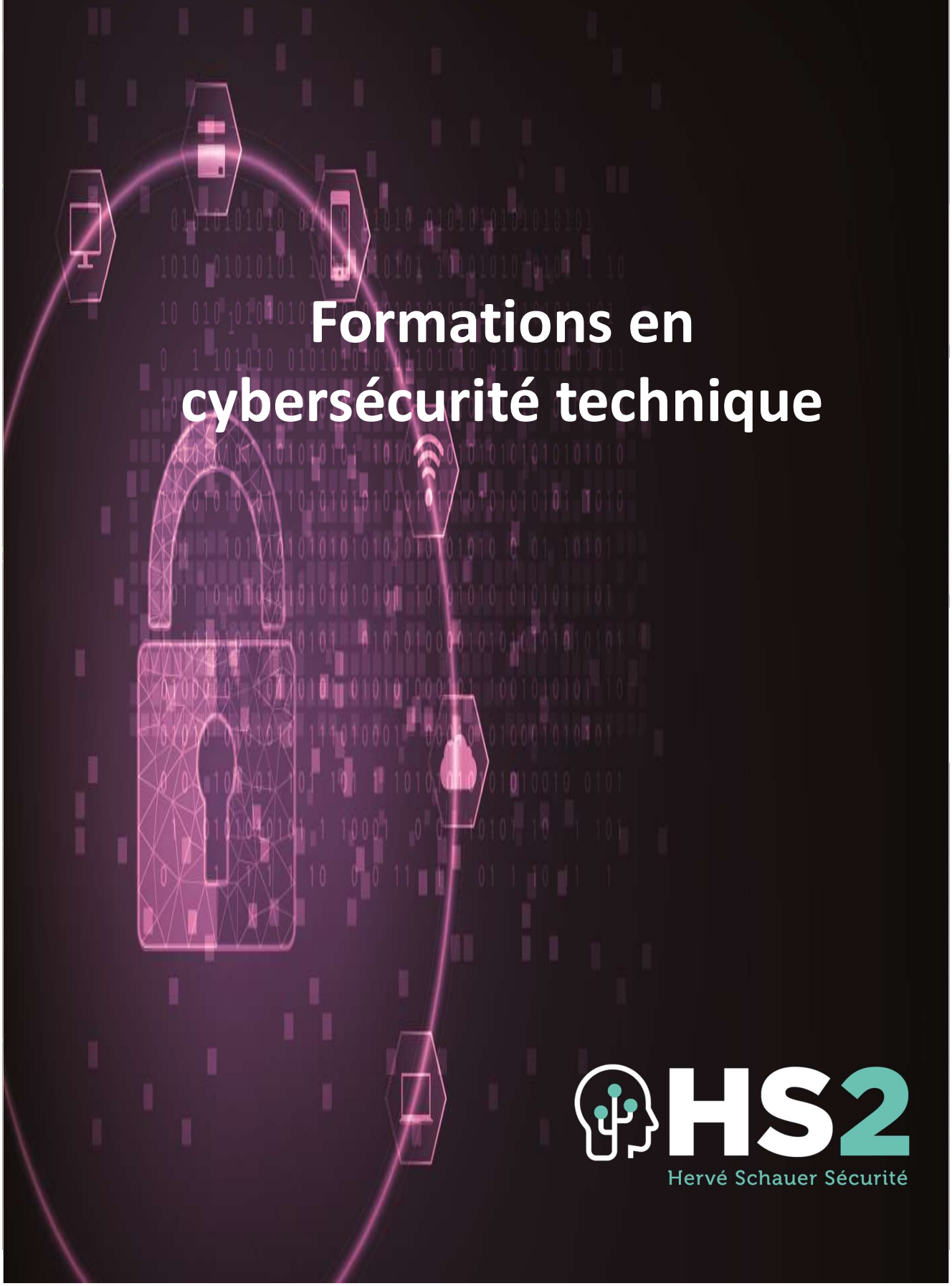
Catalogue de formations 2024



Formations en cybersécurité technique

HS2
Hervé Schauer Sécurité

SOMMAIRE ET CALENDRIER

Cybersécurité technique

***Examen de certification HS2 inclus**

Cybersécurité technique				
Réf.	Formations	Durée	Sessions	Pages
PENTEST1*	Tests d'intrusion	**5 J**	• 30 sept. au 4 octobre 2024 • 2 au 6 décembre 2024	**46-48**
PENTEST2*	Tests d'intrusion et développement d'exploits	**5 J**	• 25 au 29 novembre 2024	**49-50**
PENTESTINDUS*	Tests d'intrusion des systèmes industriels	**3 J**	• 2 au 5 avril 2024 • 28 au 31 octobre 2024	**51-53**
PENTESTWEB*	Test d'intrusion des serveurs et des applications Web	**5 J**	• 15 au 19 avril 2024	**54-56**
SPLUNK*	SPLUNK	**3 J**	• 17 au 20 juin 2024 • 14 au 17 octobre 2024	**57-59**
Nos intervenants				**60-61**
Bulletin d'inscription				**62**

***Examen de certification HS2 inclus**

Formation « Essentiels techniques de la cybersécurité »

Réf : ESSCYBER

La sécurité des systèmes d'information (SSI), aujourd'hui appelée cybersécurité, semble un jargon lointain pour certains. Il est important de démystifier en expliquant concrètement comment ça marche, et la meilleure des sensibilisations à la cybersécurité est la formation qui explicite. Grâce à sa vision pragmatique de la sécurité : connaitre l'attaque pour mieux se défendre, et aux différentes mises en application proposées, cette formation permet aux stagiaires de comprendre la nécessité de la SSI, d'en aborder les concepts théoriques (cryptographie, contrôle d'accès...) et d'identifier tous les domaines auxquels elle s'applique (système, réseau, applications...).

Objectifs

- Acquérir la connaissance des concepts fondamentaux de la SSI.
- Identifier les besoins en sécurité à tous les niveaux (système, réseau, applications...)
- Comprendre les différents types d'attaques
- Connaitre les mesures de sécurité permettant de les contrer

Durée & horaires

- 2 jours soit 14 heures
- De 09h00 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Toute personne souhaitant acquérir la compréhension de la cybersécurité
- Responsable de la sécurité (RSSI) de formation non technique
- Chef de projet et acteur d'un projet sécurité

Cette formation est accessible à un public plus large que la formation SECUCYBER en permettant aux personnes au profil non informaticien ou non technique d'obtenir une vision opérationnelle de la cybersécurité

Pré-requis

- Cette formation ne nécessite pas de prérequis particuliers, elle est accessible à un large public.

Méthode pédagogique

- Cours magistral avec de nombreux exemples pratiques

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Sécurité : concepts fondamentaux

- Concepts de base
- Gestion du risque : vulnérabilité, menace, impacts métiers
- Dans la peau d'un attaquant
- Principes de base : connaître son SI, moindre privilège, défense en profondeur

Cryptographie

- Chiffrement
- Hachage
- Signature
- TLS
- PKI/IGC

Sécurité des réseaux

- Principes de base
- Attaques
- Contrôle d'accès
- Filtrage et relayage
- Architecture sécurisée
- WiFi

Sécurité des applications

- Vulnérabilités web : le TOP 10 de l'OWASP
- Vulnérabilités mémoire
- Attaques et défenses
- Processus de développement

Sécurité des systèmes

- Contrôle d'accès
- Minimisation et durcissement
- Veille sécurité
- Mise à jour
- Sauvegarde
- Journalisation
- Protection du poste de travail
- Equipements mobiles

Formation « Fondamentaux techniques de la cybersécurité »

Réf : SECUCYBER

Si le fait d'être sensibilisé à la sécurité est important quel que soit le poste occupé, comprendre les concepts de base de la SSI est une nécessité absolue pour le personnel technique de l'entreprise. En effet, la sécurité n'est pas seulement l'affaire du RSSI et de ses équipes : administrateurs système et réseau, architectes, développeurs ont tous leur rôle à jouer dans la protection de l'entreprise et de son patrimoine.

La formation SECUCYBER, en abordant sur 5 jours tous les aspects techniques de la sécurité informatique, vise à apporter à cette population les connaissances indispensables leur permettant de choisir, d'implémenter et de maintenir les mesures de sécurité propres à leur domaine de compétence.

Objectifs

- **Être en mesure dans tous les domaines techniques de la sécurité (système, réseau, applications, cryptographie...) de :**
  - **Maîtriser le vocabulaire et les concepts principaux du domaine**
  - **Connaître différentes techniques d'attaque**
  - **Choisir et appliquer les bonnes mesures de sécurité**

Durée & horaires

- **5 jours soit 40 heures**
- **Du lundi au jeudi : de 9h00 à 12h et de 13h30 à 19h00.**
- **Le vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Administrateurs système ou réseau**
- **Architectes**
- **Développeurs**
- **Personnel débutant ou souhaitant acquérir de bonnes bases techniques en SSI**
- **Prestataires référencés par cybermalveillance.gouv.fr**

Pré-requis

- **Bonnes connaissances en informatique**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUCYBER par HS2.**

Programme

Module 1 : SSI - principes de bases

- Pourquoi la SSI ?
- Notion de risque
- Les règles de base
- Contrôle d'accès
  - AAA
  - Gestion des utilisateurs
  - Authentification
  - Gestion des privilèges

Module 2 : Cryptographie

- Concepts fondamentaux
- Fonctions de base
  - Chiffrement
  - Hachage
  - Signature
- Protocoles
  - TLS
  - IPSec
  - SSH
- PKI / IGC

Module 3 : Réseau

- Modèles théoriques : OSI, TCP/IP
- Attaques classiques
  - Découverte de ports
  - Man-in-the-Middle
- Contrôle d'accès réseau
- Segmentation
  - Qu'est qu'une bonne architecture ?
  - Comment segmenter son réseau
  - VLAN
  - Parefeu
  - Proxy
- Réseaux sans fil
- Sécuriser le Cloud

Module 4 : Applications

- Architecture n-tiers
- Protocoles
- Authentification et sessions
- Top 10 de l'OWASP
- Buffer Overflow
- Processus de développement

Module 5 : Windows

- Installation
- Bitlocker
- Mesures Windows 10 :
  - Device Guard
  - Application Guard
  - Exploit Guard
- Gestion des administrateurs
- Éviter le Pass-The-Hash

Module 6 : Linux

- Système de fichiers
- Minimisation
- Comptes utilisateurs
- Authentification
- SELinux
- AppArmor
- SSH
- Netfilter
- Journalisation

Formation « Cybersécurité des systèmes industriels »

Réf : SECUINDUS

Les systèmes industriels sont maintenant informatisés et connectés. Longtemps isolés, ils sont maintenant dans le cœur de cible des attaques informatiques. Généralement, trop peu d'automaticiens ont une expérience significative de l'état de l'art de la sécurité informatique, et trop peu d'experts en cybersécurité ont une bonne connaissance du monde de l'informatique industrielle. La présente formation s'efforce de proposer un état des enjeux, des méthodes et des moyens de sécurisation, et de la gestion d'incident.

Objectifs

- Aborder la cybersécurité des systèmes industriels par une approche pragmatique et pratique
- Développer un plan de sécurisation des systèmes informatiques industriels
- Pouvoir auditer les SI industriels
- Initier la préparation de plans de réponse à incident sur les systèmes industriels

Durée & horaires

- 5 jours soit 35 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Responsables sécurité, sureté, cybersécurité, sécurité industrielle
- RSSI
- Automaticiens
- Consultants en sécurité
- Auditeurs en sécurité

Pré-requis

- Bonne connaissance générale en informatique et en sécurité des systèmes d'information, par exemple une certification SECUCYBER d'HS2 ou CISSP d'(ISC)2.
- Aucune connaissance des systèmes industriels n'est nécessaire.

Méthode pédagogique

- Cours magistral
- Démonstrations
- Exercices de mise en œuvre

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUINDUS par HS2.**

Programme

Introduction à la cybersécurité des systèmes industriels
- Vocabulaire
- Familles de SI industriels
- Bestiaire des équipements
- Particularismes de gestion des SI industriels

Architectures des SI industriels
- Architecture ISA95
- Approches de l'ISA/IEC 62443
- Spécificité des systèmes de sureté
- Accès partenaires
- Réalité du terrain

Protocoles, applications sécurisations possibles
- Grandes familles de protocole industriels
- Exemple de ModBus
- Exemple d'OPC
- Possibilité de détection et filtrage sur les flux industriels

Incidents représentatifs et évolutions
- Principaux incidents SSI ICS publics
- Cadre des SIV LPM
- Industrial IOTs et le cloud industriel

Référentiels sur la sécurité des systèmes d'information industriels
- Guides ANSSI
- Normes IEC 62443 (ISA 99)
    - IEC 62443-2-1
    - IEC 62443-3-3
- NIST SP800-82, NERC CIP, ISO 27019, etc

Sécurisation des SI industriels
- Organisation
- Appréciation des risques
- Cartographie et inventaire
- Intégration et recette de sécurité
- Maintien en condition de sécurité
- Surveillance

Réponse à incident sur un système industriel
- Premières réactions
- Détection et marqueur de compromission
- Analyse forensique d'artefacts industriel
- Préparer sa réponse à incident

Exercices
- Audit technique
    - Analyse de traces réseaux
    - Exploitation de vulnérabilités du protocole Modbus/TCP
- Sécurité organisationnelle et architecturale du réseau industriel
    - Architecture sécurisée
    - Détermination des zones et conduites
    - Points sensibles
    - Sécurisation d'architecture
    - Détermination des niveaux de classification ANSSI
    - Analyse basée sur le guide ANSSI relatif aux réseaux industriels
- Réponse à incident
    - Recherche de compromission du système sur capture réseau
    - Analyse des projets de processus industriels

Formation « Sécurité des objets connectés »

Réf : SECUOBJ

Objectifs

- Fournir suffisamment d'éléments techniques et de langage afin de permettre aux développeurs et aux intégrateurs de solutions communicantes de comprendre l'aspect multi vectoriel de la sécurité des systèmes embarqués avec notamment une approche de défense vis à vis d'une vision attaquante.
- Être en mesure d'évaluer une solution IoT en prenant en compte l'ensemble de la chaine de données, depuis sa production jusqu'à sa consommation. Sur l'ensemble de la formation, le profil type attaquant est un attaquant opportuniste.

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Le profil type ciblé est un industriel (développeur ou intégrateur)

Pré-requis

- Avoir une bonne connaissance générale en environnement linux nécessaire, ainsi que des notions en système.

Méthode pédagogique

- Cours magistral avec échanges interactifs
- Travaux pratiques ayant pour objectif de réaliser un audit global d'une solution IoT en mode matriochka Plusieurs challenges sont imbriqués avec une construction en plusieurs niveaux. Chacun d'entre eux seront étudier tout au long du cours A chaque découverte d'une vulnérabilité, une fiche détail composée d'une description, d'un score (CVSSv3) et d'une recommandation sera réalisée. Les travaux pratiques seront basés sur la plateforme Microbit (https://microbit.org/) et sur les puces STM32 (STM32F103C8T6)

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation est certifiante. L'évaluation de la formation se fera sous la forme d'un Quiz.

Programme

Qu'est-ce que l'Iot ?

- Au cœur de la révolution industrielle et sociétale
- L'environnement IoT
- Cadre légal
- Analyse de risque
- Référentiels (ANSSI / GSMA / GIE / norme ISO / Internationale / NIST / CIS)
- Méthodologie test d'intrusion
  - MITRE ATT&CK ICS
  - PTES
  - OSTMM
  - OWASP

Caractéristiques spécifiques

- Contraintes spécifiques / contraintes d'encombrement
- Microcontrôleur vs CPU
- Notion d'architecture
- Système temps-réel
- Protocoles
- Attaque

Récupération d'information

- Lecture de documentation technique (ex. : DataSheet et cartographie)
- Suivi des pistes physiques (ex.: Gerber)
- Voyage dans le temps (ex. : Gitlog / timemachine)
- Fiches d'identité

Couche matérielle

- Liaison série (Synchrone et Asynchrone)
- Accès au microcode (port débogage / lecture mémoire)
- Accès indirect / Injection de fautes (DMA/DPA)
- Introduction aux radio fréquences (SDR)

Couche microcode

- Rétro-ingénierie ARM (ex. : R2 et Ghidra)
- Exploitation ARM (Emulateur, Debogueur, Montage des partitions de fichiers)
- Développement sécurisé
- Simulation d'une carte “alpha” (version de développement)

Couche concentrateurs

- Passerelles
  - Modèle souscription/publication
  - Modèle ad-hoc
  - Gestion par événements
- Android
  - Architecture
  - Décompilation d'une archive applicative (APK)
  - Interaction avec la pile d'exécution
  - Analyse légale post-incident (Forensic)

Couche Internet

- Terminaison API / fonctions lambda
- Application Web
- Gestion des réseaux d'énergie / villes intelligentes

Défense

- Protection du matériel
- Développement sécurité par construction (Secure design)
- Sécurité périmétrique et surveillance (Parefeu, IDS/IPS, Gestion de journaux VS SIEM)

Formation
« Audit sécurité d'applications mobiles Android et iOS »

Réf : SECUMOBILE

Vous souhaitez acquérir des compétences dans l'audit des applications mobiles Android et iOS ? Ou vous voulez approfondir vos connaissances sur les vulnérabilités propres à ces plateformes ? Ou bien vous souhaitez connaitre la démarche à adopter pour auditer une application mobile ? Cette formation vous permettra de passer en revue les techniques nécessaires pour auditer une application mobile, ainsi que les vulnérabilités les plus courantes sur ce type d'applications.

Objectifs

- Appréhender les problématiques sécurité des applications mobiles
- Savoir effectuer une analyse statique
- Utiliser Frida pour réaliser une analyse dynamique
- Intercepter le trafic d'une application mobile

Durée & horaires

- 3 jours soit 21 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 20 participants

Public visé

- Administrateurs système ou réseau
- Développeurs
- Consultant en sécurité souhaitant acquérir des compétences en audit d'applications mobiles

Pré-requis

- Bonne connaissance en informatique
- Connaissances en réseau (TCP/IP et HTTP) et Linux (savoir utiliser le terminal)
- Connaissances de base en sécurité

Méthode pédagogique

- Cours magistral
- Travaux pratiques

Supports

- Support de cours au format papier en français pour les sessions en présentiel
- Ordinateur portable mis à disposition du stagiaire

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUMOBILE par HS2.**

Programme

Jour 1

iOS

Présentation de l'écosystème iOS

- Architecture iOS et fonctionnalités de sécurité
- OWASP MSTG et MASVS
- Techniques utilisées pour auditer une application
- Jailbreak : histoire, types et évolution
- Mise en place d'un environnement de test
- Signature d'applications
- Présentation de Corellium

Analyse statique d'applications iOS

- Analyse des méta-données liées aux applications
- Déchiffrement d'une application
- Décompilation avec Hopper
  - Travaux Pratiques
    - Automatisation de l'analyse statique avec MobSF
    - Déchiffrement d'une application récupérée de l'AppStore
    - Décompilation et retro-ingénierie d'une application

Android

Présentation de l'écosystème Android

- Architecture d'Android (Composants et Sandboxing)
- Structure et contenu d'un APK
- Présentation de l'Android Manifest
- Mise en place d'un environnement de test
  - Travaux Pratiques : Développement d'une application Android

Analyse statique et modification d'applications Android

- Décompilation d'une application avec JADX
- Analyse statique avec apktool
- Modification d'une application Android avec apktool
- Signature d'une application Android
  - Travaux Pratiques
    - Recherche et identification de secrets au sein d'une application
    - Modification d'une application Android

Jour 2

iOS

Analyse des données d'applications iOS

- Les données sauvegardées par iTunes
  - Travaux Pratiques : Récupération d'informations sensibles à partir d'une sauvegarde
- Les données stockées sur le terminal
  - Travaux Pratiques : Récupération d'informations sensibles / via les journaux

Analyse dynamique d'applications iOS

- Interfaces et implémentations en Objective-C
- Rétro-ingénierie d'une application pour contourner des fonctions de sécurité
  - Travaux Pratiques : Décompilation, retro-ingénierie puis modification en mémoire d'une application avec Frida pour contourner une fonction de sécurité

Android

Analyse dynamique d'applications Android

- Revue des différentes méthodes de stockage de données
  - Shared Preferences
  - Bases de données (SQLite)
  - Stockage interne et externe
  - Travaux Pratiques : Exploitation des faiblesses de chaque méthode
- Comparaison de l'utilisation d'un émulateur ou d'un terminal physique
- Techniques de détection d'un émulateur ou d'un équipement "rooté"
- Revue des contrôles d'accès des composants Android
  - Activities
  - Content Providers
  - Travaux Pratiques : Exploitation des faiblesses de contrôle d'accès
  - Travaux Pratiques : Décompilation, rétro-ingénierie puis modification en mémoire d'une application avec Objection pour contourner une fonction de sécurité

Jour 3

Sécurité des communications des applications iOS
- Interception du trafic réseau
- Fonctionnement et implémentation du Certificate Pinning
- Techniques de contournement du Certificate Pinning
  - Travaux Pratiques
    - Interception de trafic non chiffré
    - Interception de trafic chiffré
    - Contournement du Certificate Pinning

Que faire sans terminal iOS jailbreaké ?
- Analyse des sauvegardes et des journaux
- Interception du trafic réseau
- Side-loading d'application pour embarquer un framework d'analyse (Frida/Cycript/Objection)

Android

Sécurité des communications des applications
- Revue des faiblesses courantes
- Interception du trafic réseau
- Fonctionnement et implémentation du Certificate Pinning
- Techniques de contournement du Certificate Pinning
  - Travaux Pratiques : Inteception de trafic chiffré et contournement du Certificate Pinning

Instrumentation d'applications Android avec Frida
- Présentation de Frida
- Création de scripts Frida pour instrumenter du code Java
- Utilisation de Frida pour instrumenter du code natif
  - Travaux Pratiques : Utilisation de Frida pour contourner des routines de détection de "root"

Formation « Principes et mise en œuvre des PKI »

Réf : SECUPKI

La cybersécurité repose sur une brique de base indispensable : la cryptographie. La cryptographie repose sur des conventions secrètes, des clés secrètes en cryptographie symétrique, des bi-clés : clé privée et clé publique en cryptographie asymétrique. La PKI est ce qui permet de gérer ces clés cryptographiques asymétriques et de leurs certificats. Les PKI sont indispensables à la construction de services de confiance comme la mise en place d'identités numériques, la signature électronique, le chiffrement des échanges, etc.

Objectifs

- Apprendre les technologies et les normes (initiation à la cryptographie)
- Apprendre les différentes architectures et les moyens de les sécuriser
- Comprendre les besoins métier concernant les certificats
- Acquérir les connaissances et compétences nécessaire afin de fournir un support haut-niveau aux métiers
- Apprendre les problématiques d'intégration (organisation d'une PKI, formats de certificats, points d'achoppement)
- Apprendre les aspects organisationnels et certifications
- Apprendre les aspects juridiques (signature électronique, clés de recouvrement, séquestre)

Durée & horaires

- 4 jours soit 28 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Architectes
- Chefs de projets
- Responsable sécurité/RSSI avec une orientation technique
- Développeurs séniors
- Administrateurs système et réseau senior

Pré-requis

- Formation universitaire de base ou Ingénieur en informatique
- Pas de connaissance de la cryptographie ni des certificats requis
- Constitue un plus : utilisation de la ligne de commande, bases de réseau IP
- Connaissance de Windows et de Linux ubuntu souhaitable

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours en français
- Ordinateurs portables et 'tokens' cryptographiques mis à disposition par HS2 pour les exercices
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUPKI par**
- **HS2.**

Programme

Jour 1 : Technique & cryptographie

- Primitives cryptographiques la synthèse
  - Histoire de la cryptographie
  - Mécanismes cryptographiques symétriques et asymétriques, condensé
  - Objectifs de sécurité :
    - Authentification, confidentialité, intégrité
  - Assemblages courants :
    - Signature, MAC message d'authentification, association hybride symétrique & asymétrique, clé de session, vecteur d'initialisation
  - Attaques cryptographiques :
    - De la force brute à la cryptanalyse quantique
  - Attaques « man in the middle », attaques sur la gestion des clés
    - Gestion des clés et des secrets :
    - Conteneur matériel TPM, HSM, Secure Keys
    - Conteneur logiciel cryptoAPI, API cryptoki
    - Recommandations ANSSI/NIST/ECRYPT
  - Le besoin d'une infrastructure à clés publiques

Implémentations techniques de la cryptographie

- Le certificat X509 : objectif, format, limitations et usages
- Intégration de tokens et cartes à puce : PKCS #11, Java JCE, Ms CryptoAPI
- Usages de la cryptographie :
  - Authentification, intégration dans les domaines Windows
  - Réseaux privés virtuels VPN
  - SSL/TLS : principes et attaques
  - Signature électronique : principes, usages et normes
  - Horodatage
  - Chiffrement de messagerie avec S/MIME
  - Chiffrement de disques : BitLocker, EFS

Mise en œuvre des Infrastructures à clés publiques (PKI)

- Architecture et intégration
  - Architecture PKI-X :
    - Autorité de certification racine, Autorité de certification secondaire, Autorité d'enregistrement, Autorité de validation
    - Architectures communes : déclinaisons des rôles, sécurisation
    - Définition d'une politique de certification et d'une politique de sécurité
    - Mise en place du modèle de confiance

        - Mise en œuvre
            - Génération de clés, émission des certificats, liste de révocation
            - Séquestre de clés, Définition de l'agent de récupération des clés
            - Diffusion des clés
        - Répondeurs OCSP, Agrafage OCSP
    - Aspects Organisationnels : Processus clés, contrôles

Mise en œuvre d'une Infrastructures à clés publiques

- Présentation de la PKI EJBCA
- Présentation de Microsoft Active Directory Certificate Services
- Présentation de l'architecture des produits
- Installation et configuration de l'autorité de confiance racine autonome avec le produit EJBCA sous Linux Ubuntu
- Installation et configuration de l'autorité de confiance secondaire avec le produit Microsoft ADCS
- Demande de certificats via le portail EJBCA
- Demande de certificats Microsoft pour un ordinateur via la console MMC
- Gestion de la révocation
- Publication dans l'annuaire Active Directory

Aspects légaux et perspectives

- Aspects juridiques
    - Signature électronique : valeur juridique, cadre...
    - Réglementations d'usage : limitations, escrow (tiers de confiance)

Travaux Pratiques

Les exercices pratiques seront exécutés avec le produit EJBCA sous Linux pour la partie autorité de certification racine autonome et avec Microsoft Active Directory Certificate Services (ADCS) sous Windows 2019 Server pour la partie autorité de certification secondaire.
Les travaux pratiques, les démonstrations, et les vidéos de ce cours vous permettront d'apprendre à déployer une autorité de certification racine, une autorité de certification secondaire, de générer des certificats pour vos serveurs, vos utilisateurs. Vous serez à même de mettre en œuvre la publication et la révocation de vos certificats, de définir une politique de certification et de sécurité.

Formation « Sécurité des serveurs et des applications Web »

Réf : SECUWEB

L'infrastructure Web expose directement votre société aux menaces externe. Renforcez vos défenses en sécurisant efficacement tous les vecteurs exploités par les attaquants !

Objectifs

- **Éduquer vos équipes de développement aux risques et aux enjeux de la sécurité applicative en mettant en application l'ensemble des points clés du standard OWASP**
- **Être en mesure d'augmenter rapidement la qualité et la sécurité de leurs développements de façon pertinente et efficace.**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Personnes ayant un profil technique souhaitant acquérir les connaissances suffisantes pour sécuriser leurs développements Web :**
- **DevSecOps**
- **Programmeurs,**
- **Développeurs**
- **Architectes**
- **Chefs de projet**
- **Consultants cybersécurité**

Pré-requis

- **Expérience en programmation, idéalement en développement Web**
- **Connaissance de base en cybersécurité, par exemple suivi de la formation SECUCYBER est un plus**

Méthode pédagogique

- **Cours magistral illustré par des exercices guidés pas à pas**
- **Résolution de challenges de sécurité réaliste de type Capture The Flag (CTF)**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUWEB par HS2.**

Programme

Introduction aux risques et aux enjeux de la sécurité applicative

- Quelques idées reçues
- La couche applicative – Une surface d'attaque de choix
- Prise en main de l'environnement de travaux pratiques

Rappels sur les technologies web

- Encodages (URL, HTML, Base64)
- HTTP / HTTPS
- Utilisation d'un proxy Web pour intercepter, analyser et modifier les échanges HTTP(S)

Introduction aux techniques d'attaque et aux mécanismes de défense

- Présentation de l'OWASP (guides, outils et TOP 10 de l'OWASP Web)
- Attaques et mécanismes de défense
- Utilisation du scanner de vulnérabilité OWASP ZAP

La phase de reconnaissance utilisée avant d'attaquer une application

- Axes de fuite d'informations techniques
- Utilisation d'outils de "Crawling" et d'outils de collecte d'information

Le mécanisme de gestion de l'authentification (attaque et défense)

- Mécanismes d'authentification les plus rencontrés
- Failles / Attaques qui ciblent le mécanisme d'authentification
- Moyens de défense permettant de sécuriser le mécanisme d'authentification
- "Brute-force" d'un mécanisme d'authentification
- Interception de données en transit (Sniffing)

Le mécanisme de gestion de la session (attaque et défense)

- Rappel autour des sessions
- Failles / Attaques qui ciblent le mécanisme de gestion de la session
- Moyens de défense permettant de sécuriser le mécanisme de gestion de la session
- Exploitation de la faille permettant la fixation de session

Le mécanisme de gestion des autorisations (attaque et défense)

- Droits horizontaux et droits verticaux
- Failles / Attaques qui ciblent le mécanisme de gestion des autorisations
- Attaques de type Cross-Site Request Forgery (CSRF)
- Attaques de type File Inclusion (RFI / LFI) et Path Traversal
- Moyens de défense permettant de sécuriser le mécanisme de gestion des autorisations
- Exploitation d'une faille de type Path Traversal

La gestion des entrées utilisateurs (injection de code)

- Les différents types d'attaques permettant l'injection de code (SQL, HQL, LDAP, commandes, etc.) et le principe général de ce type d'attaque
- Moyens de défense permettant de sécuriser vos entrées utilisateurs
- Exploitation de failles de type Injection SQL manuellement et de façon automatique (via l'utilisation d'un outil)

Les attaques ciblant les autres utilisateurs (attaque de type cross-site)

- Attaques de type Cross-Site Scripting (XSS)
- Le cas des clients riches JavaScript (AngularJS, Backbone, Ember, NodeJS, ReactJS, etc.)
- Moyens de défense permettant de sécuriser la navigation de vos utilisateurs et de se protéger contre l'injection de code HTML / JavaScript
- Mise en œuvre de différents scénarios d'attaques reposant sur l'exploitation d'une faille de type Cross-Site Scripting (modification de l'affichage, vol de session, redirection arbitraire, etc.)

Sécurité de la journalisation, de la gestion des erreurs et des exceptions

- Principe et enjeux de la journalisation des évènements de sécurité
- Stockage d'informations sensibles dans les journaux et attaques de type injection de "logs"
- Principe et enjeux de la gestion des erreurs et des exceptions
- Axes de prévention et bonnes pratiques dans le domaine

Sécurité des services web (Front end JavaScript, API SOAP & REST)

- Front-end à base de clients riches JavaScript
- Les failles des clients riches JavaScript
- Services Web SOAP et REST
- Failles des Services Web SOAP et des Services REST
- Axes de prévention et bonnes pratiques dans le domaine

Formation « Sécurisation des infrastructures Windows »

Réf : SECUWIN

Système d'exploitation le plus utilisé dans l'entreprise et au dehors, et sans aucun doute l'un des plus attaqués, Windows est un composant incontournable de la majorité des systèmes d'information. Ancien "mauvais élève" de la sécurité, Microsoft a depuis quelques années mis la sécurité au centre de sa stratégie, avec pour résultat une grande diversité de mesures, parfois mal connues ou sous-utilisées, et de vraies avancées technologiques.

En vous apportant la maitrise de ces mécanismes de sécurité et la connaissance des techniques d'attaques usuelles, cette formation vous donnera les moyens de sécuriser et d'auditer votre infrastructure Windows avec un maximum d'efficacité.

Objectifs

- **Durcir un serveur Windows**
- **Administrer de façon sécurisée**
- **Sécuriser vos postes de travail**
- **Auditer votre infrastructure**

Durée & horaires

- **5 jours soit 40 heures**
- **Du lundi au jeudi : de 9h00 à 12h et de 13h30 à 19h00.**
- **Le vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Administrateurs**
- **Architectes**
- **Experts en sécurité**
- **Responsables sécurité**

Pré-requis

- **Formation SECUCYBER**
- **(ou) Expérience d'administration d'infrastructure Windows**
- **(ou) Solides bases en sécurité des systèmes d'information**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUWIN par HS2.**

Programme

Introduction

Module 1 : Durcissement système et réseau

- Système
  - Nécessité du durcissement
  - Minimisation
  - Gestion des services
  - Journalisation
- Réseau
  - Utilité des protocoles obsolètes
  - Cloisonnement réseau
    - Parefeu et IPsec
  - Protocoles d'authentification
  - Autres points d'attention
- Desired State Configuration
- Focus : sécuriser votre cloud Microsoft

Module 2 : Administration sécurisée

- Qu'est-ce qu'un administrateur
- Administration sécurisée : pourquoi ?
  - TTP : Techniques, Tactiques et Procédures
  - Compromettre un Active Directory
    - Compromission initiale
    - Mouvement latéral : Pass-the-hash...
    - Élévation de privilèges
  - Vulnérabilités classiques
- Bonnes pratiques
  - Utilisateurs et groupes locaux
  - Délégation
    - Powershell et le JEA
    - Active Directory et les GPO
- Administration sécurisée
  - Forêt "bastion"
  - Administration en strates
    - Silos d'authentification
  - Environnement d'administration
- Focus : Golden Ticket et krbtgt

Module 3 : Sécurité du poste de travail

- Windows 10 et le VBS
  - Secure Boot
  - Device Guard
  - Application Guard
  - Exploit Guard
  - Credential Guard
- Bitlocker
  - Chiffrement de disque
  - Autres fonctionnalités
- Isolation réseau
- Mise à jour

Module 4 : Auditer son infrastructure

- Différents types d'audits
- Points à auditer
- SCM
- Pingcastle
- Recherche de chemins d'attaque
  - BloodHound et AD-Control-Path
  - Les extracteurs
  - Graphes d'attaques
  - Simulation et remédiation
- Examen

Formation « Sécurité Linux »

Réf : SECULIN

Linux est le socle des infrastructures de l'internet, de l'informatique en nuage, comme des systèmes embarqués. Son durcissement et son maintien en condition de sécurité sont au cœur de la réussite de sa politique de sécurité.

Objectifs

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Réduire ou éliminer les risques sur les systèmes Linux
- Configurer les services courant pour qu'ils soient robustes avant mise en production (Apache, BIND, ...)
- S'assurer de l'intégrité des données sur les serveurs Linux
- Maîtriser les outils permettant de répondre aux incidents de sécurité
- Améliorer ses connaissances des procédures, bonnes pratiques et outils de sécurité du monde Unix

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Professionnels de la sécurité
- Administrateurs systèmes expérimentés
- Auditeurs et gestionnaires d'incidents
- Analystes en sécurité, auditeurs et membres de CSIRT (CERT)

Pré-requis

- Formation SECUCYBER ou solides bases en sécurité des systèmes d'information
- Être administrateur de systèmes Unix/Linux depuis plus de 3 ans, par exemple avoir les certifications LPIC-1 et LPIC-2 ou Red Hat RHCSA

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECULIN par HS2.**

Programme

Introduction

- Panorama de l'histoire des problèmes de sécurité
  - Suivre l'actualité
  - Implication des utilisateurs
  - Discipline des administrateurs
    - Sudo

Cryptographie

- Rappels sur le vocabulaire, les principes et les algorithmes
- SSH
- GnuPG
- Certificats X.509 et infrastructures à clés publiques
  - openssl
- Certificats X.509 pour le chiffrement, la signature et l'authentification
  - application à Apache et nginx
  - application à Postfix
- Systèmes de fichiers chiffrés
  - dm-crypt
  - eCryptfs
- DNS et cryptographie
  - DNSSEC

Sécurité de l'hôte

- Durcissement de l'hôte
  - configuration de GRUB
  - configuration du système
  - bonnes pratiques de configuration des daemons
  - Détection d'intrusion sur l'hôte
  - Syslog
  - comptabilité système (accounting)
  - audit
  - détection de rootkits
  - AIDE
- Gestion des utilisateurs et authentification
  - NSS
  - PAM

Contrôle d'accès

- Contrôle d'accès discrétionnaire
  - droits d'accès
  - ACL
- Contrôle d'accès obligatoire
  - SELinux

Sécurité réseau

- Durcissement du réseau
  - nmap
  - tcpdump
  - Wireshark
- Filtrage de paquets
  - concepts et vocabulaire
  - netfilter
  - TCP Wrapper
- Réseaux privés virtuels
  - OpenVPN

Examen de certification HS2 (QCM sur ordinateur)

Formation « Comprendre SELinux et savoir modifier la politique de sécurité »

Réf : SELinux

SELinux vise à renforcer la sécurité d'un système Linux en mettant en œuvre une politique de contrôle d'accès obligatoire. SELinux est intégré en standard au noyau Linux depuis 2003 et certaines distributions (Fedora depuis 2004, Red Hat Enterprise Linux et CentOS depuis 2005) l'activent par défaut.

On constate en pratique que beaucoup d'administrateurs de systèmes Linux sur lesquels SELinux est activé par défaut le désactivent parce qu'ils ne comprennent pas son fonctionnement et que SELinux les empêche de travailler. S'il est gênant pour les administrateurs, il est également gênant pour les intrus et c'est son intérêt.

Objectifs

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Comprendre les mécanismes du fonctionnement de SELinux
- Analyser les problèmes pratiques liés à SELinux
- Savoir adapter les contextes de sécurité des fichiers et les booléens
- Savoir personnaliser la politique de sécurité

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Professionnels de la sécurité
- Administrateurs systèmes expérimentés
- Auditeurs et gestionnaires d'incidents
- Analystes en sécurité, auditeurs et membres de CSIRT (CERT)

Pré-requis

- Avoir les bases en administration de systèmes Unix, idéalement 3 à 5 ans d'expérience

Méthode pédagogique

- Cours magistral avec exercices pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Introduction

- Contexte de sécurité
- L'option `-Z` (ou `--context`)
- Mise en évidence des problèmes pratiques posés par SELinux
- États de fonctionnement
- La commande `sestatus`
- Les commandes `getenforce` et `setenforce`
- La commande `selinuxenabled`

Les booléens SELinux

- La commande `getsebool`
- La commande `setsebool`

Gestion de la politique de sécurité

- La commande `setfiles`
- La commande `restorecon`
- La commande `fixfiles`
- La commande `chcon`
- La commande `newrole`
- La commande `runcon`
- La commande `seinfo`
- La commande `semanage`
- La commande `apol`
- Les commandes `audit2why` et `audit2allow`

Modification de la politique de sécurité

- Types de fichiers permettant d'étendre la politique de sécurité
- Procédure d'extension de la politique de sécurité
- Exemple de module simple
- Exemple de module de politique
- Cas pratiques

Formation « Sécurité des Architectures »

Réf : SECUARCH

Vous vous demandez pourquoi ne pas laisser votre infrastructure reposer sur un réseau à plat ? Vous désirez migrer votre architecture dans le cloud ? Vous cherchez comment déployer une infrastructure de supervision de manière propre ? Répondez à ces questions et bien d'autres en (ré)apprenant les composants de base d'une architecture réseau complexe, les risques associés aux mises en œuvre courantes et le déploiement de certaines architectures spécifiques. Découvrez les moyens de réduire ces risques ainsi que les points d'attention à prendre en compte lors de chaque décision d'évolution de votre architecture.

Objectifs

- Connaître les problématiques liées à l'architecture des réseaux complexes
- Connaître les solutions associées
- Savoir auditer une architecture
- Développer un plan d'évolution sécurisée d'une architecture

Durée & horaires

- 5 jours soit 35 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Architectes réseaux
- Administrateurs systèmes et réseaux
- Consultants en sécurité
- Auditeurs en sécurité
- RSSI

Pré-requis

- Bonnes connaissances en informatique et connaissances de base en sécurité, par exemple une certification SECUCYBER d'HS2 ou GSEC de GIAC ou CISSP d'(ISC)2 ou équivalent.
- Très bonnes connaissances en réseaux (VLAN, pare-feux, etc), par exemple une certification CCNA+CCNP de Cisco ou NSE4 de Forninet ou CCSA de Checkpoint ou CSNA de Stormshield ou équivalent.

Méthode pédagogique

- Cours magistral
- Démonstrations
- Exercices de mise en œuvre

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUARCH par HS2.**

Programme

Introduction générale

- Logistique
- Tour de table
- Objectifs de la formation
- Non-objectifs de la formation
- Signalétique

Introduction de la formation

- Principes d'architecture
  - Exposition
  - Connectivité
  - Attractivité
- Vocabulaire
  - Segmentation / risque / persona
- Lien avec d'autres domaines
  - Administration
  - Urbanisation
  - Gestion des risques
- Dessine-moi un schéma d'architecture

Notions de réseaux

- Modèles théoriques
- Quiz introductif
- Couche 2 - Liaison
  - Domaine de collision / domaine de diffusion
  - Composants de base et adressage
  - Segmentation - LAN / VLAN / PVLAN
  - Sécuriser le lien local
- Couche 3 - Réseau
  - Composants de base et adressage
  - Segmentation
- Échanges d'informations
- Composants spécifiques
  - Diode / WDM / sonde

Flux

- Filtrage
- Modes de connexion
- Chiffrement
- Authentification

Architecture de base : risques, points d'attention, contraintes et solutions

- Notion de bulle et niveaux : tiers-{0,2}
- Séparation des environnements
  - Production vs. hors-production
- Authentification et autorisation
- Administration
  - Zones d'administration
  - Spécificités de Windows et Active
  - Postes d'administration
- Composants d'infrastructure et de sécurité
  - Services d'infrastructure
  - Cas pratiques : DNS / supervision / sauvegarde / accès Internet / VPN
- Applications, 2-tiers / 3-tiers
- Continuité
  - Redondance et haute disponibilité
  - Dépendance circulaire

Architectures spécifiques

- Virtualisation de l'infrastructure
- Cloud
- Sous-traitants
- Architectures industrielles & SCADA
- Gestion technique des bâtiments
- Divers
  - ToIP / Wi-Fi / Grid / virtualisation et infrastructures "agiles" / IoT

Formation « Red Team – Sans-fil »

Réf : REDTEAM

L'apparition de nouvelles technologies permettant d'automatiser les contrôles d'accès nécessitent aujourd'hui de nouvelles techniques en plus du social engineering et des techniques de crochetage, afin de s'infiltrer dans un bâtiment de manière discrète.

Pour cela, nous avons programmer ce cours, permettant de montrer différentes attaques actuelles visant à gagner des accès physiques en s'attaquant des technologies telles que : le RFID, Bluetooth LE (avec les serrures connectées, etc.), nRF utilisés dans les claviers/souris et Sub-GHz (alarmes, portes de garage, clés voiture, etc.).

L'objectif de ce cours est de montrer des techniques efficaces et rapides afin de réaliser des tests d'intrusions, mais aussi de montrer les aspects à sécuriser afin d'éviter certains scénarios à une entreprise qui pourrait être la cible de ces attaques.

Objectifs

- Evaluer et identifier les points faibles des systèmes de contrôles d'accès sans-fil
- Exploiter ces faiblesses afin de réaliser un Red Team de manière efficace
- Faire les bons choix technologiques pour une entreprise

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne intéressée par la compréhension de la sécurité Wi-Fi dans sa globalité.
- Auditeurs en sécurité
- Consultants en sécurité
- RSSI avec profil très technique
- Développeur de produits de sécurité employant du sans-fil
- Serruriers

Pré-requis

- Connaissances en administration Linux
- Bases en sécurité informatique
- Traiter des données sous formes binaires, hexadécimales, etc.
- Optionnellement quelques bases en sécurité hardware, qui peuvent être très complémentaires

Méthode pédagogique

- Cours magistral et rappels (environ 30%)
- Démonstrations et exercices pratiques (environ 70%)

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

RFID

- Introduction
- Outils dédiés et démonstrations
- Identification de badge LF et cas
- Attaques sur les différents badges LF (HID, EMx, etc.)
- Identification de badges HF et différents cas
- Attaques sur les badges HF courants (MIFARE Classic/Ultralight/DESFire, iClass etc.)
- Exercices sur des cas courants (tag hôtel, accès aux bâtiments, etc.)
- Les différents types de cartes « magiques » et cas d'utilisation
- Introduction à des outils plus poussés dans la recherche de vulnérabilités comme le HydraNFC

Bluetooth LE

- Introduction
- Monitorer les communications
- Outils existants
- Clonage de beacons
- Attaques Man-In-The-Middle
- Injection de trames
- Attaques sur les connexions sécurisées

nRF

- Introduction
- Analyse de la communication radio brute
- Monitoring des communications avec des outils dédiés
- Transformer un dongle de souris/clavier en implant RuberDucky à distance et en locale

Liaisons sub-GHz

- Introduction
- Identification de signal et analyse en radio-logicielle et comparaisons avec d'autres outils
- Attaque sur des communications non-sécurisées
- Analyse de communications sécurisés et défis techniques
- Attaques de communications sécurisées avec du Rolling/Hopping code
- Attaques opportunistes sur des technologies sécurisés et défauts d'implémentation

Formation « OSINT »

Réf : OSINT

Objectifs

- Réaliser des recherches avancées en source ouverte
- Rédiger des fiches opérationnelles du mode opératoire de l'attaquant
- Lier des identifiants à une ou des personnes physiques
- Mettre en place une stratégie de veille afin de suivre des attaquants ou de protéger une entreprise

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Analyste SOC
- Enquêteur
- Analyste Threat Intel (CTI)
- Pentesteur

Pré-requis

- Cette formation n'impose pas de prérequis particulier. La maîtrise des outils informatiques de base est nécessaire.
- Avoir une connexion internet

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Immersion dans le rôle d'un enquêteur suite à une compromission
- Apprentissage par application concrète tout en laissant une grande autonomie dans la démarche d'investigation

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification OSINT1 par HS2.

Programme

Jour 1

- Méthodologie d'enquête (timeline, prise de note)
- Relevé d'Indice de Compromission (IoC)
- Pivot vers de nouveaux IoCs
- Recherche avancée : expression régulière (regexp)

Jour 2

- Moteur de recherche DeepWeb
- Dorking
- Cartographie réseau
- Renseignement sur protocoles variés (hors Web)
- Exploitation des métadonnées fichiers et protocoles

Jour 3

- Recherche et analyse de code
- Reverse image
- Utilisation outil open-source
- Reconnaissance réseau
- Outil d'investigation d'adresse courriel
- Cartographie d'information

Formation « Détection et réponse aux incidents de sécurité »

Réf : SECUBLUE1

Les rapports de tous les grands acteurs de la réponse à incident sont unanimes : les compromissions, qu'elles soient l'œuvre de simples malwares ou de groupes organisés, sont légions, avec bien souvent un délai effarant de plusieurs mois entre l'arrivée de l'acteur malveillant et sa détection par les défenseurs. Dans ce contexte, la question n'est plus de savoir si cela peut nous arriver, mais bien QUAND cela va-t-il nous arriver ; L'enjeu n'est plus seulement de prévenir, mais d'aller traquer l'attaquant sur nos systèmes et réseaux afin de l'empêcher d'étendre son emprise et d'atteindre ses objectifs.

En mettant l'accent sur la compréhension des techniques d'attaque et la maitrise des outils de détection, cette formation vous donnera les moyens de tirer le meilleur parti des mesures et équipements déjà en place pour répondre rapidement et efficacement aux incidents de sécurité.

Objectifs

- **Mettre en place une architecture de détection**
- **Appliquer la notion de "prévention détective"**
- **Limiter l'impact d'une compromission**
- **Prioriser les mesures de surveillance à implémenter**
- **Maitriser le processus de réponse à incident**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Membres d'un SOC ou d'un CSIRT**
- **Administrateurs**
- **Responsables sécurité**

Pré-requis

- **Formation SECUCYBER**
- **(ou) Solides bases en sécurité des systèmes d'information**

Méthode pédagogique

- **Cours magistral avec travaux pratiques et échanges interactifs**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUBLUE par HS2.**

Programme

Module 1 : État des lieux

- Pourquoi la détection
  - Défense en profondeur
  - Tous compromis
- Renseignement sur la menace
  - CTI et renseignement
  - Cyber Kill Chain
  - MITRE ATT&CK / SHIELD
- Principes de défense

Module 2 : Comprendre l'attaque

- Objectifs de l'attaquant
- Phases d'une attaque
- Différents champs de bataille
  - Réseau
  - Systèmes d'exploitation Applications
  - Active Directory
  - Cloud

Module 3 : Mettre en place notre architecture de détection

- Détection : les classiques
  - SIEM
  - IDS/IPS, WAF, CASB
  - SandBox, Capture réseau
  - Honeypots et autres Honey-*
- Valoriser les "endpoints"
  - Parefeu, antivirus
  - Whitelisting: Application Control, AppLocker
  - Sysmon
  - AppArmor, SELinux
- Journalisation
  - Windows : configuration, choix des événements, Powershell
  - Linux : auditd
  - Centralisation: WEF, syslog-NG...
  - Focus : Journalisation
- Bonus : Données DNS

Module 4 : Détecter les différentes phases d'une attaque

- Outils & techniques
  - Wireshark/Tshark, Bro/Zeek
  - Recherche d'entropie
- Reconnaissance
  - Fuites d'information
  - scans réseau et applicatifs
- Exploitation
  - Man-in-the-Middle : ARP spoofing, Rogue DHCP...
  - Protocoles obsolètes & Responder
  - Kerberoas
  - Attaques mémoire
  - Attaques web : WAF et "Self-defense" applicative
- Mouvement latéral
  - Exécution de commandes distantes
  - Pass-The-Hash / Pass-the-Ticket
  - Attaques Powershell
- Élévation de privilège
  - Vol de secrets : Mimikatz, Impacket...
  - Recherche de chemins d'attaque : Bloodhound / SharpHound
- Persistance
  - Persistance Linux et Windows
  - Golden Ticket, Silver Ticket, SID History...
- Exfiltration et C&C
  - Tunnelling: ICMP, DNS...
  - C&C HTTP/HTTPS

Module 5 : Réponse à incident et Hunting

- SOC & CSIRT
- Triage
- Analyse de binaires
- Recherche d'IOC, Yara
- Outils de réponse : Kansa, GRR, DFIR-ORC...
- Remédiation Linux & Windows
- Partons à la chasse : Hunting

Formation « Détection et réponse aux incidents de sécurité avancée »

Réf : SECUBLUE2

Objectifs

- Enrichir une infrastructure de détection en place
- Appliquer la notion de "prévention détective"
- Identifier des chemins de compromissions potentielles
- Traiter une réponse à incident impliquant un nombre important de machine
- Mettre en œuvre des mesures de recherche de compromission

Durée & horaires

- 4 jours soit 28 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Membres d'un SOC ou d'un CSIRT
- Administrateurs
- Responsables sécurité
- Concepteur / architecte de supervision

Pré-requis

- Avoir suivi la formation SECUBLUE1
- (ou) Solide expérience dans un SOC ou un CSIRT

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours en français au format papier en présentiel et au format numérique en distanciel
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUBLUE2 par HS2.

Programme

Détection réseau (1 journée)

- Configuration du pare-feu local pour la détection d'activité malveillante
- Recherche de canaux de communication avec l'infrastructure de l'attaquant (beaconing et exfiltration)

Détection système (0,5 journée)

- Détection des persistances
- Exploitation des quarantaines des anti-virus
- Détection d'exfiltration par USB (scénario DLP)

Chemins de contrôle Active Directory (0,5 journée)

- Détection de la collecte des informations
- Recherche d'événement typique d'une exploitation de chemins de contrôle

Réponse à incident (1,5 journée)

- Utilisation de l'outil de collecte DFIR-ORC (configuration et déploiement)
- Analyse des résultats de la collecte unitaire
- Recherche à large parc

Formation « Détection des incidents de sécurité »

Réf : SECUSOC

Tous les attaquants laissent des traces ! Le SOC est la brique indispensable pour les détecter et limiter les impacts d'une compromission. Détecter est impératif face au niveau de menace actuel et ce sont l'efficacité des analystes et l'intelligence des règles qui font la différence. Vous disposez d'un SOC, ce SOC dispose d'une vision unique sur le Si grâce aux sources d'information qu'il collecte, il est en première ligne pour détecter. De nouvelles techniques de recherche d'attaquant, dont la chasse aux menaces (hunting), doivent également être mis en place pour être proactif vis à vis des nouvelles techniques et outils d'attaque.

Objectifs

- **Former les analystes SOC à la détection et aux spécificités de la détection système, en abordant les aspects méthodologiques, théoriques et pratiques de la création d'alertes et de leur investigation, en s'appuyant principalement sur l'environnement Windows.Appliquer la notion de "prévention détective"**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Analystes SOC N2 et N3**

Pré-requis

- **Avoir de bonnes bases en cybersécurité ou avoir suivi la formation SECUCYBER**
- **Connaissance d'un SIEM (ELK, Logpoint, Prelude, Qradar, Splunk, etc) ou avoir suivi une formation SPLUNK ou ELASTICSEARCH**
- **Avoir un SOC dans son organisation**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques à chaque module**

Supports

- **Support de cours en français au format papier en présentiel et au format numérique en distanciel**
- **Machine virtuelle contenant l'ensemble des exercices**
- **Ordinateur portable mis à disposition des stagiaires qui ne disposerait pas du leur**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM de savoir-faire, pas un simple test de connaissance, dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUSOC par HS2.**

Programme

Panorama de la détection système

- Chaîne de détection et terminologie
- Organisation des équipes
- Sources de données
- Quoi collecter ?
- Normalisation et standardisation des données
- Connaissance du SI supervisé et des pratiques d'administration
- Cycle de vie des signatures
- Tableaux de bord
- Environnement, contexte de détection, interaction avec les autres acteurs de la sécurité opérationnelle

Méthodologies

- Kill chain / Mitre attack
- "Pyramide of pain" et détection de menace connue vs inconnue
- Démarche de création et de hiérarchisation des nouvelles alertes
- Compréhension des apports de l'apprentissage automatique (machine learning)
  - Notions clés
  - Comment travailler avec les experts en mégadonnées (data scientists)

Techniques de détection pour Windows

- Détection grâce aux journaux d'authentification :
  - ActiveDirectory, Kerberos, NTLM, lsass, ntds, sam
  - Moyens de détection des outils et techniques de vol d'authentifiant dont mimikatz
- Techniques d'attaque et de détection Powershell
- Pré-requis et création de règles Sysmon
- Détection des techniques de latéralisation : RDP, SMB, PSRemoting, WMI
- Détection de la persistance : création de services, tâches planifiées, clés de registres, dossiers startup
- Repérage des traces générées par les outils communément utilisés par les attaquants : Cobalt Strike, Empire, Lolbins
- Fonctionnement et détection des élévations de privilège : SID, Niveau d'intégrité, token
- Détection en amont la reconnaissance faite par l'attaquant au sein du SI : adfind, bloodhoud, LOLBins

Techniques de détection de compromission d'autres environnements

- Linux : auditd, wazuh, ossec
- Réseau : scans, flux, beaconning, trafic HTTP/HTTPS sortant, trafic DNS
- Infonuagique (Cloud) : API et services
- OT (systèmes industriels, objets connectés)

Processus métier des analystes

- Processus d'investigation d'une alerte
- Processus de chasse (hunting)
- SOAR (ochestration, automatisation et réponse aux incidents de sécurité)

Examen de certification

Formation « Analyse inforensique Windows »

Réf : FORENSIC1

Les raisons ne manquent pas de vouloir effectuer une analyse inforensique :

- **Collaborateur indélicat ayant volé des documents interne de valeur**
- **Intrusion d'un poste suite à une erreur d'un utilisateur**
- **Compromission d'un serveur**

Quelle que soit la raison, FORENSIC 1 vous apprendra à analyser les différents artefacts inforensiques et finalement créer une frise chronologique de l'incident.

Objectifs

- **Gérer une investigation numérique sur un ordinateur Windows**
- **Avoir les bases de l'analyse numérique sur un serveur Web**
- **Acquérir les médias contenant l'information**
- **Trier les informations pertinentes et les analyser**
- **Utiliser les logiciels d'investigation numérique**
- **Maîtriser le processus de réponse à incident**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Personnes souhaitant apprendre à réaliser des investigations numériques**
- **Personnes souhaitant se lancer dans l'inforensique**
- **Administrateurs système Windows**
- **Experts de justice en informatique**

Pré-requis

- **Formation SECUCYBER**
- **(ou) Solides bases en sécurité des systèmes d'information**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Clé USB 64Go avec les données utilisées en travaux pratiques**
- **Kit d'investigation numérique**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC1 par HS2.**

Programme

Jour 1

- Présentation de l'inforensique
- Périmètre de l'investigation
- Trousse à outil
- Méthodologie "First Responder"
- Analyse Post-mortem
- Disques durs
- Introduction aux systèmes de fichiers
- Horodatages des fichiers
- Acquisition des données : Persistante et volatile
- Gestion des supports chiffrés
- Recherche de données supprimées
- Sauvegardes et Volume Shadow Copies
- Aléas du stockage flash
- Registres Windows
- Les structures de registres Windows
  - Utilisateurs
  - Systèmes
- Analyse des journaux
- Évènements / antivirus / autres logiciels

Jour 2 - Scénario d'investigation

- Téléchargement/Accès à des contenus confidentiels
- Exécution de programmes
- Traces de manipulation de fichiers et de dossiers
- Fichiers supprimés et espace non alloué
- Carving
- Géolocalisation
- Photographies (données Exifs)
- Points d'accès WiFi
- HTML5
- Exfiltration d'informations
- Périphérique USB
- Courriels
- Journaux SMTP
  - Acquisition coté serveur
  - Analyse client messagerie
- Utilisateurs abusés par des logiciels malveillants

Jour 3 - Interaction sur Internet

- Utilisation des Navigateurs Internet
- IE/Edge / Firefox
- Office 365
- Sharepoint
- Traces sur les AD Windows
- Présentation des principaux artefacts
- Bases de l'analyse de la RAM
  - Conversion des hyberfiles.sys
  - Bases Volatility/Rekall
  - Extraction des clés de chiffrement

Jour 4 - Inforensique Linux

- Les bases de l'inforensique sur un poste de travail Linux"
- Les bases de l'inforensique sur un serveur Linux
  - Journaux serveurs Web & Corrélations avec le système de gestion de fichiers
- Création et analyse d'une frise chronologique du système de fichier

Jour 5 - Vue d'ensemble

- Création et analyse d'une frise chronologique enrichie d'artefacts
- Exemple d'outil d'interrogation de gros volume de données
- Examen de certification HS2 (QCM sur ordinateur)

Formation « Analyse inforensique avancée »

Réf : FORENSIC2

La vraisemblance que votre entreprise ou que vos clients soient la victime d'une intrusion est importante. L'objectif de la formation est alors de vous préparer au mieux en vous présentant des techniques et des outils permettant de répondre à un incident de sécurité (du simple prestataire malveillant à des attaques plus complexes). L'ensemble de la formation sera réalisé autours d'un cas fictif d'une compromission d'une entreprise de taille intermédiaire afin de présenter les procédures et techniques à mettre en place permettant d'être scalable en fonction de la taille de votre entreprise.

Objectifs

- Appréhender la corrélation des évènements
- Retro-concevoir des protocoles de communications
- Analyser des systèmes de fichiers corrompus
- Connaître et analyser la mémoire volatile des systèmes d'exploitation

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Investigateurs numériques souhaitant progresser
- Analystes des SOC et CSIRT (CERT)
- Administrateurs système, réseau et sécurité
- Experts de justice en informatique

Pré-requis

- Avoir une bonne expérience opérationnelle en informatique
- Avoir une expérience en analyse post-mortem sous Windows et maitriser le processus d'investigation sur un poste Windows
- Ou avoir réussi la certification HS2 INFORENSIC1 ou la certification HSC INFO1 ou la certification CEH CHFI ou une des certifications GIAC GCFA ou GCFE

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Clé USB 64Go avec les données utilisées en travaux pratiques
- Certificat attestant de la participation à la formation

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC2 par HS2.**

Programme

Section 1 : Introduction à l'inforensique réseau

- Incident de sécurité
  - Présentation
    - Quels sont les étapes d'une intrusion ?
    - Quels impacts de celles-ci ?
- Indices de compromission (IOC)
  - Introduction au threat intel (Misp, Yeti, etc.)
  - Quels sont les outils / ressource à disposition ?
  - Création d'IOC
- Hunting & Triage (à distance ou en local)
  - GRR
  - Kansa
  - OS Query
  - Comment analyser et automatiser l'analyse du résultat de notre hunting ?
    - NSRLDB
    - Packing/Entropie/, etc…

Section 2 : Analyse post-mortem réseau

- Analyse des journaux des principaux services réseau (DNS, HTTP, SGBD, Pare-feux, Syslog)
- Analyse de capture réseau (PCAP)
- Analyse statistique des flux (Netflow)
- Canaux de communications avec les serveurs de Command and Control
- Détection des canaux de communications cachées (ICMP, DNS)
- Détection des techniques de reconnaissances
- Création de signatures réseaux

Section 3 : Mémoire volatile

- Introduction aux principales structures mémoires
- Analyse des processus
  - Processus "cachés"
  - Traces d'injection de code et techniques utilisées
  - Process-Hollowing
- Shellcode - détection et analyse du fonctionnement
- Handles
- Communications réseaux
- Kernel : SSDT, IDT, Memory Pool
- Utilisation de Windbg
  - Création de mini-dump
  - Analyse "live" d'un système

Section 4 : FileSystem (NTFS only)

- Introduction au FS NTFS et aux différents artefacts disponibles
- Présentation de la timerules sous Windows/Linux/OSX
- Timeline filesystem
  - Timestomping + toutes les opérations pouvant entravers une timeline "only fs"

Section 5 : Trace d'exécution et mouvement latéraux

- Trace de persistances
  - Autostart (Linux/Windows/OSX)
  - Services
  - Tâches planifiées
  - WMI
- Active Directory - Détecter une compromission
  - Comment générer une timeline des objets AD ?
  - Recherche de "backdoor" dans un AD (bta, autres outils, ...)
  - Présentation des principaux EventID et relations avec les outils d'attaques (golden ticket, etc.)

Section 6 : Super-Timeline

- Présentation
  - Cas d'utilisations
    - Timesketch

Section 7 : Quiz de fin de formation

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « Rétroingénierie de logiciels malfaisants »

Réf : REVERSE1

Comprendre le fonctionnement des logiciels malveillants est un élément clé nécessaire auprès des entreprises afin de pouvoir répondre de manière plus efficiente à vos incidents de sécurités. L'objectif de cette information est de fournir les éléments clés permettant de comprendre le fonctionnement des logiciels afin de pouvoir créer des "Indicateurs de Compromission" ainsi que des signatures permettant de détecter des versions modifiées des outils malveillants afin de détecter les mises à jour de ceux-ci sans avoir besoin de mettre à jours vos signatures. La formation vous permettra alors de pouvoir analyser tout type de menace, du client lourd à l'application "Flash" en passant par les documents malicieux (office, PDF) en passant par les sites web malveillants et les applications mobiles.

Objectifs

- Qualifier la menace d'un logiciel malfaisant
- Savoir mettre en place d'un laboratoire d'analyse des logiciels malfaisants et préparer l'outillage d'analyse
- Analyser de manière statique et dynamique le comportement de logiciels malfaisants
- Apprendre l'architecture x86
- Savoir identifier les structures logiques (boucles, branchement...)
- Savoir identifier des motifs utilisés par les logiciels malfaisants en analysant le code
- Analyser la mémoire
- Savoir contourner les techniques d'autoprotection

Durée & horaires

- 5 jours soit 35 heures
- Horaires : de 9h30 à 12h et de 13h30 à 18h00/18h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Membres d'un SOC ou d'un CSIRT
- Équipes de réponse aux incidents
- Toute personne souhaitant réaliser des analyses avancées des menaces
- Toute personne intéressée par l'analyse des logiciels malfaisants
- Professionnel de la sécurité souhaitant acquérir des connaissances en analyse de codes malfaisants
- Analystes
- Responsables sécurité

Pré-requis

- Connaître le système Windows
- Savoir programmer
- Avoir les bases en réseau
- Connaître l'assembleur

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC2 par HS2.**

Programme

Section 1 : Introduction aux bases de l'analyse de logiciels malveillants

- Processus et méthodologie générique
- Analyse statique :
  - Analyse des métadonnées
  - Analyse statique
- Analyse dynamique
  - Comportemental
  - Débugger
- Construire son laboratoire d'analyse
  - Simuler internet
  - Utilisation de la virtualisation
    - Contournement des mécanismes de protection anti-VM
    - Simulation d'architecture "exotique" (IOT)
    - Construction du laboratoire et boite à outils
  - Sandbox

Cas d'analyse

- Introduction au langage assembleur
  - Guide de survie des instructions de bases
  - Instruction modifiant le flux d'exécution
  - Présentation des registres
- Conventions d'appels
  - Spécificités des langages objets
- IDA Pro:
  - Introduction
  - Prise en main de l'outil (création de scripts)
- Chaine de compilation et binaires
  - Fuite d'informations possibles
  - Imports d'information dans IDA

Section 2 : Système d'exploitation

- Introduction aux systèmes d'exploitation
  - Processus vs thread
  - Scheduler
  - Syscall
  - Différence processus vs thread
- Format d'exécutable
  - Format PE
    - Présentation des informations
- Structures internes
  - SEH
  - TEB
  - PEB
  - SSDT
- Introduction au "kernel debugging"

Section 3 : Mécanismes de protection (DRM ou packer)

- Introduction aux outils de DRM/Protection de code
  - Comment les identifier ?
    - Quels sont les impacts ?

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

- -- Introductions aux différentes techniques de protection :
  - Anti-désassemblage
  - Anti-debogage
  - Obscurcissement du CFG
  - Machine virtuelle
  - Évasion (détection de sandbox/Virtualisation)
- Analyse de packer
  - Présentation de la méthode générique d'unpacking
  - Découverte de l'OEP
  - Reconstruction de la table d'imports
    - Miasm2 :
      - Unpacking automatique

Section 4 : Malwares

- Catégoriser les logiciels malveillants en fonction de leurs API
- Keyloggers
- Rootkits (userland et kerneland)
- Sniffers
- Ransomwares
- Bots et C2
- Injection de code
  - Technique de contournement de flux d'exécution (ie: detour)
- Shellcode
  - Techniques et outils d'analyses
  - Miasm2
  - Unicorn Engine

Section 5 : Autres types de malwares

- Malware "Web" (JavaScript/VBScript)
  - Analyse statique et dynamique
  - Limitation des navigateurs
- Malwares Flash
- Applications mobiles Android
- Documents malveillants
-
  - Suite Office
  - PDF
  - RTF
- Malwares .Net

Section 6 : Threat Intelligence

- Création de signatures Yara
- Communication et base de connaissances
  - MISP
  - Yeti

Section 7 : Avantage de l'analyse mémoire

Formation « Tests d'intrusion »

Réf : PENTEST1

Réaliser des tests d'intrusion est la méthode la plus efficace pour mettre en évidence les vulnérabilités qui seront exploitées par vos adversaires. Découvrez ces vulnérabilités par vous-même avant que celles-ci soient exploitées par d'autres !

Objectifs

- Préparer un test d'intrusion réussi
- Maîtriser toutes les phases d'un test d'intrusion (de la découverte à la post exploitation)
  - Découvrir facilement et rapidement le réseau cible
  - Exploiter en toute sécurité les vulnérabilités identifiées
  - Élever ses privilèges pour piller les ressources critiques
  - Rebondir sur le réseau compromis
- Comprendre les vulnérabilités exposées par les réseaux externes et internes
- Utiliser efficacement la trousse à outils du pentester

Durée & horaires

- 5 jours soit 35 heures
- Horaires : Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 16h00/16h30

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters
- Consultants SSI
- RSSI
- Architectes

Pré-requis

- Des notions en IT et/ou SSI
- Des notions d'utilisation d'une distribution Linux est un plus

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable mis à disposition pour la réalisation des exercices

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTEST1 par HS2.**

Programme

Introduction aux tests d'intrusion
- Équipement et outils
- Organisation de l'audit
- Méthodologie des tests d'intrusion
- Gestion des informations et des notes
- Exemple de bon rapport d'audit
- Les meilleurs pratiques : PASSI

Rappels et bases
- Les shells Unix *sh
- Les shells Windows cmd & powershell
- Rappels sur les réseaux tcp/ip
- Rappels du protocole HTTP
- Introduction à Metasploit
  - Exploits et Payloads
  - Fonctionnalités utiles
  - Base de données
- Modules
- Customisation
- ***Mises en pratique***

Découverte d'information
- Reconnaissance de la cible
  - Open Source Intelligence
- Découverte passive du SI
  - Ecoute réseau
- Scans réseau
  - Cartographie du réseau
  - Découverte de services
  - Identification des Systèmes d'exploitation
- Scanners de vulnérabilités
  - Scanner Open Source Openvas
- ***Mises en pratique***

Mots de passe
- Attaques en ligne
  - Brute force en ligne
  - Outils Open Source
- Attaques hors ligne
  - Analyse d'empreintes
  - Méthodologies de cassage
  - Les Raibow Tables
  - Outils Open Source
- ***Mises en pratique***

Exploitation
- Identification des vulnérabilités
  - Contexte des vulnérabilités
  - Étude de divers types de vulnérabilités

- Méthodologie d'exploitation
  - Identifier le bon exploit ou le bon outil
  - Éviter les problèmes
  - Configurer son exploit
- Exploitations à distance
- Exploitations des clients
- ***Mises en pratique***

Post-exploitation
- Le shell Meterpreter et ses addons
- Élévation de privilèges
- Fiabiliser l'accès
- Pillage
  - Vol de données
  - Vol d'identifiants
- Rebond
  - Pivoter sur le réseau
  - Découvrir et exploiter de nouvelles cibles
- ***Mises en pratique***

Intrusion web
- Méthodologie d'intrusion WEB
- Utilisation d'un proxy WEB
  - Proxy Open Source ZAP
- Usurpation de privilèges
  - CSRF
- Les injections de code
  - Côté client : XSS
  - Côté serveur : SQL
- Compromission des bases de données
- Autres types d'injections
- Les inclusions de fichiers
  - Locales
  - A distance
- Les webshells
  - Précautions d'emploi
- ***Mises en pratique***

Intrusion windows
- Méthodologie d'intrusion Windows

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

- Découverte d'informations
  - Identification de vulnérabilités
  - Techniques de vols d'identifiants
- Réutilisation des empreintes
  - Technique de "Pass The Hash"
- Élévation de privilèges
  - Locaux
  - Sur le domaine : BloodHound
- Échapper aux anti-virus
  - Techniques diverses
  - Outil Open Source Veil
- Outillage powershell
  - Framework Open Source PowerShell Empire
- ***Mises en pratique***

Intrusion Unix/Linux

- Méthodologie d'intrusion Linux
  - Rappels sur la sécurité Unix
- Découverte d'informations
  - Identifications de vulnérabilités
- Elévation de privilèges
  - Abus de privilèges
  - Exploitation de vulnérabilités complexes
- ***Mises en pratique***

Formation « Tests d'intrusion et développement d'exploits »

Réf : PENTEST2

Pour tester des vulnérabilités complexes, les outils et exploits grand public rencontrent parfois leurs limites. Maitrisez les concepts derrière ces outils et apprenez à concevoir des attaques vous permettant de tirer profit de toutes les situations.

Objectifs

- Maîtriser les vulnérabilités complexes
- Comprendre le fonctionnement des exploits
- Développer des outils d'attaque
- Contourner les protections système
- Élargir la surface d'attaque

Attention, cette formation ne traite pas des bases des tests d'intrusion ni de l'utilisation de Metasploit, elle va exclusivement au-delà.

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 16h00/16h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters expérimentés
- Développeurs expérimentés

Pré-requis

- Avoir suivi avec succès la formation PENTEST1
- Ou avoir une certification reconnue similaire comme OSCP, GIAC GPEN, etc
- Ou posséder une très bonne expérience des tests d'intrusion et pouvoir le démontrer

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en tests d'intrusions
- Un réseau vulnérable fidèle à la réalité sert de plateforme pour les tests
- Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés lors des missions
- Les techniques et outils classiques ainsi que modernes sont utilisés tout au long de la formation

Supports

- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTEST2 par HS2.**

Programme

WEB AVANCE
- Injections SQL en aveugle
- Injections SQL basées sur le temps
- Attaques de désérialisation
- Attaques avancées BDD
- Attaques XXE

ATTAQUES RESEAU
- Scan furtif
- Scapy
- TCP-highjack
- Network Access control (NAC)
  - Contourner un portail captif
  - Contourner le 802.1X
- VLAN-Hopping
- Rerouter le trafic
  - ARP cache poisoning
  - DNS spoofing
  - Exploitation des protocoles de routing
- Attaque PXE

LES OUTILS DE L'EXPLOITATION AVANCEE
- Python
- Assembleur
- Désassembleurs et debuggers
  - GDB/Peda, Radare2
  - Ollydbg, Immnunity, EDB

LES BASES DU DEVELOPPEMENT D'EXPLOIT
- structure basique d'un exploit (python/perl)
- Win32 shellcoding
- Exploits Metasploit
- Fuzzing
  - Sulley/Boofuzz

DEVELOPPEMENT EXPLOITS
- String Format
  - Lire à des adresses
  - Ecrire à des adresses
  - dtor
  - Ecraser la GOT
- Double free
- Off by one
- Integer Overflow

VULNERABILITES APPLICATIVES
- String Format
  - Lire à des adresses
  - Écrire à des adresses
  - dtor
  - Ecraser la GOT
- Double free
- Off by one
- Integer Overflow

BUFFER OVERFLOW
- Stack based
  - Ecraser EIP
  - Sauter vers le shellcode
    - Jump (or call)
    - Pop return
    - Push return
    - Jmp [reg + offset]
    - blind return
    - SEH
    - popadd
    - short jumps et conditionnal jumps
    - stack pivot
  - SEH Exploits
  - Egg Hunting
- Heap based
  - Heap spraying
- Encodage
  - MSFVenom
  - code polymorphique (veniatian encoding)
- Unicode Exploit

CONTOURNEMENT DES PROTECTIONS
- * NX/DEP et ASLR
  - ret2libc
  - retour dans system()
  - ROP
  - écrasement partiel d'EIP
  - NOP spray
- Stack cookies (canaries)
- SafeSEH
- SEHOP
- Outils divers
  - Mona
  - Peda
  - Pwntools

WIFI
- WEP
- WPA/WPA2
- WPS

PHISHING
- Pieces jointes vérolées
  - SCRIPT
  - DDE
- Créer une porte dérobée dans un exécutable
  - Utiliser les code cave
- Échapper aux antivirus
- Assurer la persistance
  - Le Command & Control

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « Tests d'intrusion des systèmes industriels »

Réf : PENTESTINDUS

La vérification de la cybersécurité par les tests d'intrusion est une mesure de sécurité courante (Redteam, Bug Bounty), et qui est dans l'arsenal des bonnes pratiques. Dans le cas des systèmes industriels, le matériel cible est spécifique, le contexte et sa sureté de fonctionnement et sa criticité souvent hors des contextes de tests habituels. Il est donc indispensable de comprendre cet environnement et ces composants pour pouvoir en évaluer le niveau de sécurité.

Objectifs

- Comprendre le fonctionnement des SI industriels et leurs spécificités
- Découvrir les outils et les méthodologies pour les tests d'intrusion sur SI industriel
- Mettre en pratique ses connaissances sur un environnement industriel représentatif

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Ingénieur en charge de la sécurité ou du contrôle de SI industriels
- Consultants, auditeurs et pentesteurs voulant monter en compétence sur les SI industriels
- Automaticien voulant se former à la sécurité d'un point de vue attaque et par la pratique

Pré-requis

- Bonne connaissance générale en informatique et en réseaux, par exemple une certification SECUCYBER d'HS2 ou CISSP d'(ISC)².
- Maîtrise d'un interpréteur de commande (Bash, Powershell, etc)
- Utilisation de machines virtuelles
- Une expérience en test d'intrusion est un plus
- Aucune connaissance des systèmes industriels n'est nécessaire

Méthode pédagogique

- Cours magistral
- Démonstrations
- Travaux pratiques avec un ordinateur par stagiaire, avec mise en œuvre sur plusieurs automates et exercice sous forme de concours (CTF)

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Clé USB contenant les machines virtuelles, les outils utilisés, ainsi que de la documentation complémentaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTINDUS par HS2.**

Programme

Module 1 : Introduction aux SI industriels

- Historique des SI industriels et de l'automatisme
- Vocabulaire
- Modèle CIM
- Architectures classiques
- Composants des SI industriels (PLC,HMI,SCADA,DCS,capteurs,effecteurs, RTU...)

Module 2 : Tests d'intrusion : principes & outillage

- Tests d'intrusion et autres méthodologies d'évaluation de la sécurité des SI industriels
- Différentes étapes et outil d'un test d'intrusion classique (notamment reconnaissance, exploitation, post-exploitation)
- Travaux pratiques : scans nmap, exploitation simple avec Metasploit

Module 3 : Sécurité des systèmes Windows et Active Directory

- Introduction aux environnements Windows et AD
- Méthodes d'authentifications, format et stockage des mots de passe et secrets
- Faiblesses classiques de ces environnements
- Travaux pratiques : recherche d'informations dans un AD avec Powerview, utilisation de mots de passe et condensats avec crackmapexec…

Module 4 : Vulnérabilités courantes en environnement industriel

- Segmentation réseau
- Sécurité dans les protocoles
- Supervision Sécurité
- Sensibilisation
- Gestion des tiers
- Correctifs de sécurité

Module 5 : Protocoles de communication industriels

- Présentation des protocoles les plus courants (modbus tcp, S7, OPC...)
- Travaux pratiques : analyse de capture réseau Modbus/TCP, S7 et OPC-UA

Module 6 : Introduction à la sureté de fonctionnement

- Présentation du concept
- Méthodologies d'analyse de sureté fonctionnelle
- Différentes couches de sureté
- Travaux pratiques : ébauche d'analyse HAZOP sur un exemple simple

Module 7 : Programmation d'automates programmables industriels (API)

- Présentation des différents langages
- Travaux pratiques : Exercices de programmation en ladder logic sur simulateur Schneider TM221 et SCADA Schneider IGSS

Module 8 : Tests d'intrusion sur API

- Outils de communication pour les protocoles industriels
- Surface d'attaque des automates (web, ftp, http)
- Présentation d'attaques avancées sur les API (protocoles propriétaires, ...)
- Travaux pratiques : Utilisation de mbtget pour envoi de requêtes modbus sur simulateur Schneider, bibliothèque Snap 7 pour échanger avec simulateur Siemens, opcua-gui pour échanger avec SCADA Schneider IGSS

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Module 9 : Principes de sécurisation des SI industriels

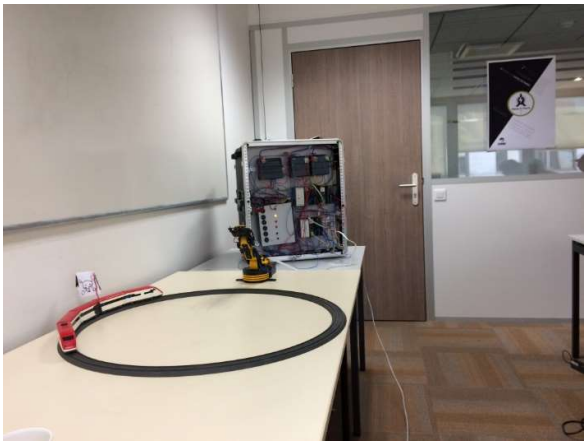
- Panel normatif
- Architectures et technologies de cloisonnement réseau
- Focus sur les diodes réseau
- Autres points d'attention particuliers

Module 10 : Étude de cas

- Analyse d'une Étude de cas présentant une description d'une société fictive, des schémas réseau, ainsi que des règles de pare-feu.
- Travail collaboratif pour identifier vulnérabilités, risques, et élaboration de plan d'action

Module 11 : Exercice sous forme de CTF (Capture The Flag)

- Mise en pratique des acquis par la réalisation d'un test d'intrusion sur un environnement représentatif :
  - Compromission d'un environnement bureautique
  - Découverte de liens réseau et rebond vers le SI industriel
  - Attaques sur les automates et la supervision pour impacter un processus physique (train miniature et bras robotisés)
    - Visuels de la maquette :



Formation « Tests d'intrusion des serveurs et des applications Web»

Réf : PENTESTWEB

L'infrastructure Web expose directement votre société aux menaces externe. Renforcez vos défenses en sécurisant efficacement tous les vecteurs exploités par les attaquants !

Objectifs

- Anticiper les besoins des tests d'intrusion
- Comprendre les principales vulnérabilités du web
- Analyser les risques encourus
- Détecter les failles de sécurité
- Exploiter les vulnérabilités pour prendre le contrôle de l'infrastructure

Durée & horaires

- 5 jours soit 35 heures
- Le lundi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Du mardi au vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Quiconque souhaite comprendre et pratiquer les techniques utilisées par les attaquants pour compromettre un système d'information depuis Internet :
  - Pentesters
  - RSSI
  - Chefs de projets
  - Développeurs
  - Architectes
  - Administrateurs systèmes

Pré-requis

- Aucun prérequis
- Des notions d'utilisation d'une distribution Linux est un plus

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs. La formation est proposée en mode présentiel et accessible en mode distanciel via ZOOM pour ceux qui ne veulent pas se déplacer

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé en présentiel / au format numérique en distanciel après signature du règlement intérieur
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTWEB par HS2.**

Programme

Le test d'intrusion
- Méthodologie et type de tests
- Équipement et outils
- Législation
- Déroulement de l'audit
- Gestion des informations et des notes
- Clôture de l'audit
- Pour aller plus loin

Le proxy applicatif
- Usages
- Burpsuite, Zap...

Les mécanismes du Web
- Le protocole HTTP (méthodes, entêtes, codes de retours, encodage...)
- Les risques du modèle client/serveur

La sécurité du client
- La SOP
- Les communications "cross-domain"
- Contournements CORS
- Contournements CSP
- Open Redirect

Cryptographie
- SSL/TLS
- Les suites cryptographiques
- Renegociation non sécurisée
- Audits et contrôles
- La PKI
- Le cassage de condensats

Reconnaissance et fuite d'informations
- Introduction et objectifs
- Découverte passive
  - Résolutions DNS et registres
  - Détournement de sous-domaine
  - OSINT
  - Les Googles Dorks
  - Les fuites
- Découverte active
  - Le transfert de zone
  - Le balayage de ports
  - Découverte de serveurs web
  - Prévisualisation des applications
  - Crawling et Spidering
  - Le WAF
- Le scan de vulnérabilités

Les processus d'authentification
- Gestion de l'identité
- Les attaques sur l'authentification
  - XML Signature Wrapping
  - Détournement d'Oauth

La gestion des sessions
- Les jetons de session
- Les cookies
- Jetons JWT
- Forge de requêtes inter-sites (CSRF)
- Fixation de session
- Forge de jetons de session
- Le cloisonnement des sessions
- Référence directe à des objets non sécurisés (IDOR)

Les injections
- Les injections coté client
  - L'injection XSS
- Les injections côté serveur
  - L'attaque CRLF (et response splitting)
  - Les injections de commandes
  - L'injection XXE
  - L'injection SQL
  - Quelques injections moins fréquentes (XPath, LDAP, NoSQL)
  - Les injections via sérialisation/dé-sérialisation
  - Forge de requête côté client (SSRF)

Les injections de fichiers
- Le téléversement de fichiers
- Les inclusions de fichiers locaux et distants

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Les Webservices et API

- Le fonctionnement des Webservices (XML-RPC, SOAP, REST)
- Les websockets
- Méthodologie d'intrusion
- Les applications mobiles

Le Cloud

- Méthodologies et spécificités
- Quelques outils
- Vulnérabilités

Les vulnérabilités plus complexes

- Tour d'horizon (Buffer Overflow...)
- Méthodologie d'exploitation

Tout au long de la semaine, vous pratiquerez les attaques présentées durant le cours sur notre infrastructure web réaliste simulé : de simple visiteur sur un site web, terminez root d'un serveur ! (Tous les outils utilisés durant les exercices sont accessibles gratuitement en dehors de la formation)

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « SPLUNK »

Réf : SPLUNK

Splunk permet à de très nombreuses équipes opérationnelles, SOC, CSIRT de réaliser efficacement leurs investigations numériques, détection d'attaques ou chasse, en facilitant les opérations de recherche & manipulation des journaux quelques soient le volume de données.

Cette formation vous permettra d'apprendre à utiliser Splunk pour les cas d'usage de la sécurité informatique, elle complète bien les formations SECUBLUE et SECUSOC en vous fournissant les clés pour exploiter au mieux cet outil puissant.

Cette formation n'est pas une présentation exhaustive des capacités de Splunk, elle a été construite pour pouvoir être efficace et pertinente dans l'utilisation de Splunk.

Objectifs

- **Découvrir le fonctionnement et les capacités de Splunk**
- **Apprendre le langage SPL pour requêter les données efficacement**
- **Enrichir les données opérationnelles à partir de sources externes**
- **Créer des tableaux de bord dynamiques pour l'aide à la décision et la synthèse d'informations**
- **Créer des requêtes matures pour la détection d'attaque**

Durée & horaires

- **3 jours soit 21 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Analystes en détection (SOC)**
- **Analyste en conception (SOC, CSIRT)**
- **Analystes forensique (CSIRT)**
- **Auditeurs**
- **Opérationnels en sécurité**
- **Responsables sécurité opérationnelle**

Pré-requis

- **Connaissances informatiques générales (qu'est-ce qu'une adresse IP, une authentification, etc.)**
- **Compréhension des enjeux généraux en sécurité informatique (qu'est-ce qu'une attaque par bruteforce, une exfiltration de données, etc.)**

Méthode pédagogique

La formation est délivrée à travers un mélange de cours magistral et démonstrations sur le produit. Les apprenants ont tous accès à un Splunk pendant toute la durée de la formation leur permettant de reproduire les exemples fournis en cours. Des travaux pratiques de mise en œuvre sont fournis aux apprenants sur les concepts clés. Les travaux pratiques possèdent tous un énoncé et une solution détaillée, permettant aux apprenants de valider leurs exercices. Les formateurs supervisent la réalisation des travaux pratiques et accompagnent les apprenants ayant besoin d'aide. Pour les apprenants venant en salle de formation, le déjeuner est offert et est un moment privilégié de partage entre apprenants et formateurs.

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification Splunk par HS2.**

Programme

Introduction à Splunk

- Produits de la marque Splunk
- Fonctions de Splunk Enterprise
- Architecture
- Flux de données

Ajouter des données

- Processus d'indexation
- Téléversement à travers l'interface graphique
- Organisation de la donnée dans les indexes
- Envoi à travers un Universal Forwarder
- Envoi à travers un collecteur syslog
- Supervision de modifications dans des fichiers
- Envoi par API
- Extraction de champs
- Normalisation des champs

Requêter

- - Accès aux données indexées
- - Filtre temporel
- - Paramètres des tâches de recherche
- - Exploration des résultats
- - Modes de recherche
- - Différences entre les événements et les statistiques
- - Commandes
    - Search
    - Fieldsummary
    - Where
    - fields
    - rename
    - rex
    - eval
        - Fonctions d'évaluation
    - dedup
    - sort
    - head
    - tail
    - fillnull
    - table
- - Calculs statistiques
    - Commande stats
    - Fonctions d'agrégations
    - Agrégats multiples
    - Combinaison des fonctions d'agrégation et des fonctions d'évaluation
- Manipulation des JSON
- Enrichissement de données
    - Types de lookups
    - Manipulation des lookups
    - Recoupement des données
    - Utilisation des lookups pour faire une chasse de marqueurs
        - Jointures
    - Macros de recherche
    - Sous-recherches

Configurer

- Fichiers de configuration
- Précédence des configurations
- Périmètres et gestion des droits
- Objets de connaissance
- Partage d'objets
- Installation d'une application

Tableaux de bord

- Utilisation des tableaux de bord Studio
- Forces et limitations du moteur

- Sélecteurs et filtres
- Commande timechart
- Requêtes chaînées
- Utilisation des tokens
- Interactivité des tableaux de bord

Requêtes avancées

- Commandes bin et transaction
- Requêtes pour l'investigation numérique
- Requêtes pour la détection
- Détection par seuil
- Création d'alertes pour un SOC

Conclusion

- Ressources pertinentes pour l'apprentissage continu

Nos Intervenants
Formations cybersécurité technique

Romain Bentz dispense la formation :
PENTEST1 - PENTEST2

Olivier Caillault dispense la formation :
SPLUNK

Marc Baudoin dispense la formation :
SECULIN - SELINUX

Danil Bazin dispense les formations :
ESSCYBER - FORENSIC1 - FORENSIC2

Matthieu Caron dispense les formations :
SECUCYBER - SECUWEB - PENTEST1 - PENTEST2

Rémi Chauchat dispense les formations :
SECUINDUS - PENTEST1

Baptiste Dolbeau dispense la formation :
FORENSIC1

Sébastien Dudek dIspense la formation :
PENTESTWIFI

Romain Du Marais dispense les formations :
SECUCYBER - SECUWEB - PENTESTWEB

Jordan Hordé dispense la formation :
SECUARCH

Olivier Houssenbay dispense la formation :
ESSCYBER - SECUCYBER - SECUWIN

Cyrille De Pardieu dispense les formations :
SECUBLUE1 - SECUBLUE2 - SECUWIN

Anthony Di Prima dispense la formation :
SECUINDUS

Igor Hermann dispense la formation :
SPLUNK

Anthony Hubbard dispense la formation :
SECUBLUE1

Stefan Le Berre dispense la formation :
FORENSIC1 - FORENSIC2 - REVERSE1

Jérôme Naucelle dispense la formation :
SECUWEB - PENTESTWEB

Michel Pruche dispense les formations :
SECUPKI

Christophe Renard dispense les formations :
SECUINDUS

Julien Reveret dispense la formation :
FORENSIC1

Jérémy Richard dispense la formation :
SECUBLUE1 - SECUBLUE2

Matthieu Schipman dispense les formations :
ESSCYBER - SECUCYBER - SECUBLUE1 - SECUWIN

Mikaël Smaha dispense la formation:
SECUARCH

Cyril Solomon dispense les formations :
FORENSIC1 - FORENSIC2 - REVERSE1

Hervé Schauer dispense la formation :
SECUINDUS

Arnaud Soullié dispense la formation :
PENTESTINDUS

Bulletin d'inscription

Merci de retourner ce bulletin soit par courrier à HS2 – 10, rue des Poissonniers – 92200 Neuilly-sur-Seine –
Soit par courriel à formation@hs2.fr

Responsable Formation

Nom et Prénom : .....
Fonction : ..... Société : .....
Adresse : .....
Code postal : ..... Ville : .....
Tél. : ..... E-mail : .....

Souhaite inscrire la ou les personne(s) suivante(s) au(x) stage(s) mentionné(s) :

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

Adresse de facturation (si différente)

Société : ..... Adresse : .....
Code postal : ..... Ville : .....
Nom du correspondant : ..... Tél. : .....
E-mail : .....
N° de TVA intracommunautaire .....

Établissez-vous des bons de commande avec des références à reporter sur notre facture ? oui ❍ non ❍
Si oui, l'inscription sera confirmée uniquement à réception de votre bon de commande.

Demande de subrogation via votre OPCO* : oui ❍ non ❍
*Dans le cas d'une subrogation de paiement via votre OPCO, l'inscription sera confirmée uniquement à réception du contrat ou de l'accord de prise en charge de votre OPCO et de notre convention de formation signée et tamponnée

Date :
Cachet et signature de l'employeur

Convention de formation : pour chacune des sessions proposées, une convention de formation est disponible sur simple demande.
Attention, la prise en compte de votre demande d'inscription sera effective uniquement à réception d'un mail de confirmation par nos services.
Pour tout renseignement complémentaire, vous pouvez contacter le service formation par mail à formation@hs2.fr ou par téléphone au +33 974 774 390.

Retrouvez-nous sur notre site : **www.hs2.fr**

Renseignement / inscription à nos formations, n'hésitez pas à nous contacter :

Lynda Benchikh / Elisa Keller / Estelle Dubois

☎ +33 (0)974 774 390

formation@hs2.fr

Déclaration d'activité enregistrée sous le numéro 11922236092
auprès du préfet de région d'Ile-de-France

Pour nous contacter :

☎ +33 (0)974 774 390 / +33 (0)644 014 072

formation@hs2.fr

Pour nous suivre :

@HS2formation

@HS2formation

@HS2formation

Datadock Organisme Référencé

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : **ACTIONS DE FORMATIONS**