Fiche de formation
Sécurité d'un réseau interne basé sur Active Directory

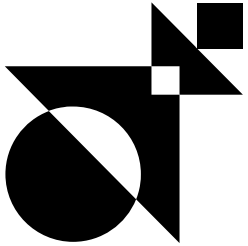
CONTACT POUR CETTE FORMATION

Miora RAHARINIRINA
Chargée de mission formation
almond.institute@almond.eu
07 64 42 71 56

- Version 1.0
- 06/12/2023

Sécurité d’un réseau interne basé sur Active Directory

Les objectifs pédagogiques



L’objectif de cette formation est d’apprendre et de comprendre les techniques les plus courantes permettant la compromission d’un environnement Active Directory, leurs causes, et comment y remédier. Cette formation simule la réalisation d’un test d’intrusion interne, du branchement du poste sans aucun compte de domaine valide, à la compromission totale de la forêt via l’obtention des privilèges d’administrateur de l’entreprise.
Plusieurs techniques seront présentées et expliquées pour chacune des étapes de cette compromission, avec pour la plupart une mise en pratique des attaques par les participants.

01. **Connaître les principales failles** liées aux réseaux internes basés sur Active Directory.

02. **Savoir détecter** la présence des failles présentées.

03. **Acquérir les bonnes pratiques** de sécurité d’administration

Sécurité d’un réseau interne basé sur Active Directory

Informations pratiques

Public

- Équipe d’administrateurs systèmes et réseaux
- Équipe de sécurité des systèmes d’information
- Équipe support utilisateurs

Modalités et délai d’accès

Le stagiaire est considéré inscrit lorsque :

- Les prérequis et besoins sont identifiés et validés
- La convention de formation signée

Les demandes d’inscription peuvent être envoyées jusqu’à 10 jours ouvrés avant le début de la formation.

Prérequis

- Notions de base en : réseau (protocoles, modèle OSI, etc.), environnement Active Directory, Système d’exploitation Windows

Pour aller plus loin

- Une formation dispensée par un expert en sécurité Active Directory ayant réalisé de nombreux tests d’intrusions internes
- Mises en pratique réalisées par les participants eux-mêmes

Évaluation des acquis

Validation en cours de formation via la réalisation d’exercices pratiques et réalisation d’un questionnaire en ligne final recouvrant l’ensemble des notions apprises.

Accessibilité

Que vous soyez reconnu en situation de handicap ou pas, rendre notre formation accessible à toutes et à tous fait partie de notre engagement.

Si vous avez besoin d’une compensation ou adaptation pour le contenu, les supports, le « lieu », le matériel utilisé, les horaires, le rythme, **nous sommes à votre écoute.**

Sécurité d'un réseau interne basé sur Active Directory

La formation en présentiel ou distanciel

Programme

Jour 1	Jour 2	Jour 3
→ **Introduction : pourquoi cibler Active Directory** → **Protocoles d'authentification (NTLM et Kerberos)** → **Principaux protocoles applicatifs (LDAP, SMB et RDP)** → **Obtenir un premier compte de domaine** ▪ Techniques : Obtenir une réponse NTLM avec des empoisonnements réseau : ARP, DHCPv4/v6, LLMNR, NBT-NS, mDNS / Casser ou relayer cette réponse NTLM /Obtention d'une liste d'utilisateurs (via relai, NULL sessions, Kerbrute), afin de mettre en place du password spraying ou ASREPRoasting / Énumérations réseau : applications web et services réseau ▪ Outils : Responder / Impacket / Bettercap / Mitm6 / Kerbrute / Wireshark ▪ Accès supplémentaires obtenus grâce à un compte de domaine	→ **Obtenir les droits d'administrateur local sur des machines** ▪ Techniques : Forcer une authentification NTLM vers sa machine / Relais d'authentification NTLM vers LDAP (RBCD, Shadow Credentials), ADCS et SMB / Kerberoast / Elévation locale de privilèges (PrivescCheck) / Downgrade NTLMv1 / Défauts de mises-à-jour (PrintNightmare, MS17-010) / Disque non chiffré sur un poste utilisateur ▪ Outils : BloodHound / Pingcastle /Impacket / PrivescCheck ▪ Accès supplémentaires obtenus grâce à un accès administrateur local	→ **Élever ses privilèges sur le domaine** ▪ Techniques : Mouvements latéraux (WMI, SMB, WinRM) / Sessions d'administrateurs ouvertes sur des machines / Extraction des mots de passe de comptes de service et tâches planifiées / Extraction des empreintes de mots de passe en cache / Délégations Kerberos / Modèles de certificats ADCS / Défauts de mises-à-jour (ZeroLogon, SamAccountName Spoofing, Certifried) / Élévation de privilèges intra-forêt : domaine enfant vers domaine parent. ▪ Outils : Rubeus / Impacket / Certipy / → **Attaquer des relations d'approbation** ▪ Techniques : SID Filtering / TGT Delegation / Réutilisation de mot de passe / Comptes inter-forêts dans des groupes d'administration

Les plus de la formation

→ Une formation dispensée par un expert en sécurité Active Directory ayant réalisé de nombreux tests d'intrusions internes

→ Mises en pratique réalisées par les participants eux-mêmes

Tarifs et infos

→ **Durée:** 3 jours

→ **Tarif:** 2750€ HT

→ **Financement:** Prise en charge OPCO