Formations Hacking

certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

3 allée des Séquoias - 69760 LIMONEST
04 28 29 72 50 - contact@certilience.fr

www.certilience.fr

Nos formations

HAC01	35 heures	*Les techniques d'attaques*
HAC02	21 heures	*Vulnérabilités Réseaux et Applicatives*
HAC03	21 heures	*Sécurité des Applications Web*
HAC04	14 heures	*Vulnérabilités de la téléphonie sur IP*
HAC05	7 heures	*Sécurité offensive avec Metasploit*
HAC06	7 heures	*Audit de vulnérabilité avec OpenVAS*
HAC07	14 heures	*Hacking Cloud Computing*
HAC08	5x 3 heures	*Club Utilisateurs - Culture de la Sécurité*

avertissement

les participants s'engagent en nom propre et sur la non-utilisation des compétences acquises à des fins « offensives » et « illicites ».

ORDINATEUR PORTABLE NON FOURNI

HAC01 Techniques d'Attaques

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en réseau, en système, en développement et en scripting	RSSI, Administrateur Réseau et Système, Consultant sécurité, Agence gouvernementale, Informaticien averti	locaux Certilience / vos locaux	35 heures (5 jours)

La formation ***Techniques d'Attaques*** permet d'acquérir des connaissances sur les techniques d'attaques pour mieux les anticiper et apprendre à les contrer.

NB : Elle comprend les formations **HAC02 *Vulnérabilités Réseaux et Applicatives*** et **HAC03 *Sécurité des Applications Web***.

OBJECTIFS DE LA FORMATION

- Acquérir les réflexions intellectuelles essentielles aux contre-mesures
- Comprendre et évaluer une faille sur le système d'information
- Identifier et prioriser les mesures correctives
- Sensibilisation des bonnes pratiques

PROGRAMME

Module Réseau : *Comprendre les attaques réseaux*

1/. recherche d'information

- Découverte des infrastructures
- Présentation des informations DNS

2/. scans et firewalking

- Présentation des outils pour les différents types de scans : Network scanning, Port scanning, Vulnerability Scanning
- TCP/IP
- Découverte de réseaux (Nmap, Ping, Metasploit, etc.)
- Firewalking : techniques et outils
- Protections

3/. attaques Réseau

- Sniffing Réseau : les outils de base (wireshark / tshark / tcpdump)
- Spoofing Réseau :
  - contournements avec 802.1x
  - récupération d'informations avec CDP (Cisco Discovery Protocol)
  - attaques sur Spanning Tree
  - attaques sur DTP
  - saut de VLAN
  - Mac Flooding/DHCP starvation/…
- Détournement de sessions : TCP hijacking
- Analyse des transmissions chiffrées

Module Système : *Démystifier les attaques applicatives*

1/. rappels sur le C

2/. prise en main d'un debugger

- l'assembleur / comment désassembler
- le CPU
- appel de fonctions
- debugger un process

HAC01 Techniques d'Attaques

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en réseau, en système, en développement et en scripting	RSSI, Administrateur Réseau et Système, Consultant sécurité, Agence gouvernementale, Informaticien averti	locaux Certilience / vos locaux	35 heures (5 jours)

PROGRAMME (suite)

3/. élaboration d'un exploit
- les exploits en C : buffer overflow, format string, use-after-free
- Shellcoding
- protections et contournements
- system() FTW

4/. présentation du fuzzing
- les différents outils
- Démonstration

5/. Framework Metasploit
- présentation
- création d'un module Metasploit

6/. contournement d'un antivirus
- les limites d'un antivirus
- challenge

7/. Les bonnes pratiques en C

Sécurité des Applis Web :
Comprendre les 10 vulnérabilités web les plus fréquentes

1/. architecture Web

2/. mapping d'une application : recherche d'informations passive et active
- "VirtualHost hacking"
- Découverte des infrastructures
- Découverte OS et technologie
- Utilisation des moteurs de recherche pour découvrir du contenu
- Carte de l'application :
  - utilisation de Crawler ou Spider
  - découverte des parties cachées : outil de brute force
- Analyse de l'application :
  - technologies
  - champs des formulaires
  - surface d'attaque

3/. rappels sur le protocole http

4/. outils
- Présentation des outils Dirbuster, Burpsuite, Metasploit, Sqlmap, Webscarab, Nmap, …

5/. le TOP 10 OWASP et les vulnérabilités web
- Violation de Gestion d'authentification et de Session
- Attaque de l'utilisateur : Cross Site Scripting (XSS)
- Injection (SQL, LDAP, etc.)
- Attaque des composants
- Attaque logique de l'application : références directes non sécurisées à un Objet
- Falsification de requête inter-sites (CSRF)
- Mauvaise configuration sécurité
- Stockage cryptographique non sécurisé
- Protection insuffisante de la couche Transport
- Redirection et Renvois non validés
- XML External Entities

6/. validation du module
- Challenges

HAC02 Vulnérabilités Réseaux et Applicatives

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en administration des systèmes d'exploitation Savoir écrire des algorithmes	RSSI, Administrateur Réseau et Système, Consultant sécurité, Responsable Développement / Développeur	locaux Certilience / vos locaux	21 heures (3 jours)

Les 2 modules de formation ***Vulnérabilités Réseaux*** et ***Vulnérabilités Système*** permettent d'acquérir une démarche intellectuelle essentielle aux contre-mesures et aux bonnes pratiques.

NB : Cette formation complétée de la HAC03 *Sécurité des Applications Web* constituent la formation **HAC01** ***Techniques d'Attaques***.

OBJECTIFS DE LA FORMATION

- Découvrir les techniques de piratage
- Comprendre et évaluer l'impact d'une faille sur un système d'information
- Identifier et prioriser les mesures correctives

PROGRAMME

Module Réseau : *Comprendre les attaques réseaux*

1/. recherche d'information

- Découverte des infrastructures
- Présentation des informations DNS

2/. scans et firewalking

- Présentation des outils pour les différents types de scans : Network scanning, Port scanning, Vulnerability Scanning
- TCP/IP
- Découverte de réseaux (Nmap, Ping, Metasploit, etc.)
- Firewalking : techniques et outils
- Protections

3/. attaques Réseau

- Sniffing Réseau : les outils de base (wireshark / tshark / tcpdump)
- Spoofing Réseau :
  - contournements avec 802.1x
  - récupération d'informations avec CDP (Cisco Discovery Protocol)
  - attaques sur Spanning Tree
  - attaques sur DTP
  - saut de VLAN
  - Mac Flooding/DHCP starvation/…
- Détournement de sessions : TCP hijacking
- Analyse des transmissions chiffrées

HAC02 Vulnérabilités Réseaux et Applicatives

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en administration des systèmes d'exploitation Savoir écrire des algorithmes	RSSI, Administrateur Réseau et Système, Consultant sécurité, Responsable Développement / Développeur	locaux Certilience / vos locaux	21 heures (3 jours)

PROGRAMME (suite)

Module Système :
Démystifier les attaques applicatives

1/. rappels sur le C

2/. prise en main d'un debugger
- l'assembleur / comment désassembler
- le CPU
- appel de fonctions
- debugger un process

3/. élaboration d'un exploit
- les exploits en C : buffer overflow, format string, use-after-free
- Shellcoding
- protections et contournements
- system() FTW

4/. présentation du fuzzing
- les différents outils
- Démonstration

5/. Framework Metasploit
- présentation
- création d'un module Metasploit

6/. contournement d'un antivirus
- les limites d'un antivirus
- challenge

7/. Les bonnes pratiques en C

HAC03 Sécurité des Applications Web

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en administration des systèmes d'exploitation Savoir écrire des algorithmes	RSSI, Administrateur Réseau et Système, Consultant sécurité, Responsable Développement / Développeur	locaux Certilience / vos locaux	21 heures (3 jours)

La formation ***Sécurité des Applications Web*** permet d'acquérir une démarche intellectuelle essentielle aux contre-mesures et aux bonnes pratiques.

NB : Cette formation complétée de la HAC02 *Vulnérabilités Réseaux et Applicatives* constituent la formation **HAC01 *Techniques d'Attaques***.

OBJECTIFS DE LA FORMATION

- Découvrir les techniques de piratage
- Comprendre et évaluer l'impact d'une faille sur un système d'information
- Identifier et prioriser les mesures correctives

PROGRAMME

Sécurité des Applis Web :
Comprendre les 10 vulnérabilités web les plus fréquentes

1/. architecture Web

2/. mapping d'une application : recherche d'informations passive et active

- "VirtualHost hacking"
- Découverte des infrastructures
- Découverte OS et technologie
- Utilisation des moteurs de recherche pour découvrir du contenu
- Carte de l'application :
  - utilisation de Crawler ou Spider
  - découverte des parties cachées : outil de brute force
- Analyse de l'application :
  - technologies
  - champs des formulaires
  - surface d'attaque

3/. rappels sur le protocole http

4/. outils

- Présentation des outils Dirbuster, Burpsuite, Metasploit, Sqlmap, Webscarab, Nmap, …

5/. le TOP 10 OWASP et les vulnérabilités web

- Violation de Gestion d'authentification et de Session
- Attaque de l'utilisateur : Cross Site Scripting (XSS)
- Injection (SQL, LDAP, etc.)
- Attaque des composants
- Attaque logique de l'application : références directes non sécurisées à un Objet
- Falsification de requête inter-sites (CSRF)
- Mauvaise configuration sécurité
- Stockage cryptographique non sécurisé
- Protection insuffisante de la couche Transport
- Redirection et Renvois non validés
- XML External Entities

6/. validation du module

- Challenges

HAC04 Vulnérabilités de la Téléphonie sur IP

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en administration des systèmes d'exploitation Savoir écrire des algorithmes	RSSI, Administrateur Réseau et Système, Consultant sécurité, Responsable Développement / Développeur	locaux Certilience / vos locaux	14 heures (2 jours)

La formation ***Vulnérabilités de la Téléphonie sur IP*** permet d'acquérir une démarche intellectuelle essentielle aux contre-mesures et aux bonnes pratiques.

OBJECTIFS DE LA FORMATION

- Comprendre les mécanismes de la téléphonie sur IP
- Découvrir les architectures types
- Comprendre les techniques d'attaques
- Acquérir les bonnes pratiques

PROGRAMME

1/. présentation de la VoIP

- Intérêts : réduction des coûts, services, convergence fixe mobile
- Architecture type (Centrex / IPBX, class 4 / class 5, téléphones IP)
- Messages SIP : enregistrement et appel
- Codage de la voix sur IP : différents codecs, notion de QoS (perte de paquets, latence, gigue)

2/. les différents types d'attaques

- Écoute illégale
- Usurpation d'identité
- Man in the middle (modification ou détournement d'appels)
- Corruptions du serveur (déni de service, changement de configuration)

3/. la sécurité dans la VoIP

- Sécuriser l'accès aux serveurs (restriction SSH et web)
- Protéger le réseau (VLAN différenciés, firewall, NAT)
- Sécuriser les appels téléphoniques : gestion des services et mots de passe, chiffrement
- Agir de façon préventive : archivage, surveillance des serveurs, détection d'attaques

HAC05 Sécurité Offensive avec Metasploit

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en administration des systèmes d'exploitation Savoir écrire des algorithmes	RSSI, Administrateur Réseau et Système, Consultant sécurité, Responsable Développement / Développeur	locaux Certilience / vos locaux	7 heures (1 jour)

La formation ***Sécurité Offensive avec Metasploit framework*** vise l'apprentissage de cet outil open-source pour le développement et l'exécution d'exploits (logiciel malveillant) contre une machine distante.

OBJECTIFS DE LA FORMATION

- Découvrir le Framework d'exploitation « Metasploit »
- Savoir installer, utiliser et exploiter Metasploit et développer un module
- Appréhender les contre-mesures aux techniques de piratage actuelles
- Pouvoir exploiter une vulnérabilité avec Metasploit

PROGRAMME

1/. introduction à Metasploit
- Présentation de l'architecture
- Présentation des fonctions

2/. les bases
- Utilisation de msfconsole
- Exploits
- Payloads

3/. récupération d'informations
- Scan de ports,
- Test de bases,
- Test de services

4/. utilisation en exploitation
- Exploitation d'une vulnérabilité
- Présentation d'un exploit
- Écriture d'un exploit

5/. Meterpreter
- Fonctionnement et Présentation
- Contexte d'utilisation
- Post exploitation

HAC06 Analyse des vulnérabilités avec OpenVAS

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissance en réseau	RSSI, Administrateur Réseau et Système	locaux Certilience / vos locaux	7 heures (1 jour)

La formation ***Analyse des Vulnérabilités avec OpenVAS (Opensource Vulnerability Assessment Scanner)*** vise la compréhension et l'apprentissage de cet outil qui permet de mesurer le niveau de sécurité d'un système d'information.

OBJECTIFS DE LA FORMATION

- Découvrir l'outil
- Savoir installer et configurer le produit
- Être capable de développer un module
- Savoir exploiter la solution au quotidien

PROGRAMME

1/. principe de fonctionnement
- introduction aux scanners
- présentation des briques
- présentation de l'architecture

2/. installation
- configuration réseau
- configuration système

3/. présentation des interfaces de l'outil
- CLI (Interface de commandes)
- GUI (Interface graphique)

4/. étape d'un scan
- renseignement du scope
- planification des taches
- reporting

5/. Écriture d'un plugin

HAC07 Hacking Cloud Computing

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Bases administration système (système, scripting,...) et de technique de virtualisation	RSSI, DSI, Consultant sécurité, Consultant Cloud Computing, Responsable et Administrateur Système	locaux Certilience / vos locaux	14 heures (2 jours)

La formation ***Hacking Cloud Computing*** permet de démystifier le Cloud Computing et de découvrir pratiquement les nouveaux problèmes de sécurité liés aux technologies sous-jacentes et à leurs nouvelles utilisations.

OBJECTIFS DE LA FORMATION

- Comprendre les nouveaux vecteurs d'attaques du Cloud Computing
- Comprendre et évaluer l'impact d'une faille sur une infrastructure Cloud Computing
- Identifier et prioriser les correctifs
- Sensibiliser aux nouvelle bonnes pratiques du Cloud Computing

PROGRAMME

1/. introduction au Cloud Computing : les définitions du NIST
- les Modèles du Cloud : IaaS, PaaS, SaaS
- les types de Cloud : Publique, Privé et Hybride
- le Cloud Security Alliance (CSA)

2/. les nouveaux vecteurs d'attaques : CSA TOP Threats
- Threat #1 : Abuse and Nefarious Use of Cloud Computing
- Threat #2 : Insecure Interfaces and APIs
- Threat #3 : Malicious Insiders
- Threat #4 : Shared Technology Issues
- Threat #5 : Data Loss or Leakage
- Threat #6 : Account or Service Hijacking
- Threat # 7 : Unknown Risk Profile

3/. exemple pratique : analyse de sécurité sur Amazon Web Services EC2
- comprendre l'analyse de sécurité
- mettre en pratique

4/. les bonnes pratiques : CSA Security Guidance
- architecture Cloud Computing
- la gouvernance dans le Cloud
- opérer un Cloud

HAC08 Club Utilisateurs - Culture de la sécurité

Niveau	Prérequis	Public	Lieu	Durée
débutant	Connaissance en réseau, en système, en développement et en scripting	Développeur, Administrateur	En ligne	5 sessions de 3h

Le ***Club des Utilisateurs Certilience*** est un pack de formations à la culture de la sécurité. Il a pour but de former les équipes techniques à différentes techniques de hacking.

Cette formation en ligne est organisée en 5 sessions de 3 heures, programmées sur l'année, permettant d'aborder chaque sujet en profondeur et d'intégrer ces nouvelles compétences.

Chaque session se déroule de la manière suivante : cours en vidéo / travaux pratiques / et évaluation sous forme de quiz.

Certilience met à la disposition des participants une plateforme de travail entièrement sécurisée, permettant de réaliser les exercices proposés et de tester chaque outils.

Après la formation, le participant a la possibilité de récupérer le contenu de la formation (vidéos, supports de formation et sujets des TPs).

Session #1 : **Découverte des vulnérabilités**

OBJECTIFS DE LA FORMATION

L'objectif de cette première séance est d'identifier rapidement des vulnérabilités sur vos périmètres. Analyse au niveau de vos réseaux et analyse sur les applicatifs web.

- Les services exposés : Nmap
- Les fuites d'information sur les services Web (WordPress) avec Wpscan

PROGRAMME

- Jouer avec Nmap
- Expliquer / démontrer les scripts NSE
- Analyser des headers http, fuite d'information sur les versions d'Apache / IIS / Tomcat, PHP, etc.
- Identifier les systèmes : Windows / Linux : jouer majuscule / minuscule, Analyse des TTL , Analyse des fenêtres TCP
- Les répertoires standards sur un Tomcat
- Évaluer la sécurité d'un blog WordPress
- Bruteforce de login sur WordPress grâce à l'énumération des utilisateurs

HAC08 Club Utilisateurs - Culture de la sécurité

Niveau	Prérequis	Public	Lieu	Durée
débutant	Connaissance en réseau, en système, en développement et en scripting	Développeur, Administrateur	En ligne	5 sessions de 3h

Session #2 : Réseau & sécurité

OBJECTIFS DE LA FORMATION

L'objectif de cette séance est de découvrir comment les données circulent sur les réseaux, et comment sécuriser ces flux.

- Analyse d'un packet sans chiffrement
- Activation du chiffrement
- Les attaques au niveau de SSL
- Présentation de l'attaque de l'homme du milieu *(attaque Man in the middle)*

PROGRAMME

- Jouer avec un flux wireshark
- Telnet vs SSH
- Présentation du SSL & attaques sur du SSL
- Déchiffrer un fichier pcap avec une clef privée
- Les bases du chiffrement (asymétrique, symétrique), exemples d'algorithmes
- MiTM avec spoofing du certificat sur un serveur Web : HSTS, certificat auto-signé, etc.

Session #3 : Mots de passe

OBJECTIFS DE LA FORMATION

L'objectif de cette session est de découvrir les différents mécanismes d'authentification et de stockage des mots de passe avec les risques associés.

- Introduction au Mot de passe :
  - Hash / Graine
  - Environnement Microsoft
- Présentation méthode d'attaque sur application Web mot de passe
- Présentation attaque type PasstheHash et/ou mot de passe administrateur local
- Préconisation ANSSI (complexité)
- Préconisation du stockage des mots de passe

PROGRAMME

- Présentation des attaques par brute force sur des applications Web
- Présentation des attaques sur des hash avec JohnTheRipper ou Hashcat
- Utilisation du moteur de recherche Google pour faire du Google Hacking, base de données
- Introduction sur les bases de données de leak (keePass)

HAC08 Club Utilisateurs - Culture de la sécurité

Niveau	Prérequis	Public	Lieu	Durée
débutant	Connaissance en réseau, en système, en développement et en scripting	Développeur, Administrateur	En ligne	5 sessions de 3h

Session #4 : Configuration par défaut et services Web

OBJECTIFS DE LA FORMATION

L'objectif de cette session est de présenter les risques d'une installation système par défaut et quelques vulnérabilités standards sur des applications.

- Serveur type par défaut :
  - Services démarrés en IPV6
  - Tomcat : interfaces d'administrateur exposées / mot de passe
  - Cups
- Application Web :
  - Injection SQL
  - Compromissions possibles

PROGRAMME

- Jouer avec SMTP : mail from / to au niveau SMTP et dans le corps du mail pour montrer la différence d'affichage sur un client de messagerie
- Jouer avec les liens HTML dans les emails pour remplacer l'URL
- Aucun filtrage vs Escape vs PDO, importance du typage de donnée, challenges sur les SQLi
- Mise en exergue d'un défaut de mise à jour (vulnérabilité récente)
- Mise en exergue d'un service RDP sur Internet, Screenshot, bruteforce : conséquence et risque (blocage de compte, 0day, etc.)

Session #5 : Metasploit

OBJECTIFS DE LA FORMATION

L'objectif de cette dernière séance est de présenter un outil global qui permet de tester l'ensemble des points abordés sur les 4 premières séances.

PROGRAMME

- Exploitation d'un WordPress
- Exploitation de service réseau standard (NFS, etc.)
- Exploitation d'environnement vulnérable type Windows (meterpreter, kiwi)