Fases de un Ataque Hacker

David Joel Mamani Quisbert
Universidad Mayor de San Andrés
Facultad de Ciencias Puras Naturales
Carrera de Informática
Análisis y Diseño de Información
joel92david@gmail.com

RESUMEN

Un ataque hacker se basa en cinco partes importantes, para poder llevado a cabo de manera exitosa.El hacker debe tomar en cuenta con suma importancia cada una de estas etapas ya que esto depende el éxito de su objetivo, ya que un ligero descuido podría provocar que el hacker sea llevado a prisión, pero viéndolo éticamente también es bueno tomar en cuenta que la víctima debe conocer la estrategia de ataque de un hacker para poder tomar medidas para poder descubrir al hacker.

Palabras Clave

Hacker, ataque, sniffers.

1. INTRODUCCION

Un ataque dentro de ethical hacking se lo hace de manera sana, es decir sin malicia sin la mentalidad destructiva, desde el enfoque ético se pueden hacer penetraciones a sistemas o redes para probar el conocimiento adquirido, es decir que un ataque exitoso para un hacker es una meta realizada. Así como es de vital importancia tomar en cuenta además de respetar estas fases para un hacker, también lo es para la víctima del ataque, ya que conociendo al menos como funciona la estrategia de un hacker podrá tomar sus medidas, como por ejemplo: si ha captado en su tráfico de red alguna dirección IP extraña, o de una dirección IP que haya falsificado su identidad, entonces si la victima observa que esto sucede a menudo debería preocuparse ya que el hacker se encontraría en la fase de mantener el acceso, en este caso bastaría capturar el tráfico de red para poder obtener mucha información del hacker que está realizando el ataque.

2. FASES DEL ATAQUE

2.1 Reconocimiento

Esta fase consiste en el estudio previo que hace un hacker hacia su víctima u objetivo, lo que se hace básicamente es extraer toda la información posible como ser: el sistema operativo que usa la víctima, las aplicaciones que usa, puertos que tiene habilitados, dirección IP de su máquina, y demás información que le servirá al hacker para posteriormente estudiar a esta víctima más a fondo y poder planear una estrategia de ataque.

2.2 Escaneo

Esta es la fase en la que el hacker organiza toda la información obtenida en la anterior fase, toma aquello que le pueda servir para hacer un análisis, luego identifica las características más importantes de toda la información y la estudia para hallar vulnerabilidades. El hacker deberá sobre todo enfocarse en los puertos ya que es una pieza clave para un ataque.

2.3 Ganar acceso

Esta es una de las fases para el hacker ya que es la fase en la que aplicara la estrategia planteada luego de que en la fase anterior haya encontrado las vulnerabilidades, para esto el hacker deberá hacer uso de todas sus habilidades mejor aún si usa herramientas que existen justamente para lo que desea realizar el hacer. El acceso puede ser localmente o de un medio externo, a través de secuestro de sesión (esto consiste en falsificar la identidad de un ordenador conocido para el ordenador de la víctima, y confundirla haciéndose pasar por esta), incluso tratando de descifrar la contraseña del ordenador de la víctima. Esta fase es decisiva ya que el hacker podrá ver el alcance de éxito que pueda tener su penetración.

2.4 Mantener el acceso

Esta fase consiste en mantener el acceso que gano en el sistema tratando de usar distintas herramientas como los sniffers que son usados para capturar el tráfico de red, este tráfico de red le servirá al hacker para poder obtener información sobre con que ordenadores interactúa su objetivo, lo que le servirá para poder hacer una falsificación de identidad haciéndose pasar por una de la direcciones conocidas y de confianza de sus objetivo, en esta fase debe iniciar sesiones telnet y FTP.

En esta fase es importante que el hacker permanezca como indetectable para el objetivo, para esto debe remover el rastro de evidencia que dejo su penetración y haciendo uso de Backdoor y Troyanos para de esta manera intentar conseguir acceso con altos niveles de privilegio es decir como un administrador, como también podrían usar caballos de Troya para transferir información como nombres de usuario, passwords y cuentas de banco que podrían estar almacenadas en el sistema del objetivo.

2.5 Cubrir las huellas

Esta es donde debe cubrir las huellas para poder terminar la obra perfecta, debe usar todas las herramientas posibles para evitar que los administradores puedan encontrar los registros de acceso de un usuario desconocido a través del análisis de tráfico que podrían hacer. Esta para mi es la fase más importante para un hacker ya que de esto depende que no encuentren evidencias, porque simplemente basta con encontrar un registro del acceso de un individuo extraño para que la víctima sospeche y si tiene un buen sistema de seguridad podrían detectarlo y así el hacker terminaría en la cárcel.

Figura 1. El ataque

En esta fase el hacker deberá tener mucho cuidado de no olvidar borrar las huellas que dejo con esto garantizar su integridad, como ya se dijo depende también mucho de la víctima, ya que la gran mayoría de los hackers llegan bien hasta esta fase pero luego son detectados y se acabó el juego para ellos.

3. CONCLUSIONES

Las etapas de un ataque son muy importantes para el hacker como también lo son para la victima que no conoce de la estrategia de ataque. La victima en caso de detectar trafico extraño deberá tratar de obtener información sobre el hacker para poder tomar represalias contra él, es decir dejar que acceda inclusive existen diferentes estrategias de respuesta que podría tener la víctima, como por ejemplo: darle información falsa, y hacerle saber que se está metiendo en un gran problema.

En síntesis el ataque hacker no siempre es malintencionado dentro del hackeo ético también se podrán hacer penetraciones a sistemas o a redes, pero no con la mala intención de usar la información extraída de manera perjudicial para el objetivo. Sin embrago también se deberá tomar en cuenta las recomendaciones mencionadas sobre todo en la etapa en la que el hacker deberá borrar todos los rastros dejados por su penetración de manera minuciosa.

4. REFERENCIAS

[31] Seguridad web, Disponible en:

jzseguridadweb.blogspot.com/p/fases-de-un-ataque-informatico.html

Ingreso: 12/06/13 22:22

[32] Ataque de un hacker, Disponible en:

http://foroicd.wordpress.com/2011/06/14/ataque-de-un-hacker/

Ingreso: 12/06/13 22:21