

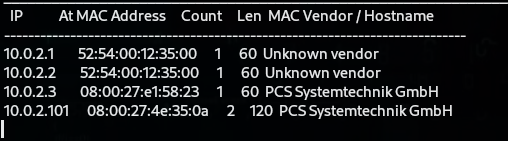
PERSISTENCIA

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:

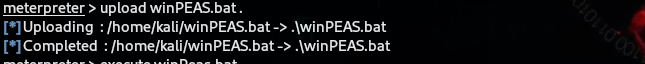
1. Una vez iniciada ambas maquinas se obtiene la IP de la maquina objetivo siendo la terminada en 101:



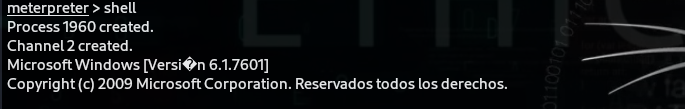
1. Con la herramienta Metasploit y usando el módulo *“ms17\_01\_eternalblu”* se logra iniciar sesión con una meterpreter con privilegios *“Authority/System”:*

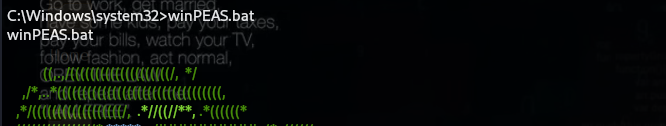


1. Se procede a usar winPEAS, herramienta **post-explotación** utilizada en pruebas de penetración para enumerar información y encontrar posibles vectores de escalada de privilegios para sistemas Windows, procediendo a subir el archivo correspondiente para su ejecución en el sistema atacado:

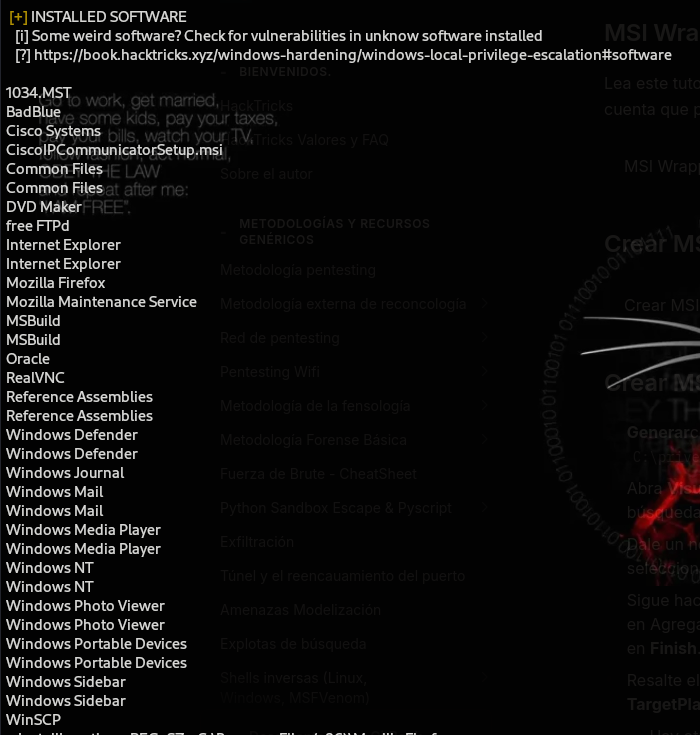


Una vez subido a la ruta que nos ha dado por defecto la meterpreter (“*/Windows/system32/”),* abrimos una shell y ejecutamos el archivo .bat:





1. 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.

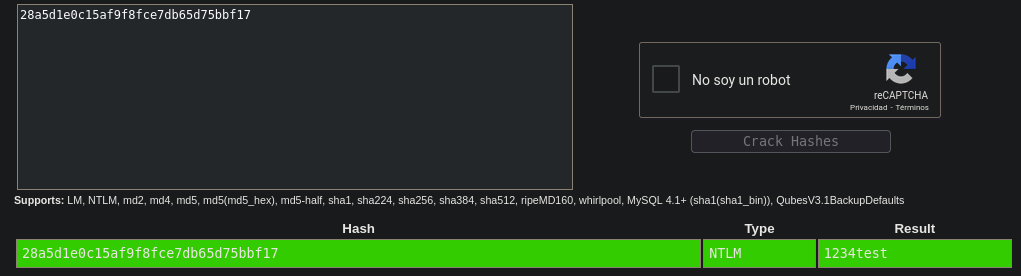


1. Se examina en Metasploit, módulos post-explotación que puedan ser compatibles a usar con el exploit EternalBlue, probando varios de ellos con resultado negativo, hasta conseguir un nuevo acceso al sistema por la via RDP, ejecutando el módulo post *“Windows/manage/enable\_rdp”,* usando para ello, la 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”.

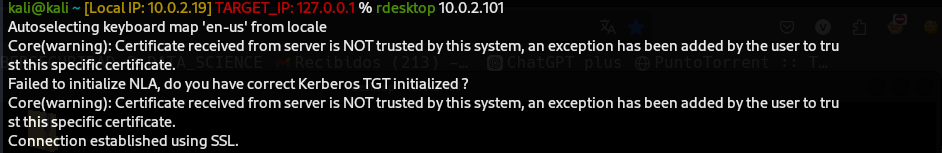


1. En la web [*https://crackstation.net/*](https://crackstation.net/), se procede a descifrar los hashes NTLM de ambos usuarios, estando sin clave alguna, el administrador y el usuario Bob con la contraseña indicada en la imagen:

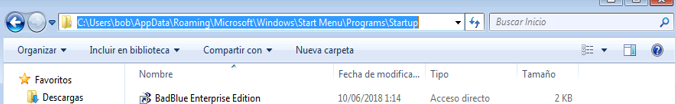


Un dato curioso que no tenga clave el administrador, pudiendo existir la posibilidad que este usuario este desactivado en el sistema.

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

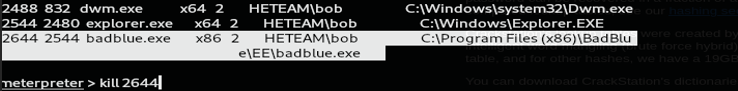


1. Una vez conectado, comprobamos la ruta donde se alojan los programas que se inician automáticamente en Windows, apareciendo uno de los programas que winPEAS aporto anteriormente: BadBlue Enterprise Edition.

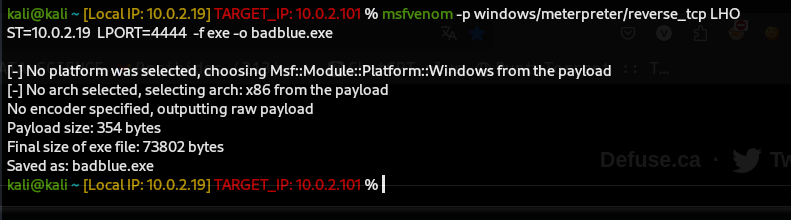


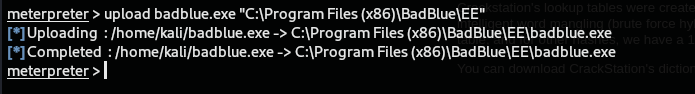
1. Con esta información volvemos a la sesión abierta de Metasploit, accediendo a la ruta donde esta el ejecutable de la aplicación BadBlue, procediendo a eliminar el proceso 2644 en el sistema de la misma.





1. 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.

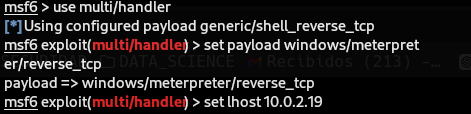




Aquí podemos observar el payload malicioso agregado al sistema, el cual, presenta permisos totales en el sistema objetivo, por lo que se ejecutara independientemente del usuario que inicie sesión la maquina infectada.



1. 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.



1. 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.

