**AUDIT DE SÉCURITÉ & CARTOGRAPHIE RÉSEAU**

**Laboratoire de Cybersécurité - Environnement Contrôlé**

**Lucie**  
**Date :** 06/2025

**Projet :** Configuration et reconnaissance d'un environnement de test isolé  
**Technologies :** Kali Linux, VMware, Nmap, Metasploit Framework, DVWA

**TABLE DES MATIÈRES**

1. [Sommaire Exécutif](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#1-sommaire-ex%C3%A9cutif)
2. [Architecture du Laboratoire](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#2-architecture-du-laboratoire)
3. [Méthodologie de Reconnaissance](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#3-m%C3%A9thodologie-de-reconnaissance)
4. [Résultats de la Cartographie](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#4-r%C3%A9sultats-de-la-cartographie)
5. [Analyse des Vulnérabilités](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#5-analyse-des-vuln%C3%A9rabilit%C3%A9s)
6. [Évaluation des Risques](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#6-%C3%A9valuation-des-risques)
7. [Recommandations de Sécurité](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#7-recommandations-de-s%C3%A9curit%C3%A9)
8. [Conclusion](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#8-conclusion)
9. [Annexes](https://claude.ai/chat/82ff27ca-f983-4445-8529-b37ab57fc6ee#9-annexes)

**1. SOMMAIRE EXÉCUTIF**

**Contexte**

Ce rapport présente les résultats d'un audit de sécurité réalisé dans un environnement de laboratoire contrôlé, configuré pour l'apprentissage et la pratique de techniques de cybersécurité éthiques.

**Objectifs**

* Configurer un environnement de test isolé et sécurisé
* Effectuer une cartographie réseau complète
* Identifier les vulnérabilités présentes sur les systèmes cibles
* Documenter les vecteurs d'attaque potentiels
* Proposer des mesures de remédiation

**Résultats Clés**

* **4 machines actives** identifiées sur le réseau 192.168.72.0/24
* **[X] vulnérabilités critiques** découvertes
* **[X] vecteurs d'attaque** identifiés et validés

**Impact**

Les vulnérabilités identifiées permettent une compromission complète des systèmes cibles, démontrant l'importance d'une approche de sécurité par couches.

**2. ARCHITECTURE DU LABORATOIRE**

**Configuration Réseau**

* **Type de réseau :** VMware Host-Only
* **Plage d'adresses :** 192.168.72.0/24
* **Isolation :** Aucun accès Internet pour les VMs vulnérables
* **Sécurité :** Communication limitée au périmètre du lab

**Machines Virtuelles Déployées**

| **Nom** | **OS** | **Rôle** | **RAM** | **IP Assignée** |
| --- | --- | --- | --- | --- |
| Kali Linux | Linux | Machine d'attaque | 2 GB | 192.168.72.136 |
| Metasploitable 2 | Linux | Cible vulnérable | 2 GB | 192.168.72.133 |
| DVWA | Linux | Application web vulnérable | 2 GB | 192.168.72.134 |
| Windows 11 | Windows | Cible Windows | 4 GB | 192.168.72.135 |

**Schéma d'Architecture**

[Internet] ❌ (Bloqué)

|

[Hyperviseur VMware]

|

[Réseau Host-Only: 192.168.72.0/24]

|

├── [Kali Linux] - Machine d'attaque

├── [Metasploitable 2] - Cible Linux

├── [DVWA] - Application web vulnérable

└── [Windows 11] - Cible Windows

**Mesures de Sécurité Implémentées**

* Isolation réseau complète
* Pas d'accès Internet pour les VMs vulnérables
* Environnement de test contrôlé
* Documentation des activités

**3. MÉTHODOLOGIE DE RECONNAISSANCE**

**Framework de Référence**

Cette reconnaissance suit la méthodologie standard de **penetration testing** :

1. **Reconnaissance passive**
2. **Découverte réseau**
3. **Énumération des services**
4. **Identification des vulnérabilités**

**Outils Utilisés**

| **Outil** | **Version** | **Usage** |
| --- | --- | --- |
| Nmap | 7.94 | Découverte réseau et énumération |
| Metasploit | 6.3.X | Framework d'exploitation |
| Dirb | 2.22 | Énumération web |
| Nikto | 2.5.0 | Scan de vulnérabilités web |

**Commandes Exécutées**

**Découverte réseau :**

nmap -sn 192.168.72.0/24

**Énumération des services :**

nmap -sV -sC -p- [IP\_CIBLE]

**Détection de vulnérabilités :**

nmap --script vuln [IP\_CIBLE]

**Énumération web :**

dirb http://[IP\_CIBLE]

nikto -h http://[IP\_CIBLE]

**4. RÉSULTATS DE LA CARTOGRAPHIE**

**Vue d'Ensemble du Réseau**

| **IP Address** | **Hostname** | **OS** | **Statut** | **Ports Ouverts** |
| --- | --- | --- | --- | --- |
| 192.168.72.1 | gateway | VMware | Actif | - |
| 192.168.72.133 | metasploitable | Ubuntu 8.04 | Actif | [Liste des ports] |
| 192.168.72.134 | dvwa | Linux | Actif | [Liste des ports] |
| 192.168.72.135 | windows11 | Windows 11 | Actif | [Liste des ports] |
| 192.168.72.136 | kali | Kali Linux | Actif | [Liste des ports] |

**Détail par Machine**

**192.168.72.133 - Metasploitable 2**

**OS Détecté :** Ubuntu 8.04 LTS  
**Services Identifiés :**

* **Port 21/tcp** - FTP (vsftpd 2.3.4) - VULNÉRABLE
* **Port 22/tcp** - SSH (OpenSSH 4.7p1)
* **Port 23/tcp** - Telnet
* **Port 25/tcp** - SMTP (Postfix)
* **Port 53/tcp** - DNS (ISC BIND 9.4.2)
* **Port 80/tcp** - HTTP (Apache 2.2.8)
* **Port 139/tcp** - NetBIOS-SSN (Samba 3.0.20)
* **Port 445/tcp** - SMB (Samba 3.0.20)

**Vulnérabilités Critiques :**

* CVE-2011-2523 (vsftpd backdoor)
* CVE-2007-2447 (Samba usermap script)
* CVE-2008-0166 (Weak SSH keys)

**192.168.72.134 - DVWA**

**OS Détecté :**   
**Services Identifiés :**

* **Port 22/tcp** - SSH (OpenSSH 9.6p1)
* **Port 80/tcp** - HTTP (Apache)
* **Port 443/tcp** - HTTPS (Apache)

**Applications Web :**

* DVWA (Damn Vulnerable Web Application)
* Interface de gestion MySQL

**192.168.72.135 - Windows 11**

**OS Détecté :** Microsoft Windows 11  
**Services Identifiés :**

* **Port 135/tcp** - RPC Endpoint Mapper
* **Port 139/tcp** - NetBIOS-SSN
* **Port 445/tcp** - SMB
* **Port 3389/tcp** - RDP (Remote Desktop)

**5. ANALYSE DES VULNÉRABILITÉS**

**Classification par Criticité**

**🔴 CRITIQUES (Score CVSS ≥ 9.0)**

| **CVE** | **Service** | **Description** | **Score CVSS** |
| --- | --- | --- | --- |
| CVE-2011-2523 | vsftpd 2.3.4 | Backdoor command execution | 10.0 |
| CVE-2007-2447 | Samba 3.0.20 | Remote command execution | 10.0 |

**🟠 ÉLEVÉES (Score CVSS 7.0-8.9)**

| **CVE** | **Service** | **Description** | **Score CVSS** |
| --- | --- | --- | --- |
| CVE-2008-0166 | OpenSSH | Weak random number generation | 7.8 |

**🟡 MOYENNES (Score CVSS 4.0-6.9)**

| **CVE** | **Service** | **Description** | **Score CVSS** |
| --- | --- | --- | --- |
| CVE-2007-6750 | Apache HTTP | Slowloris DoS | 5.0 |

**Vecteurs d'Attaque Identifiés**

1. **Exploitation de backdoor FTP**
   * Accès root immédiat via vsftpd 2.3.4
   * Aucune authentification requise
2. **Exploitation SMB Samba**
   * Exécution de commandes à distance
   * Escalade de privilèges possible
3. **Attaques sur applications web**
   * Injection SQL sur DVWA
   * Cross-Site Scripting (XSS)
   * Upload de fichiers malveillants
4. **Attaques par force brute**
   * Services SSH avec clés faibles
   * Interfaces web avec authentification basique

**6. ÉVALUATION DES RISQUES**

**Matrice de Risques**

| **Vulnérabilité** | **Probabilité** | **Impact** | **Risque Global** |
| --- | --- | --- | --- |
| vsftpd backdoor | Très Élevée | Critique | **CRITIQUE** |
| Samba RCE | Élevée | Critique | **CRITIQUE** |
| SSH weak keys | Élevée | Élevé | **ÉLEVÉ** |
| Web vulnerabilities | Élevée | Moyen | **MOYEN** |

**Impact Potentiel**

**Compromission Totale du Réseau :**

* Accès administrateur aux systèmes Linux
* Exfiltration de données sensibles
* Installation de malware persistant
* Utilisation comme point de pivot

**Interruption de Service :**

* Attaques par déni de service
* Corruption de données
* Arrêt des services critiques

**7. RECOMMANDATIONS DE SÉCURITÉ**

**Mesures Immédiates (Priorité 1)**

1. **Mise à jour des services vulnérables**
   * Remplacer vsftpd 2.3.4 par une version sécurisée
   * Mettre à jour Samba vers une version récente
   * Appliquer les correctifs de sécurité OpenSSH
2. **Durcissement des services**
   * Désactiver les services non nécessaires
   * Configurer des règles de pare-feu restrictives
   * Implémenter une authentification forte

**Mesures à Moyen Terme (Priorité 2)**

1. **Surveillance et détection**
   * Déployer un système IDS/IPS
   * Configurer la journalisation centralisée
   * Mettre en place des alertes de sécurité
2. **Segmentation réseau**
   * Isoler les services critiques
   * Implémenter des VLANs de sécurité
   * Contrôler les flux inter-réseaux

**Mesures à Long Terme (Priorité 3)**

1. **Gouvernance de sécurité**
   * Établir une politique de gestion des correctifs
   * Former les équipes aux bonnes pratiques
   * Réaliser des audits de sécurité réguliers
2. **Plan de continuité**
   * Préparer des procédures de réponse aux incidents
   * Mettre en place des sauvegardes sécurisées
   * Tester les plans de récupération

**8. CONCLUSION**

**Synthèse des Résultats**

L'audit de sécurité de ce laboratoire a révélé **[X] vulnérabilités critiques** permettant une compromission complète des systèmes cibles. La configuration actuelle présente un niveau de risque **CRITIQUE** nécessitant des actions immédiates.

**Objectifs Atteints**

✅ Cartographie réseau complète réalisée  
✅ Vulnérabilités critiques identifiées  
✅ Vecteurs d'attaque documentés  
✅ Plan de remédiation établi

**Prochaines Étapes**

1. Exploitation contrôlée des vulnérabilités identifiées
2. Mise en place des mesures de remédiation
3. Validation de l'efficacité des correctifs
4. Documentation des leçons apprises

**Compétences Démontrées**

* **Reconnaissance réseau** avec Nmap
* **Analyse de vulnérabilités** systématique
* **Évaluation des risques** selon les standards
* **Documentation technique** professionnelle
* **Méthodologie de pentest** structurée

**9. ANNEXES**

**Annexe A : Commandes Complètes Exécutées**

# Découverte réseau

nmap -sn 192.168.72.0/24

# Scan détaillé par machine

nmap -sV -sC -O 192.168.72.XXX

# Scan de vulnérabilités

nmap --script vuln 192.168.72.XXX

# Énumération web

dirb http://192.168.72.XXX

nikto -h http://192.168.72.XXX

**Annexe B : Sorties Complètes des Scans**

[Insérer ici les sorties complètes des commandes Nmap]

**Annexe C : Captures d'Écran**

[Insérer ici les captures d'écran importantes]

**Annexe D : Références Techniques**

* NIST Cybersecurity Framework
* OWASP Top 10
* Common Vulnerability Scoring System (CVSS)
* CVE Database

**Document rédigé par :** [Votre nom]  
**Date de dernière mise à jour :** [Date]  
**Version :** 1.0