Uso de las técnicas del hacking ético para la reducción de amenazas de ciberseguridad

Autor: José M. González González
Mentor: Dr. Nelliud Torres Batista
Departamento de Ingeniería Eléctrica y de Computadoras y Ciencia de Computadoras

Resumen

A medida que las empresas tanto públicas como privadas comienzan a acomodar gran parte de sus capacidades de sistemas de información en la Internet, se hacen más propensas a que hackers de índole criminal puedan utilizar sus técnicas para acceder información sensitiva a través de una aplicación web. Ante la apremiante necesidad de asegurar los sistemas, surge la necesidad de que las empresas cuenten con hackers éticos para que estos se encarguen de identificar vulnerabilidades e implementar métricas correctivas para salvaguardar el activo más importante de una empresa, la información.

Introducción

En el presente trabajo, se pretende auscultar como las técnicas del hacking ético pueden servir de ayuda para reducir las amenazas de ciberseguridad en las empresas o cualquier tipo de organización. A través de la investigación realizada, se puede constatar que los hackers éticos deben aprender y dominar las mismas técnicas y herramientas que utilizan los hackers de sombrero negro. La diferencia estriba en el uso que estos le dan. Para efectos de este trabajo, se realizará un ejercicio práctico donde se pone a prueba una vulnerabilidad en el protocolo HTTP. Se utilizará la aplicación Wireshark para capturar el tráfico asociado al protocolo HTTP para de esta manera, observando el método POST, obtener las credenciales de acceso no cifradas de un usuario en particular.

Transfondo

El hacking ético es una rama del área de seguridad de sistemas de información. También es conocido como prueba de penetración o más bien, hacking de sombrero blanco. Es un tipo de hackeo realizado por una persona u empresa que tiene el firme propósito de identificar vulnerabilidades, huecos de seguridad y fallas en los sistemas de computadoras o la seguridad de red de la organización. Cabe mencionar que las técnicas o métodos utilizados en el hacking ético son bastante similares a las utilizadas en el hacking tradicional pero la diferencia estriba en que el primero es legal y se utiliza en una forma productiva. La información obtenida del hacking ético es utilizada para mantener la seguridad de los sistemas de información y mitigar los riesgos asociados a futuros ataques potenciales [1].

Problema

Utilizar protocolos como el HTTP puede implicar que datos sensitivos tales como correos electrónicos, contraseñas y direcciones no sean cifrados. Esto es una amenaza latente, ya que herramientas como Wireshark pueden capturar fácilmente estos datos. En síntesis, el utilizar HTTP para páginas donde se requiera ingresar información de índole confidencial es una vulnerabilidad.

Metodología

Típicamente, los hackers siguen una metodología que se divide en seis (6) pasos. Estos pasos tienen la finalidad de no tan solo lograr con éxito el ataque, si no más bien mantener el acceso y no dejar huella alguna [8]. En la Figura 1, se pueden apreciar los pasos que siguen los hackers para realizar sus ataques:

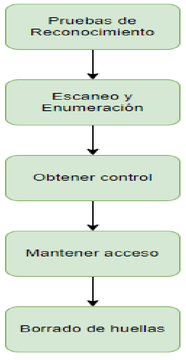


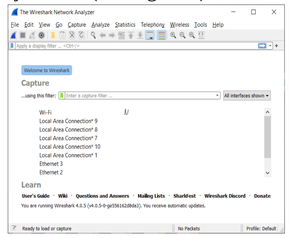
Figura 1
Metodología de los Hackers

A continuación, se describen más en detalle cada una de las fases:

- **Pruebas de reconocimiento:** Durante esta fase se trata de obtener la mayor cantidad de información del equipo o sistema que se desea atacar. Este proceso incluye identificar vulnerabilidades en el sistema [1].
- **Escaneo y enumeración**: Fase utilizada para que el hacker pueda determinar en efecto las características del sistema en términos de hardware y software.
- **Obtener acceso:** Es aquí donde realmente comienza la fase de ataque. Se utiliza la información obtenida de las dos fases anteriores con el fin de ingresar y tomar el control del sistema que se desea atacar a través de la red o de forma física. A esta fase se le conoce como "adueñarse del sistema" [1].
- **Escalación de privilegios:** Es aquí donde el hacker intenta obtener privilegios administrativos mediante la técnica de escalación de privilegios. Luego de que se logra la escalación de privilegios, el hacker podrá tener control completo del sistema e inclusive, de la red [8].
- **Mantener acceso:** Luego de ingresado al sistema en el paso anterior, el próximo paso consiste en lograr mantener acceso al sistema para que, en efecto, el hacker pueda volver a atacar el mismo.
- **Borrado de huellas**: Esta es la técnica donde el hacker intenta remover los archivos de registro u cualquier tipo de evidencia en el sistema atacado la cual pueda ser utilizada para identificarlo.

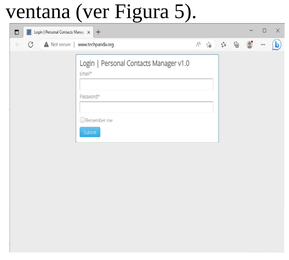
Resultados y Discusión

Para este ejercicio práctico, se hará un ataque el cual consiste en capturar el tráfico de red utilizando Wireshark para capturar los paquetes que se transmiten a través de un protocolo HTTP. Se utilizará una página web la cual pide unas credenciales de acceso para ingresar a una base de datos. Cabe mencionar que al utilizar un protocolo como lo es el HTTP, este no provee ningún mecanismo de seguridad para cifrar el nombre de usuario y la contraseña.
El primer paso consiste en ejecutar la aplicación de Wireshark en su computadora (ver Figura 2). Luego, verá la herramienta en ejecución (ver Figura 3).



Figuras 2 y 3
Aplicación de Wireshark

Se utilizará un portal de prueba que utiliza el protocolo HTTP. Este pide unas credenciales de acceso para ingresar a una base de datos (ver Figura 4). Una vez ingresado las credenciales, verá esta ventana (ver Figura 5).



Figuras 4 y 5
Captura de credenciales de acceso

Finalmente, se procedió a la captura de paquetes con Wireshark. Se aplicó el filtro HTTP para auscultar todo el tráfico que se llevó a cabo mientras se ingresó al portal y se colocaron las credenciales de acceso (ver Figura 6).

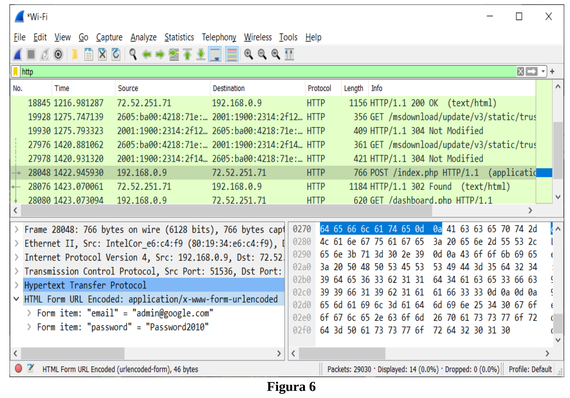


Figura 6
Captura de credenciales de acceso con Wireshark

Se recomienda implementar el protocolo HTTPS para evitar que las credenciales de acceso sean capturadas por Wireshark.

Conclusiones

Para poder proteger a una empresa de algún ataque provocado por un hacker, resulta imperativo que se contrate a un hacker ético, ya que este ciertamente tendrá todas las destrezas y habilidades necesarias para identificar las vulnerabilidades de la empresa e implementar métricas correctivas para disminuir o eliminar los riesgos asociados a ataques. A través de la investigación se pudo constatar que os hackers éticos deben tener las mismas destrezas y habilidades que un hacker de sombrero negro, con la diferencia principal que el primero utiliza sus conocimientos para el bien de la empresa. El hacking ético es un instrumento, que, si es utilizado legítimamente, puede demostrar ser efecto en el entendimiento de las vulnerabilidades de una red y como estas pueden ser explotadas y/o corregidas. Las empresas deben ver al hacker ético como un activo que busca salvaguardar su activo más importante, que es la información.

Trabajo Futuro

Como trabajo futuro, se espera realizar lo siguiente:

- Realizar este mismo experimento con el protocolo HTTPS
- El ejercicio práctico mencionado en esta presentación pertenece a la fase 2 de la metodología discutida, es decir, la fase de escaneo y enumeración. Como trabajo futuro, se espera llegar a la fase 3, es decir, lograr obtener el control de la base de datos. Esto se puede dar mediante la escalación de privilegios.
- Realizar otras pruebas de vulnerabilidad para identificar puertos abiertos utilizando NMAP para auscultar la posibilidad de contar con una puerta trasera (backdoor).
- Identificar y corregir vulnerabilidades asociadas a HTTP.

Reconocimientos

Ciertamente, reconozco a uno de mis grandes mentores y que gracias a el, he llegado hasta aquí, Dr. Nelliud Torres Batista. De igual forma, agradezco a cada uno de los profesores de la Escuela Graduada por el conocimiento y experiencia brindada durante el transcurso de los estudios graduados en la Universidad Politécnica de Puerto Rico, Recinto de San Juan.

Referencias

[1] A. Gupta and A. Anand, "Ethical hacking and hacking attacks," International Journal of Engineering and Computer Science, 2017. doi:10.18535/ijecs/v6i4.42
[2] S. Kumar and D. Agarwal, "Hacking Attacks, Methods, Techniques and Their Protection Measures," IJSART, vol. 4, no. 4, pp. 2253–2253, Apr. 2018.
[3] A. Ushmani, "Ethical Hacking," International Journal of Information Technology (IJIT), vol. 4, no. 6, pp. 1–4, 2018.
[4] L. Smith, M. M. Chowdhury, and S. Latif, "Ethical hacking: Skills to fight cybersecurity threats," EPiC Series in Computing, vol. 82, pp. 102–111, 2022.