OFFENSIVE SECURITY

Pentest Report pour projet fil rouge Ynov

v.1.0

nils.jaudon@ynov.com

OSID: 00000

Table of Contents

1.0 Sécurité offensive & Test d’intrusion

1.1 Introduction

Ce rapport présente l’ensemble des actions réalisées dans le cadre du projet de sécurisation du système d’information d’un hôpital fictif, le CHU de Ynov. Il s’inscrit dans un contexte pédagogique d’apprentissage de la cybersécurité offensive. Le rapport suit une approche méthodologique complète de type test d’intrusion interne, avec pour objectif d’identifier, d’exploiter et de documenter des failles critiques du système cible.

1.2 Objectif

Effectuer un test d’intrusion interne sur l’infrastructure d’un hôpital fictif dans le cadre du projet de fin d’année. Ce test a pour but de simuler une attaque réelle afin de :

- Évaluer la robustesse du système Active Directory du CHU fictif
- Exploiter une vulnérabilité critique non patchée (Zerologon - CVE-2020-1472)
- Utiliser des outils professionnels tels que OpenVAS, Impacket et Metasploit
- Proposer des contre-mesures adaptées
- Documenter la démarche, les résultats et les recommandations

1.3 Requirements

- **Analyse des risques et vulnérabilités**
  - Identifier les actifs critiques (ex : Active Directory, DNS, NAS, VPN ...)
  - Utiliser des outils de scan de vulnérabilités (OpenVAS, Nessus)
- **Simulation d'attaque**
  - Réaliser des tests d'intrusion sur les systèmes de sécurité de l'hôpital
  - Exploiter une ou plusieurs failles réelles (ex : Zerologon)

L'objectif de ce test d'intrusion est de simuler une attaque réelle sur le système d'information de l'hôpital fictif CHU Ynov. L'attaque s'est concentrée sur le contrôleur de domaine principal non patché, exposé à la faille critique Zerologon (CVE-2020-1472), et sur une phase de reconnaissance et d'identification des vulnérabilités à l'aide d'OpenVAS.

Durant le test, **plusieurs vulnérabilités ont été identifiées**, dont **une critique permettant une élévation de privilèges** directe jusqu'à l'obtention des droits d'administrateur de domaine. Ces vulnérabilités sont liées principalement à :

- Des systèmes non mis à jour
- Une mauvaise configuration réseau
- L'absence de segmentation ou de contrôle d'accès

La faille Zerologon a permis une compromission totale de l'annuaire Active Directory. Cette situation met en lumière la nécessité de maintenir une politique de mise à jour stricte et de segmenter les accès au contrôleur de domaine.

Les chapitres suivants présentent les détails techniques de l'attaque, les outils utilisés, les preuves collectées ainsi que les recommandations de sécurité proposées.

2.1 Sample Report - Recommendations

scan nmap avec vuln

3.0 Openvas

3.0 OpenVAS Vulnerability Scan

Un scan de vulnérabilité a été lancé avec l'outil **OpenVAS**, configuré pour analyser l'ensemble des machines de l'environnement cible. Le but était d'identifier les failles exploitables, les services exposés, et de préparer les étapes suivantes du test d'intrusion.

3.1 Sample Report – Information Gathering

La phase de reconnaissance a permis d'identifier un windows Server de 2019.

192.168.1.116

3.2 Sample Report – Service Enumeration

La phase d'énumération de services a permis d'identifier les ports ouverts et les services actifs sur les hôtes cibles. Cette étape est cruciale car elle fournit des informations essentielles sur les vecteurs d'attaque possibles, les services vulnérables et les technologies en place.

3.3 Zerologon Vulnerability Exploitation (CVE-2020-1472)

Une attention particulière a été portée à la vulnérabilité **Zerologon**, qui affecte les **contrôleurs de domaine Windows non patchés**. L'attaque repose sur une faille dans le protocole Netlogon, permettant un contournement total de l'authentification avec un hash nul.

- **Cible** : Contrôleur de domaine Windows Server 2019 (non mis à jour volontairement pour la démonstration)
- **Méthode** : Utilisation de l'exploit `CVE-2020-1472` via l'outil `impacket`
- **Résultat** : Élévation de privilèges, prise de contrôle du domaine

- **Impact** : Critique – compromission totale de l'environnement Active Directory

3.4 Post-Exploitation

Une fois les privilèges élevés obtenus grâce à l'exploitation de Zerologon, plusieurs actions de post-exploitation ont été menées afin d'évaluer l'étendue de la compromission :

- **Dump des identifiants Active Directory** via `secretsdump.py`
- **Extraction des hashs NTLM** pour les comptes critiques (`krbtgt`, `Administrator`, comptes de service)
- **Mappage du domaine** (forêts, unités organisationnelles, contrôleurs secondaires)
- **Accès aux partages de fichiers sensibles**, y compris certains répertoires SYSVOL contenant des scripts GPO potentiellement exploitables
- **Recherche de données métiers critiques** (fichiers RH, documents internes)

Ces actions ont confirmé un **contrôle total du domaine** et un accès aux **ressources internes sensibles**.

3.5 Persistence

Afin de simuler un attaquant réel, une **persistence contrôlée** a été mise en place :

- Création d'un **compte administrateur furtif** (`pentestsvc`) dissimulé dans une unité organisationnelle non surveillée
- Ajout d'une **clé de registre Run** sur le DC pour exécuter une commande PowerShell à l'ouverture de session
- Création d'un **scheduled task** pour maintenir une connexion vers un serveur C2 simulé (sans communication externe effective dans le cadre de ce test)

Toutes les actions ont été **documentées, surveillées et nettoyées** à la fin de l'intervention.

3.6 Analyse de Risques

Élément impacté	Gravité	Description
Active Directory	Critique	Compromission complète par élévation de privilèges
Données métiers	Élevée	Accès potentiel à des documents RH, GPO sensibles
Continuité de service	Moyenne	Risque potentiel de sabotage via GPO ou Scheduled Tasks
Traçabilité	Faible	Aucune alerte déclenchée durant les phases d'exploitation

3.7 Recommandations

Pour réduire le risque associé à cette vulnérabilité et renforcer la sécurité globale de l'infrastructure, les recommandations suivantes sont proposées :

- **Appliquer immédiatement le correctif Microsoft** pour CVE-2020-1472 (patch d'août 2020)
- **Surveiller les logs Netlogon** (`Event ID 5829, 5830, 5831`) pour détecter des anomalies
- **Modifier tous les mots de passe de comptes sensibles**
- **Mettre en place l'authentification multi-facteur (MFA)** pour les comptes à privilèges
- **Restreindre l'accès aux ports critiques** via des ACL réseau (445, 135, 389, etc.)
- **Activer la journalisation avancée des accès et des modifications AD**
- **Mettre en place une supervision centralisée** (SIEM, alerting sur comportements anormaux)
- **Former les administrateurs** à la détection de comportements anormaux et aux réponses post-incident