

SMB Enumeration

SMB Enumeration Techniques using Backtrack:

1. NBTSCAN

```
root@bt:~# nbtscan -r 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
10.0.2.0	Sendto failed: Permission denied			
10.0.2.10	<unknown>		<unknown>	
10.0.2.15	METASPLOITABLE	<server>	METASPLOITABLE	00-00-00-00-00-00
10.0.2.18	TEST01	<server>	TEST01	00-11-21-22-1d-4d
10.0.2.45	TEST04	<server>	TEST04	00-12-d2-34-11-55

2. NMAP

```
nmap -p 1-65535 -T4 -O -A -v 10.0.2.15
```

3. SMBCLIENT

```
root@bt:~# smbclient -L=10.0.2.15
```

Null Sessions

```
root@bt:~# smbclient \\\\10.0.2.15\\tmp
Enter root's password:
Anonymous login successful
```

SMB Enumeration Techniques using Windows Tools:

1. NetBIOS Enumerator (nbtenum)

<http://nbtenum.sourceforge.net/>