Introducción a herramientas de explotación web

Geovanny Arguello Costta, ✉ gio666nb@gmail.com

Docente: Ing. David Galarza G. M.Sc (c)

Instituto Tecnológico Quito

Análisis de sistemas

Seguridad informática

Quito

05 de julio de 2019

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN

Debido a las vastas posibilidades que permite la comunicación en la web varias entidades de todo tipo han decidido entrar en este espacio, desde pequeñas empresas hasta corporaciones multinacionales y gubernamentales en todo el mundo, prestan o corren algún servicio dentro de la web, simultáneamente la ciberdelincuencia a estado creciendo y evolucionando de la misma manera, generando así el interés en dichas entidades por mantener su espacio en la web de la forma más segura posible.

Por esta razón, expertos hackers éticos se han dado paso con el desarrollo de herramientas que permiten evaluar procesos y escenarios vulnerables dentro de un sitio en la web con el fin de garantizar la estabilidad de la infraestructura y los datos del sitio seguros en entornos controlados.

En este documento se hablará acerca de BeEF, una herramienta que funciona en el marco del navegador web, marco considerado como la puerta abierta hacia cualquier servicio o sitio que utilice un navegador como cliente.

MARCO TEORICO

Herramientas de explotación web.

Las herramientas de explotación web son software que permite realizar escaneos, monitoreos y explotación a vulnerabilidades de un objetivo en la web de manera remota, para de esta manera permitir encontrar los posibles huecos o fallos de seguridad en el objetivo y posteriormente, poder solucionarlos y garantizar la seguridad.

Vulnerabilidades.

Según el INCIBE, "una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma". [1]

Ciberdelincuencia.

Es un termino que se refiere a delitos informáticos, ataques informáticos realizados a computadoras personales, servidores, sistemas de información o infraestructuras IT. [2]

Hacker ético.

Personas expertas en seguridad informática que se encarga de identificar vulnerabilidades en sistemas de información, analizar los riesgos que se puede correr al tener vulnerabilidades, y tomar acciones para mejorar la seguridad.

BeEF.

"Es una herramienta de prueba de penetración que se centra en el navegador web." [3]

Esta herramienta permite realizar pruebas de penetración con vectores de ataque de lado del cliente.

OBJETIVOS

A. Objetivo general

Comprender la situación actual en la que se encuentra el área de seguridad informática, específicamente en ambientes web, además de los posibles usos y beneficios de la herramienta BeEF, que esta pensada para entornos que involucren un navegador web.

B. Objetivos específicos

- Analizar la situación actual de la ciberseguridad en ambientes web.
- Analizar los posibles que brinda la herramienta BeEF.
- Analizar los ambientes en los que se puede ejecutar la herramienta BeEF.

DESARROLLO

Estado del arte con respecto a las vulnerabilidades web.

En [4] se hace un análisis acera de investigaciones relacionadas con la ciberseguridad para entender el estado del arte en vulnerabilidades web, en el cual se tocan temas como el estado del arte en los escáneres de vulnerabilidades de los cuales menciona que los mas abundantes y que más resaltan aun en la actualidad son ataques de inyección de SQL y XSS, además manifiesta un análisis en el que se considera de mucha importancia la comparación de distintos frameworks o herramientas para garantizar los análisis de caja blanca[1] y caja negra[2], en base al entorno donde se desenvuelven.

En [4] también se hace referencia a la importancia actual de las herramientas basadas en reportes de vulnerabilidades cuantitativos para brindar correctos diagnósticos y correcciones en base a dichos reportes, también se analiza los nuevos enfoques de explotación a partir de URLs de las aplicaciones web utilizando protocolo HTTP y lenguaje HTML.

Otro de los resultados que se analizan es el de las vulnerabilidades en base a los ataques de denegación de servicio y la importancia del cloud computing para la disponibilidad de los datos en un posible ataque de denegación, además de las posibles fugas de información que pueden causar este tipo de ataques.

Se muestra también un análisis a los ataques posibles a cookies para secuestrar sesiones o tokens de usuarios en el navegador y las posibilidades que tiene un ataque de esta magnitud en el lado del servidor.

Otro de los análisis interesantes es el de detectar vulnerabilidades en base al uso del dominio, la cual puede ser cuantitativa y generar más tiempo al atacante por identificar la puerta de acceso mas viable.

Herramienta BeEF.

“Es una herramienta de prueba de penetración que se centra en el navegador web.” [3]

BeEF se enfoca en los vectores de ataque del lado del cliente, centrándose así en el aprovechamiento de las vulnerabilidades del navegador, comprendiendo que cada política de seguridad puede ser distinta según el navegador.

---

[1] Análisis de caja blanca o White-box analisys, hace referencia al análisis realizado al código fuente de un aplicativo.

[2] Análisis de caja negra o black-box analisys, hace referencia al análisis realizado a un aplicativo sin conocer su código fuente, sino sus entradas y salidas.

Ambientes de aplicación de la herramienta.

BeEF es una herramienta pensada para la explotación de vulnerabilidades en navegadores o en el front de algún servicio, página o lo que sea que este alojado en la web, ganando acceso desde ahí, siendo capaz de analizar la red mapeando la LAN desde el navegador web llegando hasta ingeniería social para detectar posibles robos de identidad.

CONCLUSIONES

En cuanto al estado del arte, podemos concluir que mientras se siga avanzando en el desarrollo de tecnologías en la web se seguirá viendo el incremento de las posibilidades de vulnerar y así mismo las herramientas para poder solucionar dichos fallos, sin embargo, hay que destacar que parte de este estado de arte, es la persistencia de varios tipos de ataques que se mantienen vanguardistas.

En lo que a BeEF respecta, como herramienta para pruebas de penetración basada en los navegadores web, podemos aclarar el panorama que este abre, desde el uso de ingeniería social hasta el ingreso a los servidores por XSS incluso mapeo de redes LAN desde el navegador.

En cuanto al entorno para BeEF, se deja claro que es la web, el cual abre un gran abanico de opciones con tan solo el conocimiento de las vulnerabilidades posibles en el navegador o front del cliente.

Referencias

[1] INCIBE, «Sme Instituto Nacional de Ciberseguridad de España,» 20 03 2017. [En línea]. Available: https://tinyurl.com/y3m5m2pa.

[2] INTERPOL, «International Criminal Police Organization-INTERPOL [FR],» 2019. [En línea]. Available: https://tinyurl.com/y2svapeb.

[3] BeEF, «The Browser Exploitation Framework Project,» BeEF, [En línea]. Available: https://beefproject.com/.

[4] J. L. Perea y D. A. Franco, «Instituto Internacional de Informatica y Sistematica,» Universidad de Cartagena, [En línea]. Available: https://tinyurl.com/y64dpyqe.