Hacking Ético

Transcribed on July 6, 2025 at 9:25 PM by Minutes AI

Speaker 1 (00:02)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a explicar el término ha Kinético 1, poco los pruebas que pueden realizar.

En los contenidos que vamos a ir viendo vamos a explicar lo primero que es el Hakinético.

Vamos a entenderlo como un gran proyecto, un conjunto de pruebas.

Iremos desglosando y luego iremos mostrando algún tipo de prueba que podemos encontrar en un Jainético a la hora de llevarlo a cabo.

El Jaquinético podemos definirlo como un conjunto de pruebas que permiten medir las protecciones de seguridad, es decir, las protecciones que tiene una empresa que quiere evaluar si esas protecciones son adecuadas, son eficientes y eficaces.

Si recordamos un poco cuando hablábamos del análisis y gestión del riesgo, podemos entender que el hacking ético fue una herramienta, valga el término, una herramienta que permite medir el estado de la eficacia y la eficiencia de los controles de las protecciones que tiene la organización defensa.

Este conjunto de pruebas lógicamente se realizan de forma ética, es decir, la empresa tiene que contratar a otra empresa o a otro autónomo para poder llevar a cabo esa acción.

Tiene que quedar todo encuadrado dentro de un avance, con unas condiciones y indicando en el contrato qué tipo de cosas se pueden qué tipo de cosas pueden dar.

Las pruebas deben ser completadas, es fundamental.

Las pruebas con pone un jarquinético permiten identificar mejoras y comprobar la eficacia y la eficiencia de las abuas.

Es un poco resumen que hacemos esto.

Entendemos el jarquinético como un gran proyecto donde podemos tener una, dos, tres, cuatro o n pruebas para validar las protecciones de normalización en diferentes áreas.

Bueno, podemos encontrar más información en este libro.

Y vamos a empezar ahora con las diferentes pruebas o tipos de pruebas que se pueden encontrar en un hacking ético.

Lógicamente podemos definir como cualquier tipo de prueba que sea solicitada por una organización y que pretenda medir la eficacia de las protecciones.

Puede entrar en tu moja kinético, pero las más comunes vamos a enumerarlas a continuación.

Vamos a empezar hablando de lo que es la auditoría interna, entendiendo auditoría como la identificación de todas las potenciales vulnerabilidades o posibles vulnerabilidades.

La auditoría interna al final es el proceso en el cual se va a evaluar elementos de una red interna, de una organización.

Lógicamente existen diferentes tipos de auditoría.

Hay auditoría interna orientada a la evaluación de sistemas e identificación de vulnerabilidades.

Como digo siempre es importante entender que el concepto de auditoría va ligado a intentar identificar el máximo posible de vulnerabilidades.

En otros casos la auditoría interna puede estar enfocada a la evaluación de seguridad de la red, otro tipo de sistemas o servicios.

Si nos paramos a enumerar características clave de la auditoría interna podemos encontrar el análisis de seguridad de las VLAN, por ejemplo, si tenemos una red ya sea segmentada o ya sea configurada a través de VLAN, de redes locales virtuales, llevar a cabo un análisis de ese tipo de elementos, evaluar la seguridad de los puntos de acceso a la red.

Otro tipo de características que se va a evaluar en las auditorías de red el análisis del tráfico de red, hacer un sniffing de ese tráfico de red.

Luego evaluar el cifrado de las comunicaciones a la hora de evaluar la calidad de las comunicaciones, llevar a cabo escaladas de privilegio en la red.

Estudia no solamente ligado a la red, sino también a los sistemas.

Aquí no expongo temas de características clave en sistemas, pero hacemos una mención a la auditoría interna de redes, pero en sistemas sería igual, al final es identificar servicios que se encuentran en los sistemas, identificar sistemas nativos, identificar aplicaciones, versiones de aplicaciones, identificar posibles vectores o ataque por vulnerabilidades en esas aplicaciones o en esos servicios.

Entonces tenemos que diferenciar entre la batería interna evaluando redes y evaluando sistemas.

A veces se hace en forma conjunta también.

El siguiente concepto es la auditoría externa.

En este proceso lo que se evalúa es la seguridad de los elementos externos de una organización.

Cualquier servicio externo podría ser auditado en ese mismo de trabajo.

Por poner algún ejemplo, pues tenemos una VPN, tenemos Qfywall, tenemos servidores externos como el de correo electrónico, servidor DNS, servidores web que tenga.

La auditoría externa puede estar ligada a todo este tipo de servicios.

Lógicamente dentro del concepto de auditoría externa Vamos a encontrarnos con un tipo de auditoría muy solicitado que es la auditoría web.

Como digo, es una de las pruebas más recurridas por las empresas porque todas las organizaciones tienen una, dos, tres sitios web.

Ese tipo de teoría permite identificar vulnerabilidades en los activos web de la organización.

Entonces vamos a exponer a continuación unas características clave dentro de la web que nos va a permitir entender qué tipo de situaciones, qué tipo de cosas se va a realizar en tenemos identificación de servicios, tenemos obtención de información mediante crawling spidering, es decir, reconocer el sitio web, entender todos los archivos, todos los enlaces, hacer un mapa de información de esa web.

Descubrimiento de rutas no indexadas a través de trayectorios, por ejemplo, con herramientas como Dirbuster, Dirbe o Buster.

Hay una gran cantidad de herramientas que permiten detectar ya sean directorios, archivos que están no indexados a través del servidor web o a través de la aplicación que está ejecutando en el servidor.

Detección de malas configuraciones, exposiciones excesivas, detección de vulnerabilidades y explotación de vulnerabilidades.

Análisis de esas vulnerabilidades, análisis del propio código fuente, caso de código JavaScript, o código HTML, et.

Son diferentes tipos de pruebas o diferentes tipos de elementos que se van a tratar en una batería web.

Todo esto os permite entender también todo lo que vais a vivir viendo en la formación, vais a ver un conjunto de cosas que van englobadas a ir dando soluciones de forma práctica a todo esto.

Otro tipo de otro tipo de prueba que se trabaja en un kinético pues es el pentesting.

El pentesting está asociado a diferentes áreas realmente podemos encontrar pentesting web, pentesting de sistemas, pentesting de sistemas y redes.

Ahí como veis hay diferentes tipos de test de intrusión.

Aquí el test intrusión podemos definirlo como una prueba que permite demostrar que existen formas de llegar a los objetivos marcados por la es decir, una prueba que verifica que los controles de seguridad o las protecciones no son suficientes.

Entonces se marca una serie de objetivos, por ejemplo, hay que lograr tener el controlador de dominio, hay que lograr tener el administrador de dominio, hay que lograr acceder a unas bases de datos que tiene la organización que son críticos para ellos, hay que conseguir nos marcan una serie de objetivos y lo que se pretende es demostrar que se puede llegar a esos objetivos y que hay un camino que permite lograr esto.

Entonces se demuestra que los controles de seguridad o que las protecciones no están funcionando correctamente y que se puede mejorar.

Es una forma de verificar que algo se puede mejorar.

Así que en resumen sería fijar una serie de objetivos y el pentester deberá lograrlos.

Los pentests o los test de intrusión pueden ser internos, pueden ser externos, pueden ser mixtos, híbridos y también hoy en día pues también como las empresas trabajan tanto en la nube, este tipo de pruebas tanto retorcidas como fuentes, pues se pueden realizar también sobre activos que están en cloud, que pertenezcan a la organización.

Bien, otro tipo de prueba que podemos encontrar en un hoja genético, como veis son muchas y realmente valdría cualquier tipo de prueba que pretende medir algo de la podría pedir este tipo de prueba, pero esta prueba es la prueba de rendimiento que está enfocada a verificar o validar si nuestras inversiones en seguridad, controles o en protecciones anti DDOs principalmente, son las adecuadas o tengo que mejorar.

Porque uno de los mayores miedos que puede tener una organización es quedarse fuera de Internet, no tener la actividad de negocio que de fuera, no estar disponible, tener recursos disponibles, no tener sistemas de ponibles, no tener disponibilidad, afectar gravemente la disponibilidad de la información o no tener directamente presencia en Internet porque es atacado a través de una servicio distribuida.

Este tipo de prueba lo que pretende emular es esto precisamente, la empresa puede aguantar un ataque de servicio distribuida o de servicio con pruebas de rendimiento.

Lógicamente la empresa lo que hace es solicitar este servicio a otra empresa y esta empresa lo que hace es utilizar ventanas de tiempo pequeñas, cuestión de 1 h, 2 h, normalmente en horarios nocturnos para llevar a cabo la prueba, siempre cuando la empresa que contrata indique cuándo debe realizarse.

La empresa que contrata lógicamente va a buscar un espacio horario donde el impacto sea el menor posible dentro de su actividad de negocio.

Por eso digo que es una ser ventanas de tiempo cercanas a horas de madrugada principalmente porque las empresas suelen estar bastante paradas en ese espacio de tiempo.

Pero bueno, depende un poco de la naturaleza de cada empresa.

Aquí podemos encontrar algunas características clave.

Por ejemplo, os hablamos del estudio de la infraestructura y el descubrimiento de elementos y por donde orientar estrategia de ataque.

En este tipo de pruebas hay que realizar un estudio de por dónde se va a llevar a cabo la prueba y qué tipo de técnica se va a utilizar.

Es algo importante.

Hay que hacer una preparación de entornos distribuidos.

Lógicamente la empresa que va a llevar a cabo la prueba debe disponer de los entornos adecuados.

Hoy en día con el cloud seguramente es más sencillo que antiguamente, pero hay que dedicar un tiempo para preparar, ver qué tipo de pruebas se van a realizar, porque dentro de la prueba de rendimiento puede ser las llamadas sin flu, tipo de inundación de conexiones, puede ser por temas de amplificación, puede ser por diferentes tipos de pruebas de entendimiento.

El objetivo al final es verificar que la empresa no cae o que los sistemas de la empresa no caen.

Vamos a la siguiente.

Bueno, esta es la prueba de empleados, hemos llamado la prueba de concienciación de empleados y realmente el objetivo es verificar, la empresa quiere verificar si sus empleados están concienciados, están formados y no caen ante ataques básicos como puede ser una campaña de phishing, diferentes formas.

O que en caso de haber una campaña contra la organización, los empleados tienen un procedimiento que van a cumplir.

En el momento que alguien detecte la situación debería cumplir con el procedimiento interno para que la empresa pueda tomar decisiones y solventar el problema.

Entonces este tipo de prueba lo que busca es simular ya sea una campaña de phishing o cualquier cosa similar o una campaña donde se le envía un documento automático a una serie de personas y ver un poco qué interacción tiene esa persona con esos elementos que les llegan, ya sea correo electrónico o sea altaforma.

Al final hay una serie de hitos que se pueden marcar.

Si la persona confía en el correo que le llega ya es un primer hito, si la persona clica en el enlace es 1 s hito, si la persona entrega credenciales o entrega información es un tercer hito.

Depende en lo que esté cayendo, pues es un poco la gravedad del asunto.

Esa persona, lógicamente, que cae en este tipo de pruebas, ese empleado, debe pasar por una formación, debe pasar por unas charlas de competenciación para que aprenda un poco los riesgos y lo que ha sucedido al final.

Esto es una manera también que tiene la empresa a través del hakin ético, de poder crear esa cultura de seguridad y poder evaluar si esa cultura de seguridad está calando dentro de la organización, está sentando sus bases para poder evitar este tipo de situaciones.

También es una forma de entrenar, de tener entrenado a la gente dentro de la empresa para que esté alerta y que intente cumplir el procedimiento interno.

Es decir, debíamos tener un procedimiento interno en el cual si alguien de la empresa recibe un correo, que es un prisi, en algún tipo de situación maliciosa, debería alertarlo, no debería callarse y no hacer nada, sino debería alertarlo y notificar al equipo IT, tomar el procedimiento interno que haya e intentar que todo el mundo se entere de la amenaza que llega sobre la empresa.

Porque si alguien detecta la amenaza pero no informa o no tiene un procedimiento para informar y que esa amenaza se haga pública dentro de la empresa, pues el problema es que tú no caes, pero igual la persona al lado sí cae tiempo después porque tú no has notificado esto.

Así que, bueno, esas son cosas que tenemos que tener en cuenta aquí.

También deciros que en este tipo de pruebas, en algunas ocasiones se hacen estudios de la gente que forma parte de la muestra.

Hay veces que la empresa proporciona ya las personas que van a ser, hay veces que la empresa lo hace con directivos, entonces lo que buscan es un 2,3 directivos, contratan el servicio y se hacen pruebas.

Suelen ser pruebas un poco más complejas.

Otras veces se cogen un conjunto de muestras de 20, 30,40 personas dentro de la empresa con diferentes perfiles, es decir, perfiles de contabilidad, perfiles de marketing, perfiles de IT, y se busca un poco ver si en ese conjunto de muestras las personas caen.

Se crean entornos ficticios cercanos al mundo real.

Lo más común es la típica campaña de phishing, buscando algún tipo de gancho en toda la organización, algún tipo de detalle que haga que sea más difícil de detectar, pero que siempre haya elementos que cuestionen o que permitan cuestionar que está en la velocidad del mensaje.

También nos pone aquí herramientas de control remoto y exploits.

Bueno, esto está más orientado a que en algunos tipos de pruebas y que pueden solicitar, oye, hay que intentar hacer que este usuario o estos usuarios ejecuten este tipo de archivo para una macro o en un documento informático o algo similar.

Bueno, pues también podemos encontrarlo.

Bien, pues llegamos al final de la vamos a acabar con las conclusiones.

Hemos definido lo que es el hacking ético.

Por resumirlo brevemente, es un proyecto que se engloba diferentes tipos de pruebas hacking.

Una empresa contrata a otra, esa empresa puede solicitar una prueba, dos, tres, x pruebas que le interesen para validar la eficiencia y eficacia de los controles, las protecciones que tiene.

Si lo ligamos un poco con el mundo de la necesidad de riesgos, entendemos que análisis de riesgos, la gestión del riesgo puede apoyarse en el jardín para precisamente tener indicadores de cómo esos controles están siendo suficientes o necesitan mejorar.

Y bueno, también se ha explicado, bueno, se comenta diferentes tipos, se han detallado diferentes tipos de pruebas que se pueden llevar a cabo en un hand genético, diferentes tipos de auditoría, diferentes tipos de intrusión, diferentes tipos de pruebas que se pueden llevar.

Pero quedaos también con la parte de la diferencia entre auditoría y test de intrusión.

La auditoría permite identificar el mayor número de uniones posibles, eso es lo que busca.

Y el test de intrusión no busca identificar el mayor número de vulnerabilidades posible, sino lo que busca es lograr sus objetivos, objetivos que le han marcado en el alcance.

Esa prueba es lo que intentará encontrar el Pentester, es decir, si tiene que encontrar tres vulnerabilidades y explotarlas para conseguir el objetivo que le han marcado, lo hará.

Sin embargo, en una prueba de auditoría lo que se va a intentar es identificar el mayor número de vulnerabilidades posibles.

Bien, pues con esto ahora sí finalizamos la sesión y nada, nos vemos en la próxima sesión.