**Plan de Présentation pour le Projet d'Études M1**

**Introduction (1 minute)**

* **Présentation rapide du projet :**
  + Nom du projet : Automatisation des tests d'intrusion.
  + Étudiant : Charly DELBAUCHE.
* **Objectif principal :**
  + Développer une toolbox automatisée qui simplifie et améliore l'efficacité des tests d'intrusion.
  + L'objectif est de fournir une solution automatisée pour identifier les vulnérabilités et renforcer la sécurité des systèmes informatiques.

**Contexte et Besoin (2 minutes)**

* **Contexte :**
  + Importance croissante des tests d'intrusion dans le domaine de la cybersécurité.
  + Les tests d'intrusion permettent d'identifier les failles de sécurité dans les systèmes informatiques avant que des attaquants ne les exploitent.
  + Conformité avec les normes et règlements comme la loi RGPD et les normes ISO27000.
* **Besoin spécifique :**
  + Les entreprises de cybersécurité, comme l'entreprise X, font face à des délais serrés et une charge de travail élevée.
  + La demande croissante pour des tests d'intrusion rapides et précis.
  + Besoin d'une solution automatisée pour simplifier le processus et améliorer la qualité des résultats.

**Présentation de la Toolbox (4 minutes)**

* **Architecture de la Toolbox :**
  + Description générale du fonctionnement : La toolbox est développée en Python et utilise des bibliothèques spécialisées en cybersécurité.
  + Les étapes de fonctionnement :
    1. **Configuration :** L'utilisateur configure la toolbox selon les besoins spécifiques du test.
    2. **Exploration :** Identification des ports, services et vulnérabilités.
    3. **Exploitation :** Utilisation des vulnérabilités identifiées pour accéder au système.
    4. **Post-exploitation :** Analyse approfondie du système pour identifier les données sensibles.
    5. **Reporting :** Génération de rapports détaillés et de visualisations graphiques.
* **Fonctionnalités clés :**
  + **Découverte de ports et de services :** Utilisation de scripts comme Nmap.sh pour identifier les services actifs.
    1. **Nmap :** (Network Mapper) est un outil open-source utilisé pour la découverte de réseaux et l'audit de sécurité. Il permet de scanner les ports et d'identifier les services actifs sur un système cible.
    2. Utilisation : nmap -sV <adresse\_ip> pour identifier les services et leurs versions.
  + **Détection de vulnérabilités :** Utilisation d'outils comme Nikto.sh pour scanner les vulnérabilités.
    1. **Nikto :** est un scanner de vulnérabilités web open-source qui analyse les serveurs web pour détecter des vulnérabilités telles que des fichiers dangereux, des versions obsolètes de logiciels, et des configurations incorrectes.
    2. Utilisation : nikto -h <adresse\_ip> pour lancer un scan sur le serveur web cible.
  + **Analyse de la sécurité des mots de passe :** Vérification de la robustesse des mots de passe.
  + **Tests d'authentification :** Vérification des identifiants et mots de passe.
  + **Exploitation de vulnérabilités :** Simulation d'attaques pour tester la sécurité.
  + **Post-exploitation et reporting :** Analyse et rapport des résultats des tests.
* **Démonstration brève :**
  + Présentation d'un exemple de script (Nmap.sh et Nikto.sh) et leur fonctionnement.
  + Expliquer comment lancer les scripts et interpréter les résultats.

**Analyse des Choix et Impacts (2 minutes)**

* **Choix technologiques et méthodologiques :**
  + **Python :** Choisi pour sa flexibilité et sa richesse en bibliothèques pour la cybersécurité.
  + **Outils open-source :** Utilisation d'outils disponibles gratuitement pour réduire les coûts et le temps de développement.
  + **Approche modulaire :** Conception de la toolbox pour être facilement extensible avec de nouvelles fonctionnalités.
* **Impact sur le processus de test d'intrusion :**
  + **Efficacité accrue :** Réduction du temps nécessaire pour réaliser des tests complets.
  + **Amélioration de la qualité :** Résultats plus précis et exhaustifs grâce à l'automatisation.
  + **Réduction des erreurs humaines :** Minimisation des erreurs grâce à l'utilisation de scripts automatisés.

**Conclusion et Perspectives (1 minute)**

* **Synthèse des points essentiels :**
  + Importance de l'automatisation dans les tests d'intrusion pour améliorer l'efficacité et la qualité.
  + Présentation des principales fonctionnalités et avantages de la toolbox développée.
  + Démonstration des outils utilisés : Nmap, Nikto.
* **Perspectives d'évolution :**
  + **Nouvelles fonctionnalités :** Intégration d'outils supplémentaires comme Metasploit.
    - **Metasploit Framework :**
      * **Description :** Outil de développement et d'exécution d'exploits open-source, permet de tester les vulnérabilités identifiées et de valider les failles de sécurité.
      * **Fonctionnement :** Intégration avec la toolbox pour exécuter des exploits automatisés sur les vulnérabilités découvertes. Utilisation : msfconsole pour accéder à l'interface Metasploit et exécuter des modules d'exploitation.
      * **Impact :** Amélioration des capacités de test d'exploitabilité des vulnérabilités et validation des résultats des scans de vulnérabilités.
  + **Améliorations continues :** Basées sur les retours des utilisateurs et les nouvelles menaces de sécurité.
  + **Intégration avec d'autres outils :** Développement de plugins pour une utilisation avec d'autres solutions de cybersécurité.