Godric Bouteloup
Marco Witzel

Travail pratique #2

1. Installation des Machines Virtuelles:

Pour ce TP, nous avons choisi d'utiliser VirtualBox.
Après avoir téléchargé les fichiers d'installation des deux systèmes d'exploitation, nous avons créé deux machines virtuelles utilisant Kali Linux et Metasploitable.

En ce qui concerne la configuration réseau, nous sommes allés dans les paramètres réseau des deux machines virtuelles, sous configuration, réseau, adapter 1, puis nous avons changé NAT en réseau privé hôte ("Host-Only") ce qui nous permet d'avoir des adresses IP valides pour nos deux machines virtuelles et la communication entre les celles-ci.

Les machines virtuelles Metasploitable et Kali Linux possèdent 2Go de mémoire vive pour 128 Mo de mémoire vidéo.

2. Installation de Nessus sur Kali Linux:

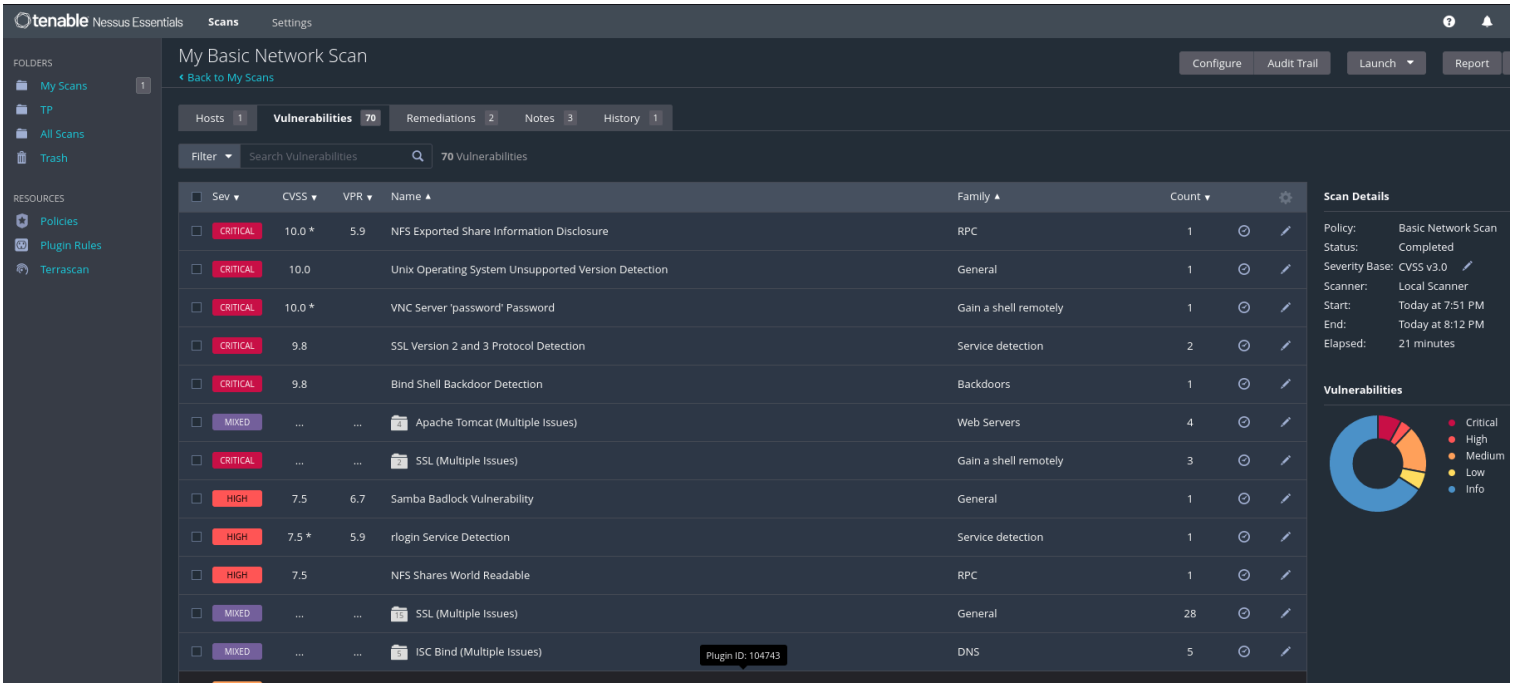
Pour installer Nessus sur Kali, nous avons suivi le tutoriel fourni.
Celui-ci consiste en appliquant premièrement les commandes **"apt update && apt upgrade"**.
Par la suite, on télécharge le package de Nessus pour linux 64 bits et on utilise la commande **"dpkg -i Nessus-10.7.1-ubuntu1404_amd64.deb"**pour l'installer.
On lance ensuite Nessus avec la commande "systemctl start nessusd". Après avoir démarré le service, l'interface web de Nessus est accessible via un navigateur à l'adresse : "https://kali:8834/", une url qui n'était pas accessible avant le lancement de Nessus.
Nous créons un compte Nessus en choisissant l'option gratuite pour les étudiants.

L'installation et la configuration de Nessus sur Kali Linux ont été réalisées avec succès. Nessus est maintenant prêt à être utilisé pour lancer des scans de vulnérabilités sur la machine Metasploitable afin d'identifier les failles de sécurité potentielles.

Godric Bouteloup
Marco Witzel

3. Scannage des Vulnérabilités avec Nessus:

Premièrement, on lance notre machine virtuelle Metasploitable, on se connecte à notre session **msfadmin** qui a comme login et mot de passe ”msfadmin”.
Par la suite on lance la commande **“ifconfig”**, nous pouvons récupérer l’adresse ip de la machine virtuelle Metasploitable.
Nous retournons sur Kali Linux et lançons le scan sur Nessus avec l’ip récupérée juste avant. Après une vingtaine de minutes nous obtenons les résultats suivants :



En relevant toutes les vulnérabilités dites “critical”, nous avons fais des recherches pour connaître leurs sens :

- **NFS Exported Share Information Disclosure (10.0)** : Cette vulnérabilité révèle des informations sensibles sur les partages de fichiers NFS, ce qui pourrait permettre à un attaquant d'accéder à des données, cela sera expliqué davantage dans la question 5.

- **Unix Operating System Unsupported Version Detection (10.0)** : Cette détection indique qu'une version non prise en charge du système d'exploitation Unix est utilisée, cela indique qu’il y a un risque de présence de vulnérabilités de sécurité non corrigées.

- **VNC Server 'password' Password (10.0)** : Cette vulnérabilité indique que le mot de passe par défaut ou un mot de passe faible est utilisé pour le serveur VNC, cela expose la machine à un risque d'accès non autorisé à travers ce système de visualisation et de contrôle de l'environnement.

- **SSL Version 2 and 3 Protocol Detection (9.8)** : Cette détection indique que les protocoles SSL version 2 et 3, connus pour leurs vulnérabilités de sécurité, sont activés sur le serveur.

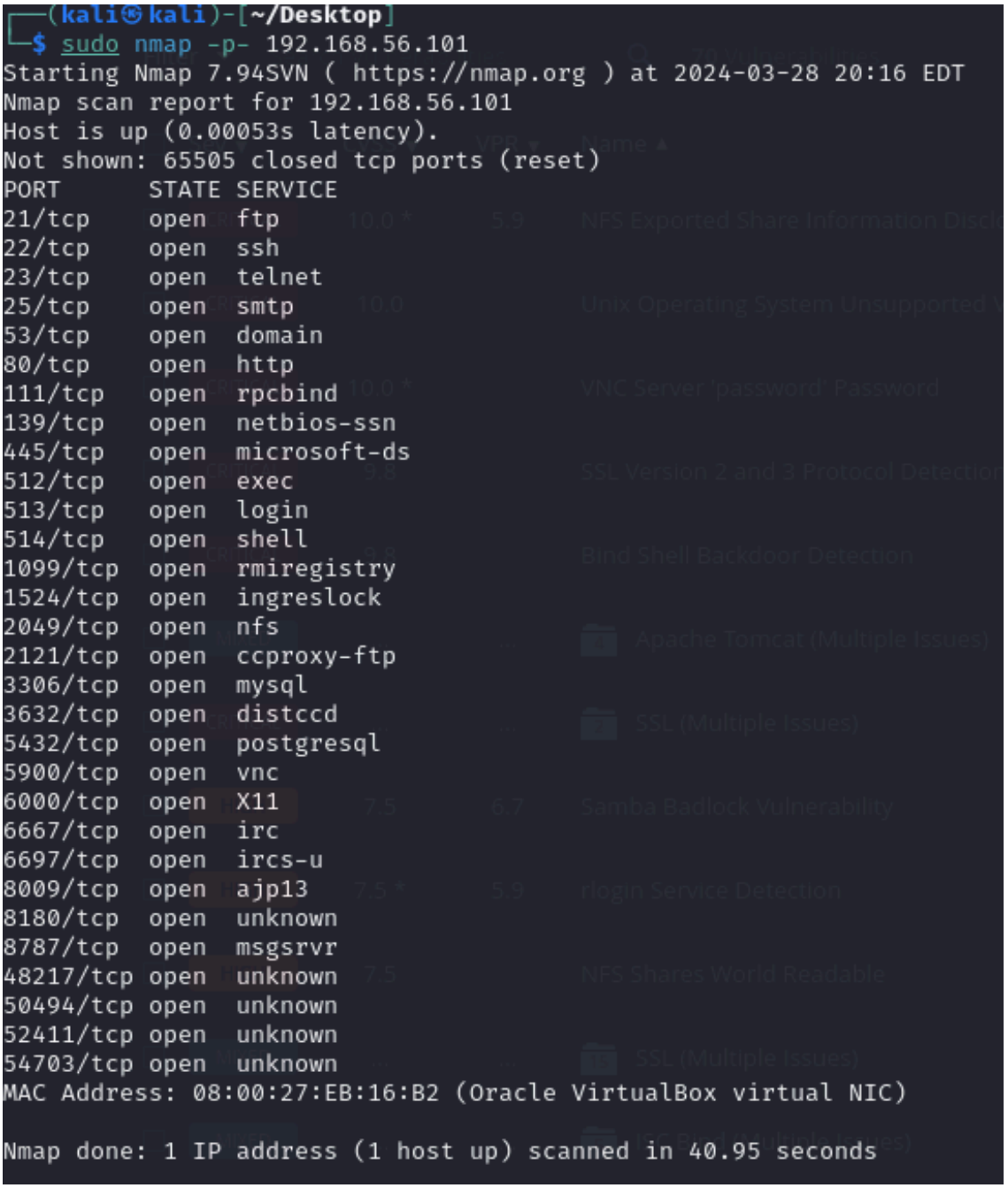
- **Bind Shell Backdoor Detection (9.8)** : Cette détection indique la présence d'une porte dérobée de type "Bind Shell", cela permet à un attaquant distant d’exécuter des commandes sur la machine, cela n’est donc pas sécuritaire.

- **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) (10.0)** : Cette faiblesse concerne la génération de nombres aléatoires dans les packages Debian OpenSSH et OpenSSL, les clés cryptographiques sont donc plus prévisibles et cela compromet la confidentialité des communications sécurisées.

Godric Bouteloup
Marco Witzel

4. Scannage des Ports avec Nmap:

Pour analyser la sécurité et la configuration du réseau de la machine virtuelle Metasploitable, l'outil de scan de ports Nmap a été utilisé depuis Kali Linux.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -p- 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-28 20:16 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00053s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
48217/tcp open  unknown
50494/tcp open  unknown
52411/tcp open  unknown
54703/tcp open  unknown
MAC Address: 08:00:27:EB:16:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 40.95 seconds
```

- **Port 21 (FTP - File Transfer Protocol) :** Le port 21 est généralement utilisé pour le transfert de fichiers et FTP est un protocole utilisé pour le transfert de fichiers. Les serveurs FTP peuvent être vulnérables à diverses attaques telles que l'ingénierie sociale, l'interception de mots de passe et les dénis de service.
- **Port 22 (SSH - Secure Shell) :** Le port 22 est le port par défaut pour SSH et SSH est un protocole de communication sécurisé utilisé pour l'accès à distance et la gestion sécurisée des systèmes.
- **Port 23 (Telnet) :** Le port 23 est le port par défaut pour Telnet et Telnet est un protocole de communication utilisé pour l'accès à distance aux systèmes. Sa

présence peut indiquer un risque potentiel de divulgation de mots de passe et de compromission du système.

- **Port 80 (HTTP - Hypertext Transfer Protocol) :** Le port 80 est le port par défaut pour les connexions HTTP non sécurisées. Sa présence indique la disponibilité d'un serveur web sur la machine Metasploitable. Les vulnérabilités courantes associées à HTTP incluent les injections SQL, les attaques par force brute sur les formulaires d'authentification, et les failles de sécurité dans les applications web.
- **Port 139 (NetBIOS-SSN) :** Ce port est celui pour le service NetBIOS-SSN. NetBIOS-SSN est utilisé pour les services de partage de fichiers, d'imprimantes et d'autres ressources sur les réseaux Microsoft. Les attaquants peuvent tenter d'accéder à ces partages ou d'exécuter des attaques de type "Man-in-the-Middle" sur les communications NetBIOS.
- **Port 445 (Microsoft-DS) :** Ce port est utilisé pour les communications SMB (Server Message Block) et est souvent associé à Microsoft-DS. Il est aussi indicateur de partage de fichiers et d'imprimantes sous Windows.
  Nous pouvons citer l'attaque faite par WannaCry qui a utilisé une faille sur les communications SBM via ce port selon l'exploit EternalBlue.
- **Port 3306 (MySQL Database) :** Ce port est celui qui désigne la possible existence d'une base de données. Un attaquant peut donc utiliser des failles connues de MySQL ou tenter d'effectuer une injection SQL.

Le scan des ports avec Nmap a permis d'identifier les services et les ports ouverts sur la machine Metasploitable. Ces informations sont essentielles pour comprendre la surface d'attaque potentielle de la machine et pour planifier des mesures de sécurité appropriées.

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

La vulnérabilité détectée **"NFS Exported Share Information Disclosure"** (NFS pour Network File System) concerne l'exposition d'informations sensibles via des partages NFS mal configurés.
Ce protocole est utilisé pour le partage de fichiers sur les réseaux Unix et Linux.

Cette vulnérabilité se produit lorsque les partages NFS sont mal configurés, permettant à des utilisateurs non autorisés d'accéder à des données sensibles.
Les partages NFS exposent souvent des informations telles que les noms de fichiers, les structures de répertoires et même les données elles-mêmes si les autorisations ne sont pas correctement définies.

Pour exploiter cette vulnérabilité, un attaquant peut utiliser des outils comme **showmount** pour identifier les partages NFS exportés sur une machine cible.
Par la suite, il peut monter ces partages localement pour accéder aux données sensibles.
La première étape est l'identification des partages NFS avec cet outil.
Une fois le partage monté, l'attaquant peut naviguer dans les répertoires et accéder aux fichiers exposés.

Celle-ci expose les organisations à un risque de divulgation d'informations sensibles si les partages NFS ne sont pas correctement sécurisés.