NEA SECURITY

Plan et déroulement du cours

Le cours suivant est destiné à préparer les étudiants au hacking éthique. Ce sera également l'opportunité d'enseigner aux étudiants des stratégies pour préparer des certifications reconnues comme la CEH et d'autres. Il faut savoir que de telles certifications nécessitent de la persévérance et du travail personnel pour les obtenir. Ce sont les critères principaux que j'attends des étudiants pour bien démarrer cette période d'enseignement.

Ainsi ma méthodologie d'enseignement s'appuie sur 3 éléments essentiels :

- La simplicité, pour rendre accessible le cours à toute personne n'ayant jamais été initiée au hacking éthique
- L'esprit de synthèse, pour aborder les points fondamentaux de manière claire et concise sur la période de 12 jours allouée
- La pratique via des ateliers et des labs

Pour rappel le hacking éthique ne peut pas s'apprendre de manière théorique, d'où le fait que je mise beaucoup sur la partie pratique.

1. Récapitulatif des dates et informations utiles :

Dates	Horaires
30 novembre 2023	14h à 19h
1 décembre 2023	8h à 13h
6 décembre 2023	14h à 19h
12 décembre 2023	14h à 19h
13 décembre 2023	14h à 19h
14 décembre 2023	14h à 19h
15 janvier 2024	8h à 13h
16 janvier 2024	14h à 19h
19 janvier 2024	8h à 13h
23 janvier 2024	14h à 19h
24 janvier 2024	14h à 19h
26 janvier 2024	8h à 13h

- Public : B2 CS BDX – Ethical Hacking
- Pré-requis : un ordinateur, anglais indispensable, utilisation de machines virtuelles Kali Linux, curiosité, créativité et esprit d'équipe. En ce qui concerne les labs, voici les liens pour télécharger les éléments requis :
  - OWASP Juice Shop : https://pwning.owasp-juice.shop/companion-guide/latest/part1/running.html
  - Machines créées par TCM Security : https://drive.google.com/drive/folders/1VXEuyySgzsSo-MYmyCareTnJ5rAeVKeH
- Objectifs de la formation : les apprenants seront capables de maitriser les bases du hacking éthique et par la même occasion de passer des certifications reconnues comme la CEH, la CompTIA Security+ et d'autres. De plus nous allons enseigner la méthodologie de travail utilisée dans la cybersécurité offensive
- Objectifs pédagogiques : les apprenants à l'issue de la formation pourront appliquer la méthodologie de pentest et travailler avec les outils de base du hacking éthique, ainsi ils pourront :
  - Faire de la recherche d'informations via l'Open-Source Intelligence (OSINT)
  - Faire du pentest d'applications Web en suivant des référentiels connus
  - Travailler avec les outils pour réaliser des opérations de pentest interne (environnement Active Directory)

2. Synopsis de la formation :

Dates	Thématique abordée	Déroulement
30 novembre 2023 au 6 décembre	Open-Source Intelligence : importance de la recherche d'informations Remise du rapport de groupe sur la thématique OSINT et revue de la principale méthodologie	présentation des principaux outils utilisés dans les opérations d'OSINT et de la méthodologie de recherche d'informations, aide individuelle avec chaque étudiant : • Gagner en anonymat : construction d'un faux profil • Outils de recherches par image • Outils de recherches de mots de passe

		• Outils de recherches d'adresses emails • Opérateurs à utiliser sur les moteurs de • recherches • Outils de recherche sur les noms • d'utilisateur • Recherches sur les sites web et les • technologies associées • Techniques de recherches sur une • organisation En tant qu'intervenant je vais ici aider chaque groupe dans la rédaction du rapport de qualité professionnelle. Par la suite à titre de correction je présenterai la méthodologie d'OSINT et les outils principalement utilisés. Atelier libre sur plateforme de pentest : TryHackMe, Hack The Box etc .
12 au 14 décembre 2023	Pentest des applications web et pratique sur le lab OWASP Juice Shop Remise du rapport de groupe sur la thématique pentest des applications web Préparation des étudiants sur la présentation orale individuelle	Présentation des principaux outils utilisés pour le pentest des applications web, démonstration d'installation du lab et préparation des outils • Mise en place du lab : OWASP Juice Shop • Présentation des principaux outils utilisés dans le pentest des applications web En tant qu'intervenant je vais

		ici aider chaque groupe dans la rédaction du rapport de qualité professionnelle. Par la suite à titre de correction je présenterai la méthodologie et les outils principalement utilisés. Ensuite les étudiants devront préparer leur présentation orale individuelle. La présentation consistera : • chaque étudiant doit présenter au moins 2 risques énoncés dans l'OWASP Top 10 des applications web accompagnée d'une démonstration dans la mesure du possible. 10 minutes max.
15 au 19 janvier 2024	Hacking éthique en pratique Remise du rapport de groupe sur la thématique Hacking éthique en pratique Présentation orale individuelle sur la thématique pentest des application web	Présentation des principaux outils utilisés pour le pentest en général via la plateforme Try Hack Me et d'autres boxes disponibles sur Internet • Domaines et sous-domaines • Scanning et énumération • Outils de scans additionnels • Autres outils complémentaires En tant qu'intervenant je vais ici aider chaque groupe dans la rédaction du rapport de qualité professionnelle. Par la suite à titre de correction je présenterai la méthodologie

		et les outils principalement utilisés. Présentation orale individuelle par chaque étudiant sur la thématique pentest des applications web.
23 janvier au 26 janvier	Évaluation : rapport de groupe sur la thématique compromission d'un environnement AD + présentation orale par chaque groupe sur la thématique compromission d'un environnement AD.	Rédaction du rapport de groupe sur la compromission d'un environnement AD. Présentation orale par chaque groupe sur la thématique compromission d'un environnement AD.

3. Rapport de groupe sur la compromission d'un environnement AD :

L'évaluation la plus importante consistera en la rédaction d'un rapport de groupe de qualité professionnelle portant sur la compromission d'un environnement Active Directory. Voici le sujet :

Considérée comme la partie plus importante, je vais inciter les étudiants à former des groupes et leur demander de me rédiger un rapport abordant cette thématique. Ainsi je vais les encourager et les accompagner dans la rédaction de ce rapport professionnel. Le but est que dans un futur proche et durant leur carrière professionnelle ils puissent ré-utiliser ce guide. Autonomie et rigueur seront exigés ici.

« Dans le cadre d'une démarche d'amélioration de la politique interne de l'organisation STREAM LAB-CITY, le responsable du pôle informatique et SI vous contacte pour lui rédiger un guide de sécurité informatique, orienté côté offensif. Le souhait de ce client est de se mettre à la place d'un attaquant qui souhaite compromettre un environnement Active Directory. »

Les attentes concernant ce guide de travail sont les suivantes :

- Présentation d'une méthodologie de pentest organisée
- Présentation des outils utilisés pour compromettre un environnement Active Directory
- Le guide doit présenter des captures d'écran, afin de détailler les principales étapes de l'utilisation d'un outil
- Le guide doit être accessible à des personnes techniques et non-techniques
    - Esprit de synthèse fortement recommandé
    - Expliquer les concepts et l'utilisation d'outils de manière simplifiée. N'oubliez pas que chaque partie prenante d'une organisation doit avoir conscience de l'importance de la cybersécurité. Ainsi votre travail sera valorisé si votre rédaction est accessible aux personnes techniques comme non-techniques.

Critères de notation : la cybersécurité, notamment la partie offensive, c'est essentiellement de la recherche d'informations. Bien que ce domaine est très vaste, ce qui fait un bon analyste en cybersécurité/pentester est la curiosité, la persévérance et l'esprit d'équipe.

- Esprit d'équipe : nous souhaitons voir une synergie, une interaction entre les étudiants. L'entraide est un élément essentiel.

- Compréhension de la méthodologie d'un attaquant : la méthodologie d'attaque et de recherche d'informations en tant qu'attaquant restent les éléments clés pour réussir à avoir un accès à un système/réseau. Nous allons observer si vous assimilez cette méthodologie en fonction de la rédaction de votre guide, de son plan et de ce qui va le composer.

- Créativité : dans votre parcours professionnel, il est essentiel de capter l'attention des personnes qui vont lire et écouter votre présentation. Ainsi, l'esprit créatif est également important. Ayez libre cours à votre imagination !

- Oral : la présentation orale doit refléter les éléments clés de votre guide. Pensez à faire des slides synthétiques.

- Rapport : attentes de qualité professionnelle, veillez à l'orthographe, à la grammaire, à la structure et à la présentation du rapport.

4. Synthèse des évaluations :

De manière plus concise voici la synthèse des évaluations qui auront lieu durant ce cours :

→ Note de groupe :

- Rapport sur la compromission d'un environnement Active Directory
- Oral par groupe suite au rapport

→ Note individuelle :

- Présentation orale individuelle sur au moins 2 risques énoncés dans l'OWASP Top 10 des applications web, accompagnée d'une démonstration technique dans la mesure du possible
- Note de participation individuelle