Cybersécurité : Niveau expert

Pratiquez les attaques avancées pour mieux se défendre

5 jours / 35 heures | **Valence** | **Ref : SECU3**

PRÉSENTATION

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 DE LA FORMATION

COMPRENDRE et détecter les attaques sur un SI
DÉFINIR l'impact et la portée d'une vulnérabilité
RÉALISER un test de pénétration
SÉCURISER un réseau et intégrer des outils de sécurité adéquats

—TEST D'INTRUSION
—CYBERSÉCURITÉ
—HACKING

PUBLIC VISÉ

RSSI, DSI
Consultants en sécurité
Techniciens
Administrateurs systèmes / réseaux
Développeurs

PRÉREQUIS

Connaissances de l'administration de postes Windows ou Linux
Connaissance de TCP/IP
Utilisation de Linux en ligne de commande

POUR ALLER PLUS LOIN..

Cloud Computing : Les fondamentaux [Ref : CLOUD1]

LES + DE LA FORMATION

PRATIQUE
80% du temps de formation est consacré aux ateliers pratiques

MISE EN SITUATION
des différentes formes d'attaques existantes

APPLICABILITÉ
directe des outils sous architectures Windows et Linux

RETOURS D'EXPÉRIENCES
d'experts de la sécurité informatique

Programme

JOUR 1

Introduction

- 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'empreintes

- Énumération des machines
- Scan de ports
- Prise d'empreintes du système d'exploitation
- Prise d'empreintes des services

JOUR 2

Attaques réseau

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

Attaques systèmes

- Scanner de vulnérabilités
- Exploitation d'un service vulnérable distant
- Élévation de privilèges
- Espionnage du système
- Attaques via un malware
  - Génération d'un malware avec Metasploit
  - Encodage de payloads
- Méthodes de détection

JOUR 3 ATTAQUES WEB

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

JOUR 4 ATTAQUES APPLICATIVES

- Escape Shell
- Buffer overflow sous Linux
  - L'architecture Intel x86
  - Les registres
  - La pile et son fonctionnement
  - Les méthodes d'attaques standards

JOUR 5 : CHALLENGE FINAL

Mise en pratique des connaissances acquises

Grenoble INP ESISAR
ÉCOLE NATIONALE SUPÉRIEURE EN SYSTÈMES AVANCÉS ET RÉSEAUX
Contact : numericlab@esynov.fr | Site internet : www.esynov.fr
NANOELEC.