ATIKAE
FORMATION - CONSEIL - ACCOMPAGNEMENT

Formation Breaching AD (2 jours – 14 heures)

« ''Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.'' - Sun Tzu « l'Art de la Guerre »

A qui s'adresse cette formation ?

- Professionnels de la sécurité informatique :
  Responsables de la sécurité des systèmes d'information (RSSI), Analystes en sécurité, Consultants en cybersécurité, Administrateurs de systèmes, Administrateurs réseaux, Ingénieurs systèmes et réseaux.
- Développeurs logiciels :
  Développeurs d'applications mobiles, Développeurs de logiciels embarqués

Prérequis

- Connaissances de base en informatique et réseaux :
  Compréhension des concepts fondamentaux de l'informatique, Connaissance des principes de base des réseaux (TCP/IP, DNS, routage, etc.).
- Notions de sécurité informatique :
  Familiarité avec les concepts de sécurité de l'information (confidentialité, intégrité, disponibilité), Connaissance des menaces courantes et des bonnes pratiques en matière de sécurité.
- Compétences techniques :
  Aisance avec les environnements de ligne de commande (Linux/Windows), Expérience de base avec les outils de sécurité (Wireshark, Nmap, etc.).

Les objectifs de la formation

- Comprendre les principales techniques d'attaques informatique dans un environnement Active Directory :
  Comprendre l'environnement Active Directory et son rôle en entreprise, Maîtriser les méthodologies et techniques couramment utilisées par les hackers, Être capable de détecter et d'analyser les tentatives d'intrusion, Appliquer des stratégies de défense efficaces basées sur la compréhension des attaques.
- Renforcer les connaissances en cybersécurité :
  Maîtriser les techniques d'obtention d'un accès initial dans un réseau AD, Apprendre à utiliser les outils de manière éthique pour tester et renforcer la sécurité, Mettre en œuvre des pratiques de sécurisation des applications et des réseaux, Enumérer et cartographier les ressources AD pour identifier les cibles privilégiées.
- Démystifier le hacking :
  Déconstruire les stéréotypes et mythes autour du hacking, Promouvoir une approche éthique et responsable du hacking, Fournir une vision claire de l'importance du hacking éthique dans la cybersécurité.

Le programme de la formation

1. Introduction au piratage éthique *(1.5 h)*

- Les concepts clés de la cybersécurité : triade CID, défense en profondeur, chaîne d'attaque.
- Les attaquants et leurs motivations.
- La méthodologie du hacking éthique

2. Active Directory : concepts de base et fonctionnalités *(1 h)*

- Rappels sur AD : domaines, forêt, objet, GPO, etc.
- Fonctionnement de Kerberos et NTLM.
- Introduction à l'architecture de sécurité d'un environnement AD.

3. Active Directory : accès initial *(1.5 h)*

- Techniques d'OSINT (recherche d'emails, noms de domaines, etc).
- Campagnes de phishing (exemples et simulation).
- Relais NTLM / attaque Web à AD.
- Vulnérabilités fréquemment exploitées pour l'accès initial.

4. Enumération Active Directory *(2 h)*

- Découverte de l'AD avec PowerView, BloodHound, Idapsearch.
- Outils automatisés et analyses manuelles.
- Enumération des groupes, droits, sessions RDP, partages, GPOs.
- Identifier les comptes sensibles (DA, backup operators...).

5. Exploitation Active Directory *(3 h)*

- Kerberoasting : vol et crack de TGS.
- AS-REP Roasting : exploitation sans pré-auth.
- Vulnérabilités d'Active Directory Certificate Services (AD CS).

6. Mouvements Latéraux *(1.5 h)*

- Pass-the-Hash / Pass-the-Ticket.
- Vol de session via outils (Mimikatz, Rubeus, SharpHound...)
- Pivot avec SMB, RDP, WMI.

7. Persistance *(1.5 h)*

- Techniques de persistance AD : SID History, Golden Ticket, Silver Ticket.
- Techniques furtives.

8. Retour d'expériences et bonnes pratiques *(1 h)*

- Présentation de cas réels (tests d'intrusion Axians).
- Analyse des chemins d'attaque identifiés en production.
- Echange interactif : questions, feedbacks et recommandations.

9. Conclusion et évaluation *(1 h)*

- Synthèse des techniques vues.
- Questionnaire de fin / Attestation de formation.

Méthodes et Moyens Pédagogiques

- Ateliers pratiques : Chaque session comprend des exercices pratiques où les participants peuvent appliquer les concepts appris dans des environnements contrôlés.
- Laboratoires virtuels : Les participants auront accès à des labs virtuels pour simuler des attaques et mettre en œuvre des stratégies de défense en temps réel.
- Exposés théoriques, suivis de mise en pratique
- La consolidation des acquis se fait par la réalisation d'exercices contenants l'ensemble des points des cours développés

Evaluation de la formation

- Exercices à valider sur une plateforme en ligne au fur et à mesure de la formation.
- Test final (QCM).
- Questionnaire de satisfaction de la fin de formation.

Organisation de la formation

- **Date :** A définir dans la convention
- **Horaire** : A définir dans la convention

- **Modalité** 10 participants maximum, Présentiel (Distanciel selon contexte)
- **Lieu** Salle
- **Adresse** A définir dans la convention
- **Accessibilité** Accessible aux personnes à mobilité réduite

- **Nous fournissons :** un Lab cloisonné hébergé dans le cloud ; accessible à distance.

- **Condition de réalisation (besoins du formateur) :**
  - Paperboard, Papier/stylos, Un projecteur / Ecran, Un accès internet
- **Pour chaque participant (besoins des apprenants) :**
  - Un ordinateur pouvant exécuter une machine virtuelle, Une machine virtuelle Kali à télécharger sur : https://www.kali.org/get-kali/#kali-virtual-machines , Un accès internet

- Formateurs

Christophe Amiable

Responsable Technique chez Axians Cybersecurity Arras Lille, avec plus de 10 ans d'expérience aussi bien dans le monde de la sécurité défensive qu'offensive. Christophe détient de nombreuses certifications techniques reconnues : OSEP, OSCP, CRTP, CRTO...

Alexandre Lecomte

Consultant chez Axians Cybersecurity Arras Lille, avec 3 ans d'expérience dans la réalisation de tests d'intrusions dans des environnements clients de tout type. Alexandre détient plusieurs certifications techniques avec une spécialité sur l'exploitation de vulnérabilités web : OSCP, OSWA, CRTO, CEH...

AXIANS CyberSecurity Arras-Lille