

Année 2025

Ensimag

Revue de Projets

PANOPTIS

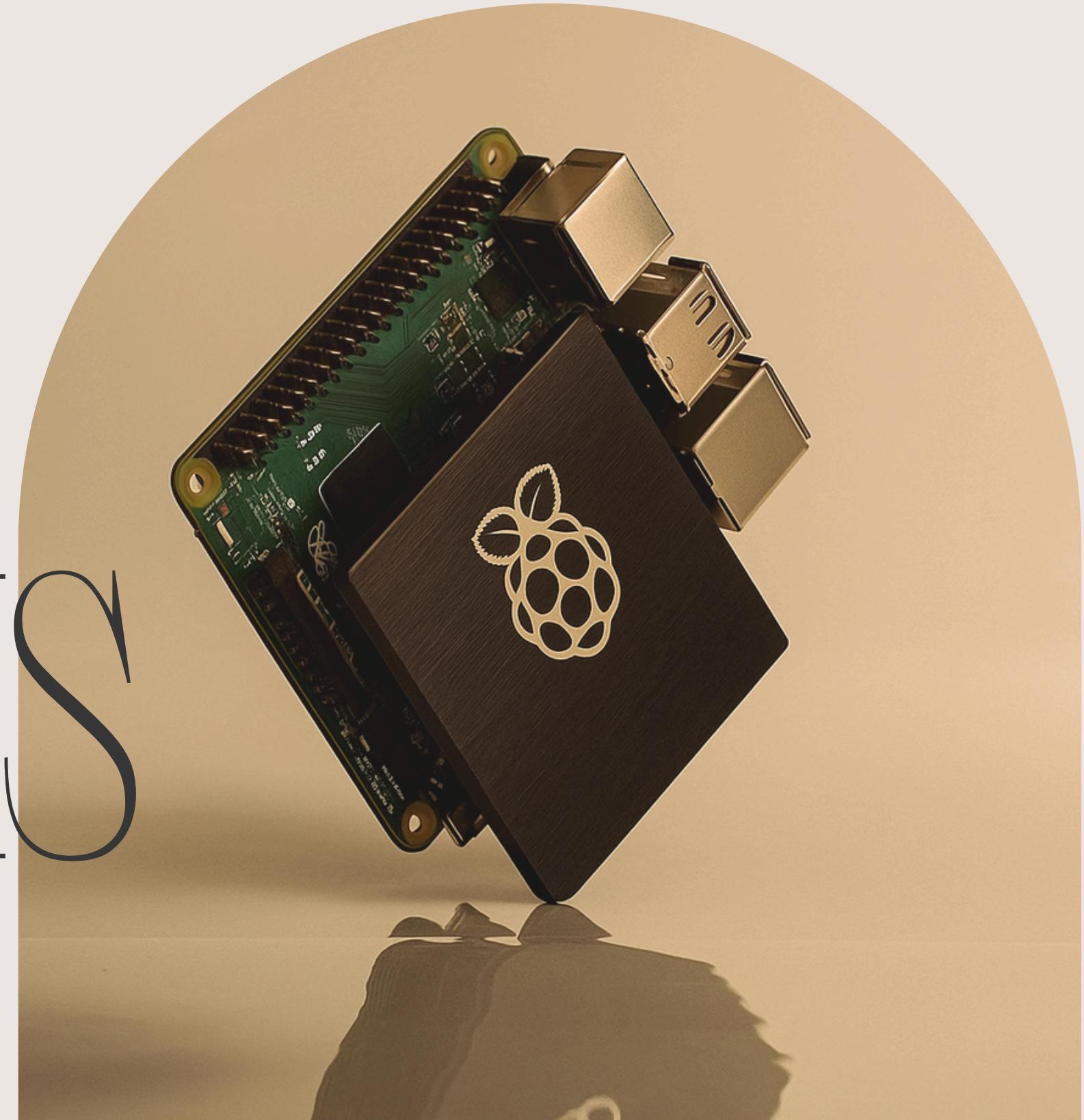
DEVOUASSOUD Matthias

GROSSI Arthur

JAILLETTE Nils

DREVOT Dylan

MARTIN Clement



SOMMAIRE

de la présentation

01

*Retour sur la vie &
l'organisation du projet*

02

Création de l'Infrastructure

05

Questions & Réponses

03

Statut d'avancement technique

04

Démonstration

01

RETOUR SUR LA VIE DU PROJET

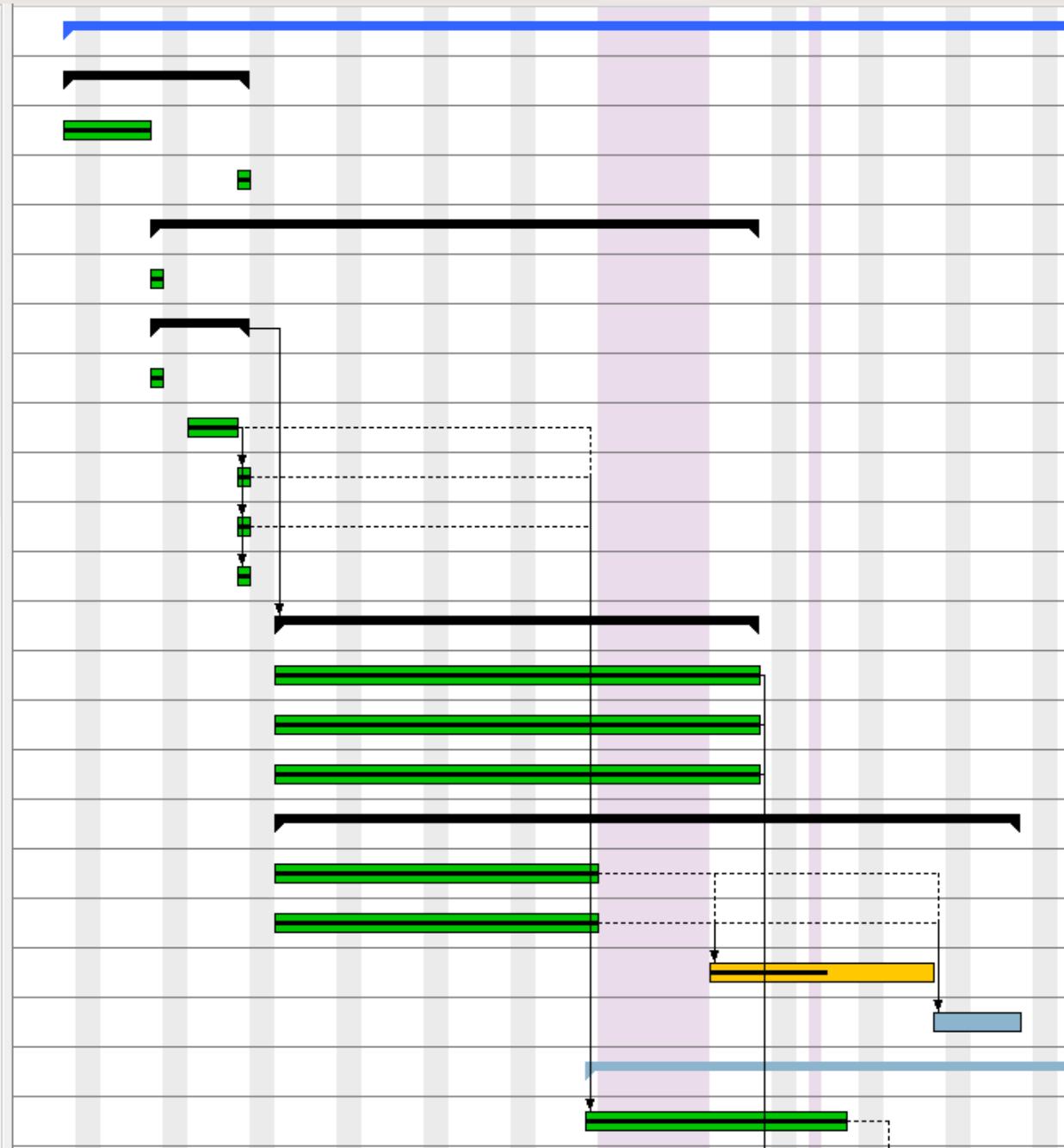
Automatisé
AUDIT TPE/PME
Système Raspberry
CyberSecurity
Windows Linux
Réseau
Infrastructure
Scan



01

L'ORGANISATION DU PROJET

Phase de développement	12/...	30/01/2026
Analyse de marché	Equipements Projet	12/...
Analyse du marché		26/09/2025
Installation Matériel		18/09/2025
Création Infra de Test		26/09/2025
Analyse des besoins		19/...
Configuration réseau		19/...
Achat de matériel		26/09/2025
Configuration VPN		25/09/2025
Configuration Switch		26/09/2025
Configuration Pare-feu		26/09/2025
Configuration Serveurs - Proxmox		26/09/2025
Configuration Système		29/...
Serveur Windows		06/11/2025
Postes		06/11/2025
Serveurs Linux		06/11/2025
Amélioration du scan réseau		29/...
Optimisation des commandes nmap		27/11/2025
Amélioration des filtre...		24/10/2025
Traitement des données		24/10/2025
Génération de la topologie de l'infra...		20/11/2025
Audit Réseau		21/...
Scan avancé des équipements		27/11/2025



GANTT

Nom	D...	Date de fin
Audit Réseau		30/01/2026
Scan avancé des...		13/11/2025
Identification des...		27/11/2025
(Optionnel) Analy...		30/01/2026
(Optionnel) Analy...		30/01/2026
Audit Windows		08/12/2025
Audit AD		28/11/2025
Analyse des G...		28/11/2025
Audit Général		28/11/2025
Durcissement Se...		08/12/2025
Durcissement Po...		08/12/2025
Audit Linux		28/11/2025
Audit Serveurs		28/11/2025
Audit Postes		28/11/2025
Génération du rapport		19/12/2025
Création du temp...		05/12/2025
Traitement des D...		12/12/2025
Windows		12/12/2025
Linux		12/12/2025
Réseaux		12/12/2025
Mise en forme de...		19/12/2025
Génération de pdf		19/12/2025

L'ORGANISATION DU PROJET

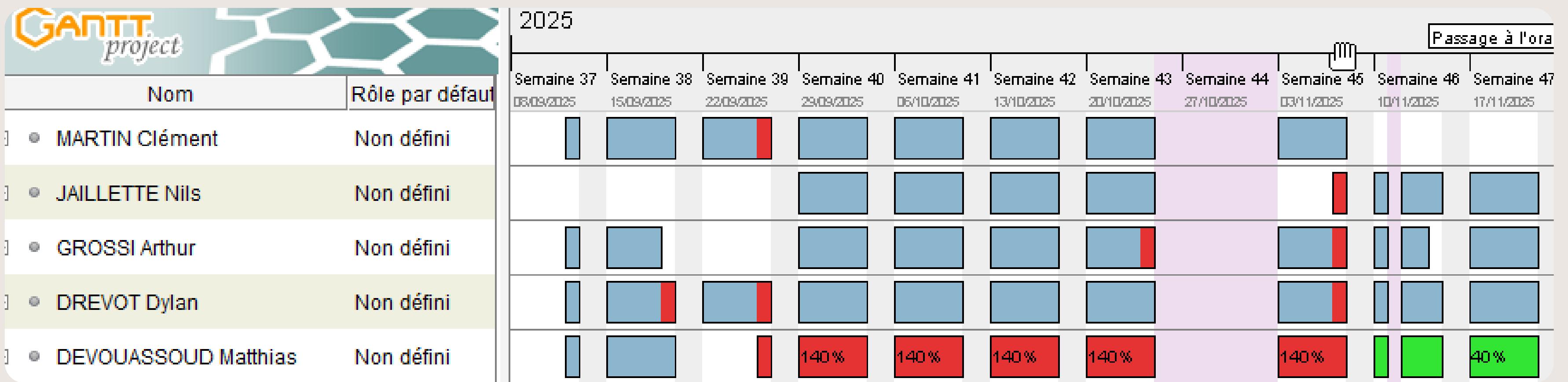
Répartition des rôles

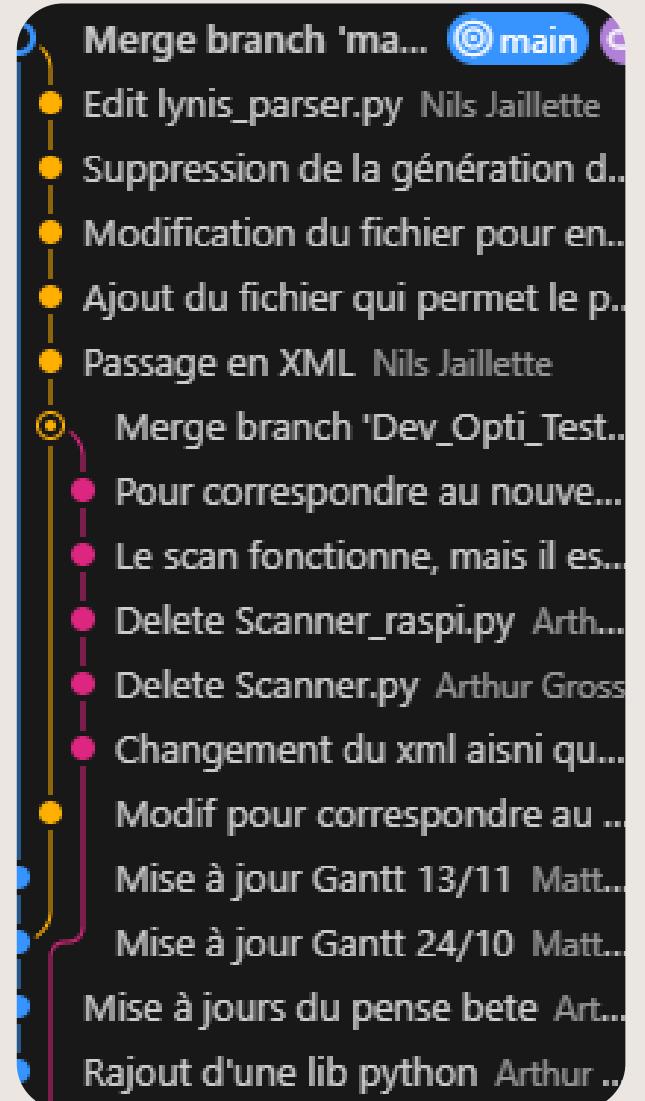
Différents pôles composent le projet, chaque pôle à son responsable :

- Réseau : Arthur GROSSI
- Audit Linux : Nils JAILLET
- Audit Windows : Dylan DREVOT
- Maintenance infra : Matthias DEVOUASSOUD & Clément MARTIN

Scrum Master : Clément MARTIN

Product Owner : Matthias DEVOUASSOUD





Utilisation de Git :

- Une branche par pôle par sprint

01

L'ORGANISATION DU PROJET

Point Positif/Négatif



Ce qui se passe bien

- Bonne entente dans le projet
- Même longueur d'onde sur le but et le produit imaginé
- Le projet est dans les temps pour les différentes deadline
- Communication
- Motivation



02

NOTRE INFRASTRUCTURE

Notre infrastructure de test/developpement

✓ Firewall

✓ Raspberry

✓ VPN

✓ Machines cibles

✓ Linux

✓ Proxmox

✓ Windows

✓ Switch



The screenshot shows the Proxmox VE 9.0.9 interface. The main area displays the 'Server View' for 'Node 'PRX1''. The tree view on the left lists the following resources:

- Datacenter (ClusterPRX)
 - PRX1
 - 100 (SRV-AD)
 - 101 (SRV-FILESYSTEM)
 - 102 (SRV-VEEAM)
 - 103 (SRV-PKI)
 - 104 (Poste-W11)
 - 105 (Poste-XP)
 - 106 (FTP-SERVER)
 - 107 (Poste-Linux)
 - 108 (metasploitable2)
 - 109 (Poste-W10)
 - localnetwork (PRX1)
 - PRX1-NVME-1 (PRX1)
 - local (PRX1)
 - local-lvm (PRX1)
 - usb-iso (PRX1)
 - PRX2
 - 120 (Veeam-APP-13)
 - localnetwork (PRX2)
 - PRX2-NVME-1 (PRX2)
 - PRX2-NVME-2 (PRX2)
 - local (PRX2)
 - local-lvm (PRX2)
 - usb-iso (PRX2)

The right sidebar contains various navigation and configuration links:

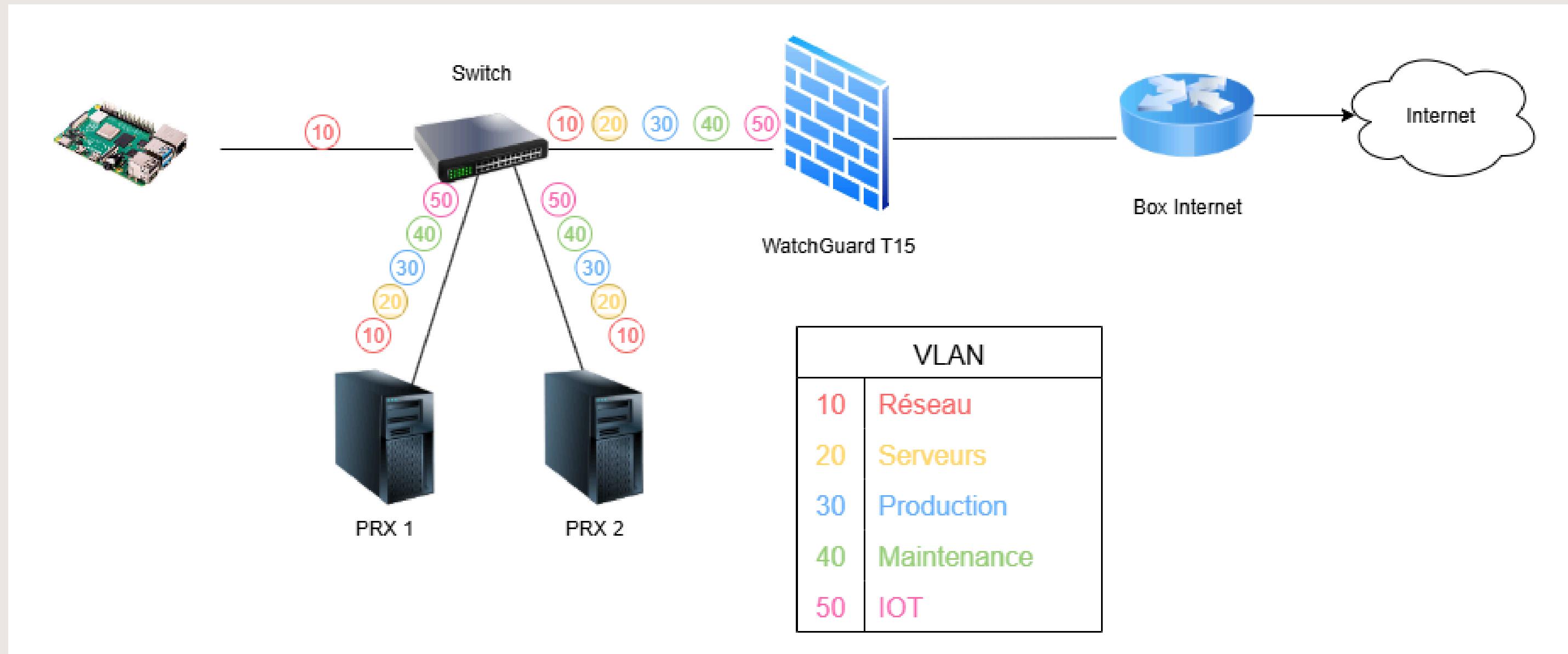
 - Search, Summary, Notes, Shell, System
 - Network, Certificates, DNS, Hosts, Options, Time, System Log
 - Updates, Repositories, Firewall, Disks
 - LVM, LVM-Thin

INFRASTRUCTURE RESEAU

VLAN Name	10.0.10.0/16	Range of addresses	Start IP	End IP	Usable IP	Number of Hosts	Device Name	Device IP	
Réseau	VLAN 1	10.0.0.0/24	10.0.0.0	10.0.0.254	10.0.0.1 - 10.0.0.254	254	if Watchguard	10.0.1.1	
							switch	10.0.1.2	
							Raspberry Pi	10.0.1.106	
Serveurs	VLAN 10	10.0.10.0/24	10.0.10.0	10.1.0.254	10.0.10.1 - 10.0.10.254	254	if Watchguard	10.0.10.1	
							Proxmox 1	10.0.10.10	
							Proxmox 2	10.0.10.20	
							dc - 2016	10.0.10.50	
							FileSystem - 2019	10.0.10.51	Windows
							PKI - 2025	10.0.10.52	
							Veeam - 2022	10.0.10.53	
							Poste W11	10.0.10.55	
							Poste W10	10.0.10.56	
							Poste XP	10.0.10.57	
							FTPServer	10.0.10.54	
							Poste Linux	DHCP	
							Metasploitable	10.0.10.105	
									Linux
Production	VLAN 20	10.0.20.0/24	10.0.20.0	10.0.20.254	10.0.20.1 - 10.0.20.254	254	if Watchguard	10.0.20.1	
							Poste Windows XP	10.0.20.50	
Maintenance	VLAN 30	10.0.30.0/24	10.0.30.0	10.0.30.254	10.0.30.1 - 10.0.30.254	254	if Watchguard	10.0.30.1	
							Poste Windows 11	10.0.30.50	
IOT	VLAN 40	10.0.40.0/24	10.0.40.0	10.0.40.254	10.0.40.1 - 10.0.40.254	254	if Watchguard	10.0.40.1	

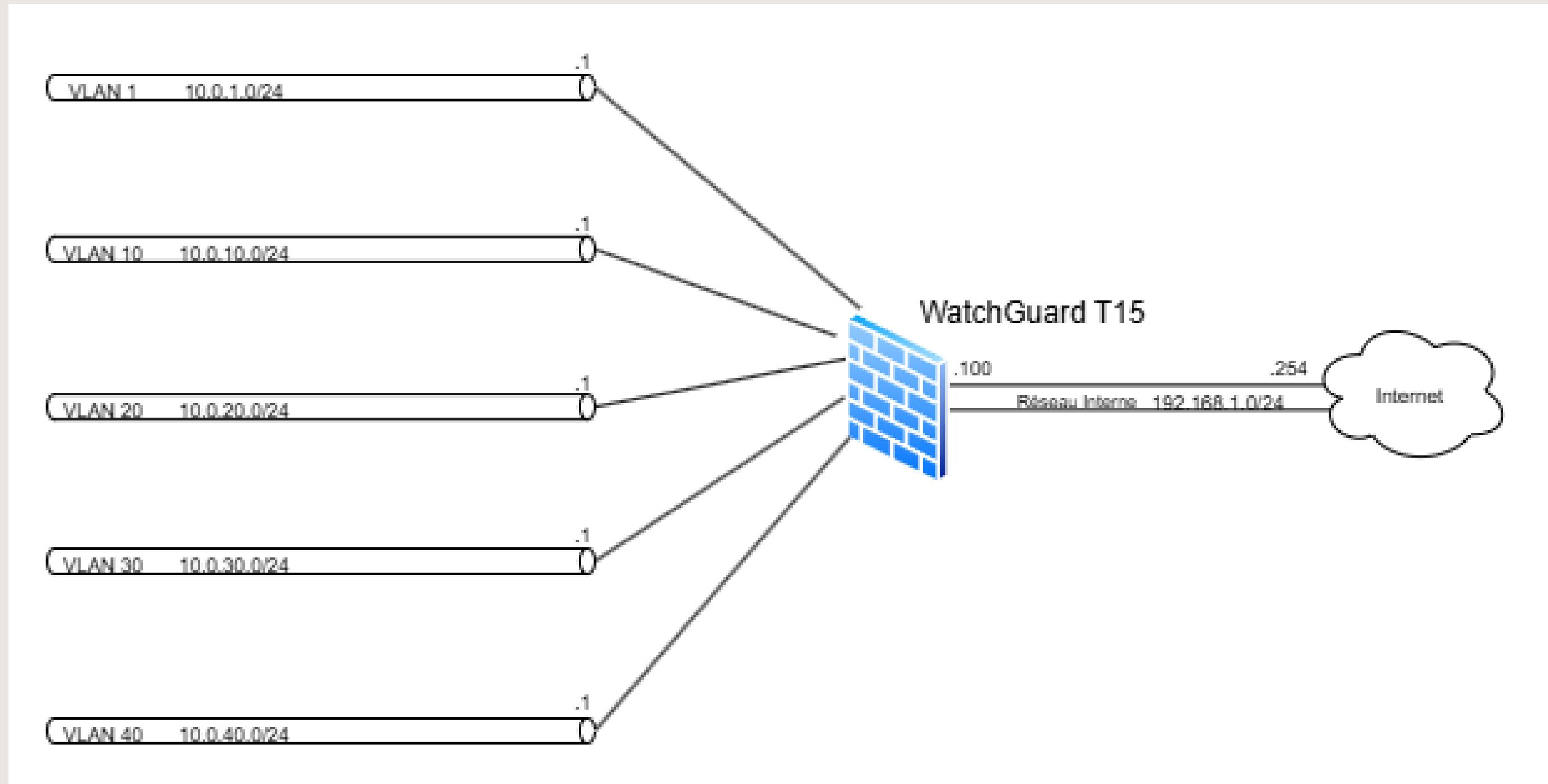
02

INFRASTRUCTURE RESEAU



02

INFRASTRUCTURE RESEAU



COMPOSANT TECHNIQUE

PRX1

HP mini Prodesk 600 g6

- *I7 10700T - 8c 16t*
- *64Go de ram*
- *NVME 2to*
- *NVME 1to*
- *SSD Sata 500go*

PRX2

HP mini Prodesk 400 g6

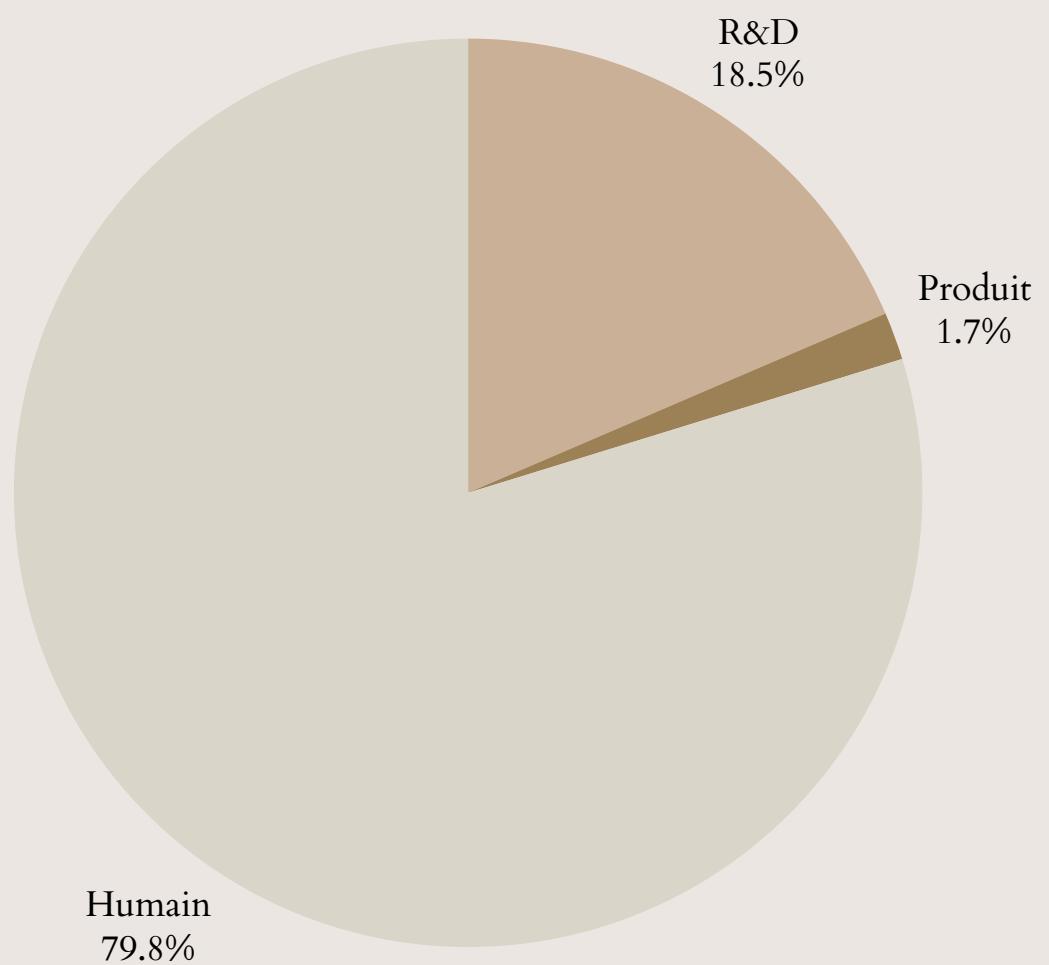
- *I5 10500T - 6c 12t*
- *64Go de ram*
- *NVME 2to*
- *SSD Sata 300go*

Raspberry Pi 4

- *1 x processeur ARM Cortex-A72 64 bits quatre coeurs à 1,5 GHz*
- *4 GB de mémoire RAM*
- *1 x interface Wi-Fi*
- *1 x interface Bluetooth*
- *1 x port Ethernet Gigabit*

02

COUT DU PROJET



R&D	Cout
HP mini Prodesk 600 g6	500€
HP mini Prodesk 400 g6	320€
WatchGuard Firebox T15-W	50€
Switch 8 ports HPE 1820-8G	30€
Cables	30€
Produit	Cout
Raspberry Pi 4	85€
Humain	Cout
200 Heures	4000€
Total	5015€

- 1 Personnalisation du scan via fichier XML
- 2 Lancement du scan NMAP
- 3 Scans approfondies
- 4 Résultats
- 5 Logs

<config>

<!-- Réseaux à scanner (notation CIDR) -->

<networks>

<network>10.0.10.0/24</network>

</networks>

<!-- Hôtes individuels à scanner -->

<hosts>

<!-- <host>192.168.1.100</host> -->

<!-- <host>192.168.1.200</host> -->

</hosts>

<!-- Exclusions (IPs individuelles ou plages) -->

<exclude>

<!-- <entry>192.168.1.1</entry> -->

<!-- <entry>192.168.1.10-20</entry> -->

</exclude>

<!-- Options de scan -->

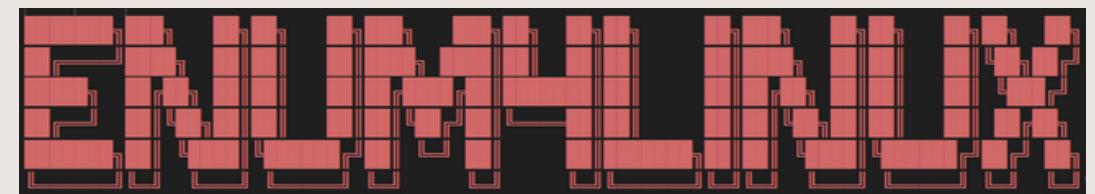
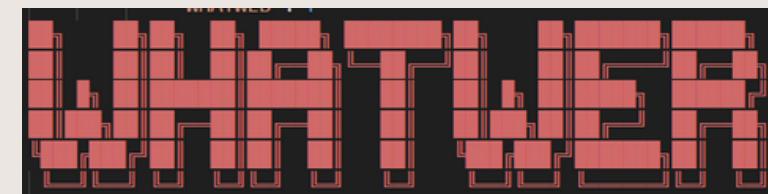
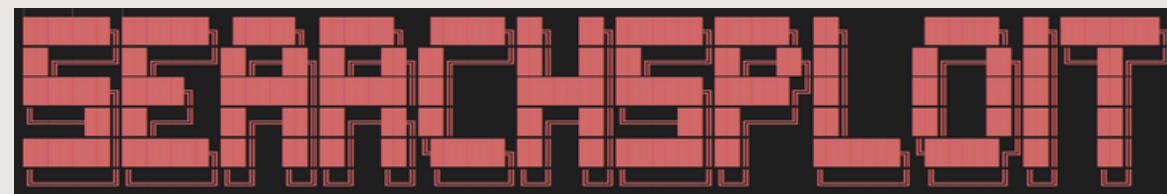
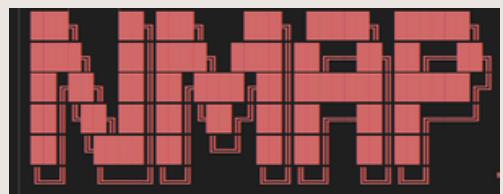
<options>

<!-- Outils additionnels (exécutés conditionnel

<search_exploits>false</search_exploits>

<samba>true</samba>

<whatweb>true</whatweb>



AUDIT ACTIVE DIRECTORY

Fonctionnement

- 1 Personnalisation : Personnalise de l'audit via fichier YML
- 2 Extraction : Décomprime PingCastle.zip Lancement du script
- 3 Transfert SMB : Création du partage SMBv3 + copie des fichiers
- 4 Exécution : Lance PingCastle via WMI/PSEexec (smbexec & evil-winrm en dev)
- 5 Récupération : Rapatrie les rapports HTML/XML + Nettoyage des traces

Contraintes Identifiées

- .NET Framework PingCastle nécessite .NET 4.7.2+
- Compte administrateur du domaine requis
- Réseau Port SMB 445 doit être accessible

Axe d'amélioration

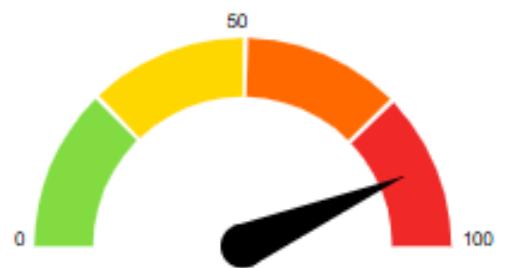
- Autre outils que pingcastle ? (SharpHound, ADRecon, GPOZaurr ..)
- Trouvé une solution pour remplacer les identifiants utilisés NTLM/Kerberos
- Continuer le développement de solution de secours / annexes WinRM 5985/5986 via Evil-Winrm
HTTP/HTTPS 80/443 serveur côté raspi
FTP/FTPS 21/990 FTP IIS
SSH/SCP/SFTP 22 (Windows plus récent)

03

AUDIT ACTIVE DIRECTORY

Fichier HTML

Indicators



It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)

<p>Stale Object : 41 / 100 It is about operations related to user or computer objects</p>	<p>Privileged Accounts : 40 / 100 It is about</p>	<p>Trusts : 0 / 100 It is about connections between two Active Directories</p>	<p>Anomalies : 87 / 100 It is about specific</p>
11 rules matc hed	4 rules matc hed	0 rules matc hed	17 rules matc hed

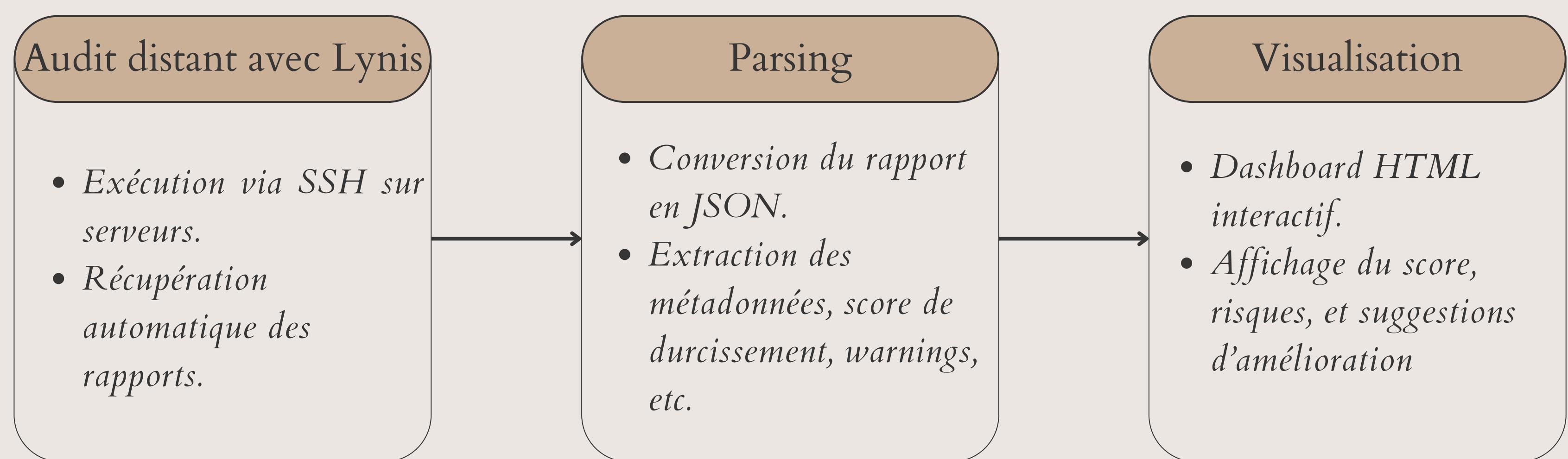
Fichier XML

```

<EngineVersion>3.3.0.1</EngineVersion>
<GenerationDate>2025-11-13T11:15:35.4281077+01:00</GenerationDate>
<Level>Normal</Level>
<MaturityLevel>1</MaturityLevel>
<DomainFQDN>panoptis.lan</DomainFQDN>
<NetBIOSName>PANOPTIS</NetBIOSName>
<ForestFQDN>panoptis.lan</ForestFQDN>
<DomainCreation>2025-11-01T21:40:47</DomainCreation>
<DomainSid>S-1-5-21-1440540841-295370347-945211225</DomainSid>
<DomainFunctionalLevel>7</DomainFunctionalLevel>
<ForestFunctionalLevel>7</ForestFunctionalLevel>
<SchemaVersion>87</SchemaVersion>
<SchemaInternalVersion>0</SchemaInternalVersion>
<IsRecycleBinEnabled>false</IsRecycleBinEnabled>
<DCWin2008Install>2025-11-01T21:41:22</DCWin2008Install>
<SchemaLastChanged>2025-11-01T21:41:22</SchemaLastChanged>
<NumberOfDC>1</NumberOfDC>
<GlobalScore>87</GlobalScore>
<StaleObjectsScore>41</StaleObjectsScore>
<PrivilegedGroupScore>40</PrivilegedGroupScore>
<TrustScore>0</TrustScore>
<AnomalyScore>87</AnomalyScore>
<ExchangeInstall>2025-11-01T21:41:22</ExchangeInstall>
<ExchangeSchemaVersion>0</ExchangeSchemaVersion>
<Trusts/>
<DomainControllers>
  <HealthcheckDomainController AdminLocalLogin="2025-11-09T22:24:07.6252386+01:00">
    <DCName>SRV-AD</DCName>
    <CreationDate>2025-11-01T21:41:22</CreationDate>
  </HealthcheckDomainController>
</DomainControllers>

```

Objectif : Automatiser la collecte et l'analyse des données pour les audits de Linux

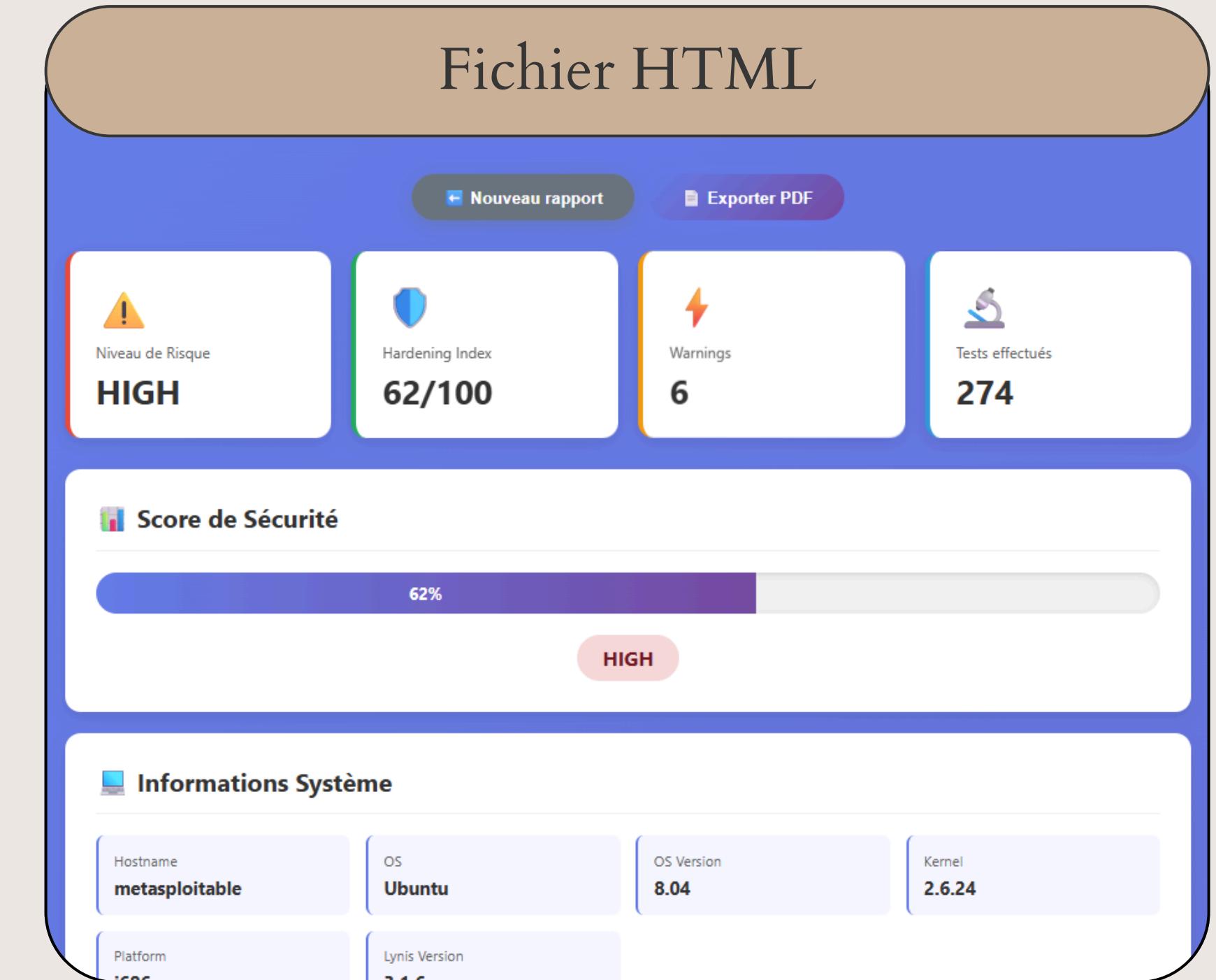


Fichier JSON

```

1  {
2      "metadata": {
3          "lynis_version": "3.1.6",
4          "os": "Linux",
5          "os_name": "Ubuntu",
6          "os_version": "8.04",
7          "kernel_version": "2.6.24",
8          "hardware_platform": "i686",
9          "hostname": "metasploitable",
10         "profile": "/tmp/lynis/default.prf",
11         "log_file": "/var/log/lynis.log",
12         "report_file": "/var/log/lynis-report.dat"
13     },
14     "score": {
15         "hardening_index": 62,
16         "tests_performed": 274,
17         "plugins_enabled": 2
18     },
19     "critical_issues": {
20         "reboot_needed": false,
21         "vulnerable_packages": false,
22         "vulnerable_services": false
23     }
24 }
```

Fichier HTML



04

DEMONSTRATION

CONCLUSION

- Schéma d'architecture (scan réseau)
- Amélioration et fusion de tous les scripts
- Parsing de tous les résultats
- Mise en forme de tous les résultats (PDF, HTML)
- Sécurité raspberry pi (clé ssh, durcissement OS...)

Questions & Réponses

Posez vos questions sur la présentation ou nos prochaines étapes.

