UQAC
Département d'informatique et de mathématique
Université du Québec à Chicoutimi

Travail pratique #2

Objectifs du travail pratique

- Se familiariser avec les scanners de vulnérabilités
- Se familiariser avec les outils de collecte de données
- Installer deux machines virtuelles: Kali Linux et Metasploitable
- Configurer Nessus sur Kali Linux pour scanner les vulnérabilités de Metasploitable
- Utiliser Nmap pour scanner les ports ouverts de Metasploitable
- Étude de cas sur l'exploitation d'une vulnérabilité

Exigences

1. **Installation des Machines Virtuelles:**
   - Téléchargez et installez VirtualBox (ou VMware).
   - Télécharger les fichiers d'image de :
     - Kali Linux : Lien de téléchargement
     - Metasploitable : Lien de téléchargement
   - Créer deux machines virtuelles distinctes dans votre logiciel de virtualisation (VirtualBox ou VMware).
   - Configurer les paramètres réseau appropriés pour permettre la communication entre les machines virtuelles.

2. **Installation de Nessus sur Kali Linux:**
   - Télécharger et installer Nessus sur Kali. Vous pouvez consulter ce site Web pour de l'information utile.
   - Configurer et activer Nessus en utilisant une licence d'évaluation gratuite. Pour démarrer le service Nessus sur Kali, vous devez utiliser cette commande : **systemctl start nessusd** ce qui vous permettra ensuite d'accéder à l'outil via un navigateur et l'adresse https://kali:8834/ par exemple.

3. **Scannage des Vulnérabilités avec Nessus:**
    - Lancer Nessus depuis Kali Linux.
    - Configurer un scan de vulnérabilités sur l'adresse IP de la machine Metasploitable. *Pour obtenir l'adresse IP, exécuter la commande ifconfig en ligne de commande.*
    - Analyser les résultats du scan et identifier les vulnérabilités détectées.

4. **Scannage des Ports avec Nmap:**
    - Utiliser Nmap depuis Kali Linux pour scanner les ports ouverts de Metasploitable : **sudo nmap [options] adresseIP**
    - Analyser les résultats du scan pour identifier les services et les ports ouverts sur Metasploitable.

5. **Étude de cas sur l'exploitation de vulnérabilités :**

    - Choisissez une des vulnérabilités détectées sur Metasploitable et recherchez des informations sur cette vulnérabilité. Quels sont les détails techniques de l'exploit associé ?
    - Discutez de comment pourriez-vous exploiter cette vulnérabilité pour obtenir un accès non autorisé à la machine Metasploitable ?

Document à remettre

- Rédiger un document PDF décrivant les étapes suivies pour installer les machines virtuelles et configurer les outils (étapes 1 et 2)
- Inclure une analyse des résultats des scans de Nessus et Nmap, en mettant en évidence les vulnérabilités détectées et les services exposés (étapes 3 et 4)
- Inclure la réponse à votre étude de cas sur l'exploitation d'une vulnérabilité (partie 5).

Date de remise

Le vendredi 29 mars 2024 via le Moodle du cours.