TP2

Découverte et Analyse des Ports et Services Réseau

Objectifs :

- Apprendre à effectuer différents types de scans réseau avec Nmap
- Découvrir les ports ouverts ainsi que les versions des services dans une machine cible.
- Analyser les résultats et déduire des informations sur les machines scannées
- Savoir manipuler des scripts NSE.

Introduction

La phase de l'analyse et découverte des ports d'une machine victime est une phase primordiale dans le processus de piratage, le but est de déterminer le type de service qui tourne dans une machine en vue de savoir s'il s'agit d'un service vulnérable ou non.

Nmap (Network Mapper) est un logiciel libre créé par Fyodor et distribué par Insecure.org permettant de scanner et de détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Nmap est équipé d'un moteur de script NSE « Nmap Script Engine » qui fournit des fonctionnalités plus puissantes et plus flexibles lors de la phase de l'analyse.

I. Scan du réseau local

1. Démarrer les deux machines virtuelles « *Student* » & « *MyServer* ».
2. Vérifier la connectivité entre les deux machines.
3. Lancer Nmap dans la machine « *Student* » et analyser le réseau local pour déterminer les machines qui sont connectées.
4. Utiliser Nmap pour déterminer le nom du système d'exploitation de la machine « *MyServer* ».
5. Déduire la version du système d'exploitation.

II. Analyse des ports de la machine MyServer

1. Utiliser Nmap pour déterminer tous les ports ouverts dans la vm
2. Réaliser une énumération de tous les services de la vm

III. Analyse d'un serveur du réseau local

1. Assurer vous que le serveur local est joignable (@ip : 192.168.246.21).
2. Utiliser Nmap pour déterminer tous les ports ouverts.
3. Réaliser une énumération des services.

IV. Analyse d'un site web

On veut réaliser une analyse du site web suivant : **`http://scanme.nmap.org`**

1. Déterminer les ports qui sont ouverts.
2. Enumérer les services qui sont activés.
3. Déterminer la version du système d'exploitation.

V. Nmap Scripting Engine

1. Afficher tous les scripts NSE disponible pour Nmap dans **/usr/share/nmap/scripts/**
2. Rechercher et appliquer un script NSE convenable pour les services découverts. On vous demande d'analyser trois services avec les scripts NSE avec la machine « Client ».
   i.e : Pour utiliser un script nse : **`nmap --script nom_du_script –p num_port @IP`**

VI. Recherche des vulnérabilités des services

1. Utiliser un site de recherche des vulnérabilités publique, vu dans le cours, pour chercher les vulnérabilités de trois services trouvés lors du scan.
2. Déterminer le CVSS ainsi que l'impact causé par l'exploitation de cette vulnérabilité.

Travail demandé :

1. Elaborer un rapport complet contenant la solution de chaque question.
2. Réaliser un imprime écran pour tous les résultats obtenus.