ELYSIUM-Formation

Sécurité AD – Niveau 2

Table des matières

Objectifs 2
Prérequis 2
Programme : description détaillée 3
Organisation 4
Moyens mis à disposition 4
Méthodes pédagogiques 4
Public concerné 4

Objectifs

- Présenter des concepts clés liés au fonctionnement d'un domaine AD ;
- Présenter les principales familles de vulnérabilités présentes dans les SI internes ;
- Mise en pratique sur des systèmes vulnérables ;
- Présenter des outils afin de vous aider à identifier certaines mauvaises configurations ;
- Mieux comprendre les points de contrôles remontés par l'outil ORADAD ;
- Aider à mieux comprendre les différentes recommandations de sécurité de certains guides.

Prérequis

- **Avoir suivi le niveau 1 (fortement recommandé)**
- Connaissances de bases du fonctionnement de l'Active Directory ;
- Maitrise des tâches d'administration de bases de l'AD (gestion comptes, gestion GPOs, etc.) ;
- Maitrise des tâches d'administration de bases des machines et serveurs de l'AD ;
- Sensibilisé aux bonnes pratiques de bases en matière de sécurité informatique.

Programme : description détaillée

Thèmes	Jour	Durée	Objectif	Remarques
Reprise sur les notions de la formation "Niveau 1"				
	1	1h	Rappel	
Sécurisation du service DNS				
	1	1h	Formation	Lab pratique
Sécurisation du services ADCS				
Rappels sur les certificats (PKI)	1	3h	Formation	Lab pratique
Mise en place de ADCS				
Kerberos et PKINIT				
Extraction et réutilisation de certificats				
Attaques ESCx				
Principes de bastion d'administration et de silos d'authentification				
	1	1h	Formation	Solutions WALLIX, Open source, etc.
Thèmes	Jour	Durée	Objectif	Remarques
Présentation des méthodes d'administration sécurisées				
Notion de dissémination / réutilisation de secret	2	3h	Formation	Lab pratique
Méthodes d'administration à risques				
Méthodes d'administration recommandées				
Concept de Tiering Model				
Catégorisation des ressources du SI	2	5h	Formation	Lab pratique
Mise en place de cloisonnements par couche				
Mettre en place de la délégation fine (JIT - Just In Time, JEA - Just Enough Administration)				Mise en pratique , œuvre nécessaire : basé sur rapport ORADAD pour durcissement

Exploiter et améliorer				

Travaux pratiques inclus dans les différentes parties

Organisation

Moyens mis à disposition

- 1 formateur expert en sécurité pour chaque session
- 1 salle de formation incluant tous les moyens nécessaires (accès Internet, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif)
- Environnement Root-Me PRO avec sélection de défis Windows/Active Directory (1 licence par apprenant, accès web) : utilisé pour illustrer la partie attaques et vulnérabilités
- Lab Active Directory (1 licence par apprenant, accès web) => utilisé pour s'entraîner à mettre en œuvre des mesures de durcissement et de protection (stratégie d'audit, LAPS, ADCS, silo de stratégie d'authentification, ...)

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices pratiques à base de défis
- Durée : **2 jours consécutifs** en présentiel uniquement / Lyon Part-Dieu
- Nombre d'apprenants par session : 8 maximum
- Programme de la formation (transmis en amont de la formation)
- Support pédagogique (transmis en début de formation)
- Pré requis pour participer : un PC + une connexion Internet
- Évaluation des objectifs pédagogiques (transmise à l'issue de la formation)

Public concerné

- Equipes SSI
- Admin systèmes & réseaux
- Personnels IT en charge du déploiement des mesures de sécurité