CYB-01 · INITIATION · PROGRAMME DE FORMATION

Techniques de hacking — Les fondamentaux

Cinq jours pour comprendre un système, puis le compromettre : de la reconnaissance à la prise de contrôle, jusqu'au rapport d'un professionnel.

DURÉE	NIVEAU	EFFECTIF	FORMAT
5 jours **35 heures**	**Initiation**	**4 à 8 stagiaires**	**Présentiel intra-entreprise ou école**

Public	Administrateurs systèmes et réseaux, techniciens support, développeurs, équipes qui débutent en sécurité, étudiants bac+3 à bac+5 en informatique
Prérequis	Bases en systèmes et en ligne de commande Linux ; notions de TCP/IP recommandées (niveau RES-01). Aucune connaissance préalable en sécurité
Lieu	Dans vos locaux (ou salle louée à proximité)
Tarif	**420 € net** par stagiaire et par jour, soit 2 100 € par stagiaire pour les 5 jours · minimum 4 stagiaires facturés, tarif plafonné à 6 stagiaires · TVA non applicable · frais de déplacement en sus · devis sur demande
Délai d'accès	2 à 4 semaines après accord sur le programme et signature de la convention

Objectifs

À l'issue de la formation, vous serez capable de :

- situer une démarche offensive dans son cadre légal, éthique et méthodologique ;
- conduire une reconnaissance passive puis active d'une cible ;
- cartographier un réseau et exécuter une attaque d'interception sur le réseau local ;
- tracer une requête web de bout en bout, du navigateur jusqu'à la base de données ;
- énumérer un poste Windows et un annuaire Active Directory ;
- exploiter des vulnérabilités système et web avec les outils de référence, puis conduire la post-exploitation ;
- restituer un test d'intrusion dans un rapport professionnel structuré.

Programme

Bloc	Contenu	Mise en pratique	Durée
0 La méthode d'un attaquant	Accueil et quiz de positionnement ; panorama de la sécurité, cadre légal et éthique, phases du test d'intrusion, reconnaissance passive et OSINT, ingénierie sociale	Mise en place du laboratoire ; reconnaissance passive d'une organisation fictive	3 h
1 Cartographier et perturber un réseau	Rappels TCP/IP, reconnaissance active avec Nmap et ses scripts NSE, détection de vulnérabilités, interception ARP et DNS, contre-mesures	Cartographier le réseau cible, intercepter un échange avec bettercap, puis le protéger	4 h
2 Une application web de bout en bout	Anatomie d'une requête HTTP, en-têtes de sécurité, du navigateur à la base de données, construction d'une requête à partir d'une saisie	Suivre une requête dans le navigateur et dans Burp Suite, repérer une première injection	3,5 h
3 Explorer un poste Windows	Architecture, comptes, privilèges, énumération locale, configurations faibles	Énumérer un poste et dresser la liste de ses faiblesses	3,5 h
4 Cartographier un Active Directory	Concepts d'annuaire, authentification dans le domaine, énumération, chemins d'élévation	Tracer le chemin d'un compte simple vers le contrôle du domaine	3,5 h

Bloc	Contenu	Mise en pratique	Durée
5 Compromettre une machine	Phases du test d'intrusion sur cible Linux puis Windows : reconnaissance, exploitation avec Metasploit, post-exploitation avec Meterpreter, élévation de privilèges	Prendre le contrôle d'une cible Linux puis Windows et y maintenir un accès	6 h
6 Attaquer une application web	Méthodologie de test web avec Burp Suite, vulnérabilités les plus courantes, contre-mesure associée à chaque faille	Exploiter DVWA puis Juice Shop, niveau après niveau	4,5 h
7 Mission finale et restitution	Intrusion autonome sur une cible composite ; trame de rapport : synthèse pour décideurs, périmètre, vulnérabilités, preuves, recommandations priorisées	Mener l'intrusion complète et rédiger le rapport ; quiz de fin	7 h

Répartition indicative : jour 1, blocs 0 et 1 ; jour 2, blocs 2 et 3 ; jour 3, bloc 4 et début du bloc 5 ; jour 4, fin du bloc 5 et bloc 6 ; jour 5, bloc 7. Horaires types : 9 h – 12 h 30 et 13 h 30 – 17 h.

Le plus de cette formation

Le stagiaire ne lance jamais un outil sans pouvoir tracer ce qu'il fait : chaque système (réseau, web, Windows, Active Directory) est d'abord compris avant d'être attaqué. La semaine se termine par une vraie mission en autonomie, sur une cible que personne n'a préparée, et par un rapport au format professionnel.

Méthodes et moyens pédagogiques

- Apports courts illustrés, démonstrations et environ 60 % de pratique.
- Laboratoire isolé et reproductible fourni par le formateur : poste d'attaque Kali Linux, cibles Linux et Windows, domaine Active Directory dédié, services en conteneurs.
- Toutes les attaques visent exclusivement les cibles du laboratoire, jamais le système d'information de votre entreprise.
- Chaque notion est introduite en ligne de commande, au plus près du protocole, avant tout outil graphique.
- Ateliers guidés et missions de mise en situation ; chaque bloc se conclut par un livrable.
- Supports remis au format PDF : diaporama, TP et trame de rapport.
- À prévoir par le client : une salle avec vidéoprojecteur, un PC portable par stagiaire (le formateur peut en fournir sur demande).

Suivi et évaluation

- Feuille d'émargement signée par demi-journée.
- Quiz de positionnement identique en début et en fin de formation : il mesure la progression de chacun.
- Évaluation continue par les livrables de fin de bloc, puis mission finale évaluée sur la rigueur, la traçabilité des actions et la qualité du rapport.
- Attestation de fin de formation remise à chaque stagiaire, avec les résultats de l'évaluation des acquis.
- Questionnaire de satisfaction rempli le dernier jour.

Accessibilité

Vous accueillez une personne en situation de handicap ? Contactez le formateur avant la formation : nous étudions ensemble les adaptations du déroulé, des supports et du matériel.

Formateur

Nicolas Lebosq : 19 ans d'expérience en réseaux et systèmes (administration réseau, encadrement d'équipe, ingénieur d'études en laboratoire de recherche), enseignant vacataire en réseaux à SeaTech, école d'ingénieurs de l'Université de Toulon, depuis 2018.

Contact et inscription

Nicolas Lebosq · nicolas.lebosq@lebosq-networks.fr · lebosq-networks.fr

Nicolas Lebosq, entrepreneur individuel (EI), nom commercial Lebosq Networks · SIRET **[SIRET]** · Déclaration d'activité enregistrée sous le numéro **[NDA]** auprès du préfet de région **[région]**. Cet enregistrement ne vaut pas agrément de l'État.

CYB-01 · version 1 · mise à jour le **[date]**