LES FONDEMENTS DE L'IDENTITÉ HYBRIDE - SERVICES ACTIVE DIRECTORY

PERSISTANCE ET DOMINATION

Propriétés	Description
Intitulé long	Dans ces ativitées nous allons exfiltrer des données de la base NTDS en utilisant des outils natifs de Windows, comme Volume Shadow Copy. La réalisation de l'attaque DC Sync et la réalisation de l'attaque du Golden ticket
Formation(s) concernée(s)	☐ Classes de première Sciences et technologies du management et de la gestion (STMG) ☐ Terminale STMG Système d'information de gestion (SIG) ☑ BTS Services Informatiques aux Organisations
Matières	☐ Sciences de gestion ☐ SIG ☐ Bloc 1 – Support et mise à disposition de services informatiques ☑ Bloc 2 SISR – Administration des systèmes et des réseaux ☑ Bloc 3 SISR – Cybersécurité des services informatiques ☐ Bloc 3 SLAM – Cybersécurité des services informatiques
Présentation	Vous êtes un technicien au sein du service informatique de la société Contoso. Vous devez mettre en place la sécurité au sein de votre système d'information.
Savoirs	Connaissances TCP/IP, Active Directory, Virtualisation
Compétences	B2A.2.1 Installer et cofigurer des éléments d'infrastrucure - B2A.2.5 Tester l'intégration et l'acceptation d'une solution - B2A.2.6 Déployer uen solution d'infrstructure - B3.3.4 Vérifier l'efficacité de la protection B3?5A Assurer la cybersécurité d'un système d'un service - B3.3.5a.3 Mettre en oeuvre et vérifier la conformité - B35A.4 Prévenir les attaques
Transversalité	
Prérequis	Connaissance d'Active Directory - DNS - Object Active Directory
Outils	VirtualBox ou VMware Workstation pro
Mots-clés	Active Directory, Volume Shadow Copy, Mimikatz, Golden Ticket
Durée	2 heures et 50 minutes
Auteur.e.s	Jérôme Bezet-Torres - Arnaud Jumelet - Equipe Microsoft
Version	v 1

Propriétés	Description
Date de publication	