ATIKAE
FORMATION - CONSEIL - ACCOMPAGNEMENT

Formation Hacking Ethique Intermédiaire

(3 jours – 21 heures)

« "Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux." - Sun Tzu « l'Art de la Guerre »

A qui s'adresse cette formation ?

- Professionnels de la sécurité informatique :
  Responsables de la sécurité des systèmes d'information (RSSI), Analystes en sécurité, Consultants en cybersécurité, Administrateurs de systèmes, Administrateurs réseaux, Ingénieurs systèmes et réseaux.
- Développeurs logiciels :
  Développeurs d'applications mobiles, Développeurs de logiciels embarqués

Prérequis

- Connaissances de base en informatique et réseaux :
  Compréhension des concepts fondamentaux de l'informatique, Connaissance des principes de base des réseaux (TCP/IP, DNS, routage, etc.).
- Notions de sécurité informatique :
  Familiarité avec les concepts de sécurité de l'information (confidentialité, intégrité, disponibilité), Connaissance des menaces courantes et des bonnes pratiques en matière de sécurité.
- Compétences techniques :
  Aisance avec les environnements de ligne de commande (Linux/Windows), Expérience de base avec les outils de sécurité (Wireshark, Nmap, etc.).

Les objectifs de la formation

- Comprendre les principales techniques d'attaques informatique :
  Maîtriser les méthodologies et techniques couramment utilisées par les hackers, Être capable de détecter et d'analyser les tentatives d'intrusion, Appliquer des stratégies de défense efficaces basées sur la compréhension des attaques.
- Renforcer les connaissances en cybersécurité :
  Connaître les différents types d'attaques (SQL injection, XSS, attaques par DDOS, etc.), Apprendre à utiliser les outils de manière éthique pour tester et renforcer la sécurité, Mettre en œuvre des pratiques de sécurisation des applications et des réseaux.
- Démystifier le hacking :
  Déconstruire les stéréotypes et mythes autour du hacking, Promouvoir une approche éthique et responsable du hacking, Fournir une vision claire de l'importance du hacking éthique dans la cybersécurité.

www.atikae.fr / 20 rue du bosquet - 62118 Monchy-le-Preux
06 86 86 46 44 - contactez-nous@atikae.fr - Retrouvez nous sur in
Siren : 912 698 073 / déclaration d'activité : 32 62 03474 62

ATIKAE

Le programme de la formation

1. Introduction au piratage éthique *(1.5 h)*

- Les concepts clés de la cybersécurité : triade CID, défense en profondeur, chaîne d'attaque.
- Les attaquants et leurs motivations.
- La méthodologie du hacking éthique

2. Empreinte et reconnaissance, OSINT *(1 h)*

- Collecte d'informations publiques.
- Google dorks, footprinting passif.
- Enumération DNS.

3. Scanning et analyse des réseaux *(1.5 h)*

- Les communications TCP / UDP.
- Les différents scans de ports.
- Utilisation de NMAP.

4. Enumération *(2 h)*

- Principe du scan de vulnérabilités.
- Outils automatisés et analyses manuelles.
- Nmap Scripting Engine (NSE).
- Enumération Netbios, SMB, SNMP, SMTP, LDAP, RPC...

5. Analyse de vulnérabilités *(1.5 h)*

- Recherche et utilisation de code d'exploitation.
- Utilisation du framework Metasploit.

6. Shell et reverse shell *(1 h)*

- Transfert de fichiers entre machines.
- Utilisation de python, netcat, msfvenom...

7. Sniffing *(1 h)*

- Attaques sur les réseaux et technologies associées.
- Analyses de capture réseau.
- Rogue DHCP, Poisonning, NAC...

8. Ingénierie sociale *(0.5 h)*

- Principes et concepts
- Quelques exemples et retours terrain de pentesteurs

ATIKAE

9. Les mots de passe *(1.5 h)*

- Algorithmes de hachage.
- La force d'un mot de passe.
- Utilisation de Hashcat et John The Ripper.

10. Elévation de privilèges *(2 h)*

- Tests et analyses manuelles sous Windows et sous Unix.
- Scripting : WinPEAS / LinPEAS.

11. Hacking de serveurs et d'applications Web *(3.5 h)*

- Les technologies et protocoles du World Wide Web
- Frontend
- Backend
- Enumération web :
- Utilisation de Burp Suite
- NMAP
- Fuzzing
- Les principales attaques web
- Bruteforce
- LFI / RFI
- Injection SQL
- XSS

12. Active Directory *(4 h)*

- Concepts clés et terminologie
- Security Group
- UO, SID, GPO
- Administrer le royaume
- Outils RSAT
- Command Prompt
- Powershell
- Enumération AD
- Powerview
- Bloodhound
- NXC
- Les mécanismes d'authentification
- NTLM
- Kerberos
- Breaching AD
- Responder
- Attaques LDAP

12. Active Directory suite…(4 h)

- Kerberosting

Méthodes et Moyens Pédagogiques

- Ateliers pratiques : Chaque session comprend des exercices pratiques où les participants peuvent appliquer les concepts appris dans des environnements contrôlés.
- Laboratoires virtuels : Les participants auront accès à des labs virtuels pour simuler des attaques et mettre en œuvre des stratégies de défense en temps réel.
- Exposés théoriques, suivis de mise en pratique
- La consolidation des acquis se fait par la réalisation d'exercices contenants l'ensemble des points des cours développés

Evaluation de la formation

- Exercices à valider sur une plateforme en ligne au fur et à mesure de la formation.
- Test final (QCM).
- Questionnaire de satisfaction de la fin de formation.

Organisation de la formation

- **Date :** A définir dans la convention
- **Horaire** : A définir dans la convention

- **Modalité** 10 participants maximum, Présentiel (Distanciel selon contexte)
- **Lieu** Salle
- **Adresse** A définir dans la convention
- **Accessibilité** Accessible aux personnes à mobilité réduite

- **Nous fournissons :** un Lab cloisonné hébergé dans le cloud ; accessible à distance.

- Condition de réalisation (besoins du formateur)
  - Paperboard, Papier/stylos, Un projecteur / Ecran , Un accès internet
- Pour chaque participant (besoins des apprenants)
  - Un ordinateur pouvant exécuter une machine virtuelle, Une machine virtuelle Kali à télécharger sur : https://www.kali.org/get-kali/#kali-virtual-machines , Un accès internet

- Formateurs

Christophe Amiable

Responsable Technique chez Axians Cybersecurity Arras Lille, avec plus de 10 ans d'expérience aussi bien dans le monde de la sécurité défensive qu'offensive. Christophe détient de nombreuses certifications techniques reconnues : OSEP, OSCP, CRTP, CRTO...

Alexandre Lecomte

Consultant chez Axians Cybersecurity Arras Lille, avec 3 ans d'expérience dans la réalisation de tests d'intrusions dans des environnements clients de tout type. Alexandre détient plusieurs certifications techniques avec une spécialité sur l'exploitation de vulnérabilités web : OSCP, OSWA, CRTO, CEH...

AXIANS CyberSecurity
Arras-Lille