windows Registry Elevation of Privilege Vulnerability
	CVE-2024-43449	Windows USB Video Class System Driver Elevation of Privilege Vulnerability
Windows Server 2022 21h2	CVE-2022-34718	This vulnerability in the TCP/IP stack allows remote code execution (RCE) with elevated privileges. It affects various Windows Server versions, including Server 2022. Exploiting this does not require user interaction, making it particularly severe. Microsoft has issued patches, and it is recommended to apply them immediately

	CVE-2022-24508	This is an RCE vulnerability in SMBv3 (Server Message Block) that affects authenticated users, including on Server 2022. While exploitation is not yet widespread, Microsoft categorizes it as "exploitation more likely." Disabling SMBv3 compression can be a temporary mitigation until the patch is applied
	CVE-2022-21849	Found in the IKE (Internet Key Exchange) Extension component, this allows remote attackers to potentially take full control of a system. It's critical to update Windows Server with the latest patches to mitigate this risk
Apache 2.34.7	CVE-2024-53949	Improper Authorization vulnerability in Apache Superset when FAB_ADD_SECURITY_API is enabled (disabled by default). Allows for lower privilege users to use this API.\n\n issue affects Apache Superset: from 2.0.0 before 4.1.0.\n\nUsers are recommended to upgrade to version 4.1.0, which fixes the issue.
	CVE-2024-53948	Generation of Error Message Containing analytics metadata Information in Apache Superset.\n\nThis issue affects Apache Superset: before 4.1.0. \n\nUsers are recommended to upgrade to version 4.1.0, which fixes the issue.
	CVE-2024-53947	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Superset. Specifically, certain engine-specific functions are not checked, which allows attackers to bypass Apache Superset's SQL authorization. This issue is a follow-up to CVE-2024-39887 with additional disallowed PostgreSQL functions now included: query_to_xml_and_xmlschema, table_to_xml, table_to_xml_and_xmlschema.\n\nThis issue affects Apache Superset: <4.1.0.\n\nUsers are recommended to upgrade to version 4.1.0, which fixes the issue or add these Postgres functions to the config set DISALLOWED_SQL_FUNCTIONS.
	CVE-2024-53677	File upload logic is flawed vulnerability in Apache Struts.\n\nThis issue affects Apache Struts: from 2.0.0 before 6.4.0.\n\nUsers are recommended to upgrade to version 6.4.0, which fixes the issue.\n\nYou can find more details in https://cwiki.apache.org/confluence/display/WW/S2-067
	CVE-2024-52338	Deserialization of untrusted data in IPC and Parquet readers in the Apache Arrow R package versions 4.0.0 through 16.1.0 allows arbitrary code execution. An application is vulnerable if it \nreads Arrow IPC, Feather or Parquet data from untrusted sources (for \nexample, user-supplied input files). This vulnerability only affects the arrow R package, not other Apache Arrow \nimplementations or bindings unless those bindings are specifically used via the R package (for example, an R application that embeds a Python interpreter and uses PyArrow to read files from untrusted sources is still vulnerable if the arrow R package is an affected version). It is recommended that users of the arrow R package upgrade to 17.0.0 or later. Similarly, it\n is recommended that downstream libraries upgrade their dependency \nrequirements to arrow 17.0.0 or later. If using an affected\nversion of the package, untrusted data can read into a Table and its internal to_data_frame() method can be used as a workaround (e.g., read_parquet (..., as_data_frame = FALSE)$to_data_frame()).\n\n\nThis issue affects the Apache Arrow R package: from 4.0.0 through 16.1.0.\n\n\nUsers are recommended to upgrade to version 17.0.0, which fixes the issue.
	CVE-2024-52318	Incorrect object recycling and reuse vulnerability in Apache Tomcat.\n\nThis issue affects Apache Tomcat: 11.0.0, 10.1.31, 9.0.96.\n\nUsers are recommended to upgrade to version 11.0.1, 10.1.32 or 9.0.97, which fixes the issue.

	CVE-2024-52317	Incorrect object re-cycling and re-use vulnerability in Apache Tomcat. Incorrect recycling of the request and response used by HTTP/2 requests \ncould lead to request and/or response mix-up between users. \n\nThis issue affects Apache Tomcat: from 11.0.0-M23 through 11.0.0-M26, from 10.1.27 through 10.1.30, from 9.0.92 through 9.0.95.\n\nUsers are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fixes the issue.
	CVE-2024-52316	Unchecked Error Condition vulnerability in Apache Tomcat. If Tomcat is configured to use a custom Jakarta Authentication (formerly JASPIC) ServerAuthContext component which may throw an exception during the authentication process without explicitly setting an HTTP status to indicate failure, the authentication may not fail, allowing the user to bypass the authentication process. There are no known Jakarta Authentication components that behave in this way.\n\nThis issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9.0.95.\n\nUsers are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fix the issue.
	CVE-2024-52067	Apache NiFi 1.16.0 through 1.28.0 and 2.0.0-M1 through 2.0.0-M4 include optional debug logging of Parameter Context values during the flow synchronization process. An authorized administrator with access to change logging levels could enable debug logging for framework flow synchronization, causing the application to write Parameter names and values to the application log. Parameter Context values may contain sensitive information depending on application flow configuration. Deployments of Apache NiFi with the default Logback configuration do not log Parameter Context values. Upgrading to Apache NiFi 2.0.0 or 1.28.1 is the recommendation mitigation, eliminating Parameter value logging from the flow synchronization process regardless of the Logback configuration.
	CVE-2024-51569	Out-of-bounds Read vulnerability in Apache NimBLE.\n\nMissing proper validation of HCI Number Of Completed Packets could lead to out-of-bound access when parsing HCI event and invalid read from HCI transport memory. \nThis issue requires broken or bogus Bluetooth controller and thus severity is considered low.\nThis issue affects Apache NimBLE: through 1.7.0. \n\n\nUsers are recommended to upgrade to version 1.8.0, which fixes the issue.
	CVE-2024-51504	When using IPAuthenticationProvider in ZooKeeper Admin Server there is a possibility of Authentication Bypass by Spoofing -- this only impacts IP based authentication implemented in ZooKeeper Admin Server. Default configuration of client's IP address detection in IPAuthenticationProvider, which uses HTTP request headers, is weak and allows an attacker to bypass authentication via spoofing client's IP address in request headers. Default configuration honors X-Forwarded-For HTTP header to read client's IP address. X-Forwarded-For request header is mainly used by proxy servers to identify the client and can be easily spoofed by an attacker pretending that the request comes from a different IP address. Admin Server commands, such as snapshot and restore arbitrarily can be executed on successful exploitation which could potentially lead to information leakage or service availability issues. Users are recommended to upgrade to version 3.9.3, which fixes this issue.

	CVE-2024-50386	Account users in Apache CloudStack by default are allowed to register templates to be downloaded directly to the primary storage for deploying instances. Due to missing validation checks for KVM-compatible templates in CloudStack 4.0.0 through 4.18.2.4 and 4.19.0.0 through 4.19.1.2, an attacker that can register templates, can use them to deploy malicious instances on KVM-based environments and exploit this to gain access to the host filesystems that could result in the compromise of resource integrity and confidentiality, data loss, denial of service, and availability of KVM-based infrastructure managed by CloudStack.\n\n\nUsers are recommended to upgrade to Apache CloudStack 4.18.2.5 or 4.19.1.3, or later, which addresses this issue. \n\nAdditionally, all user-registered KVM-compatible templates can be scanned and checked that they are flat files that should not be using any additional or unnecessary features. For example, operators can run the following command on their file-based primary storage(s) and inspect the output. An empty output for the disk being validated means it has no references to the host filesystems; on the other hand, if the output for the disk being validated is not empty, it might indicate a compromised disk. However, bear in mind that (i) volumes created from templates will have references for the templates at first and (ii) volumes can be consolidated while migrating, losing their references to the templates. Therefore, the command execution for the primary storages can show both false positives and false negatives.\n\n\nfor file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info. If the output is not empty, that might indicate a compromised disk; check it carefully."; qemu-img info -U $file | grep file: ; printf "\n\n"; done\nFor checking the whole template/volume features of each disk, operators can run the following command:\n\n\nfor file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info."; qemu-img info -U $file; printf "\n\n"; done
	CVE-2024-50378	Airflow versions before 2.10.3 have a vulnerability that allows authenticated users with audit log access to see sensitive values in audit logs which they should not see. When sensitive variables were set via airflow CLI, values of those variables appeared in the audit log and were stored unencrypted in the Airflow database. While this risk is limited to users with audit log access, it is recommended to upgrade to Airflow 2.10.3 or a later version, which addresses this issue. Users who previously used the CLI to set secret variables should manually delete entries with those variables from the log table.
	CVE-2024-50306	Unchecked return value can allow Apache Traffic Server to retain privileges on startup.\n\nThis issue affects Apache Traffic Server: from 9.2.0 through 9.2.5, from 10.0.0 through 10.0.1.\n\nUsers are recommended to upgrade to version 9.2.6 or 10.0.2, which fixes the issue.
	CVE-2024-50305	Valid Host header field can cause Apache Traffic Server to crash on some platforms.\n\nThis issue affects Apache Traffic Server: from 9.2.0 through 9.2.5.\n\nUsers are recommended to upgrade to version 9.2.6, which fixes the issue, or 10.0.2, which does not have the issue.
	CVE-2024-48962	Improper Control of Generation of Code ('Code Injection'), Cross-Site Request Forgery (CSRF), : Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Apache OFBiz.\n\nThis issue affects Apache OFBiz: before 18.12.17.\n\nUsers are recommended to upgrade to version 18.12.17, which fixes the issue.

	CVE-2024-47561	Schema parsing in the Java SDK of Apache Avro 1.11.3 and previous versions allows bad actors to execute arbitrary code.\nUsers are recommended to upgrade to version 1.11.4 or 1.12.0, which fix this issue.
	CVE-2024-47554	Uncontrolled Resource Consumption vulnerability in Apache Commons IO. \n\nThe org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input.\n\n\nThis issue affects Apache Commons IO: from 2.0 before 2.14.0. \n\nUsers are recommended to upgrade to version 2.14.0 or later, which fixes the issue.
	CVE-2024-47250	Out-of-bounds Read vulnerability in Apache NimBLE.\n\nMissing proper validation of HCI advertising report could lead to out-of-bound access when parsing HCI event and thus bogus GAP 'device found' events being sent. \nThis issue requires broken or bogus Bluetooth controller and thus severity is considered low.\nThis issue affects Apache NimBLE: through 1.7.0. \n\n\nUsers are recommended to upgrade to version 1.8.0, which fixes the issue.
	CVE-2024-47249	Improper Validation of Array Index vulnerability in Apache NimBLE.\n\nLack of input validation for HCI events from controller could result in out-of-bound memory corruption and crash.\nThis issue requires broken or bogus Bluetooth controller and thus severity is considered low.\nThis issue affects Apache NimBLE: through 1.7.0.\n\nUsers are recommended to upgrade to version 1.8.0, which fixes the issue.
	CVE-2024-47248	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Apache NimBLE.\n\nSpecially crafted MESH message could result in memory corruption when non-default build configuration is used. \nThis issue affects Apache NimBLE: through 1.7.0.\n\nUsers are recommended to upgrade to version 1.8.0, which fixes the issue.
	CVE-2024-47208	Server-Side Request Forgery (SSRF), Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz.\n\nThis issue affects Apache OFBiz: before 18.12.17.\n\nUsers are recommended to upgrade to version 18.12.17, which fixes the issue.
	CVE-2024-47197	Exposure of Sensitive Information to an Unauthorized Actor, Insecure Storage of Sensitive Information vulnerability in Maven Archetype Plugin. \n\nThis issue affects Maven Archetype Plugin: from 3.2.1 before 3.3.0. \n\nUsers are recommended to upgrade to version 3.3.0, which fixes the issue.\n\nArchetype integration testing creates a file\ncalled . /target/classes/archetype-it/archetype-settings.xml\nThis file contains all the content from the users ~/.m2/settings.xml file,\nwhich often contains information they do not want to publish. We expect that on many developer machines, this also contains\ncredentials.\n\nWhen the user runs mvn verify again (without a mvn clean), this file becomes part of\nthe final artifact.\n\nIf a developer were to publish this into Maven Central or any other remote repository (whether as a release\nor a snapshot) their credentials would be published without them knowing.

	CVE-2024-46911	Cross-site Resource Forgery (CSRF), Privilege escalation vulnerability in Apache Roller. On multi-blog/user Roller websites, by default weblog owners are trusted to publish arbitrary weblog content and this combined with a deficiency in Roller's CSRF protections allowed an escalation of privileges attack. This issue affects Apache Roller before 6.1.4.\n\nRoller users who run multi-blog/user Roller websites are recommended to upgrade to version 6.1.4, which fixes the issue.\n\nRoller 6.1.4 release announcement: https://lists.apache.org/thread/3c3f6rwqptyw6wdc95654fq5vlosqdpw
	CVE-2024-46901	Insufficient validation of filenames against control characters in Apache Subversion repositories served via mod_dav_svn allows authenticated users with commit access to commit a corrupted revision, leading to disruption for users of the repository.\n\nAll versions of Subversion up to and including Subversion 1.14.4 are affected if serving repositories via mod_dav_svn. Users are recommended to upgrade to version 1.14.5, which fixes this issue. \n\nRepositories served via other access methods are not affected.
Zabbix 7.0.0	CVE-2023-32727	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server.
Splunk	CVE-2024-53247	In Splunk Enterprise versions below 9.3.2, 9.2.4, and 9.1.7, and versions below 3.2.461 and 3.7.13 of the Splunk Secure Gateway app on Splunk Cloud Platform, a low-privileged user that does not hold the “admin“ or “power“ Splunk roles could perform a Remote Code Execution (RCE).
	CVE-2024-53246	In Splunk Enterprise versions below 9.3.2, 9.2.4, and 9.1.7 and Splunk Cloud Platform versions below 9.3.2408.101, 9.2.2406.106, 9.2.2403.111, and 9.1.2312.206, an SPL command can potentially disclose sensitive information. The vulnerability requires the exploitation of another vulnerability, such as a Risky Commands Bypass, for successful exploitation.
	CVE-2024-53245	In Splunk Enterprise versions below 9.3.0, 9.2.4, and 9.1.7 and Splunk Cloud Platform versions below 9.1.2312.206, a low-privileged user that does not hold the “admin“ or “power“ Splunk roles, that has a username with the same name as a role with read access to dashboards, could see the dashboard name and the dashboard XML by cloning the dashboard.
	CVE-2024-53244	In Splunk Enterprise versions below 9.3.2, 9.2.4, and 9.1.7 and Splunk Cloud Platform versions below 9.2.2406.107, 9.2.2403.109, and 9.1.2312.206, a low-privileged user that does not hold the “admin“ or “power“ Splunk roles could run a saved search with a risky command using the permissions of a higher-privileged user to bypass the SPL safeguards for risky commands on “/en-US/app/search/report“ endpoint through “s“ parameter. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The authenticated user should not be able to exploit the vulnerability at will.
	CVE-2024-53243	In Splunk Enterprise versions below 9.3.2, 9.2.4, and 9.1.7 and versions below 3.2.462, 3.7.18, and 3.8.5 of the Splunk Secure Gateway app on Splunk Cloud Platform, a low-privileged user that does not hold the “admin“ or “power“ Splunk roles could see alert search query responses using Splunk Secure Gateway App Key Value Store (KVstore) collections endpoints due to improper access control.

	CVE-2024-45741	In Splunk Enterprise versions below 9.2.3 and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.108 and 9.1.2312.205, a low-privileged user that does not hold the "admin" or "power" Splunk roles could create a malicious payload through a custom configuration file that the "api.uri" parameter from the "/manager/search/apps/local" endpoint in Splunk Web calls. This could result in execution of unauthorized JavaScript code in the browser of a user.
	CVE-2024-45740	In Splunk Enterprise versions below 9.2.3 and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a malicious payload through Scheduled Views that could result in execution of unauthorized JavaScript code in the browser of a user.
	CVE-2024-45739	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6, the software potentially exposes plaintext passwords for local native authentication Splunk users. This exposure could happen when you configure the Splunk Enterprise AdminManager log channel at the DEBUG logging level.
	CVE-2024-45738	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6, the software potentially exposes sensitive HTTP parameters to the `_internal` index. This exposure could happen if you configure the Splunk Enterprise `REST_Calls` log channel at the DEBUG logging level.
	CVE-2024-45737	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.108, and 9.1.2312.204, a low-privileged user that does not hold the "admin" or "power" Splunk roles could change the maintenance mode state of App Key Value Store (KVStore) through a Cross-Site Request Forgery (CSRF).
	CVE-2024-45736	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.107, 9.1.2312.204, and 9.1.2312.111, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a search query with an improperly formatted "INGEST_EVAL" parameter as part of a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms) which could crash the Splunk daemon (splunkd).
	CVE-2024-45735	In Splunk Enterprise versions below 9.2.3 and 9.1.6, and Splunk Secure Gateway versions on Splunk Cloud Platform versions below 3.4.259, 3.6.17, and 3.7.0, a low-privileged user that does not hold the "admin" or "power" Splunk roles can see App Key Value Store (KV Store) deployment configuration and public/private keys in the Splunk Secure Gateway App.
	CVE-2024-45734	In Splunk Enterprise versions 9.3.0, 9.2.3, and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could view images on the machine that runs Splunk Enterprise by using the PDF export feature in Splunk classic dashboards. The images on the machine could be exposed by exporting the dashboard as a PDF, using the local image path in the img tag in the source extensible markup language (XML) code for the Splunk classic dashboard.
	CVE-2024-45733	In Splunk Enterprise for Windows versions below 9.2.3 and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could perform a Remote Code Execution (RCE) due to an insecure session storage configuration.

	CVE-2024-45732	In Splunk Enterprise versions below 9.3.1, and 9.2.0 versions below 9.2.3, and Splunk Cloud Platform versions below 9.2.2403.103, 9.1.2312.200, 9.1.2312.110 and 9.1.2308.208, a low-privileged user that does not hold the "admin" or "power" Splunk roles could run a search as the "nobody" Splunk user in the SplunkDeploymentServerConfig app. This could let the low-privileged user access potentially restricted data.
	CVE-2024-45731	In Splunk Enterprise for Windows versions below 9.3.1, 9.2.3, and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could write a file to the Windows system root directory, which has a default location in the Windows System32 folder, when Splunk Enterprise for Windows is installed on a separate drive.
	CVE-2024-36997	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312, an admin user could store and execute arbitrary JavaScript code in the browser context of another Splunk user through the conf-web/settings REST endpoint. This could potentially cause a persistent cross-site scripting (XSS) exploit.
	CVE-2024-36996	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109, an attacker could determine whether or not another user exists on the instance by deciphering the error response that they would likely receive from the instance when they attempt to log in. This disclosure could then lead to additional brute-force password-guessing attacks. This vulnerability would require that the Splunk platform instance uses the Security Assertion Markup Language (SAML) authentication scheme.
	CVE-2024-36995	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could create experimental items.
	CVE-2024-36994	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a View and Splunk Web Bulletin Messages that could result in execution of unauthorized JavaScript code in the browser of a user.
	CVE-2024-36993	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a Splunk Web Bulletin Messages that could result in execution of unauthorized JavaScript code in the browser of a user.
	CVE-2024-36992	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a View that could result in execution of unauthorized JavaScript code in the browser of a user. The “url” parameter of the Dashboard element does not have proper input validation to reject invalid URLs, which could lead to a Persistent Cross-site Scripting (XSS) exploit.

	CVE-2024-36991	In Splunk Enterprise on Windows versions below 9.2.2, 9.1.5, and 9.0.10, an attacker could perform a path traversal on the /modules/messaging/ endpoint in Splunk Enterprise on Windows. This vulnerability should only affect Splunk Enterprise on Windows.
	CVE-2024-36990	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.2.2403.100, an authenticated, low-privileged user that does not hold the admin or power Splunk roles could send a specially crafted HTTP POST request to the datamodel/web REST endpoint in Splunk Enterprise, potentially causing a denial of service.
	CVE-2024-36989	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200, a low-privileged user that does not hold the admin or power Splunk roles could create notifications in Splunk Web Bulletin Messages that all users on the instance receive.

RSECURE

Guide de maintenance

Equipe Cybersécurité Technobel

technobel

Guide de maintenance

1) ACCESS VPN

1.1) USER ACCOUNT

Name	Type	Two-factor Authentication	Groups	Status	Ref.
Chantale.B	LOCAL	✗	Télétravail	Enabled	1
José.A	LOCAL	✗	Agents INDEX	Enabled	1
Patrick.I	LOCAL	✗	VPN Management Group	Enabled	1

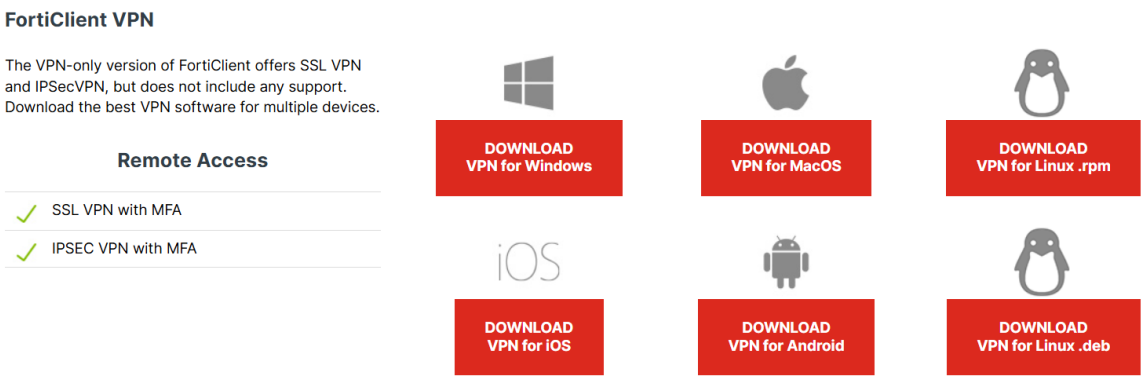
MOTS DE PASSE : **** (cf: Corporate Governance).

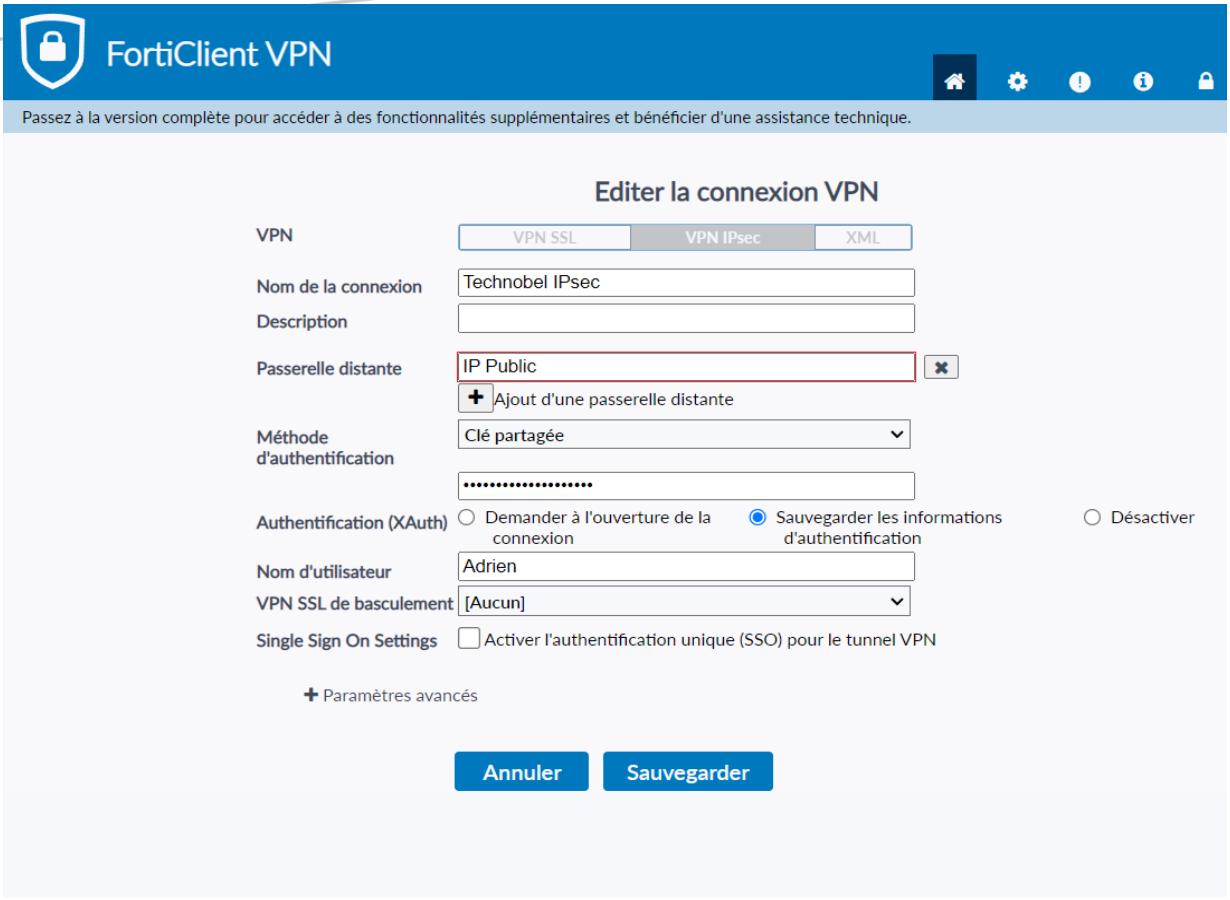
1.2) CONNECTION TO VPN

Procédure connexion VPN Management

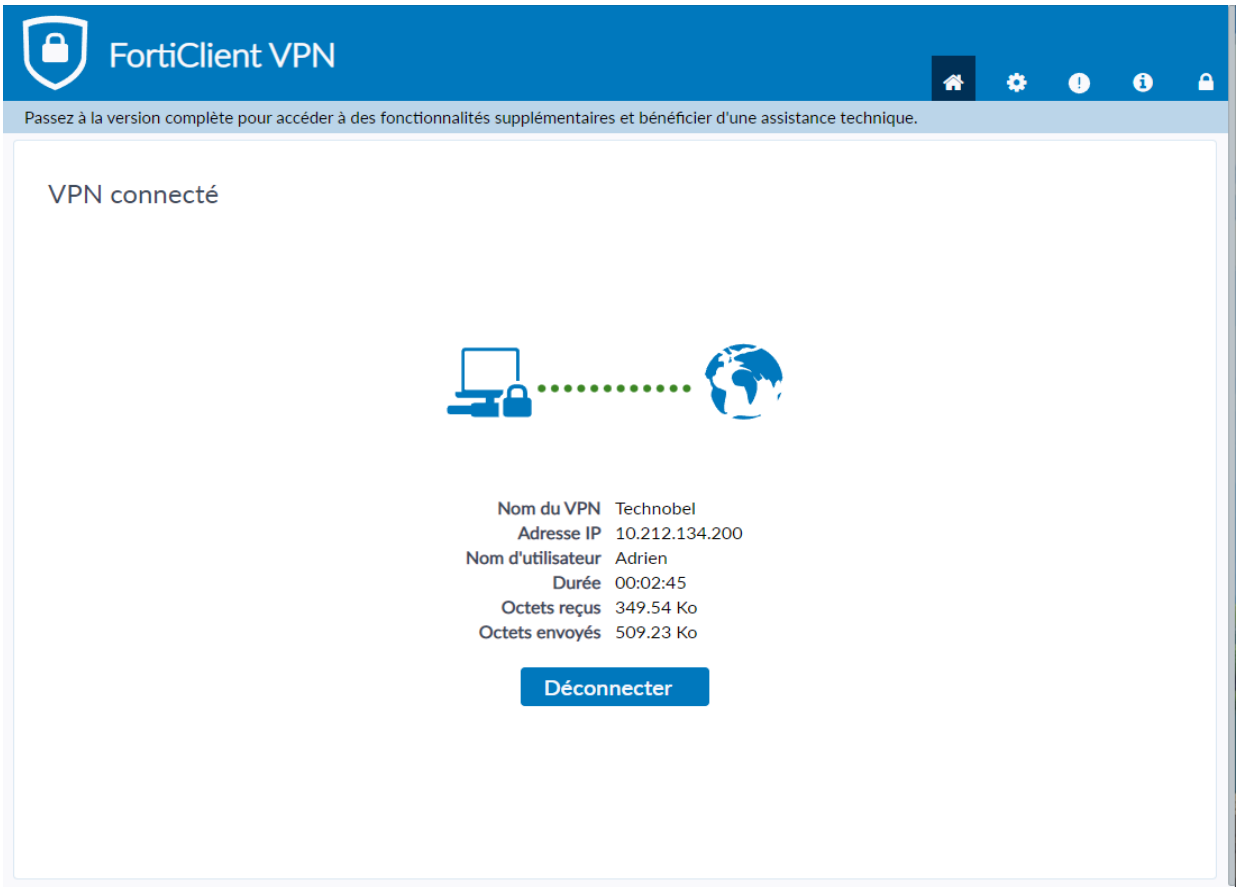
1. https://www.fortinet.com/fr/support/product-downloads (Lien pour télécharger FortiClient)

Installé la version : FortiClient VPN





Connexion établie.



1.3) CREATE USER

1) Create New
2) “Local User”
3) “Username” **** “Password” ****
4) Ne pas activé le “Two-faction Authentication” sauf en cas de licence active. (NIS2)
5) “Enable” and “User Group” Choisis le groupe où l’associer.

2) ACCESS AD

2.1) USER ACCOUNT

Firstname	Lastname	Username	Password	OU
Dumois	Bruno	B.Dumois	[redacted]	OU=Bourgmestre;OU=Conseil Communal;DC=ADRCommune;DC=lab
Clara	Morel	C.Morel	[redacted]	OU=Echevins_Service_Citoyen;OU=Conseil Communal;DC=ADRCommune;DC=lab
Nathan	Villiers	N.Villiers	[redacted]	OU=Echevins_Service_Citoyen;OU=Conseil Communal;DC=ADRCommune;DC=lab
Patrick	Marteau	P.Marteau	[redacted]	OU=Departement IT;DC=ADRCommune;DC=lab
Élodie	Garnier	É.Garnier	[redacted]	OU=Comptabilité;DC=ADRCommune;DC=lab
Sophie	Delacroix	S.Delacroix	[redacted]	OU=Comptabilité;DC=ADRCommune;DC=lab
Antoine	Roussel	A.Roussel	[redacted]	OU=Ouvriers;DC=ADRCommune;DC=lab
Lucal	Verneuil	L.Verneuil	[redacted]	OU=Ouvriers;DC=ADRCommune;DC=lab
Victor	Chabé	V.Chabé	[redacted]	OU=Ouvriers;DC=ADRCommune;DC=lab
Manon	Dupuis	M.Dupuis	[redacted]	OU=Administration Générale;DC=ADRCommune;DC=lab
Camille	Laurent	C.Laurent	[redacted]	OU=Administration Générale;DC=ADRCommune;DC=lab

2.2) CONNECTION TO AD

1) Accéder à l’interface graphique du serveur ESXI depuis le WEB. (10.0.8.254)

2) Accéder à la VM (DC1/DC2).

2.3) CREATE USER

User ➔ New User ➔ Create a new user.

3) ACCESS LAN | EDGE | Data Center

3.1) ACCESS LAN

1) Lancé “Putty” ou autres services SSH.

2) Entré l’adresse ip servant à accéder à votre appareil.

S1-SW1 : 10.0.70.1

S1-MLS1 : 10.0.70.3

S1-FW1 : Accéder à l’interface graphique. (http://10.0.6.2)

3) Si besoin d’accès physique se connecter en console.

3.2) ACCESS EDGE

1) Accès direct via un câble série depuis le PC de Patrick (IT) si présent sur place.

2) Se rendre sur le réseaux interne via le VPN, si vous n’êtes pas présent a même le site.

3) Utilisé RDP depuis votre PC pour gérer le PC de Patrick (IT) et y avoir accès depuis un service SSH.

3.3) ACCESS Data Center

1) Accéder à l'interface graphique du serveur ESXI depuis le WEB. (10.0.8.254)

3.4) ACCESS Server WEB

1) Ouvrez une page WEB et introduisez "http://rcommune.lux.pz/"

4) IP addressing plan

4.1) LAN

IP						
Device	**MAC Adress**	**Interface**	**Interface de sortie**	**IP**	**Mask**	**Gateway**
HP LAN		INFRA PLAYZONE		10.0.0.70	/24	10.0.0.1
S1-SW1		vlan70		10.0.70.1	/24	10.0.70.3
S1-SW2		vlan70		10.0.70.2	/24	10.0.70.3
S1-MLS1		vlan70		10.0.70.3	/24	10.0.2.1
		vlan100		10.0.0.1	/24	
		vlan 150		10.0.150.3	/24	
		g0/1		10.0.2.2	/24	
		g0/4		10.0.3.2	/24	
S1-MLS2		vlan70		10.0.70.4	/24	10.0.5.1
		g0/1		10.0.5.2	/24	
		g0/4		10.0.4.2	/24	
		vlan100		10.0.0.2	/24	
		vlan150		10.0.150.4	/24	
S1-FW1		Interface1		10.0.2.1	/24	
		Interface2		10.0.4.1	/24	
		DMZ		10.0.8.1	/24	
S1-FW2		Interface1		10.0.3.1	/24	
		Interface2		10.0.5.1	/24	
		DMZ		10.0.13.1	/24	
		Wan1		10.0.7.2	/24	
S2-SW1		vlan69		10.0.70.5	/24	10.0.20.1
S2-MLS1		vlan69		10.0.70.6	/24	10.0.22.1
		vlan20		10.0.20.1	/24	
		vlan150		10.0.150.6	/24	
		g0/3		10.0.23.2	/24	
		g0/4		10.0.22.2	/24	

4.2) EDGE

IP						
Device	**MAC Adress**	**Interface**	**Interface de sortie**	**IP**	**Mask**	**Gateway**
S1 - R1		G0/0	WAN1 / FW1	10.0.6.1	24	10.0.6.1
S1 - R2		G0/0	WAN1 / FW2	10.0.7.1	24	10.0.7.1
S1 - R1		G0/1	WAN1	172.20.224.100	24	172.20.224.1
S1 - R2		G0/1	WAN 2	172.20.192.100	24	172.20.192.1
FW1		WAN1	G0/0	10.0.6.2	24	10.0.6.1
FW2		WAN1	G0/0	10.0.7.2	24	10.0.7.1
S1 - R1		G0/0	Wan Public	IP PUBLIC	32	FAI
S1 - R2		G0/0	Wan Public	IP PUBLIC	32	FAI
S1 - R1		G0/2	Wan Public	10.0.25.1	24	10.0.25.1
S1 - R2		G0/2	Wan Public	10.0.25.1	24	10.0.25.1

4.3) Data Center

Adressage IP DC					
Device	**MAC Adress**	**Interface**	**IP**	**Mask**	**Gateway**
DC1		VswitchPfsense	10.0.8.0 (Wan);10.0.11.0 (Web) ; 10.0.1.0 (AD)	/24	
		VswitchDB	10.0.60.0 (DB - WEB) ; 10.0.61.0 (DB - DB)	/24	
DC2		VswitchAD	10.0.1.0	/24	
DC3		VswitchAD	10.0.1.0	/24	

	VM	IP	Gateway	Vswitch	VMkernel	VLAN	
DC1		10.0.1.20	10.0.1.1	vswitchpfsense			
DC2		10.0.1.21	10.0.1.1	vswitchpfsense			
MS1		10.0.1.11	10.0.1.1	vswitchpfsense			
MS2		10.0.1.10	10.0.1.1	vswitchpfsense			
Web (web)		10.0.11.10	10.0.11.1	vswitchpfsense			
Web (db)		10.0.60.1	10.0.60.253	vswitchDB			
DNS		10.0.11.11	10.0.11.1	vswitchpfsense			
Data Base		10.0.61.10	10.0.61.1	vswitchDB			
PFSense				vswitchpfsense			
Data Base Tmp		10.0.11.50	10.0.11.1	vswitchpfsense			
remote-web		10.0.11.100	10.0.11.1	vswitchpfsense			
remote-ad		10.0.1.100	10.0.1.1	vswitchpfsense			
PfSense-DB (WAN --> DB-WEB)		10.0.60.253	10.0.60.1	vswitchDB			
PfSense-DB (LAN --> DB-DB)		10.0.61.1		vswitchDB			
Reverse Proxy		10.0.11.12	10.0.11.1	vswitchpfsense			

5) Corporate governance

5.1) UPDATE

5.1.1) UPDATE AD

Bonnes pratiques pour les mises à jour des Active Directory (AD) :

Les Active Directory étant cruciaux pour la gestion des accès :

1. **Maintenir les serveurs AD à jour** en appliquant tous les correctifs de sécurité publiés par Microsoft dans un délai de **14 jours** après leur sortie.
2. Avant toute mise à jour, effectuer une **sauvegarde complète** de l'AD pour garantir une récupération rapide en cas de problème.
3. Tester les mises à jour AD dans un environnement de test pour détecter d'éventuels conflits ou erreurs.
4. Assurer la mise à jour des **contrôleurs de domaine (DC)** en priorité, tout en planifiant les redémarrages pour limiter les interruptions.
5. Vérifier que les configurations critiques (politiques de groupe, DNS, etc.) restent intactes après chaque mise à jour.
6. Former régulièrement les administrateurs AD aux dernières recommandations de Microsoft et NIS2 concernant la sécurité et les mises à jour.

5.1.2) UPDATE Windows System

Bonnes pratiques pour les mises à jour des machines Windows :

Pour garantir la sécurité et la conformité aux normes NIS2 :

1. **Activer les mises à jour automatiques** sur toutes les machines Windows pour recevoir les correctifs dès leur publication.
2. Effectuer une **vérification manuelle mensuelle** pour s'assurer qu'aucune mise à jour critique n'a été manquée.
3. Installer rapidement les **mises à jour de sécurité prioritaires**, surtout celles classées comme critiques par Microsoft.
4. Planifier les mises à jour hors des heures de travail pour limiter l'impact sur les utilisateurs, tout en respectant un délai maximum de **30 jours** pour appliquer les correctifs.
5. Tester les mises à jour sur un environnement de préproduction avant de les déployer à grande échelle, surtout pour les systèmes critiques.
6. Vérifier que les pilotes et logiciels tiers installés sur les machines restent compatibles avec les nouvelles mises à jour pendant la phase de test.

5.2) PASSWORD

Bonnes pratiques pour les mots de passe des comptes utilisateurs :

Pour garantir la sécurité, chaque utilisateur doit :

1. Créer un mot de passe unique d'au moins **12 caractères** comprenant lettres, chiffres et caractères spéciaux. (GPO)
2. Éviter d'utiliser des informations personnelles (nom, date de naissance, etc.) dans les mots de passe. (GPO)
3. Ne jamais partager son mot de passe, même avec des collègues.
4. Changer son mot de passe régulièrement (au moins tous les **6 mois**) ou immédiatement en cas de suspicion de compromission. (GPO)
5. Activer l'**authentification à deux facteurs (2FA)** sur les plateformes qui le permettent.

Bonnes pratiques pour les mots de passe des comptes administrateurs :

Les comptes administrateurs, étant plus sensibles, nécessitent une sécurité renforcée :

1. Utiliser des mots de passe d'au moins **16 caractères**, générés aléatoirement.
2. Activer obligatoirement l'**authentification multifactorielle (MFA)**.
3. Ne jamais utiliser les mêmes mots de passe pour plusieurs systèmes ou plateformes.
4. Limiter l'accès aux comptes admin uniquement aux tâches nécessaires (pas d'usage quotidien).
5. Conserver les mots de passe dans un **gestionnaire sécurisé** et jamais sur papier ou dans des fichiers non protégés.
6. Changer les mots de passe administrateurs immédiatement après chaque intervention critique ou en cas de départ d'un membre de l'équipe ayant eu des accès.

5.3) DOC

Bonnes pratiques pour la documentation des changements en conformité avec NIS2 :

Une documentation rigoureuse est essentielle pour assurer la traçabilité et la conformité aux normes NIS2. Voici les étapes clés à suivre :

1. **Créer une fiche de suivi pour chaque changement :**
    a. Décrire le changement (mise à jour, modification, intervention).
    b. Inclure la date, l'heure et l'auteur du changement.
    c. Indiquer le système ou composant impacté (ex. : machine, Active Directory).
2. **Justifier les décisions :**
    a. Documenter pourquoi le changement est nécessaire (par ex. : correction de vulnérabilités ou amélioration de la sécurité).
    b. Ajouter des références, comme les bulletins de sécurité Microsoft ou des recommandations officielles.
3. **Conserver les validations et approbations :**
    a. Enregistrer les validations des responsables ou des équipes concernées avant la mise en œuvre.
    b. Documenter les tests effectués en préproduction.
4. **Tenir à jour un journal des incidents liés aux changements :**
    a. Noter les problèmes ou pannes survenus après une mise à jour, et les actions correctives prises.
5. **Centraliser la documentation :**
    a. Stocker les informations dans un espace sécurisé et partagé (par ex. : SharePoint ou un outil de gestion de documentation).
    b. Utiliser une structure claire et normalisée pour faciliter l'accès et les audits.
6. **Effectuer des revues régulières :**
    a. Planifier des revues trimestrielles pour valider que la documentation est complète et à jour.
7. **Former les équipes :**
    a. Sensibiliser tout le personnel IT à l'importance de documenter les actions, même mineures.
    b. Mettre en place des modèles standard pour simplifier la rédaction (ex. : fiches de modification ou rapports post-intervention).

RSECURE

Time Sheet

Équipe Cybersécurité Technobel

technobel

Time Sheet

Dates	Tâches	Nom des personnes travaillant	Nbr de personnes	Nbr d'heures de travail totales	Nbr d'heures de travail effectives	Heures facturées	Taux horaire	Total effectif	Facturation	Facturation effective
14/11/2024	HLD	Edy, Adrien, Marc, Yann	4	8	7	0	37,5	1050	Non	0
	NIS2	Jean, Amélio, Jonathan, Aurélien	4	4	4	0	37,5	600	Non	0
	Questions	Julien, Hasan, Maxime	3	3	3	0	37,5	337,5	Non	0
15/11/2024	Capsule HLD	Tous ;expert: Jean Thomas	11	2	2	0	37,5	825	Non	0
	HLD/LLD	Tous	10	6	6	0	37,5	2250	Non	0
18/11/2024	Définition module + LLD	Tous	9	3	3	0	37,5	1012,5	Non	0
	LAN	Amélio, Aurélien, Hasan	3	4	4	0	37,5	450	Non	0
	EDGE	Marc, Adrien, Edy	3	4	4	0	37,5	450	Non	0
	DC	Julien, Jonathan, Jean	3	4	4	0	37,5	450	Non	0
19/11/2024	LAN	Amélio, Aurélien, Hasan, Maxime	4	8	7	0	37,5	1050	Non	0
	EDGE	Marc, Adrien, Edy	3	4	3	0	37,5	337,5	Non	0
	DC	Julien, Jonathan, Jean, Yann	4	8	7	0	37,5	1050	Non	0
	Implémentation physique	Marc, Adrien, Edy	3	3	3	3	37,5	337,5	Oui	337,5
20/11/2024	Configuration des appareils	Maxime	1	8	7	7	37,5	262,5	Oui	262,5
	Documentation config des appareils	Amélio, Aurélien, Hasan	4	8	7	3	37,5	1050	Oui	450
	Recherche et implémentation infra EDGE	Marc, Adrien, Edy	3	8	7	0,5	37,5	787,5	Oui	56,25
	Installation Serveur Web, DNS, DC, MS	Julien, Jonathan, Jean, Yann	4	8	7	3,5	37,5	1050	Oui	525
21/11/2024	Mise en place infra	Amélio	1	5	5	5	37,5	187,5	Oui	187,5
	Doc STP/MSTP	Amélio	1	3	3	2	37,5	112,5	Oui	75
	Doc SOC/NOC/vlan monitoring	Hasan	1	8	7	0	37,5	262,5	Non	0
	Config LAN (Switch/MLS)	Maxime	1	8	7	7	37,5	262,5	Oui	262,5
	LLD / Doc port security	Aurélien	1	8	7	3	37,5	262,5	Oui	112,5
	Recherche et implémentation infra EDGE	Marc, Adrien, Edy	3	8	7	0	37,5	787,5	Non	0
	Correction infra ESXi Vswitch/Pfsense/Vlan + connexion fortigate et doc	Julien, Jean	2	8	7	0	37,5	525	Non	0
	Documentation GPO	Yann	1	8	7	3	37,5	262,5	Oui	112,5
	Gestion et suvi doc + préparation réunion client	Jonathan	1	8	7	3	37,5	262,5	Oui	112,5
25/11/2024	Envois PV + VPN client server/ site à site + Test hors infra	Adrien, Jonathan	2	8	7	0	37,5	525	Non	0
	AD	Yann	1	8	7	0	37,5	262,5	Non	0
	Implémentation et recherche LVM + Server web	Julien, Jean	2	8	8	1,5	37,5	600	Oui	112,5
	Doc splunk + gestion d'équipe	Amélio	1	3	2	0	37,5	75	Non	0
	Installation ESXi + configuration Rocky	Amélio, Edy	2	3	3	3	37,5	225	Oui	225
	Doc, config ip réseau data center dans acl PAT + routes routeur et S1-FW1 + aide	Marc	1	8	7	0,5	37,5	262,5	Oui	18,75
	Recherche analyse de risque	Maxime	1	8	7	0	37,5	262,5	Non	0
	Recherche VRRP	Hasan	1	8	7	0	37,5	262,5	Non	0
	Doc NFS + doc securité couche 2	Aurélien	1	8	7	3	37,5	262,5	Oui	112,5
26/11/2024	VPN client server/ site à site + Test hors infra	Adrien, Jonathan	2	8	7	0	37,5	525	Non	0
	config rocky + accès internet SOC + Documentation, Installation et configuration Splunk	Amélio	1	8	7	1,5	37,5	262,5	Oui	56,25
	Documentation Securité Couche 2 + Vérification config LAN + implémentation des routes	Aurélien	1	8	7	2	37,5	262,5	Oui	75
	Recherche analyse de risque et rédaction doc	Maxime	1	8	7	0	37,5	262,5	Non	0
	Documentation AD	Yann	1	8	7	3	37,5	262,5	Oui	112,5
	Documentation VRRP / IPS - IDS	Hasan	1	7	7	0	37,5	262,5	Non	0
	La lecture doc MariaDB + aide	Marc	1	8	7	0	37,5	262,5	Non	0
	Implémentation et recherche LVM + Server web + DB	Julien, Jean	2	10	10	3	37,5	750	Oui	225
27/11/2024	VPN client server/ site à site + Test dans l'infra	Adrien, Jonathan	2	8	7	0	37,5	525	Non	0
	Doc + Installation MariaDB	Marc	1	8	7	3,5	37,5	262,5	Oui	131,25
	Doc et sécurité chouche 2	Aurélien	1	8	7	3	37,5	262,5	Oui	112,5
	Implémentation et recherche LVM + Server web + DB	Julien, Jean	1	8	8	4	37,5	300	Oui	150
	Doc forwarders splunk + doc splunk + création VM test pour analyse de log	Amélio	1	8	5,5	2	37,5	206,25	Oui	75
	Doc VRRP / IPS - IDS	Hasan	1	8	7	3	37,5	262,5	Oui	112,5
	DOC AD	Yann	1	8	7	3	37,5	262,5	Oui	112,5
	Analyse de risques	Maxime	1	8	7	3	37,5	262,5	Oui	112,5
	Doc zabbix + création dashboard	Edy	1	8	7	3	37,5	262,5	Oui	112,5
28/11/2024	Lire la doc + La gestion Maria DB	Marc	1	8	7	0	37,5	262,5	Non	0
	Implémentation VPN S1-SOC	Adrien, Jonathan	2	8	7	3	37,5	525	Oui	225
	Prépartation raport client + Analyse de Risques + Doc vrrp	Maxime / Hasan	2	8	7	3	37,5	525	Oui	225
	Implémentation et recherche LVM + Server Web + DB	Julien, Jean	2	8	7	4	37,5	525	Oui	300
	Doc AD	Aurélien + Yann	2	8	7	3	37,5	525	Oui	225
	Doc splunk + gestion d'équipe	Amélio	1	8	7	3	37,5	262,5	Oui	112,5
29/11/2024	Préparation réunion client + débrief	Tous	11	5	5	0	37,5	2062,5	Non	0
	Doc VPN site à site	Adrien, Jonathan	2	2	2	1	37,5	150	Oui	75
	Implémentation module web	Julien, Jean	2	3	3	3	37,5	225	Oui	225
	DB + création utilisateur	Marc	1	2	2	2	37,5	75	Oui	75
	Analyse de risques SWOT	Maxime	1	2	2	2	37,5	75	Oui	75
	Gestion d'équipe	Amélio	1	3	3	0	37,5	112,5	Non	0
	Documentation	Hasan	1	2	2	0	37,5	75	Non	0
	Documentation GPO	Yann	1	2	2	2	37,5	75	Oui	75
02/12/2024	Doc VPN S2S et Client/server + documentation globale	Adrien, Jonathan	2	8	7	2	37,5	525	Oui	150
	Implémentation module web	Julien, Jean	2	8	7	5	37,5	525	Oui	375
	Recherche fortigate/bastion + inspection des routes implémentées	Aurélien	1	8	7	0	37,5	262,5	Non	0
	Modification du code PHP pour comm avec DB	Marc	1	8	7	3	37,5	262,5	Oui	112,5
	Création user AD	Yann	1	8	7	3	37,5	262,5	Oui	112,5
	configuration Zabbix	Edy	1	8	7	5	37,5	262,5	Oui	187,5

	intervention fortigate pour comm soc-infra	Amélio	1	8	7	4	37,5	262,5	Oui	150
	Documentation	Hasan	1	8	7	2	37,5	262,5	Oui	75
03/12/2024	Aide connectivité Lan + recherche PHP	Marc	1	8	7	2	37,5	262,5	Oui	75
	VPN Ipsec + SSL + Aide LAN	Adrien, Jonathan	2	8	7	3	37,5	525	Oui	225
	Configuration zabbix + SNMP + agent	Edy	1	8	7	4	37,5	262,5	Oui	150
	Configuration SPLUNK + vérif infra EDGE et LAN	Amélio	1	8	7	4	37,5	262,5	Oui	150
	Analyse des risques SWOT	Maxime	1	8	7	7	37,5	262,5	Oui	262,5
	Implémentation AD	Yann	1	8	7	4	37,5	262,5	Oui	150
	Documentation	Hasan	1	8	7	2	37,5	262,5	Oui	75
	Implémentation web	Julien, Jean	2	8	7	4	37,5	525	Oui	300
	Recherche fortigate + inspection LAN	Aurélien	1	8	7		37,5	262,5	Oui	0
04/12/2024	VRRP	Hasan	1	8	7	2	37,5	262,5	Oui	75
	Zabbix	Edy	1	8	7	4	37,5	262,5	Oui	150
	Installation VPN	Adrien	1	8	7	4	37,5	262,5	Oui	150
	Config et vérif LAN	Marc, Jonathan	2	8	7	5	37,5	525	Oui	375
	Analyse de risques SWOT	Maxime	1	8	7	6	37,5	262,5	Oui	225
	Recherche fortigate + installation forwarder splunk sur l'AD	Amélio	1	8	7	4	37,5	262,5	Oui	150
	Implémentation AD	Yann	1	8	7	4	37,5	262,5	Oui	150
	Recherche et implémentation règles fortigate	Aurélien	1	8	7	6	37,5	262,5	Oui	225
	Implémentation web + DB	Jean, Julien	2	8	7	6	37,5	525	Oui	450
05/12/2024	Préparation réunion client + vérif doc	Julien, Jonathan	2	8	7	4	37,5	525	Oui	300
	VPN IPSEC	Adrien	1	8	7	5	37,5	262,5	Oui	187,5
	Config agent sur zabbix et splunk	Amélio, Edy	2	8	7	5	37,5	525	Oui	375
	Vérif data base	Marc	1	8	7	4	37,5	262,5	Oui	150
	Implémentation AD	Yann	1	8	7	6	37,5	262,5	Oui	225
	Envois de doc + préparation doc pentest/audit	Maxime	1	8	7	4	37,5	262,5	Oui	150
	Documentation DHCP	Hasan	1	8	7	2	37,5	262,5	Oui	75
	Implémentation règles fortigate	Aurélien	1	8	7	5	37,5	262,5	Oui	187,5
	Doc web	Jean	1	8	7	4	37,5	262,5	Oui	150
06/12/2024	Préparation réunion client + répétition + Débrief	Tous	11	8	7	2	37,5	2887,5	Oui	825
	Mise en place et préparation dernière semaine	Tous	11	8	7	2	37,5	2887,5	Oui	825
	Rédaction doc finale	Adrien, Jonathan	2	8	7	7	37,5	525	Oui	525
09/12/2024	Pentest/audit	Amélio, Julien	2	8	7	7	37,5	525	Oui	525
	Préparation powerpoint présentation	Edy, Hasan, Yann	3	8	7	7	37,5	787,5	Oui	787,5
	Préparation peech	Marc	1	8	7	7	37,5	262,5	Oui	262,5
	Rédaction doc finale	Adrien, Jonathan	2	8	7	7	37,5	525	Oui	525
10/12/2024	Pentest/audit	Amélio, Julien, Aurélien	3	8	7	7	37,5	787,5	Oui	787,5
	Préparation powerpoint présentation	Edy, Hasan, Yann	3	8	7	7	37,5	787,5	Oui	787,5
	Préparation peech	Marc	1	8	7	7	37,5	262,5	Oui	262,5
	Rédaction doc finale	Adrien, Jonathan	2	8	7	7	37,5	525	Oui	525
11/12/2024	Pentest/audit	Amélio, Julien, Aurélien	3	8	7	7	37,5	787,5	Oui	787,5
	Préparation powerpoint présentation	Edy, Hasan, Yann	3	8	7	7	37,5	787,5	Oui	787,5
	Préparation peech	Marc	1	8	7	7	37,5	262,5	Oui	262,5

Total Heures effectives	Total effectif
724,5	53831,25
Total Heures facturées	Total Facturé
330	20737,5

Avancement Des Tâches

Tâche	Avancement
EDGE	
Planner	
ACL Bogons	
PAT	
VPN site a site (1 à 2)	
VPN client / sever télé	
VPN client / sever agents	
VPN site a site NOC/SOC	
Data Center	
Active Directory	
Pfsense	
WAF	
Reverse Proxy	
DNS	
WEB	
Data Base	
NFS	
ESXI	
LAN	
Port security / DAI	
cluster FW	
plan des routes	
DHCP Relay	
IPS/IDS	
SOC / NOC	
Zabbix	
Splunk	
VPN (edge)	
FW	
SOC - R1	
CLIENT	
PV	
Délivrable	
Time Sheet	
Présentation final + répet	
Analyse de risque	
Visuel	

Légende
Pas réalisée
Réalisé
En cours
Annulé (POC)

Active directory		General	
DC 1		Audit	
DC 2		Pentest	
MS 1		Verif	
MS 2		Validation	
DHCP		DOCS	
SMB		NIS2	
DFS			
DFSR			
GPO			
DNS			

ANALYSE DE RISQUE SWOT

ÉQUIPE DE CYBERSÉCURITÉ SECOPS PLAYZONE 2024

TABLE DES MATIÈRE

AVANT – PROPOS

Ce document se concentre sur l'analyse swot imposé dans le cahier des charges et appliquée au projet. Cet outil est fondamental pour évaluer de manière exhaustive les facteurs internes et externes susceptibles d'influencer le succès du projet. Contrairement à d'autres approches purement techniques ou normatives, l'analyse swot offre une vue d'ensemble stratégique et pragmatique.

L'analyse permet de mettre en lumière les forces et opportunités qui serviront de leviers pour le projet tout en identifiant les faiblesses et menaces qui nécessitent des plans d'atténuation. Cette méthode facilite une planification proactive et adaptable, essentielle dans un contexte de projets innovants où les contraintes de temps, de ressources, et de conformité (notamment à la directive NIS2) jouent un rôle prépondérant.

AVANT – PROPOS

Cette approche flexible s'intègre parfaitement aux méthodologies modernes telles que scrum, en offrant une base solide pour la prise de décision et la priorisation des tâches. En tant que guide pour les parties prenantes, cette analyse swot vise à garantir que le projet repose sur des fondations solides tout en anticipant les défis éventuels, afin de maximiser les chances de succès et de conformité dans un environnement en constante évolution.

Ce document s'adresse à toutes les parties prenantes impliquées dans le projet, afin de les accompagner dans la compréhension des enjeux stratégiques et techniques de ce (POC) pour la play-zone 2024.

INTRODUCTION AU PROJET

Étude de cas :

Développer un Proof of Concept (POC) d'une infrastructure réseau sécurisée et modulaire pour le service des eaux d'une administration communale, composée de 10 personnes.

Le projet sera réalisé durant la play-zone sur 24 jours, en mettant l'accent sur la défense en profondeur, le security by design, le moindre privilège, le zero trust et la conformité à la directive NIS 2.

INTRODUCTION AU PROJET

Mise en conformité avec la directive NIS2 : Renforcement de la sécurité des systèmes d'information pour l'administration communale des eaux.

Mise à jour hardware et infrastructure it :

- Installation et configuration d'un nouveau serveur interne sur site.
- Ajout de 2 nouveaux postes de travail en plus des 8 existants.

Mise en place d'un système de gestion de documents :

- Gestion sécurisée des documents avec des canaux sécurisés pour la communication interne.

Partage de fichiers sécurisé (in/out externe) :

- Mise en place d'un système de partage de fichiers avec d'autres administrations et acteurs du secteur de la gestion des eaux (y compris les auditeurs externes, écoles, etc.).

Support du télétravail :

- Télétravail autorisé uniquement depuis la Belgique avec accès sécurisé aux ressources internes.

Budget alloué : 30 000 €, incluant la gestion de projet et le suivi.

OBJECTIF DU PROJET

Objectif : Développer un Proof of Concept (POC) d'une infrastructure réseau sécurisée et modulaire pour le service des eaux d'une administration communale (15 personnes). Le projet met l'accent sur :

- Security by design
- Moindre privilège
- Zero trust
- Conformité NIS 2

Cadre de gestion : Utilisation du framework scrum avec les rôles suivants :

- Product Owner : Définition des besoins.
- Scrum Master : Facilitation du processus scrum.
- Consultant en Cyber Sécurité : Implémentation des meilleures pratiques de sécurité.

Composants Clés

- Infrastructure réseau
    - Architecture modulaire documentée (hld/lld).
    - Redondance via deux accès wan distincts.
- Cluster de Firewalls FortiGate

OBJECTIF DU PROJET

- Modèle FortiGate-60F en haute disponibilité (ha) déjà acquis.
- Basculement automatique entre wan.

• Architecture Active Directory
- Gestion des utilisateurs par rôles (responsables, it ouvriers, etc.).
- Hébergement d'un modèle de Tiers (0, 1, 2).
- Partage smb sécurisé (dfs/dfsr).

• Services Déployés
- Web Server Intranet accessible via vpn, utilisé pour le relevé des index.
- Partage de fichiers interne (nfs) avec auto montage.
- Télétravail limité à la Belgique via vpn sécurisé.

• Sécurité et Monitoring
- Surveillance de l'infrastructure.

• Documentation et Audits
- Schéma des flux de données internes et externes.
- Audit fonctionnel et tests de pénétration.

• Conformité NIS 2
- Gestion des risques et continuité des opérations.
- Documentation de la réponse aux incidents.

OBJECTIF DU PROJET

Livrables

- Documentation technique (lld/hld).
- Rapports d'audit et de tests de pénétration.
- Guide de maintenance pour l'équipe it.
- Timesheet des tâches effectuées.

Budget Alloué : 30 000 €

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Forces (Strengths) :

• Compétence interne : les compétences actuelle de l'équipe permette la mise en place des concepts moderne de cyber sécurité (défense en profondeur, zero trust et security by design).
• Investissement financier : Budget dédié de 30 000 €, l'infrastructure et la gestion de projet.
• Meilleurs productivité et performance : Grace à la mise en place de nouveaux serveurs et postes de travail.
• Partage sécurisé et meilleurs collaboration : Mise en place de systèmes sécurisés pour la gestion et le partage des fichiers, avec les parties externes(Protocoles smb et nfs pour une gestion efficace des données).
• L'équipement de qualité : Le choix des équipements Cisco (switch, mls routeur) et Fortinet (firewall, vpn) garantit une solution robuste et performante avec une capacité de gestion avancée des réseaux et de la sécurité.
• Délégation du soc-noc : permettant de bénéficier d'une expertise spécialisée, d'une surveillance 24/7, et d'une optimisation des coûts tout en réduisant la charge de travail interne et en concentrant les ressources sur les activités stratégiques.

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Forces (Strengths) suite:

• Gestion de projet efficace : Utilisation de la méthodologie agile scrum.
• Continuité d'activité assuré : Utilisation de FortiGate-60F en haute disponibilité (ha), offrant une redondance et un basculement automatique pour la sécurité réseau.
• Surveillance continue de l'infrastructure : service de monitoring avec Splunk et Zabbix.
• transparence : Remise d'une documentation technique complète suite aux différents test que nous avons réaliser.
• Meilleurs gestion des risques : Documentation sur les risques et réponse aux incidents.
• Télétravail sécurisé pour tout les employé depuis la belgique.
• Bon dimensionnement et optimisation : L'utilisation des serveurs physiques ThinkSystem ST550 de Lenovo, combinée à la virtualisation via ESXi, permet d'optimiser l'utilisation des ressources matérielles tout en assurant une haute disponibilité et une fiabilité accrue tout en réduisant ainsi les coûts et maximisant l'efficacité opérationnelle.
• Gestion des Données : Base de données centralisée : La mise en place de MariaDB dans une architecture sécurisée permet une meilleure gestion de l'information et des données.

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Faiblesses (weaknesses) :

• Équipe en apprentissage : Mise en œuvre plus difficile pour une équipe d'apprenants avec moins d'expérience dans des concepts avancés.
• Temps limité : Le projet doit être finalisé en 24 jours, ce qui pourrait amener à faire des choix pour finir dans le temps imparti.
• Ressources humaines : Une équipe de 11 personnes peut être insuffisante pour mener à bien toutes les tâches.
• Formation du personnel interne : Le niveau de connaissance actuelle des utilisateurs finaux nécessitera potentiellement une formation sur les nouveaux systèmes et bonnes pratiques de cybersécurité.
• Budget restreint :
    • Un budget supplémentaire n'as pas été validé pour répondre aux imprévus et aux adaptations
    • cout des licence et du double accès wan.
• Ressources humaines spécialisées nécessaires : Expertise requise pour gérer les firewalls, l'Active Directory et les audits de sécurité.

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Faiblesses (weaknesses) :

• Résistance au changement : Les employés pourraient être réticents à adopter les nouvelles technologies ou procédures et nouveaux matériels.
• Pannes matérielles : Échec ou défaillance des nouveaux équipements (serveurs, postes de travail).
• Équipement vieillissant : Le matériel (par exemple, les switches Cisco 2960) pourrait devenir obsolète dans quelques années, ce qui pourrait augmenter le risque de pannes matérielles.
• Le vol de données : Dû à des vulnérabilités dans la gestion des accès utilisateurs ou à une mauvaise configuration des services exposés, constitue une menace sérieuse. Une vigilance accrue est essentielle pour prévenir ces risques, notamment par une gestion rigoureuse des configurations et la mise en place de bonnes pratiques de sécurité (AD).

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Opportunités (Opportunities) :

• Renforcement de la sécurité : Réduction significative des risques liés aux cyberattaques et violations de données sensibles.
• Confiance accrue pour le citoyen et partenaire : Amélioration de la perception de la sécurité par les citoyens et partenaires externes.
• Collaboration facilitée avec les autres acteurs : Création d'une infrastructure permettant une collaboration fluide avec d'autres administrations et acteurs du secteur.
• Conformité au NIS2 comme atout : Le respect des normes NIS2 pourrait servir de modèle pour d'autres administrations communale ou public.

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Opportunités (Opportunities) suite :

• Exemple pour d'autres administrations : Le projet pourrait servir de modèle, être améliorer et suivis pour des initiatives similaires.
• La montée en compétence : Les membres de l'équipe vont acquérir une expérience précieuse en gestion de projets it sécurisés et de nouvelles connaissances techniques.
• Facilitation des audits : Documentations précises (flux de données, rapports) rend les futures inspections plus fluides.

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Menaces (Threats) :

• Visibilité du projet : En raison de sa visibilité, le projet pourrait devenir une cible privilégiée pour des acteurs malveillants cherchant à porter atteinte ou à exploiter ses failles.
• Résistance au changement : Les partenaires externes pourraient être réticents à adopter les nouvelles technologies ou procédures et nouveaux matériels.
• Problèmes de conformité des sous traitants : En cas de défaillance du sous-traitant le projet pourrait ne pas satisfaire pleinement les exigences NIS2.
• Coût évolutif de la sous traitance : Les ajustements ou ajouts de services postérieurs à la signature du contrat chez le sous- traitant sélectionner pourraient entraîner une hausse futur des coûts du soc-noc.

ANALYSE SWOT DU PROJET (POC) PLAYZONE 2024

Menaces (Threats) suite :

• Communication entre les différents acteurs : recevoir les information et les documents dans un délais permettant la bonne poursuite du travail.
• Retards potentiels : En cas de mauvaises planifications ou de dépendances externes (livraison des équipements, dépendant des administrateurs système pour certain matériel, etc.)
• Soc/noc externalisé avec un sous traitant : obligation pour le sous traitant d'être conforme au NIS2. Une mauvaise définition ou négociation ainsi que les closes du contrat pourrait entraîner un manque de clarté sur les responsabilités, les SLA (Service Level Agreements), et les pénalités en cas de non-respect des engagements.
• Manque de contrôle direct :

  La délégation réduit la capacité de réagir rapidement en cas d'incident critique et complique la surveillance de l'efficacité des opérations.

  Il est essentiel de s'assurer que le sous-traitant communique les informations pertinentes en temps réel et de manière fiable.

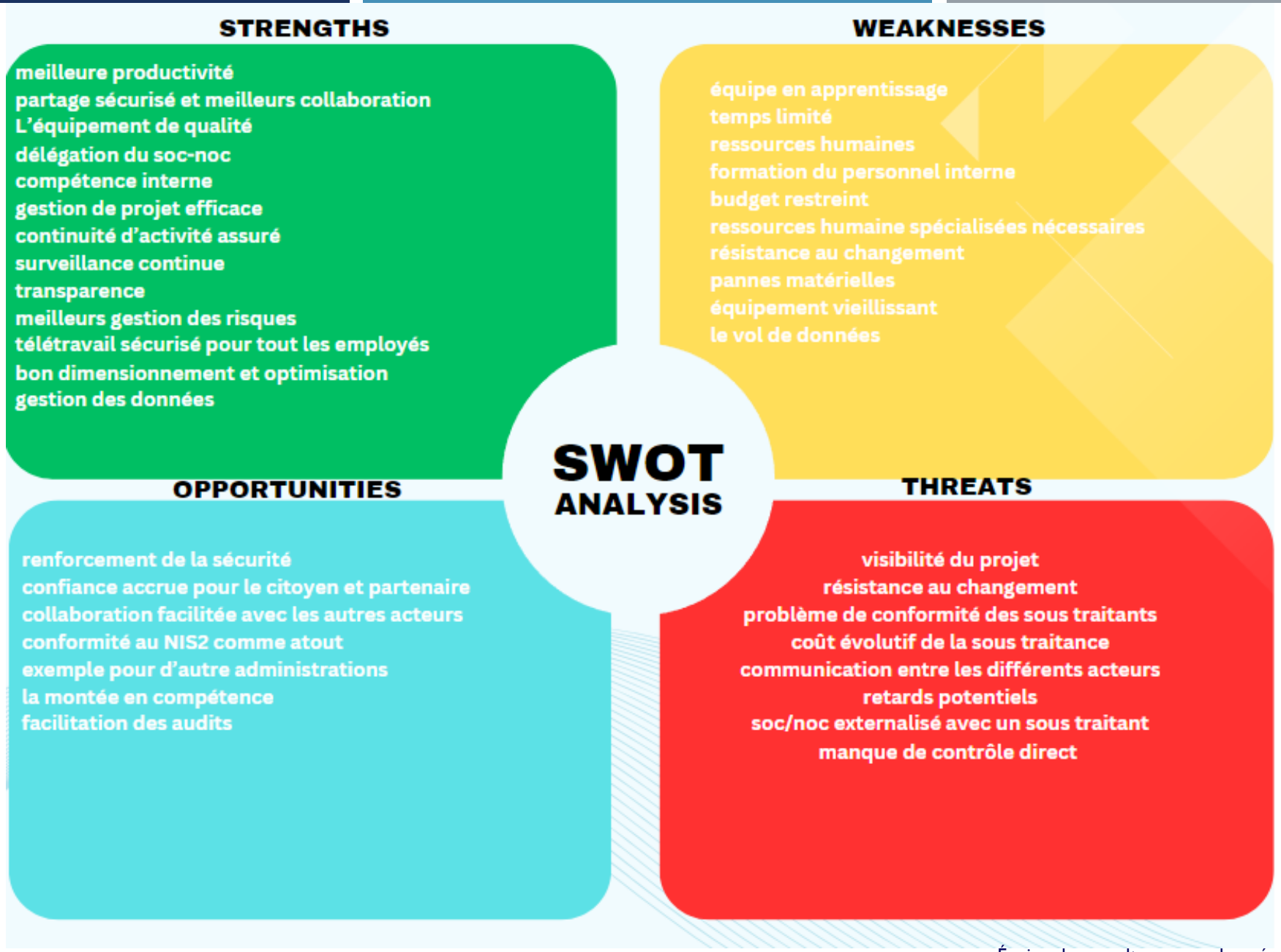
• Risques de ciblage du soc-noc ou d'exploitation des vulnérabilités dans Splunk/Zabbix.

SYNTHÈSE SWOT DU PROJET (POC) PLAYZONE 2024

Complément :

Le projet adopte une approche sécurisée et flexible, conforme aux normes de cybersécurité, garantissant ainsi une grande résilience et respectant les exigences de la directive NIS2. Cependant, il présente des défis liés à sa complexité, à sa dépendance à certaines technologies et à l'évolution rapide des menaces. Il est essentiel de gérer ces aspects avec soin. Le projet doit aussi prendre en compte les risques d'obsolescence et la capacité à évoluer facilement pour rester performant sur le long terme.

TEMPLATE SWOT DU PROJET (POC) PLAYZONE 2024



Analyse Swot Play-zone 2024

Projet (POC) : conception et mise en œuvre d'une infrastructure réseau sécurisé et modulaire pour le service des eaux d'une administration communale.

Participant au projet : amélio, aurélien, julien, jonathan, hassan, yann, jean, adrien, maxime, marc, edy.