**Document de cadrage de la SAÉ 41**

**Sécuriser un système d’information :**

**Sécurisation d’Active Directory et des accès réseaux pour l’IUT de Vélizy**

**version 1.0 du 21 avril 2023**

1. Contexte professionnel de la SAÉ 41

Avec le passage du DUT au BUT R&T et son parcours cybersécurité, la DSI de l’IUT de Vélizy souhaite améliorer la sécurité de son Système d’Information pour se prémunir d’attaques qui pourraient être mises en œuvre par les étudiants formés à ces pratiques. La DSI souhaite :

* Vérifier la sécurité d’Active Directory, élément critique pour la gestion des identités et l’authentification
* Renforcer la sécurité de l’accès à son réseau pour ses administrateurs avec 802.1X avec certificats
* Sécuriser les switches dans les salles de TP en appliquant DHCP snooping pour éviter qu’un étudiant ayant installé un serveur DHCP lors d’un TP ne perturbe le fonctionnement du réseau

L’IUT a mandaté un prestataire pour réaliser ce travail qui se déroulera en 3 phases :

* Présentation d’une maquette représentant le SI de l’IUT avec les améliorations de sécurités souhaitées
* Déploiement de la solution
* Formation des administrateurs de l’IUT

Votre équipe est en charge de la réalisation de la maquette, de la présentation de la solution et de la formation des administrateurs.

1. Objectifs de la SAÉ

Vous devrez reproduire sur une maquette l’infrastructure de l’IUT et :

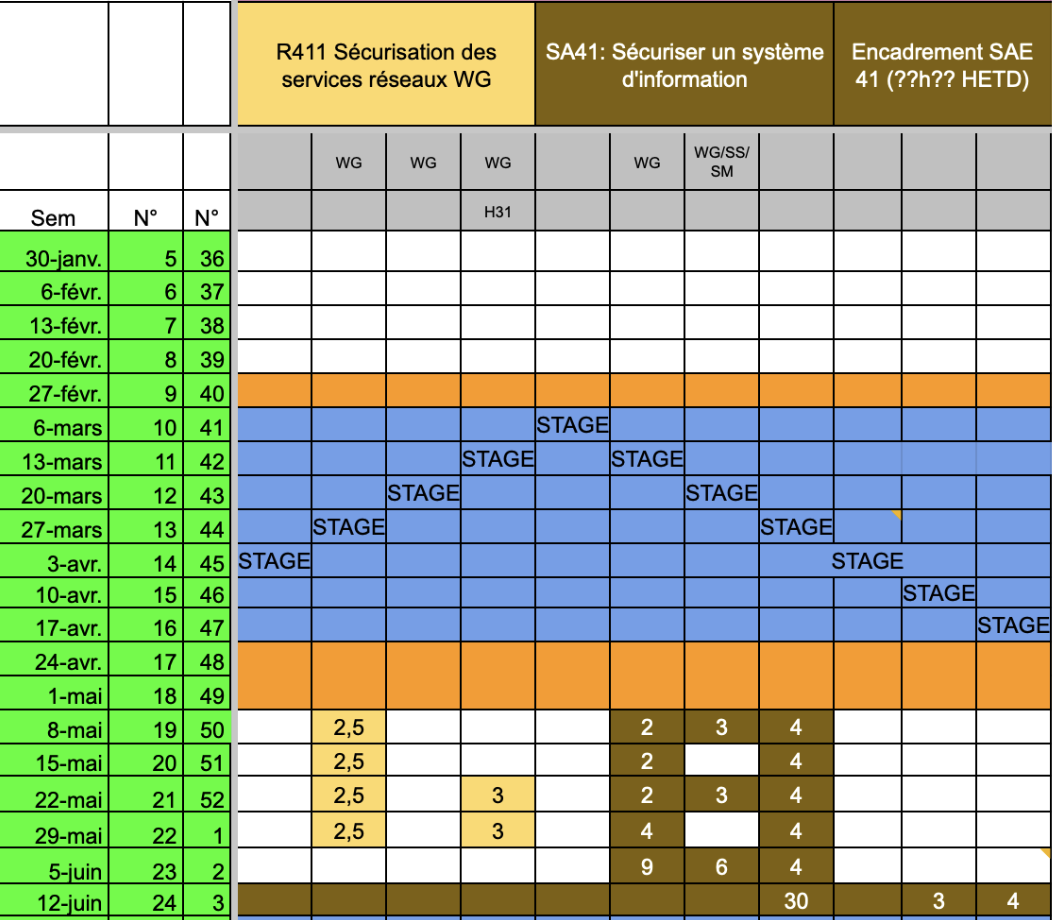
* Montrer les failles de sécurité courantes dans une infrastructure Active Directory et faire des préconisations pour la sécurisation
* Former la DSI de l’IUT à ces problématiques de sécurité
* Montrer la faisabilité et le fonctionnement de la mise en place de 802.1X avec certificats à l’aide d’un serveur de certificats Microsoft ADCS et d’un serveur RADIUS Microsoft Network Policy Server NPS
* Montrer la faisabilité et le fonctionnement de DHCP snooping sur les switchs des salles de TP

1. Organisation

La SAÉ s’étale de la semaine du 8 mai à la semaine 12 juin avec un volume horaire total de 94h étudiant (comprenant les TP du module Sécurisation des services réseaux). La ressource « Sécurisation des services réseaux » vous présentera la sécurité d’Active Directory ainsi que PowerShell.

Il y aura 1 seul groupe de projet et vous serez donc 9 soit un volume horaire total de travail de 9 étudiants x 94h = 846h. A vous de vous répartir les tâches et de vous organiser et faire un planning prévisionnel détaillé mais le chef de projet a estimé grossièrement le travail de la manière suivante :

* 27h par étudiant pour l’installation de l’infrastructure (soit 270h de travail pour les 9 étudiants) sur les semaines 8-15-22 mai (avec réalisation des documentations techniques de l’installation). La semaine du 29 mai donnera lieu à une évaluation du travail réalisé sur l’infrastructure.
* 67h par étudiant pour la partie sécurité les semaines du 29 mai, 5 et 12 juin. Les soutenances se dérouleront le lundi 19 matin.



La SAÉ se déroulera en salle : H31.

1. Rendu

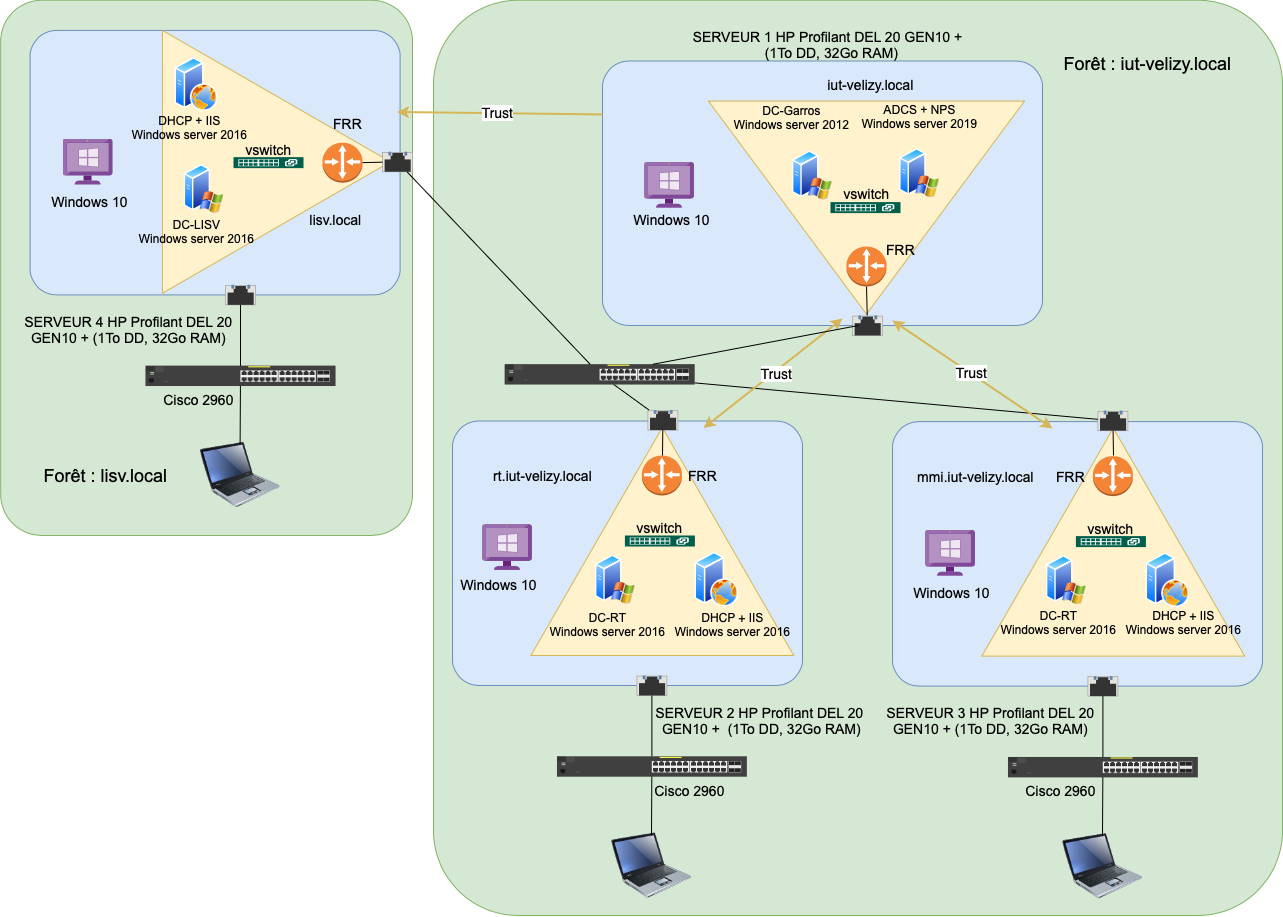
Vous devrez fournir les rendus suivants :

* Un rapport détaillant certaines procédures d’installation de l’infrastructure et des configurations de sécurité (plan d’adressage IP, conversion d’une machine VirtualBox vers ESXi, installation et configuration de FRR, configuration des trusts, scripts expliqués sur la configuration d’AD, configuration du SSO sur le serveur Web et la navigateur, …)
* Un diaporama pour la présentation de la SAÉ présentant rapidement l’infrastructure et les scripts de configuration puis détaillant la partie sécurité

La soutenance orale durera 15 minutes par étudiant soit 2h15 de présentation au total et 1h00 de questions pouvant donner lieu à des démonstrations sur la maquette.

1. Travail à réaliser

L’architecture de l’infrastructure demandée est listée ci-dessous :



Partie 1 : Installation de l’infrastructure

Les tâches à réaliser (volontairement dans le désordre) sont listées ci-dessous :

* Télécharger l’iso Windows 2012 serveur sur (clé : VQ7PG-M7N9B-VG22X-MX8V4-GXWGB) :

<https://drive.google.com/drive/folders/1HIAns_yJOTygmsRShyGg3Q6j_QmKXv-c>

* Installer cette machine sur le serveur ESXi.
* Télécharger les autres serveurs Microsoft sur le centre d’évaluation de Microsoft
* Installer les routeur FRR
* Proposer une organisation des OU et quelques GPO sur chaque DC.
* Créer des scripts pour créer les utilisateurs, groupes OU et GPO sur les DC.
* Effectuer le câblage
* Choisir un plan d’adressage IP
* Tester le fonctionnement
* Se répartir les tâches
* Faire une présentation à l’enseignant
* Réaliser le rapport avec les procédures d’installation
* Réaliser les diapositives pour le diaporama final
* Configurer le serveur Web et le navigateur pour le SSO
* Faire un planning prévisionnel sous forme d’un diagramme de Gant avec les différents étudiants concernés et les tâches qui leur sont attribuées.

Partie 2 : Sécurité

Partie sécurité d’AD

L’objet de la ressource et de cette SAE n’est pas d’apprendre à contourner l’antivirus et l’EDR (vous verrez ces fonctionnalités au S5). Vous pourrez donc désactiver par exemple avec un GPO ces logiciels sur la machine Windows 10 servant à réaliser l’énumération et les différentes attaques.

Vous effectuerez l’énumération avec Powerview (1 binôme), crackmapexec (1 binôme) et Bloodhound (1 binôme sur Linux et 1 sur Windows).

Vous montrerez et expliquerez les attaques sur la résolution de nom, le credential dumping, NTLM et Kerberos. Enfin vous donnerez des conseils d’implémentation pour limiter ces attaques.

Partie sécurité réseau et certificats

Vous activerez le protocole 802.1X afin que les administrateurs soient associés à un Vlan Administration (depuis ce Vlan ils pourront donc administrer les serveurs Windows). Le serveur d’authentification sera le service NPS (Network Policy Server) de Windows Server. L’accès aux serveurs étant hautement sensible, l’authentification de chaque administrateur sera réalisée avec des certificats (Windows Server comprend une fonctionnalité permettant de créer sa propre autorité de certification: Microsoft ADCS). Pour rappel, lors de la ressource R414 Sécurité des Réseaux LAN, vous avez utilisé 802.1x pour que des utilisateurs soient reliés à un port du switch assigné automatiquement à leur Vlan. L'authentification des utilisateurs se faisait alors par un identifiant et un mot de passe. Autre rappel, lors de la ressource R401 Infrastructure de Sécurité, vous avez créé votre propre IGC pour authentifier un site Web, dans cette SAé ce seront les administrateurs qui seront authentifiés.

La configuration demandée dans cette SAé peut être complexe. Il vous faudra donc procéder de façon méthodique et être capable d’exposer votre stratégie pour mener à bien ce projet. Un schéma illustrant les différents acteurs (serveur, switchs, services mis en œuvre….) ainsi que les échanges, devra être réalisé.