Catalogue de formations
Sécurité offensive – Hacking Éthique

Ce catalogue a été conçu en cycle de 20 jours proposant un panorama des différentes techniques de hacking éthique.
Chaque formation peut être réalisée indépendamment et être **adaptée** à vos besoins.

CYBERWINGS
ACADEMY

Ce document est la propriété de Cyberwings Academy. Toute reproduction même partielle est strictement interdite sans accord écrit. Version 04/2025.

Cyberwings Academy – 565 Avenue du Prado, 13008 Marseille - www.cyberwings.academy
RCS Marseille 98413556600011 – **APE** 8559A – Numéro Activité Formation : 93 13 22155 13

Les fondamentaux du hacking éthique

Cette journée introductive au cycle de hacking vous permettra de poser les bases juridiques et d'appréhender la philosophie du hacking.

OBJECTIFS PÉDAGOGIQUES

- Comprendre ce qu'est le hacking
- Identifier les acteurs
- Appréhender l'approche réglementaire lié au hacking

PROGRAMME

Histoire et personnalités du hacking

État d'esprit et définitions

Approche offensive, la cyber-kill chain, le modèle du PTES

Ingénierie sociale et OSINT

Généralités juridiques, organisationnelles et techniques

Contexte et communautés internationales

Les référentiels liés aux tests d'intrusion

Les certifications

Ref : SSI-H-001

Séminaire

1 jour, soit 7 heures

PUBLIC :

Pentesteurs, RSSI, Directeur Cybersécurité

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz, test d'auto-positionnement en début et fin de formation
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 890 € HT / pers.
Devis personnalisé : nous consulter

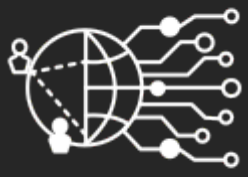
PROCHAINES SESSIONS :

Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CONFIDENTIEL. Ce document est la propriété de Cyberwings Academy.
Toute reproduction même partielle est strictement interdite sans accord écrit.



Hacking réseau

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre système d'information et plus particulièrement de vos réseaux.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les attaques réseaux
- Découvrir les différents outils
- Apprendre comment détecter ces attaques

PROGRAMME

Sniffing

Outils de sniffing passifs
Outils de sniffing actifs
Comprendre Wireshark et un pcap
Divers outils d'analyse réseau
Détection du sniffing

Scanning

Les différents scans
Outils de scan
Nmap et scripting
Scapy
Détection de filtrage

Prises d'accès sur le réseau

Interception et Man In The Middle
DoS et DdoS
Attaques sur les VLANs
Attaques sur les protocoles DHCP, DNS, FTP, SNMP …
Attaques sur le routage

Contournement des équipements de protection

NIDS & SIEM : leur rôle dans la détection des menaces
Firewall classique, firewall applicatif, firewall DPI : les différences
Contournement des règles de détection
Canaux cachés

WIFI et protocoles sans fil

Rappel des protocoles
Principes des attaques WIFI et sur les autres protocoles sans fil : Evil Twin, PMKID Attack, Handshake Capture, Offline Cracking, WPS Attack...

TRAVAUX PRATIQUES

- Tous les outils et attaques seront mis en pratique par les stagiaires

Ref : SSI-H-002

Stage pratique

5 jours, soit 35 heures

PUBLIC :

Pentesteurs, Admin Sys et réseau

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : bonnes connaissances Linux et réseau (avoir réaliser les formations IT-R-001 et IT-L-002 avec Cyberwings Academy) ou avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et des TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 3 090 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CONFIDENTIEL. Ce document est la propriété de Cyberwings Academy.
Toute reproduction même partielle est strictement interdite sans accord écrit.

Hacking web

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre site web et réaliser des tests d'intrusion sur vos sites Web en suivant l'OWASP.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les attaques web
- Découvrir les différents outils
- Apprendre comment détecter ces attaques

PROGRAMME

Introduction

Rappel sur le protocole HTTP et HTTPS
Rappel sur la cryptographie
Les vecteurs d'attaque sur les applications Web
L'OWASP et le TOP 10 de l'OWASP
Réglementation applicable sur les application Web

Panorama des attaques Web

Présentation des plateformes et outils dvwa, bwapp, burp suite, sqlmap, fimap, weevely
Exposition de données sensibles
XSS (Cross Site Scripting)
Csrf (cross site request forgery)
Injections SQL, LDAP, PHP, HTML ...
Api non protégée
Références directes non sécurisées à un objet
Mauvaise configuration de sécurité
Compréhension des différentes protections autour des architectures client-server (csp, x-frame, hsts, httponly, secure cookie, WAF)

TRAVAUX PRATIQUES

- Tous les outils et attaques seront mises en pratique par les stagiaires

Ref : SSI-H-003

Stage pratique

4 jours, soit 28 heures

PUBLIC :

Pentesteurs, Admin Sys et réseau, Développeurs Web, Chef de projets web, Développeurs DevOp

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : connaissances en technologie du web (avoir réaliser les formations SSI-D-005 avec Cyberwings Academy) ou avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et des TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 2 890 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Sir demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CONFIDENTIEL. Ce document est la propriété de Cyberwings Academy.
Toute reproduction même partielle est strictement interdite sans accord écrit.

Hacking applicatif

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité d'une application et comprendre les mécanismes de reverse engineering.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les principaux mécanismes d'attaques sur les binaires
- S'initier à la cryptanalyse
- Comprendre et étudier le fonctionnement d'un malware

PROGRAMME

Introduction

Fonctionnement d'un binaire et d'un processus
Rappel sur la cryptographie

Cryptanalyse

Reconnaissance d'un algorithme de chiffrement
Panorama des attaques
Attaques sur le hachage, rainbow tables et bruteforce

Attaques sur les binaires

Buffer overflow
String format
Shellcode

Reverse engineering

Principe de base
Les outils
Protection des binaires et contournements
Analyse d'un malware

La plateforme Metasploit

Les différents modules
Meterpreter
Création de malware

TRAVAUX PRATIQUES

- Tous les outils et attaques seront mises en pratique par les stagiaires.

Ref : SSI-H-004

Stage pratique

4 jours, soit 28 heures

PUBLIC :

Pentesteurs, Admin Sys et réseau, Développeurs, Chef de projets développement

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : connaissance en développement : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et des TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 3 990 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CONFIDENTIEL. Ce document est la propriété de Cyberwings Academy.
Toute reproduction même partielle est strictement interdite sans accord écrit.

Hacking windows

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre système windows, d'une infrastructure microsoft et du service Active Directory.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les principales attaques d'un système windows
- Comprendre les principales attaques sur l'active directory
- Savoir mettre en place les mesures suffisantes de protection

PROGRAMME

Introduction

Rappel des mécanismes de sécurité de windows

Rappel des mécanismes d'authentification de windows (NT, NTLM, Kerberos)

Rappel sur le projet Metasploit

Attaques sur les mécanismes de protection windows

Attaques sur Pass-the-hash

Bypass des protections antivirales proposées par microsoft

Panorama des vulnérabilités connues (RDP, Eternal Blue...)

Attaques sur l'AD

Les différents outils

Kerberoasting

Pass-the-ticket, golden ticket, silver ticket

TRAVAUX PRATIQUES

- Tous les outils et attaques seront mises en pratique par les stagiaires

Ref : SSI-H-005

Stage pratique

3 jours, soit 21 heures

PUBLIC :

Pentesteurs, Admin Sys et réseau, Intégrateurs Microsoft

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : connaissance en système windows : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et des TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 2 790 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CONFIDENTIEL. Ce document est la propriété de Cyberwings Academy.
Toute reproduction même partielle est strictement interdite sans accord écrit.

Réaliser un test d'intrusion

Cette formation avancée pratique (0,5 jours de théorie, 2,5 jours de pratique) vous permettra d'acquérir une méthodologie pour organiser un audit de sécurité de type test de pénétration sur son SI.

OBJECTIFS PÉDAGOGIQUES

- Acquérir une méthodologie pour réaliser un test d'intrusion
- Savoir rédiger un rapport final suite à un test d'intrusion
- Savoir formuler des recommandations de sécurité

PROGRAMME

Méthodologie d'un pentest

Méthodologie de l'audit
Rappel du contexte juridique
Rédaction du rapport
Restitution auprès du client
Panorama des outils

TRAVAUX PRATIQUES

- Sur l'une des thématiques hacking (Web, applicatif, réseau ou Windows), mener pendant 2,5 jours un test d'intrusion puis réaliser un rapport et une restitution.

Ref : SSI-H-006

Stage pratique

3 jours, soit 21 heures

PUBLIC :

Pentesteurs, Admin Sys et réseau

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : connaissance des diverses techniques d'attaques et des outils Hacking (avoir réalisé au moins deux modules parmi SSI-H-002, SSI-H-003, SSI-H-004, SSI-H-005 avec Cyberwings Academy) ou avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et des TP, test d'auto-positionnement en début et fin de formation, restitution finale évaluée par le formateur
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 3 900 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CONFIDENTIEL. Ce document est la propriété de Cyberwings Academy.
Toute reproduction même partielle est strictement interdite sans accord écrit.

Comment financer votre formation ?

Vous êtes salarié

Votre formation est financée par votre entreprise ou pas des fonds gérés par les OPCO via :

- le plan de développement des compétences
- les actions collectives ou clé en main
- les dispositifs étatiques en cours
- une dotation sur votre CPF si formation certifiante

Vous êtes travailleur non salarié *

Votre formation peut être financée par :

- les fonds d'assurance formation (FAF)
- votre CPF si formation certifiante
- vos fonds propres

** Dirigeant, président, profession libérale, autoentrepreneur*

Vous êtes demandeur d'emploi

Votre formation peut être financée par :

- l'aide individuelle à la formation (AIF)
- l'aide individuelle régionale vers l'emploi (AIRE)
- votre région
- votre CPF si formation certifiante
- vos fonds propres

Votre démarche est personnelle

Vous êtes salarié mais vous souhaitez financer votre formation sans passer par votre entreprise ?

Vous pouvez utiliser :

- votre CPF si formation certifiante
- vos fonds propres

OPCO opérateurs de compétences · France Travail · MON COMPTE FORMATION · Ministère du Travail, de l'Emploi et de l'Insertion – FNE Formation

Modalités d'accès

Vous pouvez vous inscrire pour suivre une de nos formations jusqu'à la veille de la date de démarrage si la formation est financée directement par votre entreprise ET si le nombre maximum de participants n'est pas atteint.

Nos locaux sont accessibles aux Personnes à Mobilité Réduite.
Pour les personnes en situation d'handicap, vous pouvez contacter notre référente handicap au 07 52 05 10 68 ou à l'adresse inclusion@cyberwings.fr.

Nos conseillers sont disponibles pour vous accompagner dans toutes vos démarches. Nous sommes en mesure de mobiliser les expertises, les outils nécessaires pour vous accueillir, vous accompagner et vous former.

Qualiopi processus certifié – RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée par **AFNOR Certification** au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

CYBERWINGS ACADEMY

Cyberwings Academy – 565 Avenue du Prado, 13008 Marseille - www.cyberwings.academy
RCS Marseille 98413556600011 – **APE** 8559A – Numéro Activité Formation : 93 13 22155 13

Qui sommes-nous ?

Cyberwings Academy

Cyberwings Academy est le fruit de l'évolution du département Formation de l'entité Cyberwings, capitalisant sur plus de 20 années d'expérience dans le hacking éthique et le management de l'information stratégique.

Nos experts

Nos experts qui animent la formation sont des spécialistes des matières abordées. Nous tenons en effet à cette dénomination « d'experts » formateurs dans la mesure où ces hommes et femmes sont avant tout des professionnels passionnés par leur activité, fort d'expériences variées, significatives et mises à profit de nos stagiaires.

Nos thèmes pédagogiques

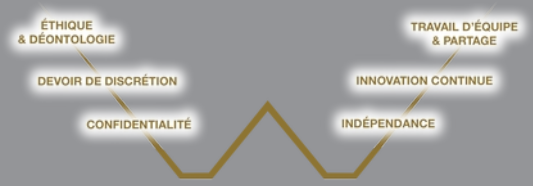
Techniques

- Hacking
- Techniques défensives
- Détection d'intrusions
- Réseaux informatiques
- Linux
- Cryptographie
- Blue / Red team
- Windows expertise
- ...

Non techniques

- Sécurité de l'information
- Secret des affaires
- Données personnelles
- Intelligence économique
- OSINT
- Cyber-stratégies
- Guerre de l'information
- ....

Nos valeurs



Les labels du groupe

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée par **AFNOR Certification** au titre de la catégorie d'actions suivantes :
ACTIONS DE FORMATION

CYBERWINGS ACADEMY

Cyberwings Academy – 565 Avenue du Prado, 13008 Marseille - www.cyberwings.academy
RCS Marseille 98413556600011 – **APE** 8559A – Numéro Activité Formation : 93 13 22155 13