AJC FORMATION

CYCLE

25 jours – 175 heures

CYBERSECURITE OFFENSIVE

Filière

AJC FORMATION – 6 rue Rougemont 75009 - 01 81 51 64 85 –formonsnous@ajc-formation.fr
S.A.R.L. au capital de 10 000 € - SIRET : 50096702100030
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)

www.ajc-formation.fr
www.ajc-classroom.fr

PROGRAMME DE LA FILIERE

AJC FORMATION – 6 rue Rougemont 75009 - 01 81 51 64 85 –formonsnous@ajc-formation.fr
S.A.R.L. au capital de 10 000 € - SIRET : 50096702100030
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)

www.ajc-formation.fr
www.ajc-classroom.fr

FILIERE CYBER OFFENSIVE

Programme

OBJECTIFS

- Acquérir les fondamentaux de la cybersécurité offensive
- Se familiariser avec les défenses pour mieux les contourner
- S'initier aux méthodes et process réglementés de l'audit/Pentest
- Proposer des solutions de sécurité avancée
- Connaitre les différentes typologies d'attaques
- Savoir rechercher et exploiter des vulnérabilités
- Mettre en pratique

METHODES ET MOYENS PEDAGOGIQUES

Méthodes pédagogiques. Pour l'ensemble des stagiaires, le cours intégrera les suivantes :

- Alternance d'exercices, cas pratiques, QCM et de notions théoriques
- Evaluations

Moyens pédagogiques

- AJC met à la disposition de chaque stagiaire un accès à notre plateforme à distance ainsi qu'éventuellement les logiciels utiles dans le cadre de chaque module
- Les supports de cours seront remis via notre la plate-forme de téléchargement Quest et/ou AJC Classroom

PRE-REQUIS

- Une formation ou une première expérience en système et Python serait un plus

PARTICIPANTS

- Toute personne cherchant à acquérir toutes les compétences nécessaires pour devenir un spécialiste Audit/Pentest

LIEU

Distanciel

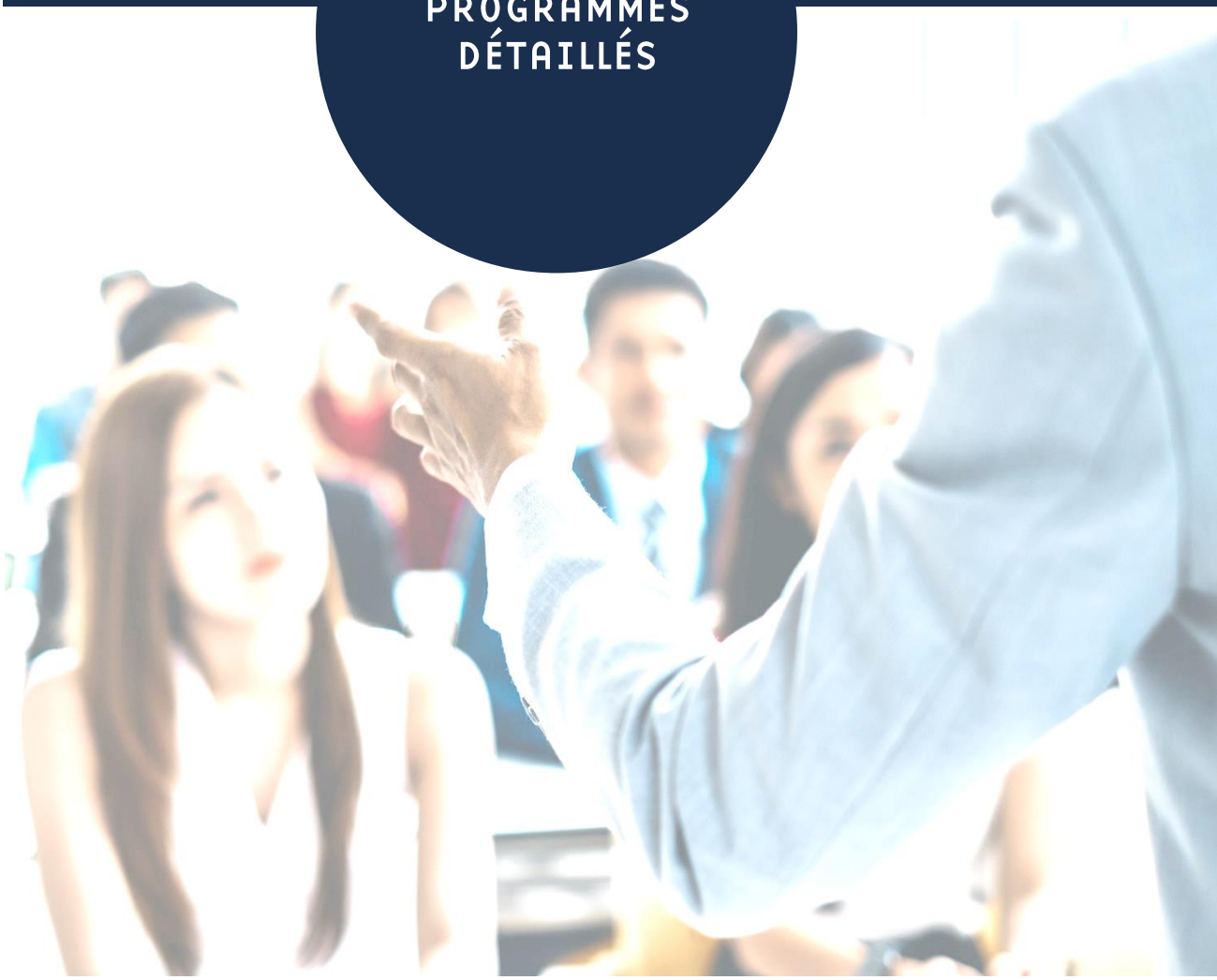
CERTIFICATION / ATTESTATION

Attestation de formation

Programme - Contenu pédagogique

INTEGRATION	LES FONDAMENTAUX DE LA CYBERSECURITE OFFENSIVE	1 jour
LES ATTAQUES, METHODE ET PROCESS	LES DIFFERENTES TYPOLOGIES D'ATTAQUES	1 jour
	METHODOLOGIE ET NORME	1 jour
	DECOUVERTE ET EXPLOITATTION D'UNE VULNERABILTE	1 jour
SECURISATION DE L'ARCHITECTURE ET DES APPLICATIONS	SECURISATION SYSTÈME (Linux, Windows, AD...)	2 jours
	SECURISATION RESEAU (Firewall, Waf, IPS, IDS...)	2 jours
	SCRIPTING (Python, Shell)	2 jours
RECHERCHE ET EXPLOITATION DES VULNERABILITES	QU'EST-CE QU'UN AUDIT/PENTEST ?	2 jours
	L'UTILISATION DES OUTILS OFFENSIFS	4 jours
	LES ATTAQUES WEB ET APPLICATIVES	3 jours
	L'ACTIVE DIRECTORY ET L'ELEVATION DES DROITS	3 jours
PROJET	PROJET FINAL	3 jours

PROGRAMMES DÉTAILLÉS



INTEGRATION

CYBER OFFENSIVE

FONDAMENTAUX DE LA CYBERSECURITE OFFENSIVE

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Introduction

- Définitions et concepts clés
- Les enjeux
- Attaques classiques et exemples d'incidents
- Les bonnes pratiques
- Les produits de sécurité
- Les normes et standards
- Labellisation de sécurité
- Introduction à la crypto

Introduction aux systèmes

- Définitions et concepts clés
- Les composants d'un système
- Les langages de programmation
- Les protocoles et bus de terrain
- Les architectures
- Panorama des normes et standards
- Introduction à la sûreté de fonctionnement

La cybersécurité pour les systèmes

- Les enjeux
- Etat des lieux, contraintes, mythes et légendes
- Les incidents, les attaquants, les motivations
- Les vulnérabilités et vecteurs d'attaques régulièrement rencontrés
- Les bonnes pratiques et les recommandations (organisationnelles et techniques)
- La gouvernance de la cybersécurité des systèmes industriels
- La réglementation (notamment LPM et NIS)

OBJECTIFS

- Comprendre les enjeux de la cybersécurité des systèmes
- Identifier les particularités de ce domaine
- Acquérir les fondamentaux de la cybersécurité des systèmes

PROGRAMME DETAILLE

LES ATTAQUES METHODE ET PROCESS

AJC FORMATION

CYBER OFFENSIVE

LES DIFFERENTES TYPOLOGIES D'ATTAQUES

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Les différentes attaques

- Attaque informatique par déni de service distribué (DDoS)
- Chevaux de Troie(Trojan)
- Logiciels espions (Spyware)
- Détournement de domaine
- Man in the middle
- Hameçonnage (*Phishing*)
- Virus
- Logiciel malveillant (Malware)
- Piratage
- Cryptovirus et Cryptolocker
- Vers informatiques (Computer Worm)
- Vol d'appareils portatifs ou mobiles (Theft)

Vulnérabilités Réseaux

- Différents types de scan
- Firewalking
- Analyse des transmissions chiffrées
- Sniffing réseau
- Spoofing réseau
- Détournement de sessions TCP

Vulnérabilités Web

- Cross Site Scripting (XSS)
- Injection de code
- Inclusion de fichier
- Accès à une référence interne
- Cross Site Request Forgery (CSRF)
- Divulgation d'information
- Vol de session
- Sécurité du stockage
- Sécurité des échanges
- Restriction d'URL

Dans le détail

- Les méthodes d'attaque et de propagation
- Les cibles
- Les conséquences immédiates et à venir
- La détection
- Les actions préventives et curatives

OBJECTIFS

- Identifier les différentes attaques
- Imaginer les attaques possibles en fonction de la cible
- Détecter les attaques visibles et dormantes
- Prévenir plutôt que guérir

PROGRAMME DETAILLE

AJC FORMATION

CYBER OFFENSIVE

METHODOLOGIE ET NORME

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Aspect règlementaire

- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions
- Points importants du mandat

Exemples de méthodologies et d'outils

- Préparation de l'audit
- Déroulement
- Cas particuliers (Habilitations, Dénis de service, Ingénierie sociale....)

Déroulement de l'audit

- Reconnaissance
- Analyse des vulnérabilités
- Exploitation
- Gain et maintien d'accès
- Comptes rendus et fin des tests

Éléments de rédaction d'un rapport

- Importance du rapport
- Composition
- Synthèse générale
- Synthèse technique
- Evaluation de risque
- Exemples d'impacts
- Se mettre à la place du mandataire

OBJECTIFS

- Organiser une procédure d'audit de sécurité de type test de pénétration sur son SI
- Se mettre en situation réelle d'audit
- Mettre en application vos compétences techniques des cours HSF/HSA dans le cadre d'une intervention professionnelle
- Apprendre à rédiger un rapport d'audit professionnel

PROGRAMME DETAILLE

AJC FORMATION

CYBER OFFENSIVE

DECOUVERTE ET EXPLOITATION D'UNE VULNERABILITE

1 jour,
7 heures

DISTANCIEL

PROGRAMME DU MODULE

Les menaces et les risques

- Qu'est-ce la sécurité informatique ?
- Comment une négligence peut-elle créer une catastrophe ?
- Les responsabilités de chacun.
- L'architecture d'un SI et leurs vulnérabilités potentielles.
- Les réseaux d'entreprise (locaux, distantes, Internet).
- Les réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
- La base de données et système de fichiers. Menaces et risques.
- La sociologie des pirates.

La sécurité du poste de travail

- La confidentialité, la signature et l'intégrité. Les contraintes liées au chiffrement.
- Les différents éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Les différentes menaces sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ?
- Les ports USB. Le rôle du firewall client.

Le processus d'authentification

- Les contrôles d'accès : l'authentification et l'autorisation.
- L'importance de l'authentification.
- Le mot de passe traditionnel.
- L'authentification par certificats et par token.
- La connexion à distance via Internet.
- Qu'est-ce qu'un VPN ?
- Pourquoi utiliser une authentification renforcée.

Prise d'information

- Sources ouvertes
- Active

Scanning

- Scan de ports
- Scan de vulnérabilités

Les outils d'attaque

- Outils réseau
- Outils d'analyse système
- Outils d'analyse web
- Frameworks d'exploitation
- Outils de maintien d'accès

OBJECTIFS

- Comprendre les risques et les menaces qui peuvent atteindre le SI
- Connaître les conséquences possibles d'une attaque informatique
- Identifier les mesures de protection de l'information
- Apprendre les actions nécessaires à la sécurisation de son poste de travail

PROGRAMME DETAILLE

SECURISATION DE L'ARCHITECTURE ET DES APPLICATIONS

AJC FORMATION

CYBER OFFENSIVE

SECURISATION SYSTÈME (Linux, Windows, AD...)

2 jours,
14 heures

DISTANCIEL

PROGRAMME DU MODULE

LINUX

Mise en place des premières sécurisations

- Secure Boot
- Signatures MOK / EFI
- Grub
- Attaques DMA

Gestion des droits et des accès

- Le système d'authentification PAM
- SUDO
- Kernel capabilities
- SELinux / AppArmor

Sauvegardes

- Gestion des sauvegardes
- Sauvegardes complètes
- Sauvegardes bases de données

Système de fichier

- Permissions
- ACL / Quotas
- Chiffrement
- ZFS/BTRFS
- Effacement sécurisé

Sécurisation des services de domaine Active Directory

- Sécuriser les contrôleurs de domaine
- Mettre en œuvre les stratégies de mots de passe et de verrouillage des comptes
- Audit des authentifications

WINDOWS

Protection du BIOS/UEFI

Protection du système

- Mises à jour
- Journaux d'événements Windows
- La suite d'outils Sysinternals
- La base SAM et le stockage mots de passe
- Les méthodes d'authentification Windows
- Chiffrement du disque avec Bitlocker

Administration de Powershell

Protection des utilisateurs

- Gestion des droits
- SmartScreen
- Applocker
- Device Guard
- UAC

Déploiement d'un domaine sécurisé

- Stratégie de groupe essentielle
- Déploiement de la solution LAPS
- La technologie ATA
- Déploiement de certificat
- Tester la configuration de son infrastructure (BTA, BloodHound, etc.)
- Segmentation en silos

Protection de la mémoire sous Windows

- DEP, ASLR, Stack canary, SEHOP

Protection des services

- Déployer une autorité de certification
- Infrastructure à clé publique
- Durcissement des services (LDAP, SMB, SQL, Bureau à distance, DNS, IIS...)

OBJECTIFS

- Savoir exploiter les vulnérabilités applicatives sur des systèmes récents, en contournant les protections usuelles
- Être capable d'exploiter une vulnérabilité applicative sur les systèmes Linux et Windows
- Comprendre les failles pour sécuriser le SI et le poste de travail

PROGRAMME DETAILLE

AJC FORMATION

CYBER OFFENSIVE

SECURISATION RESEAUX (Firewall, Waf, IPS, IDS...)

2 jours,
14 heures

DISTANCIEL

PROGRAMME DU MODULE

La sécurité des accès, firewall, Waf, Proxy, Nac

- L'accès des stations aux réseaux d'entreprise,802.1X, NAC
- Les différents types de firewalls
- Les règles de filtrage
- Les règles de la translation d'adresse (NAT)
- La mise en œuvre d'une zone démilitarisée (DMZ)
- La détection et surveillance avec les iDS
- L'intégration d'un firewall dans le réseau d'entreprise
- La gestion et l'analyse des fichiers log

La sécurité des systèmes d'exploitation

- Le Hardening de Windows
- Le Hardening d'Unix/Linux
- Le Hardening des nomades : IOS / Android

La sécurité des applications avec exemples d'architectures

- Les serveurs et clients Web
- La messagerie électronique
- La VoIP IPbx et téléphones

La sécurité des échanges, la cryptographie

- Le cryptage et les fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap,chap,Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN réseau privé virtuel site à site et nomade

OBJECTIFS

- Sécuriser les réseaux d'entreprise
- Déployer des configurations robustes et appliquer les bonnes pratiques
- Protéger efficacement les utilisateurs
- Défendre les points d'entrée extérieurs
- Configurer correctement les équipements de protection

PROGRAMME DETAILLE

CYBER OFFENSIVE

SCRIPTING (Python, Shell)

2 jours,
14 heures

DISTANCIEL

PROGRAMME DU MODULE

Découvrir le langage Python

- Installation de Python
- Découverte de l'invite interactive de Python
- Variables et expressions dans Python

Programmer en Python

- Langage de programmation interprété.
- Python propose les outils standards de la programmation

Base de Python

- Premières opérations
- Types élémentaires de Python
- Instanciation et affectation
- Opérations, expressions, enchaînements
- Transtypage
- Opérateurs de comparaison

Entrées et sorties

- Saisie et affichage

Procédures et fonctions

- Généralités sur les fonctions et les modules sous Python
- Définition des fonctions
- Appels des fonctions
- Valeur par défaut
- Passage de paramètres
- Fonction renvoyant plusieurs valeurs (1)
- Imbrication des fonctions

Les modules

- Principe des Modules - Les modules standards de Python
- Autres utilisations possibles
- Importation d'un module personnalisé

Les tuples

- Création des tuples et accès aux données
- Plus loin avec les tuples
- Bilan sur les tuples

Les listes

- Liste – Le type list
- Modification de taille et de contenu
- Les « List Comprehensions » (traduite en « listes en intension »)
- Traitement par le contenu
- Une variable de type liste est une référence
- Un exemple : somme de valeurs saisies par l'utilisateur
- Boucle directe sur les éléments de la liste

Chaines de caractères

- Une chaîne de caractères est une liste particulière avec des méthodes associées
- Transformation explicite en liste (pour traitements)

Les dictionnaires

- Le type dict
- Modifications, ajouts et suppressions
- Les clés

OBJECTIFS

- S'initier aux méthodes et réflexes de la programmation orientée objet
- Acquérir la maîtrise opérationnelle du langage Python.

PROGRAMME DETAILLE

RECHERCHE ET EXPLOITATION DES VULNERABILITES

AJC FORMATION

CYBER OFFENSIVE

QU'EST-CE QU'UN AUDIT / PENTEST

2 jours,
14 heures

DISTANCIEL

PROGRAMME DU MODULE

Objectifs et types de PenTest

- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test
- Le cycle du PenTest
- Différents types d'attaquants
- Types d'audits
  - Boîte Noire
  - Boîte Blanche
  - Boîte Grise
- Avantages du PenTest
- Limites du PenTest
- Cas particuliers
  - Dénis de service
  - Ingénierie sociale

Prise d'information

- Objectifs
- Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d'information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d'exploits

OBJECTIFS

- Bien délimiter un audit
- Connaître les méthodes existantes , les règles, les engagements d'un audit, et ses limitations
- Connaître les méthodologies reconnues
- Mettre en place une situation d'audit à l'aide d'outils spécifiques

PROGRAMME DETAILLE

AJC FORMATION

CYBER OFFENSIVE

L'UTILISATION DES OUTILS OFFENSIFS

4 jours,
28 heures

DISTANCIEL

PROGRAMME DU MODULE

Attaques à distance

- Introduction à Metasploit Framework
- Scanner de vulnérabilités
- Attaques d'un poste client
- Attaque d'un serveur
- Introduction aux vulnérabilités Web

Prise d'information

- Informations publiques
- Moteur de recherche
- Prise d'information active

Scan et prise d'empreinte

- Enumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

Attaques réseau

- Idle Host Scanning
- Sniffing réseau
- Spoofing réseau
- Hijacking
- Attaques des protocoles sécurisés
- Dénis de service

Techniques de scan

- Différents types de scans
- Personnalisation des flags
- Packet-trace
- Utilisation des NSE Scripts

Détection de filtrage

- Messages d'erreur / Traceroute
- Sorties nmap
- Firewalking avec le NSE Firewalk

Plan d'infrastructure

- Problématiques / Erreurs à ne pas faire
- Eléments de défense

Forger les paquets

- Commandes de base
- Lire des paquets à partir d'un pcap
- Créer et envoyer des paquets

Sniffer les paquets

- Exporter au format pcap
- Exporter au format PDF
- Filtrage des paquets avec le filtre - filter
- Modifier des paquets via scapy
- Les outils de fuzzing de scapy
- Création d'outils utilisant scapy
- Détournement de communications

Système

- Metasploit
- Attaques d'un service à distance
- Attaque d'un client et bypass d'antivirus
- Attaque visant Internet Explorer, Firefox
- Attaque visant la suite Microsoft Office
- Génération de binaire Meterpreter
- Bypass AV (killav.rb, chiffrement, padding etc.)

Utilisation du Meterpreter

- Utilisation du cmd/Escalade de privilège
- MultiCMD, attaque 5 sessions et plus
- Manipulation du filesystem
- Sniffing / Pivoting / Port Forwarding

Attaque d'un réseau Microsoft

- Architecture / PassTheHash
- Vol de token (impersonate token)

Rootkit

OBJECTIFS

- Comprendre et mener les attaques sur un SI
- Définir l'impact et la portée d'une vulnérabilité
- Réaliser un test de pénétration
- Corriger les vulnérabilités
- Sécuriser un réseau

PROGRAMME DETAILLE

AJC FORMATION

CYBER OFFENSIVE

LES ATTAQUES WEB ET APPLICATIVES

3 jours,
21 heures

DISTANCIEL

PROGRAMME DU MODULE

Attaques Web

- Cartographie du site et identification des fuites d'information
- Failles PHP (include, fopen, Upload,etc.)
- Injections SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Bonnes pratiques

Attaques applicatives

- Escape shell
- Buffer overflow sous Linux
- L'architecture Intel x86
- Les registres
- La pile et son fonctionnement
- Présentation des méthodes d'attaques standards
- Ecrasement de variables
- Contrôler EIP
- Exécuter un shellcode
- Prendre le contrôle du système en tant qu'utilisateur root

Vulnérabilités Web

- Mise en place d'une solution de Proxy
- Cross-Site Scripting (XSS)
- XSS Réfléchie , Stockée Dom-Based
- Contournement des protections
- Démonstration avec l'outil d'exploitation

Cross-Site Request Forgery (CSRF)

- Exploitation d'un CSRF
- Requête HTTP GET , HTTP POST

Injection SQL

- Injection dans un SELECT
- Injection dans un INSERT
- Injection dans un UPDATE
- Injection dans un DELETE
- Technique d'exploitation – UNION
- Technique d'exploitation – Injections booléennes
- Technique d'exploitation – Injection dans les messages d'erreurs
- Technique d'exploitation – Injection par délais
- Technique d'exploitation – Injection dans des fichiers
- Exemple d'utilisation avec SQLMap

Injection de commandes

- Chainage de commandes
- Options des commandes
- Exploitation
- Exemple d'exploitation avec commix

Service Side Includes (SSI)

Injection d'objet

Inclusion de fichier

- Inclusion de fichiers locaux (LFI)
- Inclusion de fichiers distants (RFI)
- Contremesures

Envoi de fichier (Upload)

- Exploitation basique
- Vérification de Content-type
- Blocage des extensions dangereuses
- Contremesures

XML External Entity (XXE)

- Les entités
- Découverte de la vulnérabilité
- Exploitation de la vulnérabilité
- Contremesures

Service Side Template Injection (SSTI)

OBJECTIFS

- Comprendre et exploiter les différentes vulnérabilités d'un site Web
- Augmenter le champ d'exploitation des vulnérabilités pour un test d'intrusion
- Être en mesure de réaliser un audit d'application Web

PROGRAMME DETAILLE

AJC FORMATION

CYBER OFFENSIVE

L'ACTIVE DIRECTORY ET L'ELEVATION DES DROITS

3 jours,
21 heures

DISTANCIEL

PROGRAMME DU MODULE

L'architecture Active Directory (AD)

- Vue d'ensemble des différents rôles Active Directory
- Intérêts et interconnexion des rôles
- Cas typiques d'utilisations des rôles
- Vue d'ensemble d'Active Directory Domain Services (AD DS)
- Architecture et concepts
- Présentation d'une GPO
- Mise en oeuvre et administration des GPO
- Cadre et traitement de la GPO

Recherches

- Objets abandonnés : comptes inactifs, protocoles ou OS obsolètes, etc. ;
- Comptes à privilèges : utilisation des groupes d'administration natifs, permissions abusives, etc. ;
- Relations d'approbation : absence de filtrage des SIDs, présence de SID History, etc. ;
- Anomalies de sécurité : politiques de mots de passe insuffisantes, présence de mots de passe dans les GPOs, etc.
- Identification des utilisateurs privilégiés et des droits qui leur sont applicables, afin de savoir si l'un d'eux peut être compromis par un droit trop permissif
- Contrôle de permissions critiques, telles que celles relatives à l'objet AdminSDHolder qui peuvent être utilisées pour constituer une porte dérobée
- Analyse de la santé du schéma d'annuaire
- Identification de stratégies de mot de passe anormales,

Techniques de compromission de l'Active Directory

- Elévation des droits
- Recherche de mots de passes par défauts
- Mouvement latéraux

OBJECTIFS

- Se familiariser à Active Directory et les permissions mises en œuvre par le mécanisme de contrôle d'accès discrétionnaire
- Identifier les privilèges illégitimes ou inadaptés acquis via les permissions de l'annuaire
- S'initier aux techniques de compromission de l'Active Directory

PROGRAMME DETAILLE

PROJET

CYBER OFFENSIVE

PROJET FINAL

3 jours,
21 heures

DISTANCIEL

PROGRAMME DU MODULE

Déroulement du module

- Les stagiaires travaillent en toute autonomie, en binôme. Ils sont libres d'effectuer les choix adaptés, de développer les parties dont ils jugent avoir le plus besoin et d'apporter leurs propres solutions aux problèmes posés.
- Le formateur encadre les stagiaires par sa présence et répond aux questions. Il intervient pour épauler un binôme en difficulté ou pour faire le point à l'ensemble du groupe sur des notions non acquises. Il peut être amené à approfondir ou compléter certaines connaissances.

OBJECTIFS

- Mettre en application les acquis de la formation en complétant les mini projets réalisés dans tout le cursus

PROGRAMME DETAILLE

AJC FORMATION

NOUS CONTACTER

AJC FORMATION
01 81 51 64 85
formonsnous@ajc-formation.fr
6 rue ROUGEMEONT
75009 PARIS

www.ajc-formation.fr
www.ajc-classroom.fr