GUARDIA

CYBERSECURITY SCHOOL

CAHIER DES CHARGES

Techniques de pentesting & hacking éthique (pentest-1)

INTRODUCTION

Nom du module : Techniques de pentesting & hacking éthique (Pentest-1)

Nom de l'UE : Culture Cyber

Nombre de crédits ECTS : 5

Date : 14 oct au 31 oct

Classe : GCS1

MODALITÉS

- Groupes de 4 étudiants à former avant le début du projet

CONTEXTE ET DESCRIPTION DU PROJET

Ce projet s'inscrit dans un contexte où les attaques informatiques sont de plus en plus fréquentes. L'objectif est d'apprendre à tester la sécurité des sites web, trouver des failles et apprendre à les corriger.

Les étudiants travailleront dans des environnements virtuels pour tester des sites web. Ils devront identifier des vulnérabilités (failles de sécurité), leur montrer comment rédiger un rapport détaillé et présenter leurs résultats en classe.
Les sujets abordés incluent :

- Utilisation de **machines virtuelles** pour simuler des environnements de test.
- Utilisation de la ligne de commande sous **Linux**.
- Introduction aux technologies web (**HTML, CSS, PHP, Javascript**) pour comprendre comment fonctionnent les sites.
- Le **protocole HTTP** pour analyser la communication entre un site et un navigateur.
- **Burp Suite Community Edition** pour détecter et exploiter les vulnérabilités.

- Identification et exploitation de vulnérabilités : comme les **injections SQL** ou les **failles XSS**.

OBJECTIFS PÉDAGOGIQUES ET PROFESSIONNELS DU PROJET

À l'issue de ce projet, les étudiants seront capables de :

Savoirs

- Expliquer ce qu'est une machine virtuelle et ses avantages pour la sécurité.
- Lire et comprendre du code HTML, CSS, PHP, et Javascript pour analyser des applications web.
- Décrire comment fonctionne le protocole HTTP (requêtes, réponses, en-têtes, etc.).
- Expliquer les bases des systèmes d'exploitation et des serveurs web.
- Comprendre les concepts de base en sécurité web, comme l'authentification, les sessions et la gestion des cookies.

Savoir-être

- **Travailler en équipe** : savoir collaborer, répartir les tâches et respecter les délais.
- **Être autonome** : être capable de rechercher et appliquer de nouvelles informations ou outils.
- **Communiquer efficacement** : savoir expliquer des concepts techniques complexes à un public non technique.
- **Gérer les responsabilités** : chaque étudiant doit assumer le rôle qui lui est attribué dans le projet (par exemple, documentation, exploitation des failles, présentation).

Savoir-faire / Compétences

- **Utilisation de la ligne de commande sous Linux** : manipuler des fichiers, configurer des serveurs web et exécuter des scripts.
- **Configurer un serveur web sur une machine virtuelle** : déployer un site et le tester dans un environnement sécurisé.
- **Utiliser Burp Suite Community Edition** : capturer et analyser le trafic HTTP, identifier des vulnérabilités comme XSS, SQLi, etc.
- **Exploiter des failles de sécurité** : comprendre comment des failles comme les injections SQL, les failles XSS ou CSRF peuvent être utilisées pour compromettre un site web.
- **Proposer des solutions** : après avoir identifié une faille, savoir proposer des solutions concrètes pour la corriger (par exemple, validation des entrées, filtrage des caractères, etc.).
- **Automatisation des tests de sécurité** : créer des scripts pour effectuer des tâches répétitives (par exemple, utiliser Python ou Bash pour scanner des vulnérabilités).
- **Utiliser des systèmes de gestion de versions** : maîtriser Git et GitHub pour collaborer efficacement sur le code du projet.

RESSOURCES

1. **A savoir/à apprendre** (Ce travail pourra être évalué / noté en début de projet) :
    - Notions de base en réseau et sécurité informatique.
    - Comprendre les protocoles TCP/IP, HTTP, HTTPS.
2. **A lire/à consulter** :
    - OWASP Top Ten – Les dix failles de sécurité les plus courantes sur le web.
    - Documentation officielle de Burp Suite.
    - Tutoriels Hack The Box ou TryHackMe pour se familiariser avec des scénarios de pentesting.
3. **A installer/pré-requis techniques** :
    - Installer Burp Suite Community.
    - Installer VirtualBox.
    - Un système Linux (Kali Linux)

TRAVAIL PRÉPARATOIRE

Se familiariser avec les concepts de virtualisation, les outils de pentesting, et la sécurité web.

ROADMAP

DESCRIPTION

Veuillez trouver ci-dessous une description des livrables attendus ainsi que les dates d'échéance associées. Il est essentiel de respecter les échéances suivantes pour assurer une progression harmonieuse et structurée du projet. Chaque livrable représente une étape importante dans le processus de réalisation et permet d'évaluer l'avancement du travail. Les dates limites fixées doivent être rigoureusement respectées afin de garantir une évaluation équitable et de permettre un feedback constructif en temps opportun.

Jalon	Livrables attendus	Date limite	Moyens / formats
1	**Travail préparatoire : Recherche et préparation des outils nécessaires (VirtualBox, Burp Suite, etc.).**	**14 octobre**	**Preuve d'installation des outils (captures d'écran des environnements configurés).**
2	• **Réalisation d'un site personnel : Création et déploiement d'un site web personnel en utilisant les templates de HTML5UP et des images d'Unsplash.** • **Publication du site sur GitHub Pages.**	**14 octobre**	• **Code source du site disponible sur un dépôt GitHub public.** • **URL du site web hébergé sur GitHub Pages.**
3	• **Réalisation d'un audit de la machine Silverhand avec**	**30 octobre**	• **Liste des flags trouvés avec captures d'écran des flags.**

	identification et capture des flags de sécurité. • **Rapport détaillé incluant les étapes suivies, les vulnérabilités trouvées et les flags récupérés.**		• **Rapport écrit en format PDF ou Markdown avec des captures d'écran et des explications.**
4	**Présentation orale des résultats de l'audit : doit inclure les failles identifiées, les méthodes d'exploitation, et les recommandations.**	**31 octobre**	• **Présentation PowerPoint ou équivalent.** • **Documentation de soutien (si nécessaire) à distribuer pendant la présentation.**

EVALUATION

L'évaluation du projet est conçue pour être complète, prenant en compte non seulement le produit final, mais aussi le processus de travail, les compétences acquises et les attitudes démontrées tout au long du projet. La grille d'évaluation est basée sur trois catégories principales : savoirs, savoir-faire, et savoir-être. La note finale est sur 20.

SYSTÈME DE NOTATION

Savoirs (Connaissances)

- **Compréhension théorique** : Évaluée soit en amont du projet pendant la semaine théorie soit lors de la soutenance et restitution du projet. Cela

permet de mesurer la compréhension des concepts fondamentaux et des connaissances liées au projet des étudiants.

Savoir-faire (Compétences)

- **Compétences techniques et application** : Évaluées à travers la soumission finale du projet. Cela inclut la qualité, la fonctionnalité, et la précision technique du travail produit.
- **Gestion de projet** : Évaluée en fonction de l'organisation, du respect des échéances, et de l'utilisation efficace des ressources. Cela peut être évalué à travers la documentation du projet et les journaux de processus.

Savoir-être (Attitudes/Compétences interpersonnelles)

- **Travail d'équipe et collaboration** : Évalués à travers des évaluations par les pairs et les membres du groupe. Les critères incluent la communication, la coopération, et la contribution aux tâches du groupe.
- **Autonomie et initiative** : Évaluées en fonction des contributions individuelles, de la capacité à travailler de manière autonome, et de la résolution proactive des problèmes.
- **Soutenance** : Évaluées lors de la présentation finale du projet. Les critères incluent la clarté, la cohérence, et la capacité à articuler et défendre les résultats du projet.

Grille d'Évaluation

- Savoirs théoriques (8 points)
- Compétences techniques et application (8 points)
- Gestion de projet (4 points)
- Travail d'équipe et collaboration (4 points)
- Autonomie et initiative (2 points)
- Soutenance (2 points)
- La note finale est sur 20 points. Les évaluateurs fourniront des commentaires détaillés pour chaque catégorie afin de donner un retour constructif aux étudiants.

EVALUATION

EXAMEN INDIVIDUEL DE FIN DE PÉRIODE
Notez ici les éléments relatifs au partiel : acquis à valider / modalités envisagées

Acquis à Valider :

- Compréhension des concepts théoriques abordés durant le cours (virtualisation, HTTP, technologies web, etc.).
- Application pratique des compétences en pentesting et hacking éthique.
- Capacité à analyser, identifier, et exploiter des vulnérabilités sur des environnements simulés.
- Compétences en documentation et présentation des résultats d'audit.