cheet

Virtual Box

Set VM internet:

- **Bridge** --> conn a internet (selezioni il ponte in base a se sei conn al wifi o ethern)
- Nat --> conn a internet + conn tra diverse vm

Per Nat:
devi creare una NatNetwork => - File > Tools > Network Manager
- seleziona Nat Networks
- Create

Tools

Netdiscover

tools for scanning the entire net to find hosts ip (using arp)
`sudo netdiscover -r 10.0.2.0/24` -r = scan a given range instead of
auto scan

Nmap

tools for scanning ports to identify open ports
`nmap -T4 -p- -A 10.0.2.152`

`nmap -Pn --script smb-vuln* -p 139,445 10.0.2.152`

`-T4` —> set scan velocity from 1 to 5 (1 slow but complete - 5 fast but)
`-p-` —> scan all ports (without scann only 1000 most known)
`-A` —> show me all that you found
`-Pn` --> treat all hosts as online -- skip host discovery

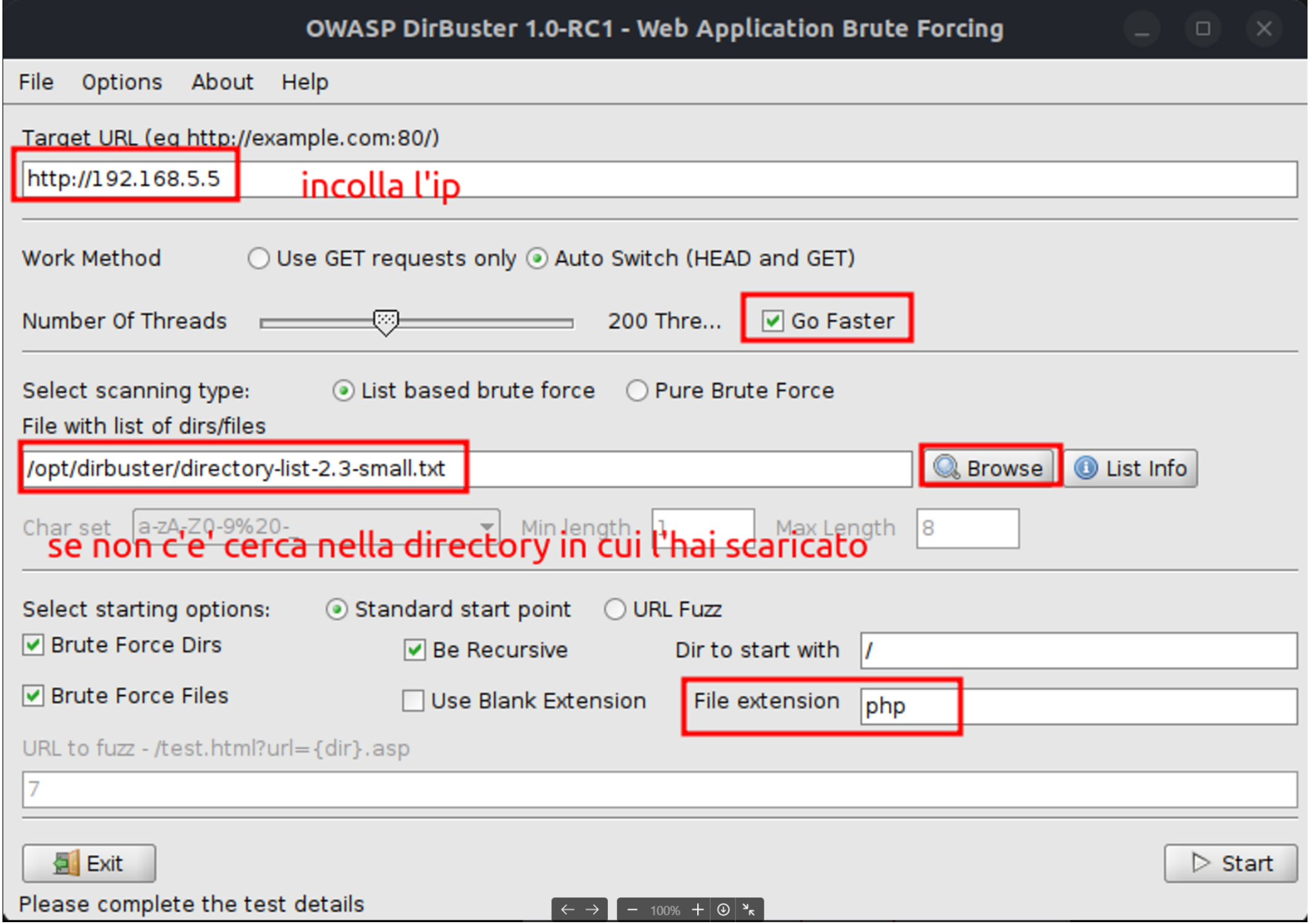
Enumerating HTTP e HTTPS

Nikto

scanning website vulnerabilities
`nikto -h http://10.0.2.152` -h = host

Dirbuster

finds hidden file/subdirectories website
`dirbuster`

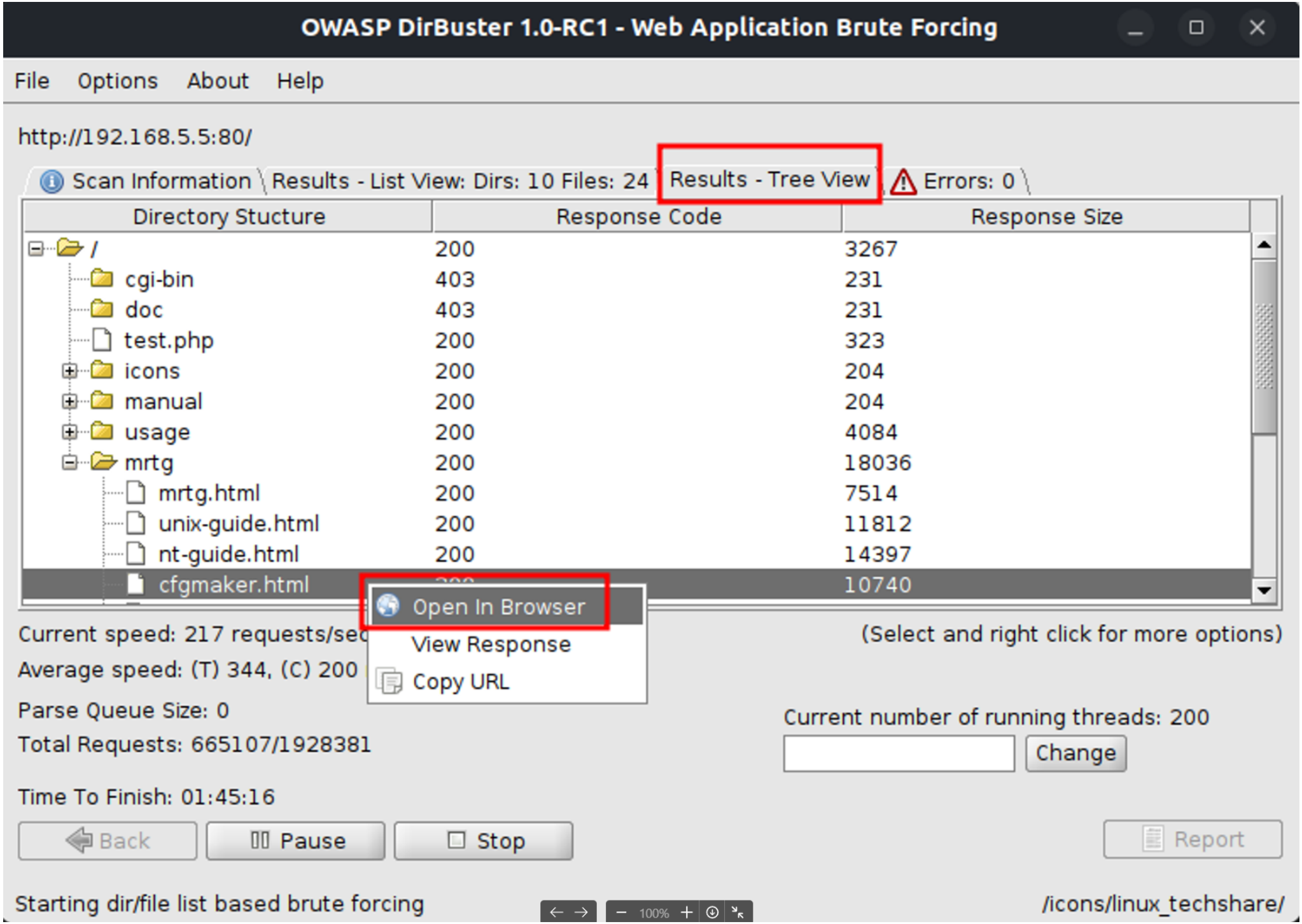

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Target URL (eg http://example.com:80/)
http://192.168.5.5
incolla l'ip
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
200 Thre...
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/opt/dirbuster/directory-list-2.3-small.txt
Browse
List Info
Char set
a-zA-Z0-9%20-
Min Length
1
Max Length
8
se non c'e' cerca nella directory in cui l'hai scaricato
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
7
Exit
Start
Please complete the test details
100%

- Faremo una scansione usando una wordlist predefinita di dirbuster
- La wordlist —> contiene tanti subdomains noti (es /admin, /root, /…)
- Proverà per ciascuno di essi a vedere se esiste: es http://10.0.2.152/admin e così via
- L'estensione serve a specificare quali tipologie di subdomain deve cercare
- mettendo solo php ⇒ cercherà l'esistenza di tutte le directory nella wordlist add il .php alla fine es http://192.168.5.5/admin.php

Altre possibili estensioni —> pdf, rar, zip, docx … (+ ne metti e + è lunga la scans)

- Clicca su Tree View per vedere la struttura ad albero dei file trovati.

- Se clicchi con il tasto dx su un file e apri nel browser ti mostrerà la pagina



Enumerating SMB

Metasploit

If you don't know a lot of a protocol => search for it inside metasploit to see the modul

`search smb`

`use 0`

`info`

`options`

`set RHOSTS ...`

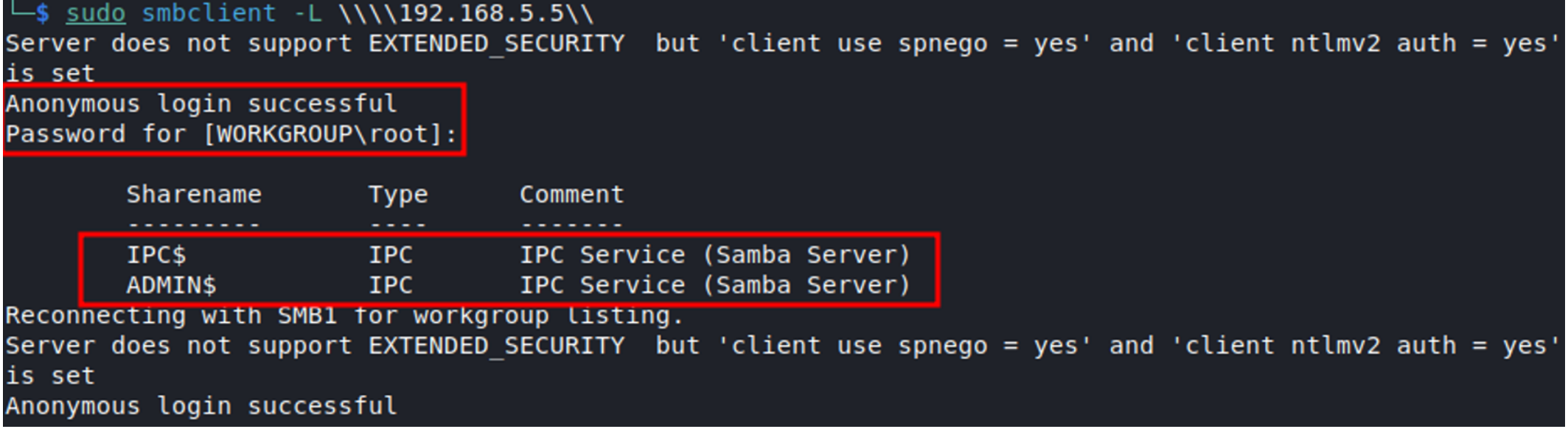
`run`

Smbclient

tries to connect anonimmously to smb file sharing

`smbclient -L \\\\\\\\10.0.2.152\\\\` (-L list)

> **ⓘ Se da questo errore**
>
> `protocol negotiation failed: NT_STATUS_IO_TIMEOUT`
>
> ⇒ modifica il file `/etc/samba/smb.conf`
>
> Aggiungendo sotto “global”:
>
> `client min protocol = CORE`
>
> `client max protocol = SMB3`



Try to connect to ADMIN:\$smbclient -L10.0.2.152ADMIN$`

leave password empty