Sensibilisation Cybersécurité / Hacking

Module 02

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES
07 63 53 46 81
CONSEILS@BCOPIN.COM

Principes du hacking éthique

Hacking Ethique

Hacking éthique vs hacking malveillant :

- **Hacking éthique** : Aussi appelé "white-hat hacking", il s'agit de l'utilisation des techniques de hacking dans le but de tester et de renforcer la sécurité des systèmes informatiques. Les hackers éthiques, ou "testeurs d'intrusion", cherchent à identifier les vulnérabilités avant que des attaquants malveillants ne les exploitent.
- **Hacking malveillant** : Aussi appelé "black-hat hacking", ce type de hacking implique l'exploitation de vulnérabilités pour des fins illégales ou nuisibles. Cela peut inclure le vol de données, les attaques par ransomware, ou le sabotage de systèmes.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Hacking Ethique

Le cadre légal et les responsabilités du hacker éthique :

- Le hacking éthique est réalisé dans un cadre légal précis. Un hacker éthique doit obtenir l'autorisation formelle de l'organisation avant de procéder à des tests d'intrusion.
- La loi impose des responsabilités strictes : les hackers éthiques ne doivent jamais causer de dommages intentionnels, exécuter des attaques sans permission, ou voler des informations. La transparence et la confidentialité sont cruciales.
- Par exemple, avant de commencer un test d'intrusion, un hacker éthique doit signer un contrat spécifiant les actions autorisées et les limites du test.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Hacking Ethique

Rôle des tests d'intrusion et importance des rapports :

- **Tests d'intrusion (Pentesting)** : Ces tests sont réalisés pour simuler des attaques sur un système afin d'identifier des failles de sécurité. Ils permettent aux entreprises de renforcer leur infrastructure avant que des hackers malveillants ne les exploitent.
- **Rapports** : Après chaque test, un rapport détaillé est fourni pour expliquer les vulnérabilités découvertes, les techniques utilisées pour les exploiter, et les recommandations pour corriger ces failles. Ces rapports sont essentiels pour que l'organisation puisse comprendre les risques et mettre en place des mesures correctives.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Outils de Hacking

Outils de hacking

- **Kali Linux** : C'est l'une des distributions Linux les plus populaires dans le monde du hacking éthique. Elle regroupe une vaste collection d'outils de test d'intrusion, de piratage éthique et de cybersécurité. Kali Linux est un environnement complet pour les hackers éthiques.
- **Nmap** : Un outil utilisé pour scanner les réseaux, détecter les hôtes actifs et identifier les services qu'ils offrent. Il est très utile pour la phase de reconnaissance d'un test d'intrusion.
- **Metasploit** : Un framework d'exploitation des vulnérabilités, qui permet de simuler des attaques sur des systèmes. Il contient des exploits prêts à l'emploi pour tester les failles.

Outils de hacking

- **Wireshark** : Un outil de capture et d'analyse de paquets réseau. Il permet aux hackers éthiques d'analyser le trafic réseau et de repérer les vulnérabilités potentielles, comme les informations sensibles qui circulent en clair.
- **Burp Suite** : Un ensemble d'outils utilisés pour tester la sécurité des applications web. Burp Suite est particulièrement efficace pour les tests de sécurité sur des sites web, en permettant d'analyser le trafic HTTP/HTTPS et de détecter des failles comme les injections SQL et XSS.

Outils de hacking

Configurer un environnement virtuel pour le hacking éthique :

- Il est important de configurer un environnement sécurisé, généralement à l'aide de machines virtuelles, pour tester des attaques sans risquer d'endommager des systèmes en production. Cela permet d'imiter des environnements réels dans un cadre contrôlé.
- Des outils comme VirtualBox ou VMware peuvent être utilisés pour configurer des machines virtuelles isolées. Ces machines peuvent simuler des cibles vulnérables, permettant ainsi des tests d'intrusion en toute sécurité.

Outils de hacking

Présentation des systèmes de test comme les machines vulnérables :

- **Hack The Box** et **TryHackMe** sont des plateformes en ligne qui offrent des environnements de test pour les hackers éthiques. Ces sites proposent des machines vulnérables et des scénarios de piratage dans lesquels les utilisateurs peuvent s’entraîner à identifier et exploiter des failles de sécurité dans un environnement légal.
- Ces plateformes permettent aux participants de se confronter à des défis réels et d'améliorer leurs compétences tout en respectant les bonnes pratiques de la cybersécurité.

Mise en Pratique

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Questions ?

Formateur : Bertrand Copin
Linkedin : https://www.linkedin.com/in/bertrand-copin/
Site : https://www.bcopin.com
Mail : conseils@bcopin.com
Tél : 07 63 53 46 81

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES