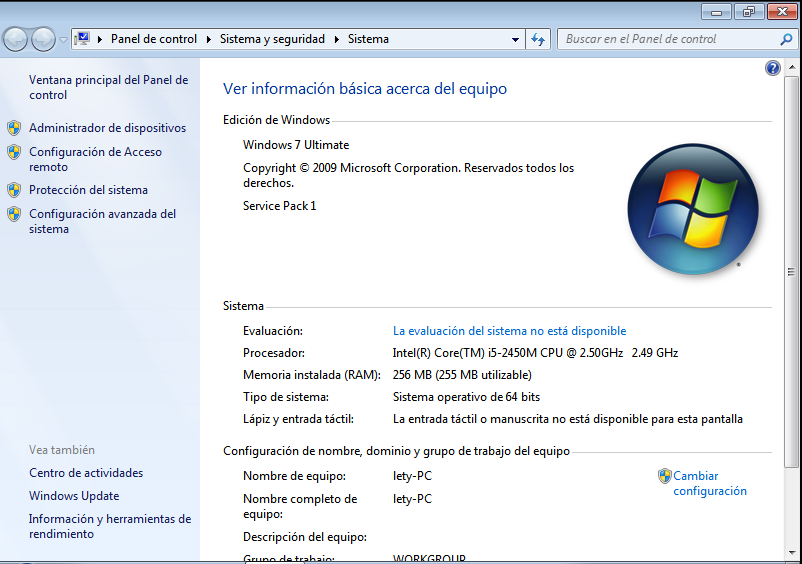
**DENEGACIÓN DE SERVICIO CON METASPLOIT**

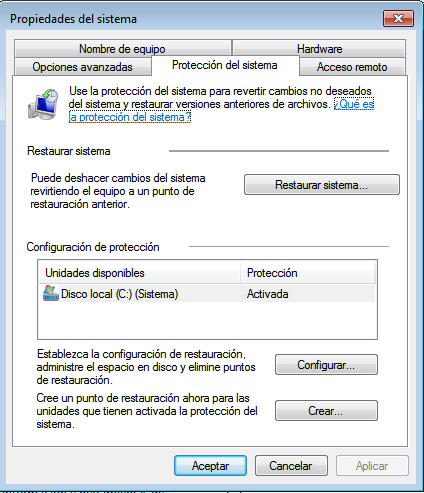
**Escenario 1**

En este escenario se procede a realizar un ataque denegación de servicio al sistema de escritorio remoto de Windows 7. Para este caso verifica que el servicio RDP permita todas las conexiones con otros equipos de escritorio remoto de forma insegura.

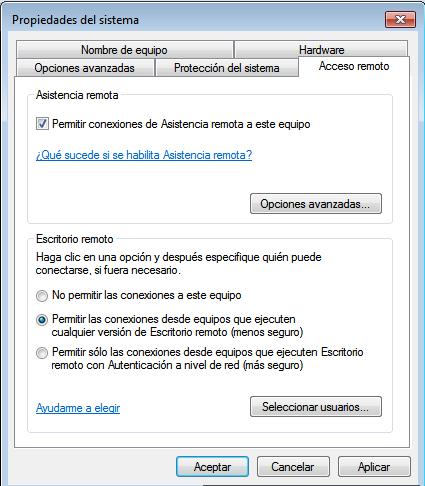
* Verificar protección del sistema



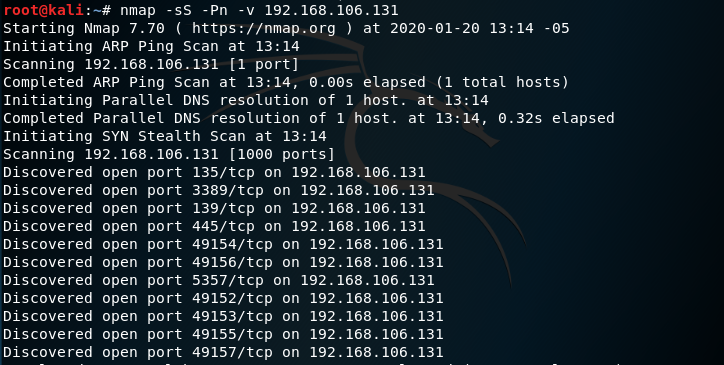
* Acceso a la opción de acceso remoto.



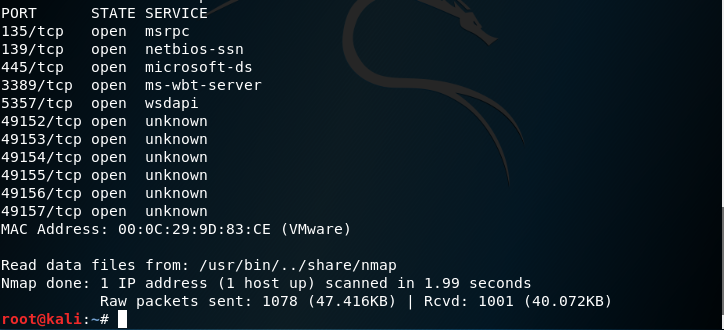
* Verificación de todas las conexiones de equipos con cualquier versión de escritorio remoto.



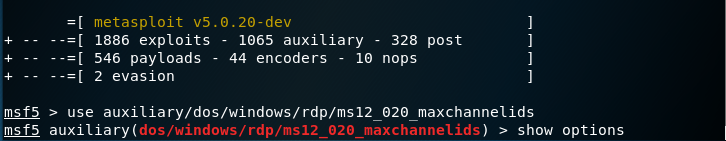
Una vez identificado la opción de permitir conexiones con ordenadores con escritorio remoto de cualquier versión se procede a realizar un escaneo de puertos, mediante el comando NMAP a la dirección IP de Windows 7.



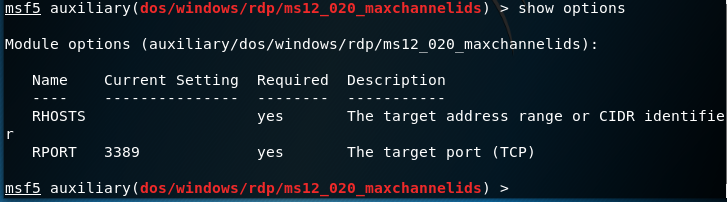
Por medio del escaneo de puertos a la dirección IP de Windows 7 se verifica que el puerto donde se ejecuta el servicio de escritorio remoto queda totalmente activo ya con esta vulnerabilidad se procede a realizar el ataque denegación de servicio.



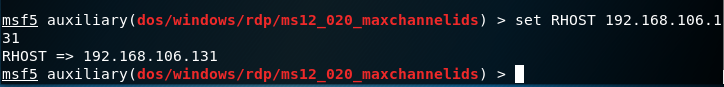
Una vez realizado el escaneo de puertos a la dirección IP del sistema operativo Windows 7 se procede a ejecutar el Metasploit mediante el comando msfconsole. Una vez activado este framework se digita el comando use auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids.



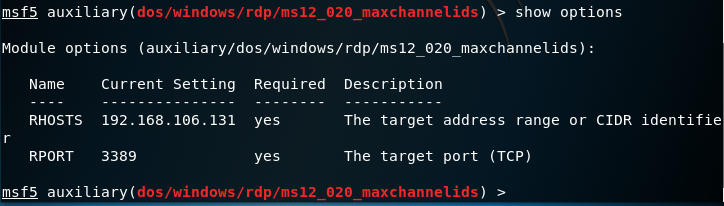
Una vez empleado el Exploit del servicio de escritorio remoto de Windows 7 se procede a verificar el puerto 3389 mediante el comando show options.



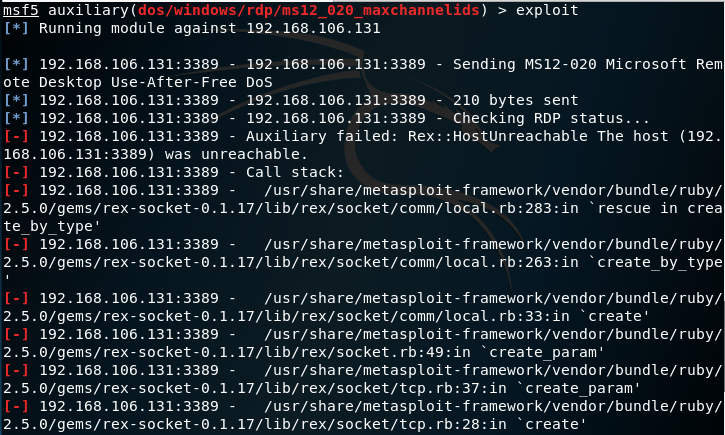
En este proceso se asigna la dirección IP del ordenador víctima de Windows 7 para que la máquina atacante establezca una conexión remota con el sistema cliente.

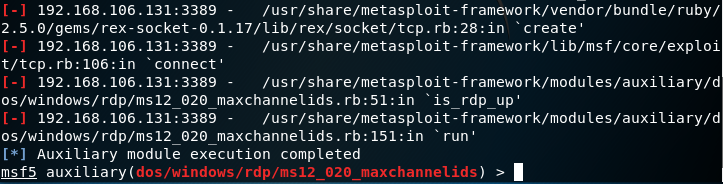


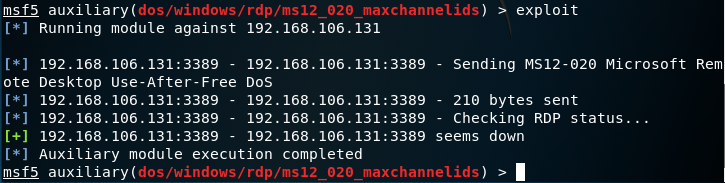
Una vez asignada la dirección IP de la víctima a la máquina atacante ya se puede realizar el ataque denegación de servicio al sistema operativo Windows 7 cliente a través del puerto 3389.

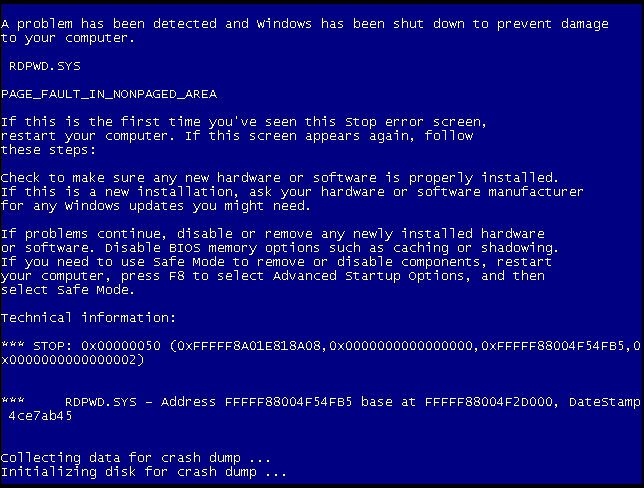


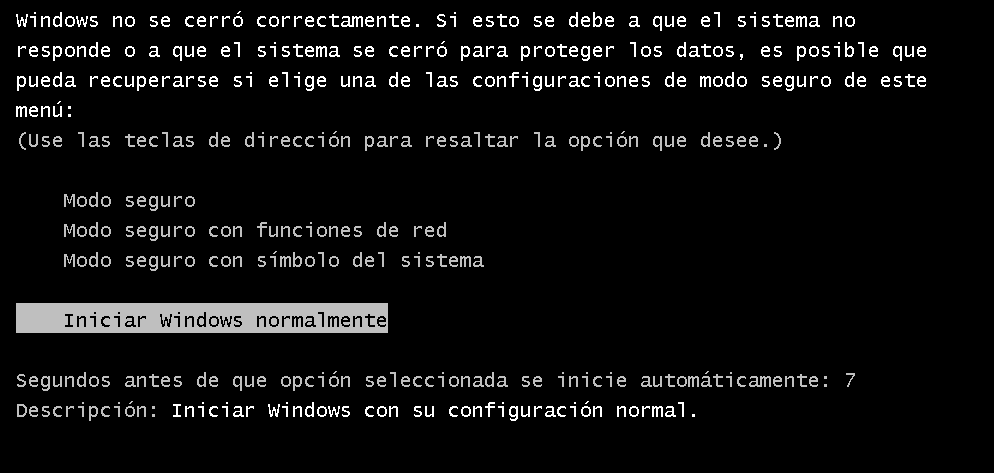
En este proceso se ejecuta el comando exploit y se verifica como en el sistema operativo Windows 7 aparece un pantallazo azul de forma inesperada y después el sistema da la opción de iniciar Windows normalmente.







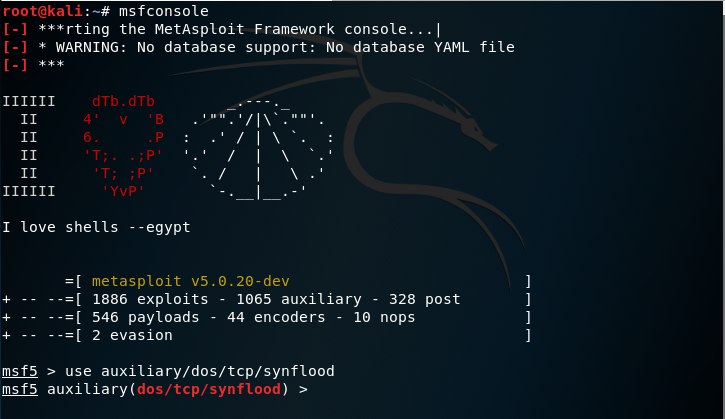




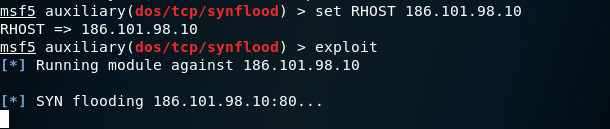
**DOS A SITIOS WEB MEDIANTE METASPLOIT**

* Escenario 2

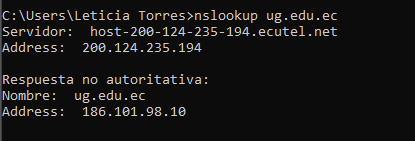
En este escenario se habilita nuevamente el Metasploit mediante el comando msfconsole donde se procese a utilizar el Exploit use auxiliary/dos/tcp/synflood



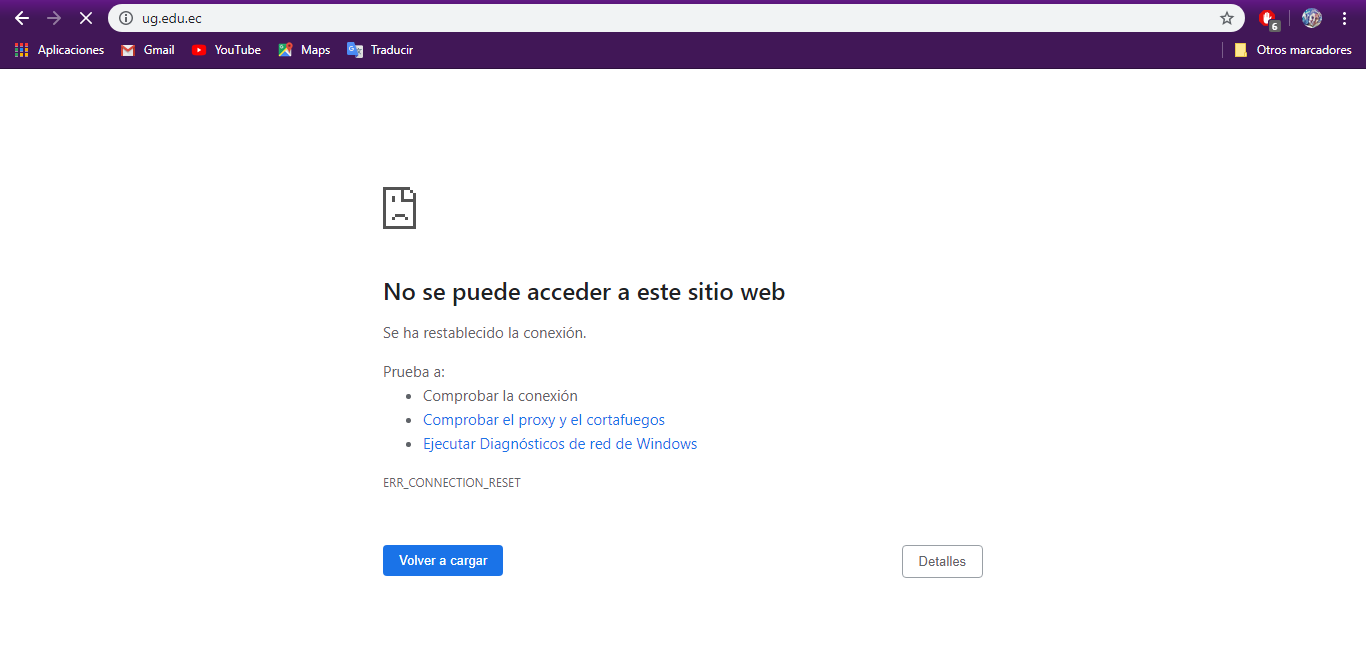
Una vez aplicado este Exploit se procede a asignar la dirección IP Pública del servidor web de una institución de educación superior y se ejecuta el comando exploit.



Antes de asignarle a dirección IP Pública del servidor web de la institución de educación superior se procede a verificar la misma IP mediante el comando nslookup a través de una consola de comandos de Windows 10.



Una vez ejecutado el ataque denegación de servicio mediante Metasploit se procede verificar si dicho ataque tuvo éxito digitando el dominio de la institución de educación superior en la barra de direcciones web del navegador de Google Chrone. Adicionalmente el mismo ataque se ejecuta para otro dominio de otra institución de educación superior, pero se verifica que tienen un nivel de seguridad óptimo para mitigar estos ataques DoS.



Una vez culminado con el ataque denegación de servicio el dominio de la institución superior vuelve a restablecerse por completo en la cual ya se puede verificar la página web.



