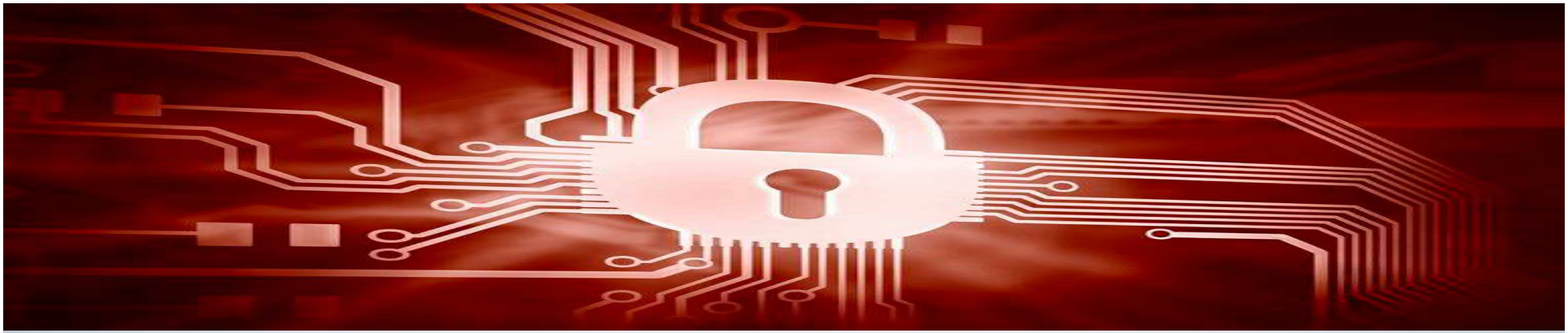

Hackgates

PRESENTATION

Hackgates a pour but de fournir des services relatifs à la sécurité informatique ISO 2700X ainsi qu'à l'intégration des réseaux et l'intégration de solutions WEB /Télécom.

En plus de la partie networking, Hackgates dispose d'un département entièrement dédié à la formation en cyber sécurité

Tous ces services sont fournis par des ingénieurs hautement qualifiés ce qui assure à notre clientèle un service de qualité supérieur.
Le siège social de Hackgates S.A. se trouve à Nyon.

Hackgates

Sommaire Programme de cours

- ***Ethical Hacking***
  - ***Les fondamentaux***
  - ***Avancé***
  - ***Hacking & Sécurité Expert V.4***
  - ***Test Intrusion mise en situation d'audit***
  - ***Audit Site Web***
  - ***Méthode d'audit d'un SI***
  - ***Recherche & Exploitation de vulnérabilités Sur APPs Android***
  - ***Certified Ethical Hacker V.10***

Hackgates

Sommaire Programme de cours

- ***Sécurité défensive***
  - ***Lutte contre la Cyber Criminalité Mise en pratique***
  - ***Sécurisation des réseaux***
  - ***Mise en place d' un SIEM***
  - ***Sensibilisation au Développement sécurisé***

Hackgates

Sommaire Programme de cours

- ***Hackforensic***
  - ***Malware détection, identification,eradication***
  - ***Analyse forensic avancée et réponse aux incidents***

Hackgates

Une réelle expertise au service de la formation en sécurité informatique

Depuis 2019, nous proposons des contenus de formation en sécurité informatique et de cybersécurité pertinents grâce à notre expérience terrain.

Le but est de formé des professionnels ayant déjà une formation / ou une connaissance en informatique et les employés des entreprises.
Nos intervenants sont tous des experts dans le domaine
de la sécurité, ils partagent leur activité entre la formation, le pentest et la recherche.
Nous privilégions la mise en application concrète des points abordés par des études de cas et la mise en pratique (en moyenne 70% de mise en œuvre pratique
dans nos formations sécurité offensive, défensive ou inforensique). Notre offre répond aux besoins et attentes de chaque public (RSSI, DSI, ingénieurs ou techniciens IT, consultants,
auditeurs, étudiants, employés et toute personne s'intéressant à la sécurité informatique.
Nous nous engageons par ailleurs à conserver une parfaite indépendance vis à vis de toute solution informatique
matérielle ou logicielle. Nous conservons ainsi une parfaite objectivité dans l'information communiquée
à nos stagiaires, nos recommandations et choix techniques.

Définition du forensique

- Le forensique consiste à appliquer la science (dans ce cas, des techniques informatisés) pour des fins de recherches légales suite à un incident ou crime.
- Méthodologie de techniques et procédures pour la récupération de preuves
- Investigation
- Preuves légalement valides
- Orientation Ethique
- Techniques utilisées par les Hackers

Hackgates

Sommaire Programme de cours

- *Compliance*
  - *Introduction à ISO 27001*
  - *Introduction à ISO 27005 Gestion des risques*
  - *Loi sur la protection des données*
  - *RGPD*

Hackgates

Description du cours Ethical Hacking

Les fondamentaux

- ✓ Cette formation est une première approche des pratiques et des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises. Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes. L'objectif est de vous fournir les premières compétences techniques de base, nécessaires à la réalisation d'audits de sécurité (test de pénétration), en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI.
  Il s'agit d'une bonne introduction au cours HSA pour toute personne souhaitant acquérir les connaissances techniques de base.
  La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).

Objectifs

- ✓ Comprendre et détecter les attaques sur un SI
- ✓ Exploiter et définir l'impact et la portée d'une vulnérabilité
- ✓ Corriger les vulnérabilités
- ✓ Sécuriser un réseau et intégrer les outils de sécurité de base

Hackgates

Description du cours Ethical Hacking

Les fondamentaux

Jour 1

•Introduction
- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test
- Prise d'information

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

Réseau
•Rappels modèles OSI et TCP/IP
•Vocabulaire
•Protocoles ARP, IP, TCP et UDP
•NAT
•Scan de ports
•Sniffing
•ARP Cache Poisoning
•DoS / DDoS

Jour 2

- Attaques locales
- Cassage de mots de passe
- Elévation de privilèges
- Attaque du GRUB

- Ingénierie sociale
- Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes
- Phishing
- Outils de contrôle à distance

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

Se sécuriser
- Les mises à jour
- Configurations par défaut et bonnes pratiques
- Introduction à la cryptographie
- Présentation de la stéganographie
- Anonymat (TOR)

Hackgates

Description du cours Hacking & Sécurité : Avancé v6

Pratiquez les attaques avancées pour mieux vous défendre

Ce cours est une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises. Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes.
L'objectif est de vous fournir les compétences techniques nécessaires à la réalisation d'audits de sécurité (tests de pénétration), en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI.
La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).

Objectifs

Comprendre et détecter les attaques sur un SI
Définir l'impact et la portée d'une vulnérabilité
Réaliser un test de pénétration
Corriger les vulnérabilités
Sécuriser un réseau, et intégrer des outils de sécurité adéquats

Hackgates

Description du cours Hacking & Sécurité : Avancé v6

Jour 1

•Rappel TCP/IP / Réseau Matériel
•Protos / OSI - Adressage IP

Introduction à la veille
•Vocabulaire
•BDD de Vulnérabilités et Exploits
•Informations générales

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

Scan et prise d'empreinte
•Enumération des machines
•Scan de ports
•Prise d'empreinte du système d'exploitation
•Prise d'empreinte des services

Jour 2

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

Attaques système
•Scanner de vulnérabilités
•Exploitation d'un service vulnérable distant
•Elévation de privilèges
•Espionnage du système
•Attaques via un malware
•Génération d'un malware avec Metasploit
•Encodage de payloads
•Méthode de détection

Jour 5

Challenge final

Jour 3

Attaques Web

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

Jour 4

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

Hackgates

Description du cours Sensibilisation à la cybersécurité

Comprendre pour appréhender au mieux les menaces informatiques

Cette formation vise à sensibiliser les participants aux menaces informatiques. L'aspect organisationnel lié à la sécurité informatique au sein de l'entreprise sera tout d'abord évoqué. Une présentation des différentes attaques ainsi que des cas pratiques seront ensuite réalisés, et cela dans l'objectif de démontrer techniquement la faisabilité des attaques. Enfin, un ensemble de bonnes pratiques de sécurité sera présenté pour permettre de pallier aux problèmes abordés.

Objectifs

- **Découvrir et assimiler la sécurité informatique**
- **Appréhender et comprendre les attaques informatiques**
- **Identifier les menaces informatiques**
- **Adopter les bonnes pratiques pour se protéger**

Hackgates

Description du cours sensibilisation à la cybersécurité

Jour 1

- Acteurs au sein de l'entreprise
- Système d'information (SI)
- Sécurité des systèmes d'information (SSI)
- Objectifs de la sécurité informatique
- Vulnérabilités et attaques informatiques
- Risques et enjeux pour l'entreprise
- Motivations d'une attaque

Le cadre législatif

- Politique de sécurité
- Charte informatique
- Protection des données personnelles
- RGPD
- LPD

Les attaques locales

- Ports USB
- Ports d'extension haute vitesse (DMA)
- Câble Ethernet
- Disque dur interne

Les attaques distantes

- Interception sur le réseau
- Téléchargement
- Réseau sans-fil
- Système non à jour

L'ingénierie sociale

- Messagerie
- Téléphone
- Navigation web
- Pièce jointe

Exemple d'attaques par logiciel malveillant

- Zeus
- Stuxnet
- Locky
- WannaCry

Les mots de passe

- Rôle et usage
- Importance de la complexité
- Attaque par recherche exhaustive
- Intérêt de la double authentification
- Utilité de stockage sécurisé
- Post-attaque sur la machine
- Problème lié à la réutilisation de mots de passe

Les protections et bons réflexes

- Ports de communication (USB, Firewire, PCI Express, etc.)
- Chiffrement du disque
- Verrouillage du poste
- Mises à jour
- Antivirus et pare-feu
- Connexion sur un réseau inconnu
- Détection et remontée d'alertes

Hackgates

Description du cours Social Engineering

Comprendre les failles humaines pour mieux s'en prémunir

Cette formation vise à sensibiliser les participants aux attaques par manipulation que peuvent mettre en place les attaquants. Les concepts clés du social engineering et les principales techniques de manipulation y seront abordés. Vous apprendrez à identifier les menaces et à adopter les bonnes pratiques afin d'éviter de vous faire manipuler.

Objectifs

- **Comprendre le social engineering**
- **Apprendre les différentes techniques utilisées par les attaquants**
- **Savoir identifier les menaces**
- **Adopter les bonnes pratiques**

Hackgates

Description du cours Social Engineering

Jour 1

Introduction au social engineering
•Qu'est-ce que le social engineering ?
•Qui l'utilise et dans quel but ?
•Quels sont les risques liés au social engineering ?

Le modèle de communication

- **Présentation**
- **Développer son modèle de communication**

L'incitation

- **Le principe**
- **Le but**
- **Préparer sa cible**
- **Comment être efficace**
- **Exemples courants d'incitations**

L'imposture, ou comment devenir n'importe qui

- **Le principe**
- **Les points clés pour réussir**
- **Exemples d'impostures réussies**
- **L'importance de la psychologie**

- **Les différents modes de perception**
- **Les sens**
- **Le visuel**
- **L'auditif**
- **Les micro-expressions**

Quelques techniques de SE

- **La gestuelle**
- **L'ancrage**
- **L'imitation**

- **La persuasion**
- **Le principe**
- **Les points clés**
- **Importance de l'influence**
- **La réciprocité**
- **L'obligation**
- **La concession**
- **L'attractivité**
- **L'autorité**
- **Le cadrage (framing)**

Le social engineering appliqué au pentest

- **Prise d'information**
- **Présentation outils**
- **Shodan**
- **DNS**
- **Réseaux sociaux et outils collaboratifs**
- **Choix de/des victimes**
- **Exploitation humaine**
- **SET**
- **Création d'une pièce jointe piégée**
- **Prévention et réduction du risque**

Hackgates

Description du cours Test d'intrusion: Mise en situation d'audit

Le PenTest par la pratique

**Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur votre S.I.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise.
En effet, le PenTest est une intervention très technique, qui permet de déterminer le potentiel réel d'intrusion et de destruction d'un pirate sur l'infrastructure à auditer, et de valider l'efficacité réelle de la sécurité appliquée aux systèmes, au réseau et à la confidentialité des informations.
Vous y étudierez notamment l'organisation et les procédures propres à ce type d'audit ; ainsi qu'à utiliser vos compétences techniques (des compétences équivalentes au cours HSA sont recommandées) et les meilleurs outils d'analyse et d'automatisation des attaques (outils publics ou privés développés par nos équipes) pour la réalisation de cette intervention.**

Objectifs

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

Hackgates

Description du cours mise en situation d'audit

Jour 1

Méthodologie de l'audit
La première journée sera utilisée pour poser les bases méthodologiques d'un audit de type test d'intrusion.
L'objectif principal étant de fournir les outils méthodologiques afin de mener à bien un test d'intrusion.
Les points abordés seront les suivants :
Objectifs et types de PenTest

- Qu'est-ce qu'un PenTest?
- Le cycle du PenTest
- Différents types d'attaquants
- Types d'audits
  - Boîte Noire
  - Boîte Blanche
  - Boîte Grise
- Avantages du PenTest
- Limites du PenTest
- Cas particuliers
  - Dénis de service
  - Ingénierie sociale

Aspect règlementaire

- Préparation de l'audit
  - Déroulement
  - Cas particuliers
  - Habilitations
  - Dénis de service
  - Ingénierie sociale
- Déroulement de l'audit
  - Reconnaissance
  - Analyse des vulnérabilités
  - Exploitation
  - Gain et maintien d'accès
  - Comptes rendus et fin des tests
- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions
- Points importants du mandat

Exemples de méthodologies et d'outils

Éléments de rédaction d'un rapport

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

Une revue des principales techniques d'attaques et outils utilisés sera également faite afin de préparer au mieux les stagiaires à la suite de la formation.

Hackgates

Description du cours mise en situation d'audit

Jour 2,3,4

Une mise en situation d'audit sera faite afin d'appliquer sur un cas concret les outils méthodologiques et techniques vus lors de la première journée.
L'objectif étant de mettre les stagiaires face à un scénario se rapprochant le plus possible d'un cas réel, un réseau d'entreprise. Le système d'information audité comportera diverses vulnérabilités (Web, Applicatives, etc.) plus ou moins faciles à découvrir et à exploiter. L'objectif étant d'en trouver un maximum lors de l'audit et de fournir au client les recommandations adaptées afin que ce dernier sécurise efficacement son système d'information.
Pour ce faire, le formateur se mettra à la place d'un client pour qui les stagiaires auront à auditer le système d'information. Ces derniers seront laissés en autonomie et des points méthodologiques et techniques seront régulièrement faits par le formateur afin de guider les stagiaires tout au long de la mise en situation.
Le formateur aura un rôle de guide afin de :
faire profiter les stagiaires de son expérience de terrain
mettre en pratique la partie théorique de la première journée
d'élaborer un planning
d'aider les stagiaires à trouver et exploiter les vulnérabilités présentes
formater les découvertes faites en vue d'en faire un rapport pour le client

Jour 5

Le dernier jour sera consacré au rapport. La rédaction de ce dernier et les méthodes de transmission seront abordées.
Préparation du rapport
•Mise en forme des informations collectées lors de l'audit
•Préparation du document et application de la méthodologie vue lors du premier jour
Écriture du rapport

•Précautions nécessaires
•Méthodologie de transmission de rapport
•Que faire une fois le rapport transmis ?

Hackgates

Description du cours Audit de site Web

L'audit Web par la pratique

Ce cours vous apprendra à mettre en place une véritable procédure d'audit de site Web.
Vous serez confrontés aux problématiques de la sécurité des applications Web. Vous y étudierez le déroulement d'un audit, aussi bien d'un côté méthodologique que d'un côté technique.
Les différents aspects d'une analyse seront mis en avant à travers plusieurs exercices pratiques.
Cette formation est destinée aux personnes qui souhaitent pouvoir effectuer des tests techniques lors d'un audit ou d'un déploiement de sites Web.

Objectifs

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

Hackgates

Description du cours Audit de site Web

Jour 1

Introduction
Rappel méthodologie d'audit
Boite noire
Boite grise
Plan d'action
Prise d'information
Scan
Recherche et exploitation de vulnérabilités
Rédaction du rapport

Reconnaissance

Reconnaissance passive
- Base de données WHOIS
- Services en ligne
  - Netcraft
  - Robtex
  - Shodan
  - Archives
- Moteurs de recherche
- Réseaux sociaux
- Outils

Reconnaissance active
- Visite du site comme un utilisateur
- Recherche de page d'administration
- Recherche de fichiers présents par défaut
- robots.txt, sitemap
- Détection des technologies utilisées

Contremesures
- Limiter l'exposition réseau
- Filtrer les accès aux pages d'administration et aux pages sensibles
- Remplacer les messages d'erreurs verbeux par des messages génériques

Scan

Les différents types de scanner
- Scanner de ports
- Scanner de vulnérabilité
- Scanners dédiés

Limites des scanners

Hackgates

Description du cours Audit de site Web

Jour 2

Vulnérabilités

Vulnérabilités de conception
- Politique de mise à jour
- Chiffrement des communications
- Politique de mot de passe
- Mots de passe par défaut
- Mots de passe faibles
- Stockage des mots de passe

Isolation intercomptes Accès aux données d'autres utilisateurs
Modification d'informations personnelles

- Gestion des sessions
- Sessions prédictibles
- Session transitant dans l'URL
- Contremesures
- Mise à jour des applications et des systèmes
- Chiffrement des communications
- Utilisation et stockage des mots de passe
- Vérification des droits utilisateurs
- Système de session non prédictible avec une entropie élevée
- Drapeaux des cookies

Vulnérabilités Web

- Mise en place d'une solution de Proxy (Burp Suite)
- Cross-Site Scripting (XSS)
  - XSS Réfléchie
  - XSS Stockée
  - XSS Dom-Based
  - Contournement des protections
  - Démonstration avec l'outil d'exploitation BeEF
  - Contremesures
- Cross-Site Request Forgery (CSRF)
  - Exploitation d'un CSRF
    - Requête HTTP GET
    - Requête HTTP POST
  - Contremesures

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

- Contremesures
- Injection de commandes
- Chainage de commandes
- Options des commandes
- Exploitation
- Exemple d'exploitation avec commix
- Contremesures
- Service Side Includes (SSI)
- Exemples d'attaques
- Contremesures
- Injection d'objet
- Exploitation
- Contremesures

Hackgates

Description du cours Audit de site Web

Jour 3

- Inclusion de fichier
- Inclusion de fichiers locaux (LFI)
- Inclusion de fichiers distants (RFI)
- Contremesures
- Envoi de fichier (Upload)
- Exploitation basique
- Vérification de Content-type
- Blocage des extensions dangereuses
- Contremesures
- XML External Entity (XXE)
- Les entités
- Entités générales
- Entités paramètres
- Entités caractères
- Entités externes
- Découverte de la vulnérabilité
- Exploitation de la vulnérabilité
- Contremesures
- Service Side Template Injection (SSTI)
- Exemple d'utilisation de Twig
- Exemple d'exploitation sur Twig
- Exemple d'exploitation sur Flask
- Contremesures

Challenge final

Hackgates

Description du cours Sécurité VPN, sans-fil et mobilité

Approche ludique de la sécurité des technologies sans-fil

**Les réseaux sans-fil sont des facteurs essentiels du développement de la mobilité des outils informatiques.
Cette évolution est liée au phénomène BYOD (Bring your own Device), qui se manifeste par l'utilisation de dispositifs personnels (smartphones, tablettes et une multitude de périphériques) dans les locaux professionnels.
Nous ferons le point sur les enjeux de sécurité et passerons en revue les vulnérabilités des différents protocoles sans-fil: WiFi, Bluetooth, GSM, 3G/4G, etc.
Des travaux pratiques seront mis en œuvre ou démontrés avec du matériel dédié (carte WiFi, HackRF One, Yard Stick One, Ubertooth One, antennes, etc.).
Nous parlerons des différents moyens de protection à disposition.**

Objectifs
•Former et sensibiliser des équipes techniques aux problématiques de sécurité liées
•aux réseaux sans-fil, dans le contexte actuel de forte mobilité des outils technologiques

Hackgates

Description du cours Sécurité VPN, sans-fil et mobilité

Jour 1

Introduction: dispositifs sans-fil, enjeux de la mobilité et BYOD

- WiFi
  - Rappels sur les technologies WiFi
  - Revue des modes de chiffrement
  - Présentation du matériel offensif
  - Description des différentes techniques d'attaque
  - Présentation des moyens de protection
- TP WiFi
  - Configuration d'un routeur dans les différents modes
  - Attaques dans les différents cas de figure (dont injections avec une carte Alpha)
  - Durcissement de la configuration
  - Présentation du WiFi Pineapple
- VPN
  - Présentation des différentes technologies et protocoles
  - Sécurisation du transport des données
  - Limites et exemples d'attaques

Jour 2

Bluetooth
- Principes de fonctionnement du Bluetooth (BR, EDR et Low Energy)
- Les principaux risques
- Le paradoxe de la difficulté de détection (attaque et défense)
- Présentation de l' Urbertooth One

TP Bluetooth
- Sniffing du trafic BLE

Jour 3

Bluetooth
- Principes de fonctionnement du Bluetooth (BR, EDR et Low Energy)
- Les principaux risques
- Le paradoxe de la difficulté de détection (attaque et défense)
- Présentation de l'Urbertooth One

TP Bluetooth

Prise en main de l' Ubertooth

Sniffing du trafic BLE

Hackgates

Description du cours EC-Council Certified Security Analyst v10

La certification du pentester - « Accredited Training Center » by EC-Council

Le programme ECSAv10 est la continuité logique après avoir étudié le CEHv10.
Le nouveau ECSAv10 présente un plan de cours mis à jour et une méthodologie de pentest étape par étape, largement et globalement reconnue par le marché. Cela va permettre aux stagiaires d'augmenter leurs compétences en apprenant de nouvelles techniques à travers challenges et labs.
A l'inverse d'autres programmes de formation pentest, le cours ECSA présente un ensemble de méthodologies completes et diverses pouvant répondre aux prérequis des différents marchés. C'est un cours interactif, exhaustif, basés sur des normes, se dispensant en 5 jours qui permettra aux stagiaires d'apprendre à mener des vrais pentest professionnels.
Ce cours fait partie de la « VAPT Track » d'EC-Council (Vulnerability Assessment Penetration Testing).
C'est un cours de niveau "Professionnel", avec le CEH étant le cours principal et le LPT étant la certification « Master ».
Dans ce nouveau programme ECSAv10, les stagiaires passant l'examen de certification ECSAv10 auront la possibilité de poursuivre un examen entièrement pratique (en option), leur proposant donc de tester leurs compétences en obtenant la certification ECSA Practical.

Objectifs
•Apporter une méthodologie de pentest étape par étape
•Apprendre à mener de vrais pentests professionnels

Toutes les informations sur https://cert.eccouncil.org/ece-policy.html

Hackgates

Description du cours EC-Council Certified Security Analyst v10

Plan de cours

1. Introduction to Penetration Testing and Méthodologies
2. Penetration Testing Scoping and Engagement Methodology
3. Open Source Intelligence (OSINT) Methodology
4. Social Engineering Penetration Testing Methodology
5. Network Penetration Testing Methodology- External
6. Network Penetration Testing Methodology- Internal
7. Network Penetration Testing Methodology- Perimeter Devices
8. Web Application Penetration Testing Methodology
9. Database Penetration Testing Methodology
10. Wireless Penetration Testing Methodology
11. Cloud Penetration Testing Methodology
12. Report Writing and Post Testing Actions

Directement disponible en fin d'examen.
Maintien de la certification
Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année.

Pour plus d'information, vous pouvez consulter le site d'EC-Council.

Modules en auto-apprentissage

1. Penetration Testing Essential Concepts
2. Password Cracking Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing
6. Physical Security Penetration Testing
7. Surveillance Camera Penetration Testing
8. VoIP Penetration Testing
9. VPN Penetration Testing
10. Virtual Machine Penetration Testing
11. War Dialing
12. Virus and Trojan Detection
13. Log Management Penetration Testing
14. File Integrity Checking
15. Telecommunication and Broadband Communication Penetration Testing
16. Email Security Penetration Testing
17. Security Patches Penetration Testing
18. Data Leakage Penetration Testing
19. SAP Penetration Testing
20. Standards and Compliance
21. Information System Security Principles
22. Information System Incident Handling and Response
23. Information System Auditing and Certification

Hackgates

Description du cours EC-Council Certified Security Analyst v10

Certification ECSAv10 (incluse avec la formation)

L'ECSA Practical est un examen rigoureux de 12 heures, qui demandera aux participants de démontrer leurs capacités à suivre la méthodologie de pentest enseignée dans la formation ECSA. Les candidats commenceront par des challenges sur les sujets suivants: scan avancé de réseau derrière le périmètre de défense, menant à des analyses de vulnérabilité automatiques et manuelles, sélection d'exploits ou encore les manœuvres post-exploitation.
L'ESCA Practical testera également les compétences des candidats en recherche d'exploits et de menaces, à comprendre les exploits existants, à écrire leurs propres exploits ainsi que la capacité à prendre les décisions critiques durant les différentes phases de pentest. Il sera demandé aux candidats d'écrire un rapport de pentest avec les éléments et les instructions essentiels permettant à l'organisation de prendre des décisions en s'appuyant sur ce rapport.
L'ECSA Practical apporte une garantie que les candidats possèdent les compétences requises dans le domaine et fera office de témoignage à leur capacité à se soumettre à la rigueur de cette profession.

Passage de l'examen

Cet examen aura lieu en ligne, en direct et automatiquement supervisé par un Proctor à distance.
•Titre de l'examen: EC-Council Certified Security Analyst (Practical)
•Nombre de challenges pratiques : 8
•Durée : 12 heures
•Langue: anglais
•Score requis : minimum de 5 challenges réussis et validation du rapport

Destinataire de l'examen

Toute personne officiellement et dûment certifiée ECSA (toute version) pourra se présenter à l'examen ECSA Practical.

Processus d'éligibilité

Les candidats intéressés par ce programme devront au préalable remplir un formulaire d'éligibilité.
Cette éligibilité, qui est généralement validée entre 5 et 10 jours par EC-Council, est ensuite valable pour 3 mois.
A réception du code Dashboard, à activer sous ASPEN, le candidat aura également 3 mois pour tester et compléter les différents challenges proposés.

Hackgates

Description du cours Mener un audit de sécurité: méthode d'audit d'un SI

Mettre en place des audits de sécurité de qualité au sein de votre SI

Aujourd'hui, pour affirmer avoir un niveau de protection suffisant sur l'ensemble de son infrastructure, il est nécessaire de réaliser des audits.
Ce cours a pour objectif d'illustrer toutes les méthodes pour éprouver les systèmes avec l'ensemble des attaques connues.
Mener un audit impose des règles et des limitations qu'il est nécessaire de connaître.
Cette formation décrit les différentes méthodologies d'audit ainsi que leur particularité.
Une présentation des outils indispensables ainsi que des travaux pratiques pour comprendre et connaître leur utilisation sera faite. Pour finir une étude de cas de systèmes vulnérables sera étudiée pour illustrer les principales vulnérabilités rencontrées et comment l'évaluation d'une vulnérabilité est faite en fonction de son impact, de sa potentialité.

Objectifs
•Bien délimiter un audit, connaître les méthodes existantes
•Connaître les règles et les engagements d'un audit, et ses limitations
•Quelles sont les méthodologies reconnues
•Mettre en place une situation d'audit
•Les outils nécessaires pour réaliser un audit

Hackgates

Description du Mener un audit de sécurité: méthode d'audit d'un SI

Jour 1

•Définition du test d'intrusion
•L'intérêt du test d'intrusion
•Les phases d'un test d'intrusion
- Reconnaissance
- Analyse des vulnérabilités
- Exploitation
- Gain et maintien d'accès
- Comptes rendus et fin des tests

Règles et engagements

•Portée technique de l'audit
Responsabilité de l'auditeur
•Contraintes fréquentes
•Législation : articles de loi
•Précautions usuelles
Les types de tests d'intrusion
•Externe
•Interne
Méthodologie
•Utilité de la méthodologie
•Méthodes d'audit
•Méthodologies reconnues

Particularités de l'audit
•d'infrastructure classique
•d'infrastructure SCADA
•web
•de code

Jour 3

Étude de cas
•Application de la méthodologie et des outils sur un cas concret

Les livrables
•Évaluation des risques
•Impact, potentialité et criticité d'une vulnérabilité
•Organiser le rapport
•Prestations complémentaires à proposer

Jour 2

Les outils d'audit de code
•Outils d'analyse de code
•Outils d'analyse statique
•Outils d'analyse dynamique

Les outils de prise d'information
•Prise d'information
- Sources ouvertes
- Active

•Scanning
- Scan de ports
- Scan de vulnérabilités

Les outils d'attaque
•Outils réseau
•Outils d'analyse système
•Outils d'analyse web
•Frameworks d'exploitation
•Outils de maintien d'accès

Hackgates

Description du cours Lutte contre la cybercriminalité : mise en pratique

Apprenez à vous défendre face aux cybermenaces

Cette formation permet de faire une revue des vulnérabilités et des menaces actuelles en proposant des contre-mesures associées. Nous aborderons les différents mécanismes de sécurité ainsi que les moyens de protection. La partie pratique de la formation vous préparera à faire face aux enjeux de la cybersécurité.

Objectifs
•Comprendre les enjeux liés à la cybersécurité
•Définir les acteurs
•Connaître les risques numériques
•Mieux comprendre la législation française vis-à-vis de la cybercriminalité

Hackgates

*Description du cours*Lutte contre la cybercriminalité : mise en pratique

Jour 1

Notion de vulnérabilité, attaque et menace

Mécanisme de sécurité et moyen de protection
- **Protection contre les logiciels malveillants**
- **Chiffrement**
- **Contrôles d'accès logiques**
- **Isolation réseau**
- **Sécurité physique**
- **Audibilité**
- **Norme et conformité**
- **Formation et sensibilisation**

Menaces
Détection
Contre mesure (Monitoring et journalisation)

Jour 2

Mise en place de contre mesure par thème
Internet des objets et Smartphones
- **Menaces**
- **Détection**
- **Contre mesure (Mobile Security Management)**

Réseaux sociaux, Arnaques
- **Menaces**
- **Détection**
- **Contre mesure (Programme de sensibilisation et formation)**

Surface Web
- **Menaces**
- **Détection**
- **Contre mesure (Audit, Bug Bounty, Firewall applicatif)**

Jour 3

- **Menaces**
- **Détection**

Menaces
Détection
Contre mesure (Monitoring et journalisation)

Fuites d'informations et vie privé
- **Menaces**
- **Détection**
- **Contre mesure (Veille quotidienne et o**

Cloud et Infrastructure critiques
- **Menaces**
- **Détection**

Contre mesure (Veille sécurité et mise à jour)

Hackgates

Description du cours Sécurisation des Réseaux

Protégez votre réseau des attaques informatiques

**Cette formation a pour but de passer en revue les différentes attaques visant les protocoles et équipements réseau.
Une démonstration et mise en pratique des attaques sera faite ainsi que l'explication des contre-mesures à apporter.
Nous étudierons dans un premier temps les attaques visant ou utilisant les protocoles de couche 2 qui profitent de problèmes
de configuration des commutateurs (switch). Suivront les attaques ciblant les routeurs et les systèmes VPN.
Enfin, nous nous intéresserons aux équipements permettant de renforcer la sécurité d'un réseau informatique (Pare-feu, IDS/IPS, Proxy, etc.)**

Objectifs

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

Hackgates

Description du cours Securisation des réseaux

Jour 1

Présentation des enjeux de la sécurité des réseaux

Démonstration des attaques ciblant les équipements de niveau 2 et leurs contre-mesures

- **ARP**
- **VLAN**
- **CDP**
- **Spanning Tree**
- **Etc.**

Jour 2

Attaque et protection des équipements et protocoles de niveau 3

- **Ipv4 et Ipv6**
- **RIP**
- **OSPF**
- **EIGRP**
- **BGP**

Jour 3

Les outils de protection réseau

- **Pare-feu**
- **IDS/IPS**
- **Serveur mandataire**

- **VRRP**
- **HSRP**
- **GLBP**

Attaques et contre-mesures sur les VPN

Chiffrement des communications: utilisations et bonnes pratiques

Attaques et contre-mesures sur les passerelles virtuelles

Hackgates

Description du cours SIEM et Veille Technologique Sécurité

Maîtrisez votre gestion d'évènements et restez au cœur de l'actualité
en mettant en œuvre une veille efficace

Ce cours est un guide pratique visant à présenter les technologies défensives autour de la terminologie SIEM et de la détection d'intrusion. Le contenu est indépendant de tout constructeur et vise à donner une vue globale et impartiale, sur les aspects fonctionnels et techniques. L'objectif est de fournir au stagiaire les outils et les connaissances nécessaires pour aborder un marché où les solutions sont multiples, complexes et parfois difficiles à discerner.

Nous étudierons la mise en place de sondes de détection d'intrusion autour des solutions Suricata et OSSEC. Les stagiaires apprendront notamment à écrire des règles de détection Snort et OSSEC. Nous apprendrons ensuite comment centraliser et gérer les journaux en provenance de ces sondes et d'autres sources des systèmes d'exploitation.

Après un bref rappel des menaces contemporaines et des défis posés aux équipes de supervision comme aux outils historiques, nous nous attacherons enfin à décrire le fonctionnement d'une solution SIEM et de ses avantages dans le cadre de la gestion de ces évènements.

Nous réaliserons la mise en pratique des connaissances sur une plateforme libre, au code source ouvert, et très en vogue : ELK (Elastic Search, Logstash, Kibana).

De plus ce cours sera accompagné par une présentation des méthodes de mise en place d'une veille technologique efficace et organisée. La démonstration d'outils collaboratifs offrant la possibilité d'échanger simplement des informations cruciales sur l'émergence de nouvelles vulnérabilités et de techniques d'attaque sera faite. L'information étant n'importe où, des techniques de recherche avancées seront exposées.

En somme, cette formation permettra de faire un tour des points clés à retenir dans le cadre d'un appel d'offre pour choisir la solution du marché la plus adaptée à son besoin.

Objectifs

•Devenir efficace dans la veille technologique
•Obtenir les clés pour monter une équipe de veille au sein d'une organisation
•Comprendre les limites des outils de sécurité classiques
•Découvrir les principes technologiques derrière l'acronyme SIEM
•Apprendre à détecter les menaces parmi un grand volume d'information

Hackgates

Description du cours Sensibilisation au développement sécurisé

Sensibilisez-vous aux attaques les plus utilisées afin de mieux protéger vos applications

Cette formation vous explique les vulnérabilités web et applicatives les plus utilisées par les attaquants afin de mieux comprendre comment vous protéger. Vous apprendrez les bonnes pratiques et les bons réflexes de développement afin de minimiser les risques de compromission. Cette formation couvre l'essentiel du développement sécurisé dans différents langages, de la conception au déploiement.

Objectifs

- **Comprendre les enjeux de la sécurité des applications classiques et sur le web**
- **Acquérir les bonnes pratiques et les bons réflexes pour le développement d'applications**
- **Savoir utiliser les outils pour développer de façon sécurisée**

Hackgates

Description du cours Malwares: détection, identification et éradication

Apprenez Apprenez les bases de l'analyse de malwares sous Windows

Cette formation aborde l'historique et le fonctionnement des malwares. Vous apprendrez à distinguer les grandes familles de malwares et leurs techniques d'infection, de propagation et de persistance, mais également à effectuer une analyse avancée et à établir un plan de remédiation.

Objectifs
- **Connaitre les différents types de malwares**
- **Identifier un malware**
- **Analyser un malware**
- **Mettre en œuvre des contre-mesures adéquates**

Hackgates

Description du cours Analyse inforensique avancée et réponse aux incidents

Préparez-vous à l'analyse post-incident
Ce cours vous apprendra à mettre en place une procédure complète d'analyse inforensique sur des environnements hétérogènes.
Vous y aborderez la réponse à incidents d'un point de vue organisationnel.
Vous étudierez également les méthodologies et outils appropriés utilisés dans la phase technique de la réponse à incident, à savoir l'analyse inforensique (ou post-incident).
À l'issue de la formation, vous serez capable de préserver les preuves numériques pour en effectuer l'analyse ultérieure et les présenter dans le cadre d'un recours judiciaire.
Objectifs
•Être capable de définir et mettre en place un processus de réponse à incident rigoureux
•Collecter correctement les preuves nécessaires à une analyse de qualité et à d'éventuelles poursuites judiciaires
•Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion

Hackgates

Description du cours Computer Hacking Forensic Investigator v9

La certification de l'investigation numérique - « Accredited Training Center » by EC-Council

Les nouvelles technologies sont en train de changer le monde professionnel. Les entreprises s'accommodant rapidement aux technologies numériques comme le cloud, le mobile, le big data ou encore l'IoT, rendent l'étude du forensique numérique dorénavant nécessaire.
Le cours CHFIv9, dernière version du programme, a été développé pour des professionnels en charge de la collecte de preuves numériques après un cyber crime. Il a été conçu par des experts sur le sujet et des professionnels du secteur, il présente les normes mondiales en matière de bonnes pratiques forensiques. En somme, il vise également à élever le niveau de connaissances, de compréhension et de compétences en cybersécurité des acteurs du forensique.
Le programme CHFIv9 offre une approche méthodologique détaillée du forensique et de l'analyse de preuves numériques. Il apporte les compétences nécessaires à l'identification de traces laissées par un intrus mais également à la collecte de preuves nécessaires à sa poursuite judiciaire. Les outils et savoirs majeurs utilisés par les professionnels du secteur sont couverts dans ce programme. La certification renforcera le niveau de connaissances de toutes les personnes concernées par l'intégrité d'un réseau et par l'investigation numérique.
Objectifs
•Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires
•Se préparer à l'examen CHFI 312-49