Eduardo E. Palomar M.

El Hacking Ético

22 de octubre del 2020

Concepto

El hacking ético es una forma de referirse a una persona que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información. El hacking externo es cuando se realiza desde Internet sobre la infraestructura de red pública del cliente; es decir sobre aquellos equipos de la organización que están expuestos a Internet porque brindan un servicio público. Otra variante es el hacking interno, el cual se ejecuta en la red interna del cliente, desde el punto de vista de un empleado de la empresa, un consultor o un asociado de negocios que tiene acceso a la red corporativa.

Herramientas del hacking

Metasploit

Herramienta clásica de piratería para evaluar la vulnerabilidad de un sistema. Permite lanzar ataques usando comandos cortos y es muy utilizado.

Wireshark

Se trata de un analizador de protocolos de red multiplataforma. Permite recolectar datos de diferentes fuentes y conexiones. Está altamente demandada porque es muy eficaz al permitir todos los formatos de archivo de captura existentes en el mercado, a la vez que es compatible con gran parte de los sistemas operativos. Además, permite exportar todos los resultados a otros formatos.

Nmap

Pueden detectar sistemas operativos de huellas dactilares o identificar paquetes en bruto entre otras muchas utilidades, y destaca también por identificar tanto los sistemas que ejecutan como las aplicaciones de servidor.

OWASP Zed

Está especializada en detectar grietas en las aplicaciones web.

John The Ripper

Puedes descifrar tanto contraseñas sencillas y débiles como cifrados más complejos como los utilizados por los servidores de bases datos por ejemplo.

Kismet

Kismet detecta redes inalámbricas que tiene la gran ventaja de poder realizar el examen de forma pasiva, lo que permite detectar también redes ocultas o inutilizadas. La utilizan

mucho los hackers para hacer funciones de reconocimiento y consultar las redes disponibles en un lugar determinado.

Nikto

Es un potente servidor web que realiza pruebas en los equipos de destino. Puede incluso crear una auditoría de seguridad en los objetivos pretendidos por el lanzamiento de una serie de pruebas de evaluación. Básicamente está diseñado para encontrar debilidades y vulnerabilidades en los sistemas de destino y es muy sencillo de utilizar.

La suite Aircrack

Este conjunto de herramientas para hackear redes inalámbricas trabaja de manera conjunta y ordenada. Su uso es variable; pueden manipular flujos de datos, elaborar paquetes y analizar el tráfico de red capturado.

Cain and Abel

Se trata de una alternativa para descifrar contraseñas, especialmente en el caso de Windows. También puede ejercer funciones más complejas como la grabación de llamadas Vo-IP.

THC-Hydra

Se trata de un cracker de red optimizado. Es muy usada para cortar los dispositivos de red porque tiene muchas compatibilidades ya que trabaja con muchos protocolos diferentes, incluidos los más utilizados como HTTP o POP3, al igual que servicios y aplicaciones protegidas.

Social-Engineer

Su kit de herramientas es bastante popular al tratarse de un código abierto diseñado para lanzar exploits y ataques de ingeniería social. Sencillo de utilizar y personalizable a la hora de diseñar los ataques. Incluso permite crear códigos personalizados adaptados a las situaciones requeridas. Permite una gran variedad de ataques diferentes con muchas opciones de compatibilidad incluso con otras herramientas como Nmap.

Proyecto Tor

Es la red anónima internacional más utilizada por todos aquellos que desean navegar desde la privacidad. Tor traza una telaraña de seguridad muy potente a través de una serie de cruces que complican sobremanera el seguimiento por parte de los servicios de internet, administradores de sistema y propietarios de servicios.

Eduardo E. Palomar M.

El Hacking Ético

22 de octubre del 2020

Perfil de un hacer en la actualidad

Hay que tener en cuenta que como todo y sobre todo en esto, todo se va actualizando al igual que el perfil que se debe tener para ser hacker.

- Lo primero que se requiere son ganas de aprender, debido a los constantes cambios en las tecnologías que hacen que los Hackers requieran de un aprendizaje constante para mantenerse siempre actualizados.
- Conocimientos de idioma inglés.
- Conocer sobre sistemas operativos y sus usos, especialmente sobre Microsoft y Linux o Unix que son los más utilizados.

- Estar familiarizado con los requisitos de hardware necesarios para las tareas que se pretende llevar adelante.
- Manejar algunos lenguajes de programación, sin depender de un lenguaje específico.
- Entender las medidas de seguridad cibernética, como por ejemplo los firewalls.
- Conocimiento de las leyes de cada país y los límites que se pueden cruzar, así como también aquellos que implicarán una pena o castigo.
- Saber manejar los recursos de internet, logrando navegar en línea como un verdadero profesional.

Tipos de hacking

Dependiendo de la modalidad que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de las 3 modalidades: Black-box Hacking, Grey-box Hacking, White-box Hacking. la modalidad escogida afectará el costo y la duración de las pruebas de intrusión, puesto que a menor información recibida mayor será el tiempo invertido en investigar por parte del auditor.

Black Box Hacking

Esta modalidad se aplica a pruebas de intrusión externas. se llama de este modo, por que el cliente solamente le proporciona el nombre de la empresa a auditar al consultor, por lo que esta obra a ciegas, la infraestructura de la organización es una caja negra para él.

Grey Box Hacking

El cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como las direcciones IP y el Tipo/Función del equipo (Router, Firewall, Web-Server, etc.).

Eduardo E. Palomar M.

El Hacking Ético

22 de octubre del 2020

White Box Hacking

El Hacking de caja blanca, algunas veces denominado Hacking Transparente, aplica pruebas de intrusión solamente y se llama de esta forma por que la empresa cliente le da al auditor información completa de las redes y los sistemas a auditar. Este tipo de Hacking suele tomar menos tiempo para ejecutarse y por ende reduce costos también.