Exploitation

Contournement de pare-feu

Rebonds : redirection de port

Sous Windows

- Netsh
  - `netsh interface portproxy add v4tov4 listenport=4422 listenaddress=192.168.1.111 connectport=80 connectaddress=192.168.0.33`
- Meterpreter
- Socat
  - `socat TCP4-LISTEN:4422,reuseaddr, fork TCP4:192.168.0.33:80`
- Netcat
  - `mkfifo backpipe`
    `nc -l 4422 0<backpipe | nc 192.168.0.33 80 1>backpipe`
- SSH
  - `ssh -L 127.0.0.1:445:192.168.211.1:445 test@192.168.210.1`

    `(ssh -L port-local:ip-cible:port-distant machine-distante)`
  - `ssh -R 445:127.0.0.1:135 test@192.168.210.1`

    `(ssh -R port-distant:HOSTNAME:port-local  machine-distante)`

Exploitation

Contournement de pare-feu

Rebonds : redirection de port

ssh -L port-local:ip-distant:port-distant machine-distante

```
ssh -L 127.0.0.1:4445:192.168.211.1:445 test@192.168.210.1
```

192.168.211.1

127.0.0.1

192.168.210.1