PROJET DE CYBERSÉCURITÉ

Test d'Intrusion Complet sur Environnement Contrôlé

Contexte du Projet

Ce projet éducatif consistait en l'exploitation complète d'une machine Metasploitable2, une distribution Linux spécialement conçue pour l'apprentissage du pentesting. L'objectif était de maîtriser l'ensemble du processus d'attaque dans un environnement sécurisé et contrôlé.

Objectifs Pédagogiques

•Comprendre le cycle complet d'un test d'intrusion
•Maîtriser les techniques de reconnaissance réseau
•Apprendre l'exploitation de vulnérabilités connues
•Pratiquer l'élévation de privilèges sous Linux
•Expérimenter les techniques de persistance

Environnement Technique

Machine d'attaque : Kali Linux
Cible : Metasploitable2
Réseau : Environnement virtuel isolé
Durée : 1 journée

Méthodologie Employée

Phase 1 : Reconnaissance

•Découverte des actifs réseau
•Cartographie complète des services exposés
•Identification des versions logicielles
•Analyse des vecteurs d'attaque potentiels

Phase 2 : Exploitation

•Sélection d'exploits appropriés aux services vulnérables
•Compromission de multiples services (FTP, SMB, HTTP)
•Obtention d'accès initiaux via différents vecteurs
•Validation des accès obtenus

Phase 3 : Élévation de Privilèges

•Analyse des configurations système
•Recherche de vulnérabilités locales
•Exploitation de failles de permission
•Obtention des privilèges administrateur

Phase 4 : Post-Exploitation

•Analyse de l'environnement compromis
•Test de techniques de persistance
•Documentation des findings

Apprentissages Clés

Compétences Techniques Acquises

•Maîtrise des outils de scanning réseau
•Gestion des exploits et payloads
•Techniques d'élévation de privilèges Linux
•Méthodologie de pentest structurée

Vulnérabilités Rencontrées

•Services avec versions vulnérables
•Configurations par défaut non sécurisées
•Permissions excessives sur binaires système
•Absence de mécanismes de protection modernes

Valeur Ajoutée

Ce projet démontre une compréhension approfondide des :

•**Processus d'attaque** : De la reconnaissance à la persistance
•**Bonnes pratiques** : Méthodologie structurée et reproductible
•**Sécurité défensive** : Compréhension des vulnérabilités pour mieux les contrer

---

Perspectives

Cette expérience sert de fondation pour des projets plus avancés incluant :

•Tests d'intrusion sur environnements Windows
•Audits d'applications web
•Exercices de chasse aux menaces
•Développement de contre-mesures

« Comprendre l'attaque pour mieux défendre »
Projet réalisé dans un cadre purement éducatif sur infrastructure dédiée