

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2025
ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)	
Épreuve E6 - Administration des systèmes et des réseaux (option SISR)	

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 2
Nom, prénom : <i>Petricca Anthony</i>		N° candidat : 02148344183
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 30 / 04 / 2025
Organisation support de la réalisation professionnelle - Lycée Saint-Marc Nivolas-Vermelle		
Intitulé de la réalisation professionnelle : Analyse de sécurité d'une infrastructure avec GVM		
Période de réalisation : Septembre 2024 - Mai 2025 Lieu : Lycée Saint-Marc Nivolas-Vermelle		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (ressources fournies, résultats attendus) Ressources fournies : Switch D-link, Switch Cisco, Pare-feu Stormshield, Serveur Proxmox, Oracle VirtualBox, ISO Windows Server, ISO Ubuntu. Résultats attendus : Séparation du réseau avec VLANs, mise en place d'un Pare-Feu avec règles de filtrages et NAT/PAT pour assurer la sécurité et accéder à internet. Installation d'un Active Directory et d'un GLPI sur deux machines virtuelles différentes et installation d'OpenVAS en machine virtuelle sur VirtualBox pour scanner les vulnérabilités liées aux CVE trouvées sur l'Active Directory Windows Server et le GLPI d'Ubuntu.		
Description des ressources documentaires, matérielles et logicielles utilisées² Ressources documentaires : Youtube, Forums, IT-Connect, Manuels d'utilisations des équipements/logiciels, Microsoft Learns, Chatbot IA (ChatGPT, Mistral IA,...) Matériels utilisés : Laptop Lenovo, 1x Pare-feu Stormshield, 1x Switch ubiquiti, 1x Switch Cisco, Machines virtuelles (Proxmox: Windows Server, Ubuntu / VirtualBox: Greenbone OpenVAS) Logicielles/Plateformes utilisés : Putty, Google Drive, Trello, Keepass, Draw.io, OpenVAS		
Modalités d'accès aux productions³ et à leur documentation⁴ Modalité d'accès aux productions : Première connexion en câble console puis en utilisant des câbles RJ45, accès Web du pare-feu Stormshield https://192.168.210.1/admin/ , accès aux Switch Cisco via SSH sur Putty en 192.168.210.201 & 192.168.210.202 et switch Ubiquiti en 172.20.210.250 via Unifi, avec comptes et mots de passes notés ci-dessous dans la documentation technique. Modalité d'accès aux documentations : A la suite en PDF		

¹ En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.



**ACADÉMIE
DE GRENOBLE**

*Liberté
Égalité
Fraternité*

Anthony PETRICCA – BTS SIO Option A SISR



BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

SESSION 2025

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle

(verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Documentation Technique – Projet n°2

Analyse de sécurité d'une infrastructure avec GVM



0 - Sommaire :

Sommaire

1 - Introduction (*Page 3 → Page 5*)

1.1 Contexte de la réalisation

1.2 Idées principales

1.3 Modalités d'accès à la production (identifications, liens...)

2 - Présentation du Projet (*Page 5 → Page 6*)

2.1 Besoins exprimés & Objectifs

2.2 Cahier des charges simplifié

2.3 Contraintes techniques (sécurité, matériel, logiciels...)

3 - Mise en place de la solution (*Page 7 → Page 10*)

3.1 Architecture réseau (avec schéma de niveau 2 & 3) et branchements

3.2 Choix des équipements et logiciels

3.3 Planification des tâches et gestion du projet

3.4 Test et validation

4 - Conclusion (*Page 10 → Page 11*)

4.1 Bilan de la réalisation

4.2 Difficultés rencontrées et solutions apportées

4.3 Perspectives d'amélioration

1 - Introduction :

- 1.1 Contexte de la réalisation

Réalisation du projet n°2 dans le cadre du BTS SIO en lien avec l'option SISR (Solutions d'Infrastructures, Systèmes et Réseaux) effectué au Lycée Saint-Marc à Nivolas Vermelle. Projet visant à sécuriser, en analysant la sécurité des équipements et serveurs, l'infrastructure réseau d'une entreprise existante qui fait appel à moi, en utilisant l'outil GVM (Greenbone Vulnerability Management).




- 1.2 Idées principales




Le projet consiste à concevoir une architecture réseau segmenté par un vlan pour le séparer du réseau principal. Cette segmentation se fait à l'aide d'un switch de la marque Cisco et également avec un pare-feu de la marque Stormshield qui me sert à filtrer les flux rentrant et sortant, sans l'utilisation d'un proxy, et à recevoir Internet.

De plus, le projet contient 2 machines virtuelles, un Active Directory et un GLPI, qui sont mal configurées ou configurées par défaut (mauvaises configurations, ICMP activé, Tomcat non désactivé, versions obsolète...) de manière à être remonté par l'outils OpenVAS (Vulnerability Assessment Scanner).




- 1.3 Modalités d'accès à la production (identification, liens...)




Ci-dessous les mots de passe d'accès aux équipements de l'infrastructure :




Title:	Stormshield_FW	Icon:	
Username:	admin		
Password:	iBKjhYQb2JK)+/		...
Repeat:			
Quality:	<div><div></div></div> 87 bits	14 ch.	
URL:	192.168.210.1		

Title:	Switch Cisco	Icon:	
User name:	SW-AnthoP2		
Password:	DknK?UA_Er&w4+		...
Repeat:			
Quality:	<div><div></div></div> 92 bits	14 ch.	
URL:	192.168.210.254		




Ci-dessous les mots de passe d'accès aux différents comptes :




Title:	Proxmox	Icon:	
User name:	apetricca		
Password:	@AnthoProx/+		...
Repeat:			
Quality:	<div><div></div></div> 71 bits	12 ch.	
URL:	https://172.20.1.1:8006/		
Notes:	Proxmox VE		

Title:	Active Directory Windows Server	Icon:	
User name:	AD/Administrateur		
Password:	E#akJ4YF+usp/R		...
Repeat:			
Quality:	<div><div></div></div> 91 bits	14 ch.	
URL:	192.168.210.200 / 172.20.210.200		

Title:	GLPI	Icon:	
User name:	glpi_user		
Password:
Repeat:		
Quality:	<div><div></div></div> 68 bits	12 ch.	
URL:	192.168.210.220		

Title:	MariaDB - GLPI	Icon:	
User name:	glpi_db		
Password:	@Glpi_MDB38+		...

Title:	Openvas	Icon:	
User name:	AdminVAS		
Password:	3n6?j/sPV,wX		...
Repeat:			
Quality:	<div><div></div></div> 79 bits	12 ch.	
URL:	http://192.168.210.100		
Notes:	Default: admin, admin		

Title:	Openvas	Icon:	
User name:	UserVAS		
Password:	OG3_fpe5/a		...
Repeat:			
Quality:	<div><div></div></div> 65 bits	10 ch.	
URL:	http://192.168.210.100/		

Ci-dessous le lien d'accès aux configurations et backup des équipements de l'infrastructure réseau :

[Lien backup & configurations](#)

2 - Présentation du Projet :

- 2.1 Besoins exprimés & Objectifs

L'objectif de cette mission était de vérifier l'état de sécurité d'une infrastructure déjà en place. Aucun audit de sécurité n'avait été réalisé jusque-là. Il fallait donc :

- S'assurer de la bonne configuration des équipements constituant l'infrastructure
- Scanner chaque serveur pour détecter et identifier les vulnérabilités présentes
- Être conscient des risques encourus et prévenir l'entreprise en cas d'action à réaliser
- Prioriser les actions correctives en établissant un plan d'action

- 2.2 Cahier des charges simplifié

- Concevoir une solution d'infrastructure réseau
- Installer, tester et déployer une solution d'infrastructure réseau
- Exploiter, dépanner et superviser une solution d'infrastructure réseau

- 2.3 Contraintes techniques (sécurité, matériel, logiciels...)

Il n'y avait qu'un seul câble console pour toute la classe, il fallait donc se le partager et trouver d'autres moyens d'accéder à nos équipements ou alors faire autre chose.

De plus, il y a eu un changement de l'infrastructure réseau au niveau du lycée, il a donc fallut réadapter le projet et changer les adresses IP des machines virtuelles en ajoutant une seconde carte réseau.

Enfin, on a dû gérer son espace de travail physique qui est partagé avec nos camarades tel que la baie (5 U chacun), les câbles (câble management et rangement), la disponibilité des équipements pour que chacun puisse réaliser son projet.

Affectation @IP :

Réseau principal classe	172.20.0.0/16
Patte OUT pare-feu	172.20.210.1
Gateway	172.20.255.254
Switch 1 / Vlan 1	172.20.210.254
PC personnel	192.168.210.10
Réseau privé	192.168.210.0/24
Gateway (in parefeu)	192.168.210.1
Switch 1 / Vlan 1010	192.168.210.254
Serveur OpenVAS	192.168.210.100
VM Windows (Active Directory)	192.168.210.200
VM Ubuntu (GLPI)	192.168.210.220

Allocation de ports sur switch :

Switch Cisco :

1	3	5	7	9	11		13	15	17	19	21	23
2	4	6	8	10	12		14	16	18	20	22	24

Légende:

Trunk (Cisco Lycée):		Vlan 1 / GW FW OUT		Shutdown	
Vlan 1010		Vlan 1010 /FW IN		N/A	

Notes:

Nombres de câbles réseau nécessaires pour la maquette complètes (Total = 4) :	1X câbles jaunes (1 m (FW IN -> SW Cisco Interne Port 13))	1X câbles rouges (1 m (FW -> SW Cisco Interne Port 2))	1X câbles rouges (1 m (CISCO Lycée -> Port 1 SW Cisco interne Port 1))	1X câble jaune (0,5 m (SW -> Ordinateur))
---	--	--	--	---

- 3.2 Choix des équipements et logiciels

J'ai fait le choix de prendre un switch Cisco pour ce projet car en quelques lignes de commandes je pouvais facilement ajouter mes VLANs aux interfaces que j'avais défini.

Ensuite, le choix de prendre un pare-feu Stormshield à la place du pare-feu Cisco s'explique par la simplicité d'utilisation de ce dernier et également car c'est celui que j'ai le plus utilisé aux cours des deux années passées.

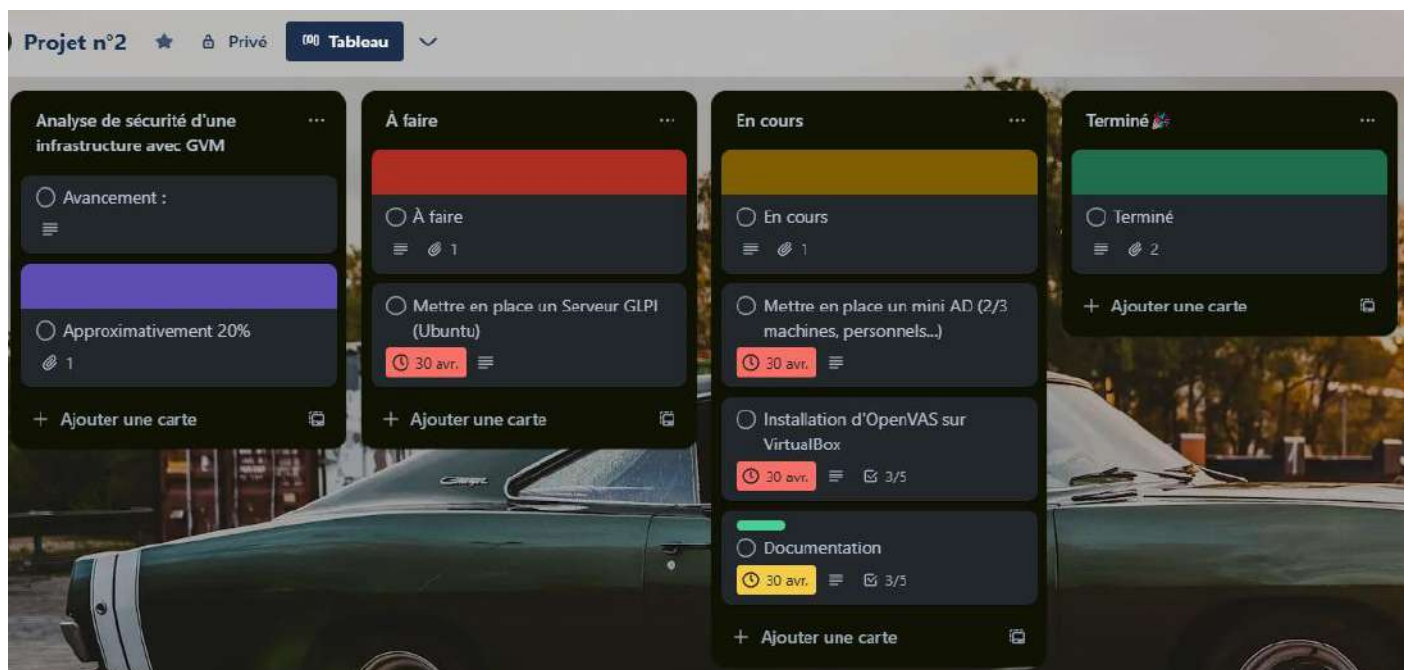
De plus, j'ai décidé d'utiliser l'outil OpenVAS de Greenbone car c'est un outil open source qui n'impose aucune limite de « Host » (nombres de ports maximums à pouvoir être scanné) contrairement à d'autres outils similaires comme Nessus de Tenable. D'ailleurs j'ai fait le choix de l'héberger sur Oracle VirtualBox en local sur mon ordinateur car c'est ce qui paraissait le plus logique dans le contexte de mon projet.

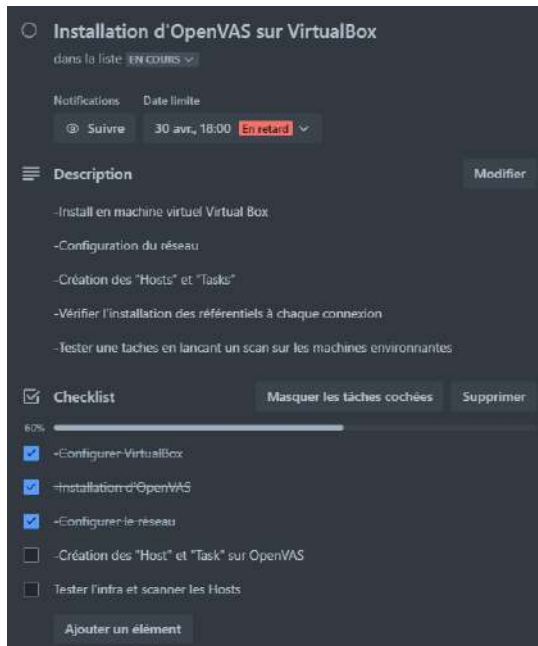
Enfin, j'ai utilisé Draw.io en ligne pour les schémas réseaux car je connais cet outil et il est facile à prendre en main. J'ai également eu besoin de Trello, Keepass et Putty pour différentes tâches comme la gestion du projet, la gestion des mots de passe et l'accès au switch en SSH, pour la même raison. Et j'ai fait le choix de stocker mes documentations en cloud via Google Drive pour faciliter la gestion du projet tout au long de l'année et pour assurer un stockage distant.

- 3.3 Planification des tâches et gestion de projet

J'ai priorisé la méthode agile de gestion de projet nommé « Méthode kanban » à l'aide de l'outil en ligne Trello pour faciliter l'avancée du projet et pour me permettre de m'y retrouver facilement à chaque retour d'entreprise.

Exemple de la gestion du projet à un moment donné :





- 3.4 Test et validation

Les tests effectués ont été :

- Scan de l'host du serveur Active Directory
- Scan de l'host du serveur GLPI
- Tentative d'accès
- Accès à Internet

4 - Conclusion :

- 4.1 Bilan de la réalisation

Cette réalisation a été réalisé de A → Z pour permettre d'être cohérent avec le contexte du projet qui est la mise en place de l'outil OpenVAS et le scan des serveurs pour identifier les vulnérabilités et les régler. Les actions réalisées ont été :

- Création de VLAN interne pour cloisonner le réseau.
- Règles de filtrage sur le pare-feu.
- Mise en place des VM Proxmox et configuration de leur carte réseau secondaire
- Documentation technique rédigée pour l'administrateur de manière à connaître son infrastructure pour être plus efficace lors des maintenances.

- 4.2 Difficultés rencontrées et solutions apportées

J'ai rencontré un souci vers la fin de ma réalisation où mon disque SSD a subi un défaut menant à la perte de dossiers importants notamment de la base de données des mots de passe KeePass qui contenait tous les mots de passe des équipements du projet et des comptes d'accès aux machines virtuelles.

Heureusement, j'avais encore les backups dans mon cloud des équipements ce qui m'a permis de restaurer partiellement les configurations, ceci-dit j'ai dû recommencer pour le reste. D'où l'importance d'avoir des sauvegardes sur différents supports et même hors du réseau.

- 4.3 Perspectives d'amélioration

Il est tout à fait possible d'améliorer ce projet si l'on avait du temps, en ajoutant par exemple :

- Un EDR ou XDR (Endpoint Detection and Response / Extended Detection and Response) au sein de l'infrastructure du client pour vérifier périodiquement l'état du parc informatique, tel que Sophos ou Snort.
- L'intégration d'une solution de supervision plus globale avec un SIEM (security Information and Event Management), tel que Splunk qui est open source.
- WEF intégré à l'Active Directory Windows (Windows Event Forwarding) pour centraliser les logs des journaux d'évènement.