ELYSIUM SECURITY
29 bis chemin de grave 69450 Saint-Cyr-au-Mont-d'Or
Email : contact@elysium-security.com
Tél : +33 (0)4 28 29 63 37

Annexe 1 – Programme et moyens pédagogiques

1. Objectifs pédagogiques

Les objectifs de la formation « **Administration sécurisée d'environnements Active Directory** » sont :

- Comprendre les concepts clés liés au fonctionnement d'un système Windows :
- Comprendre les concepts clés liés au fonctionnement d'un domaine Active Directory ;
- Présenter les principales familles de vulnérabilités présentes dans les SI internes ;
- Proposer une liste d'outils afin d'aider à l'identification de certaines mauvaises configurations ;
- Aider à mieux comprendre les différentes recommandations de sécurité de certains guides.

2. Programme du cours

Le programme du cours est le suivant :

Rappels sur les environnements Active Directory

- Les systèmes de gestion d'identité (IAM) en entreprise ;
- Rappels sur les principaux composants qui constituent l'AD (ADDS, ADCS, LDAP, Kerberos, etc.) ;
- Notion de classes et d'objets dans l'annuaire ;
- Méthodes d'accès aux ressources de l'AD.

Analyse en mode « boite noire »

- Reconnaissance du réseau interne ;
- Recherche des composants faiblement sécurisés (imprimantes, applications, etc.) ;
- Attaques sur les protocoles de résolution de noms (LLMNR, NBTNS, etc.) ;
- Attaques sur les configurations par défaut (WPAD, IPv6, etc.).

Analyse en mode « boite grise »

- Reconnaissance du domaine AD et extraction des données de l'annuaire LDAP ;
- Recherche et identification des « chemins de contrôle » ;
- Mauvaises pratiques d'administration (mots de passe, partages de fichiers, GPO, etc.) ;

Méthodes de durcissement

- Importance de l'isolation réseau ;
- Désactivation des protocoles vulnérables ;
- Gestion des droits utilisateurs ;
- L'importance de l'audit (log) et de sa sécurisation ;
- Bonnes pratiques d'administration sur AD ;

Travaux pratiques inclus dans les différentes parties

ELYSIUM SECURITY
29 bis chemin de grave 69450 Saint-Cyr-au-Mont-d'Or
Email : contact@elysium-security.com
Tél : +33 (0)4 28 29 63 37

3. Méthode pédagogique

La formation est conçue autour d'une pédagogie active, faisant appel à la participation des stagiaires, notamment en matière de retours d'expérience.
Elle s'appuie sur l'alternance d'apports théoriques et d'exercices pratiques en lien avec les situations professionnelles des stagiaires.
Cette démarche pragmatique, axée sur la démonstration et la pratique, aide les stagiaires, dès leur retour de formation, à être plus attentifs aux situations à risque et à utiliser les outils de sécurité conformément à ce qui est recommandé.

4. Moyens pédagogiques

Le formateur met à disposition son PC portable, connecté à un vidéoprojecteur, permettant l'accès à des schémas d'explications théoriques, des bases d'exercices progressifs ou des études de cas, ainsi que tout type de supports multimédias nécessaires à la formation.
Les supports de cours, remis aux stagiaires en fin de session, réfèrent aux points essentiels de l'intervention. Ils sont conçus sur la base du déroulé du cours qui leur a été présenté. Ces supports de cours sont remis au format PDF.
Les démonstrations sont réalisées sur les équipements du formateur afin de ne pas porter atteinte à la sécurité de l'entreprise.
Le stagiaire doit amener son PC portable pour réaliser les exercices pratiques.