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 « **SEC-AD - Administration sécurisée - Niveau 2** » sont :

- Présenter les principales familles de vulnérabilités sur les services ADCS, DNS et ADFS ;
- Mettre en pratique certaines attaques courantes sur des systèmes vulnérables ;
- Comprendre le principe de dissémination de secrets en mémoire lors des actions d'administration ;
- Expliquer les fondements du « Tiering Model » (classification, cloisonnement, mutualisation) ;
- Mieux comprendre les résultats de certains outils (PingCastle, ORADAD, Purple Knight, etc.) ;
- Aider à mieux comprendre les différentes recommandations de sécurité de certains guides.

2. Programme de la formation

Le plan de la formation est la suite logique à la formation « SEC-AD - Administration sécurisée - Niveau 1 ». Celle-ci a pour finalité de couvrir différents sujets non traités durant le « Niveau 1 » et de présenter le « Tiering Model » afin d'aider à sa mise en place ou sa bonne exploitation par les équipes techniques.

Sécurité du service ADCS

- Rappels sur les systèmes de type PKI (clé public/privée, certificat, norme X.509, etc.) ;
- Analyse d'un certificat (notion d'extensions, SAN, EKU, OID, etc.) ;
- Service ADCS (création d'une CA, stockage dans l'annuaire, notion de templates, etc.) ;
- Kerberos et certificat (rappels sur le protocole Kerberos, PKINIT, etc.) ;
- Attaques sur les certificats (export des clés privées, Pass-The-Certificate, Shadow Credentials, etc.) ;
- Attaques ESCx (Certipy, ESC1, ESC2, ESC3, ESC4, etc.).

Sécurité des services DNS et ADFS

- Service DNS et stockage dans l'annuaire ;
- Sécurité des enregistrements DNS (mise à jour non sécurisée, wildcard, ACLs, etc.) ;
- Risques du groupe « DNSAdmins » (compromission du service DNS) ;
- Risques de la fonctionnalité de transfert de zones ;
- ADFS et compte de service (Kerberoasting, mot de passe faible, etc.) ;
- Exposition du service ADFS (exposition sur Internet, attaque Golden SAML, etc.).

Méthodes de connexion et dissémination de secrets

- Rappels sur les « Logon Type » (Interactive, Remote Interactive, Network, etc.) ;
- Rappels sur les notions de « secrets en mémoire » et « principe de dissémination » ;
- Comparatif des méthodes de connexions (session locale, runas, RDP, RDP RA, MMC, WinRM, etc.) ;
- Principe de connexion avec « identité implicite » et « identité explicite ».

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

Tiering Model - Classification

- Présentation du « Tiering Model » (zones de confiances, Enterprise Access Model, etc.) ;
- Caractéristiques du T0, T1 et T2 (nombre de ressources, niveau d'exposition, criticité, etc.) ;
- Identification des chemins d'attaques (chemins de contrôles AD, erreurs de configurations, etc.) ;
- Problématiques de classification (infrastructure de virtualisation et de sauvegarde, agents et gestion centralisée, WSUS, sécurité physique, ADCS, Microsoft Exchange, etc.).

Tiering Model - Cloisonnement

- Familles de cloisonnements (logique, réseau, système, physique, etc.) ;
- Processus de cloisonnement (identification, analyse, catégorisation, etc.) ;
- JEA - Just Enough Administration (principe, mise en place en PowerShell Remoting/WinRM) ;
- JIT - Just In Time (principe, options en PowerShell, solutions PAM, etc.) ;
- Groupe « Protected Users » (caractéristiques et apports en sécurité) ;
- Durcissements sur Kerberos (blindage, revendications, stratégies d'authentification, etc.) ;
- Silo d'authentification (dépendances à Kerberos, mise en place, particularités) ;
- Restriction d'ouvertures de sessions via GPOs (mise en place, particularités) ;
- Système de délégation des droits dans l'AD.

Tiering - Mutualisation

- Principe de mutualisation dans les actions d'administration ;
- Architectures possibles (poste physique dédiée, poste physique multiniveaux, serveur de rebond) ;
- Isolation des environnements (dual boot, machines hors-domaine, virtualisation, etc.).

Travaux pratiques inclus sur la plateforme Root-Me PRO durant la formation + accès pendant 30 jours post-formation à l'ensemble des environnements de challenges.

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.

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

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.
Les travaux pratiques sont réalisés sur les équipements informatiques à disposition des stagiaires (PC portable d'entreprise et logiciels installés).