Sécurité des Architectures Windows

VOTRE FORMATION

DURÉE : 5 JOURS

35 heures

PROCHAINE SESSION :

1, 2, 3, 9 et 10 juillet 2020

LIEU : En distanciel

PRIX : 1 495 €

net de taxes

LE PUBLIC

Responsables sécurité du SI, chefs de projets informatiques, ingénieurs, administrateurs systèmes.

LES OBJECTIFS

Connaître les principales menaces sur l'environnement Windows et les différentes solutions qui s'y rapportent.

Pouvoir mettre en place les contre-mesures de base contre des attaques courantes.

PRÉ-REQUIS

Etre familiarisé avec le système d'exploitation Windows. Avoir des connaissances de base en sécurité des systèmes d'information

MODALITES

Formation 100 % à distance

De 4 à 16 participants

9h –17h30

Financement éligible au FNE Formation pour tout salarié d'entreprise en activité partielle

VOTRE CONTACT :

Andrea FALLOURD
Conseillère en formation
06 74 51 44 97
afallourd@itescia.fr

ITESCIA - Campus de Pontoise
8 rue Pierre de Coubertin
95300 PONTOISE

www.itescia.fr

VOTRE PROGRAMME

Cette formation propose un tour d'horizon complet des faiblesses des composants et services du monde Windows ainsi que l'arsenal des outils disponibles pour assurer la sécurité des environnements Windows

Introduction des fondamentaux Windows

Composants d'un système Windows
Authentification
La vision d'un attaquant
Structure générale d'une attaque
Cibles privilégiées

Authentification Windows

Introduction aux mécanismes d'auth Windows
NTLM Auth
- Fonctionnement NTLM
- Faiblesses et attaques sur NTLM
- Mesures de remédiation

Kerberos Auth
- Fonctionnement NTLM
- Faiblesses et attaques sur NTLM

Autorisation Windows

Introduction aux mécanismes d'autorisation Windows
Structures clés d'autorisation sur Windows
- Process Token
- Security Descriptor
- ACL & ACE
- Etude de cas : demande d'autorisation Windows

Attaques sur les mécanismes d'autorisation Windows

L'authentification

Grands principes
Authentification NTLM
Attaque « Pass The Hash »
Authentification Kerberos

Elévation de privilèges

Processus LSASS
Informations sensibles en mémoire
Déplacement latéral
Compromission d'un domaine
Relations inter-domaines

Attaques sur le réseau

Contrôle d'accès au réseau (Filaire & Wi-Fi)
Attaques de type Man in the Middle
Protocoles en « clair » (HTTP, LLMNR, etc.)
Attaques de relai
Restrictions Firewall & contournement

Sécurité physique

Attaques physiques
Chiffrement des postes
Attaque « Evil Maid »

Logging et monitoring

L'importance de la documentation

Windows 10 & Windows Server 2016

Les travaux pratiques seront réalisés sur la plateforme d'entrainement **SECURITY DOJO** unique en son genre.

Les scénarii de LABs de SEC-DOJO sont tirés de cas réels avec des vulnérabilités récentes et d'actualité.

Avec les LABs de Sec-Dojo, pour monter l'infrastructure nécessaire aux travaux pratiques, vous n'avez ni à télécharger des iso, ni à installer, ni à configurer, ni à paramétrer et ni à déboguer. Vous êtes directement au cœur du sujet « la sécurité ».