

TigerWeb: Una herramienta de análisis de la seguridad perimetral en redes IP

TigerWeb es una herramienta de análisis de seguridad perimetral en redes IP. Mediante una extensa serie de pruebas sobre máquinas que disponen de una dirección IP externa, busca potenciales vulnerabilidades que puedan ser utilizadas por usuarios malintencionados para acceder, corromper, destruir o impedir el acceso a dichos sistemas.

Como resultado del análisis genera un informe en castellano del estado de la seguridad de los sistemas analizados.

Introducción

Hoy en día están conectados a Internet la gran mayoría de las empresas, organizaciones y gran cantidad de usuarios a nivel particular. En general, independientemente de la naturaleza de la organización de que se trate, todos tienen un conjunto de máquinas internas, habitualmente conectadas en red, y un conjunto de máquinas directamente accesibles desde Internet.

Para todas las redes IP, la seguridad de sus máquinas internas depende en gran medida de la seguridad de las del perímetro, por ser estas las únicas inicialmente visibles desde el exterior de la red. Un intruso¹, para acceder a las máquinas de cualquier red IP, lo que primero encontrará será justamente las máquinas del perímetro, que por estar directamente conectadas a la red, disponen de una dirección IP externa.

Si un intruso consigue acceder a las máquinas visibles de la red, puede que averigüe contraseñas del sistema o que se aproveche de defectos de ciertas aplicaciones para obtener cuentas no legítimas, para detener los sistemas, para corromper los datos, para acceder a información sensible de la empresa, o incluso puede que utilice estas máquinas como plataforma para realizar ataques a otros sistemas, provocando con ello severos problemas de seguridad. Por tanto, la seguridad del perímetro es crucial para disponer de seguridad en toda la red IP.

Las máquinas del perímetro suelen ser costosas de instalar y configurar y en muchos casos complejas de mantener, lo que provoca que habitualmente encontremos redes completas muy inseguras, por falta de un nivel adecuado de seguridad en el perímetro.

TigerWeb es una herramienta que ayuda a los administradores de redes IP a mantenerse informados y actualizados sobre las potenciales vulnerabilidades que pueden ser encontradas en sus sistemas, permitiendo mayores niveles de seguridad.

Objetivos de TigerWeb

Con frecuencia los sistemas presentan vulnerabilidades importantes en lo referente a la seguridad, dependiendo del sistema

operativo y de las aplicaciones que están instaladas. Continuamente van apareciendo nuevas vulnerabilidades, lo que provoca que los administradores de las redes se vean poco a poco desbordados por la multitud de comprobaciones que deben realizar.

Diferentes estudios y análisis muestran una tendencia creciente en cuanto a incidentes de seguridad. Por ejemplo, el Centro de Coordinación del CERT dio a conocer un incremento significativo en el número de incidentes de seguridad que le fueron reportados desde el año 2000, hasta el segundo trimestre del 2003 (Figura 1)

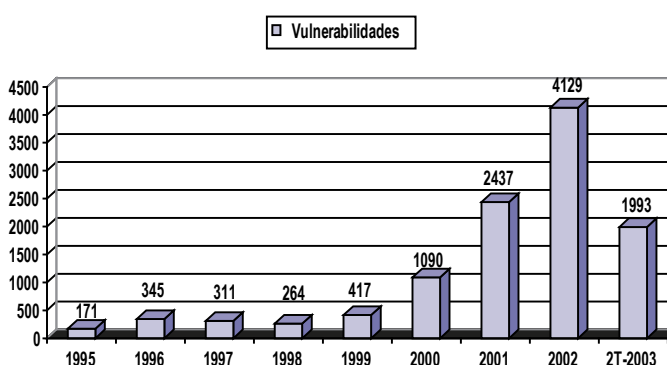


Figura 1: Evolución de las vulnerabilidades detectadas por el CERT/CC (fuente www.cert.org).

Estos defectos pueden corromper los requerimientos básicos de seguridad, alterando la integridad, confidencialidad y disponibilidad de la información de estos sistemas. Para garantizar estos principios y poder subsanar las potenciales vulnerabilidades, es necesario el uso de herramientas encargadas de auditar la seguridad de las redes.

La existencia de herramientas que de una manera automatizada analizan todos los "puntos de acceso" a los sistemas se revela de un valor muy significativo. Las primeras herramientas de auditoría automatizadas que surgieron — podemos destacar como precursoras *Cops* y *Tigre* — están destinadas a la realización de auditorías locales en sistemas Unix, pero únicamente comprueban las vulnerabilidades de la máquina, sin indicar posibles soluciones.

Posteriormente aparecieron las herramientas de análisis remoto de redes como *Saint*, sucesora de *Satan*. Estas herramientas permiten analizar remotamente subredes completas. Sin embargo, al tener que ser configuradas para efectuar los análisis, pueden ser difíciles de entender por personas no expertas en seguridad. Además hay que

¹ Utilizamos el término intruso para referirnos de forma genérica a cualquier persona que intente acceder sin autorización a las redes de cierta organización, desde el exterior de la propia red.

mantenerlas continuamente actualizadas para que puedan detectar las últimas vulnerabilidades aparecidas en los sistemas.

TigerWeb es una herramienta web que proporciona de forma remota auditorías de seguridad para redes IP, identifica, analiza e informa acerca de amenazas de seguridad, observando las redes desde la perspectiva de un intruso externo.

El objetivo de TigerWeb es detectar las vulnerabilidades que presentan las máquinas y los servicios de red, debilidades que podrán ser utilizadas por usuarios malintencionados para acceder, corromper, destruir datos de una manera ilegítima o impedir el acceso a dichos sistemas por parte de usuarios autorizados.

Para ello la herramienta realiza una extensa serie de pruebas sobre nodos IP de forma remota. Una vez efectuado dicho proceso de análisis, genera un informe, en castellano, con las vulnerabilidades detectadas y sus posibles soluciones.

Con esta herramienta cualquier usuario podrá efectuar análisis en el momento que crea más conveniente, para saber qué puede ver y hacer una persona desde el exterior sin conocer previamente ningún aspecto organizativo de la empresa, así como tampoco de sus sistemas. Y de esta manera, tomar las acciones correctoras oportunas para prevenir posibles ataques externos.

Estructura de TigerWeb

TigerWeb está compuesta de diferentes módulos, los cuales proporcionan un servicio de análisis e información actualizada de vulnerabilidades de los sistemas, efectuando una auditoría completa de seguridad.



Figura 2: Interfaz web.

Interfaz Web

La herramienta será accesible desde una interfaz Web (Figura 2), desde la que un usuario podrá solicitar que se realice un análisis de seguridad al perímetro de su red.

Desde la interfaz los usuarios introducen las direcciones IP de los ordenadores de su perímetro y ordenan el comienzo del análisis. Además también pueden realizar un seguimiento histórico de los

análisis previos que hayan realizado, así como acceder a información puntual sobre las vulnerabilidades que más puedan afectar a los sistemas analizados.

Motor de Análisis

Durante el análisis se simula a un atacante externo con intenciones maliciosas. Para ello el motor realiza una serie de pruebas sobre las direcciones seleccionadas con el fin de comprobar el nivel de seguridad de los sistemas. Actualmente el motor dispone de más de 1700 pruebas que tratan de buscar vulnerabilidades conocidas.

De los tipos de pruebas que se realizan podemos destacar:

- Escaneo de puertos, con la detección de puertos abiertos, cerrados, bloqueados y servicios en ejecución.
- Detección de sistema operativo y análisis de vulnerabilidades asociadas, así como en fallos de configuración.
- Análisis de vulnerabilidades en componentes de red como enrutadores, cortafuegos, impresoras, etc.
- Explotación de vulnerabilidades encontradas.
- Ataques de fuerza bruta a servicios conocidos como FTP, NETBIOS, POP3, HTTP, IMAP, TELNET y SNMP.
- Otros.

Para llevar a cabo el proceso, el motor combina varias herramientas entre las que destacan nmap, la cual permite un gran número de técnicas para el escaneo de puertos, así como la detección remota del sistema operativo, y nessus, una herramienta de análisis remoto de vulnerabilidades de última generación. Se trata de herramientas de amplia difusión, muy probadas y con altos niveles de calidad. Además de estas dos herramientas, TigerWeb está diseñado para incorporar cualquier otra herramienta orientada a la detección de vulnerabilidades, de forma que el administrador del servicio, pueda en cada momento, seleccionar aquellas más flexibles y potentes disponibles en el mercado o incluso elaborar alguna propia de propósito específico.

Base de Datos

Para llevar a cabo los servicios ofrecidos por la aplicación un usuario necesita almacenar datos, tanto de carácter identificativo como relativos a sus sistemas a analizar. Además, para poder realizar un seguimiento exhaustivo de los sistemas, se gestionan todos los datos históricos de vulnerabilidades encontradas en análisis que se han efectuado con anterioridad.

Puesto que el principal objetivo de esta herramienta es informar al usuario de los fallos encontrados en los análisis efectuados, TigerWeb cuenta con una base de datos documental de vulnerabilidades conocidas y de utilidades para verificar si las vulnerabilidades están presentes o no en un sistema determinado.

La base de datos está permanentemente actualizada con la información de vulnerabilidades que publican determinados organismos internacionales, entre los que destacamos *Bugtraq*, una lista de nuevas vulnerabilidades publicada y actualizada por *Security Focus, Inc.*, la lista de vulnerabilidades comunes *CVE* de la organización *MITRE*, recomendaciones del Centro de Coordinación

del CERT (*Computer Emergency Response Team*) y diversos sitios web dedicados a seguridad.

La base de datos está generada en castellano y adaptada al estándar de nomenclatura *CVE (Common Vulnerabilities and Exposures)*, una iniciativa mundial para estandarizar el código de todas las vulnerabilidades que son públicamente conocidas. Utilizando estos nombres comunes se crea mayor facilidad para compartir información entre herramientas de diversos fabricantes y distintas bases de datos.

Generador de Informes

De los datos resultantes del análisis y de la base de datos de vulnerabilidades, se genera un informe del estado de la seguridad de los sistemas frente ataques externos (Figura 3). En el informe se describen las pruebas de seguridad realizadas, y el resultado obtenido de ellas, detallando tanto las vulnerabilidades encontradas, como soluciones y recomendaciones para subsanar las deficiencias, referencias técnicas a las vulnerabilidades, así como sitios web con información adicional, descargas para actualizaciones, etc. Además de estas informaciones, se proporciona el código *CVE* y/o *Bugtraq* asignado a la vulnerabilidad.

Protocolo: FTP	Servicio: Administración de usuarios
Nombre:	Lista de los usuarios locales que nunca han cambiado su contraseña.
Descripción:	Esta prueba lista los nombres de los usuarios locales que nunca han cambiado su contraseña.
Resultados:	Las siguientes cuentas de usuario nunca han cambiado su contraseña: Alvaro Para mitigar el riesgo de esto, los usuarios deberían cambiar regularmente su contraseña.
Criticidad:	Baja
Nombre:	Lista de cuentas locales que tienen privilegios elevados.
Descripción:	Esta prueba verifica los nombres de las cuentas locales de privilegios.
Resultados:	Las cuentas locales con privilegios elevados deberían estar suspendidas. root Para mitigar el riesgo de esto, las cuentas de privilegios permanentemente deberían inhabilitarse.
Criticidad:	Baja

Figura 3: Ejemplo de informe de vulnerabilidades.

De las vulnerabilidades se especifica el nivel de criticidad asociado, es decir, una estimación del impacto que pueden tener en el sistema analizado. De cualquier forma, cada usuario debe hacer su propia valoración final, dado que depende tanto de la situación concreta en que se dé la vulnerabilidad como de la organización.

Los niveles de criticidad TigerWeb pueden tomar los siguientes valores:

1. Ninguna:

- No conlleva ningún riesgo, obteniendo únicamente información general como podría ser el sistema operativo detectado.

2. Baja:

- La información obtenida resulta de utilidad para el atacante, aunque no se considera una amenaza, puede ayudarle a encontrar otras vulnerabilidades en el sistema. Por ejemplo, información sobre tipo de servidor y número de versión, etc.

3. Media:

- Permite a un atacante acceder a datos que son contrarios a las especificaciones de derechos asignados en esos datos. Por ejemplo, obtener información específica sobre cuentas del sistema, como listado de usuarios que nunca han entrado en el sistema o cuyas contraseñas nunca han sido cambiadas, etc.

4. Alta:

- La vulnerabilidad permite a un atacante violar la protección de seguridad y ganar el control completo del sistema. Por ejemplo, conseguir acceder al sistema como un usuario con privilegios de administrador.

5. Grave:

- A causa de la vulnerabilidad se obtiene información extremadamente útil para el atacante. Por ejemplo, poder leer ficheros con información sensible en la máquina remota.

6. Muy grave:

- La máquina remota ya ha sido comprometida, como la existencia de un caballo de troya en el sistema.

A partir de los resultados del informe final de seguridad, el usuario puede eliminar o reducir las vulnerabilidades encontradas en el análisis, aumentando de este modo el grado de seguridad de sus sistemas.

Administración del Servicio

TigerWeb incluye un módulo web de administración del servicio, de gran utilidad para el equipo técnico encargado del seguimiento y control de las auditorías solicitadas por los usuarios.

A través de este módulo se gestionan las nuevas direcciones IP que introducen los usuarios, realizando la previa verificación y validación por parte del equipo técnico, así como el control de los servicios solicitados o en ejecución y la administración de informes finales resultantes de las auditorías realizadas.

Descripción del Servicio

Al servicio TigerWeb se accede mediante la interfaz web, el usuario configura las direcciones IP objeto de las pruebas, y solicita el servicio de análisis. Una vez iniciado el proceso, se pone en marcha el motor de análisis y se obtiene el informe de vulnerabilidades encontradas (Figura 4).

La aplicación utiliza constantemente el correo electrónico para la interacción con el usuario mediante mensajes firmados digitalmente. La mayoría de acciones importantes se realizan por correo electrónico, donde el usuario debe pinchar en cierto enlace web, que contiene una cadena única, para accionar la orden solicitada, como es el inicio de un análisis. Estas acciones, junto a los mensajes firmados digitalmente, son registrados en el servicio como prueba de la actividad solicitada por el usuario.

Por otra parte, los mensajes enviados al usuario, le permiten guardar un registro documental de los servicios proporcionados y de cada una de las tareas realizadas por TigerWeb.

Dado el tipo de análisis a efectuar, es necesario que el usuario esté registrado y haya dado conformidad a las condiciones del servicio mediante un contrato legal antes de poder utilizarlo. Así, una vez registrado un usuario el sistema permite dar de alta las direcciones IP que quiere analizar. Únicamente se pueden registrar direcciones IP públicas y fijas de la organización. No permite por tanto registrar ninguna dirección perteneciente a subredes privadas.

Estas direcciones IP registradas, permanecen en estado “no validadas” hasta que los responsables del servicio TigerWeb comprueban la autenticidad de las direcciones, quedando el proceso

en todo momento esta informado de los pasos del análisis, recibiendo correos electrónicos indicando tanto que el proceso ha sido iniciado como finalizado.

Como resultado del análisis recibe un informe final con las vulnerabilidades detectadas en sus sistemas. Asimismo, el usuario puede realizar un control de seguridad continuo, consultando el resultado de los análisis efectuados con anterioridad y documentándose sobre las vulnerabilidades encontradas.

Evaluación de la Herramienta

TigerWeb se utiliza como herramienta de auditoría informática. En el marco de una auditoría extensa, que involucra tanto la verificación del perímetro, como el análisis de las redes internas, los servicios y el flujo de la información, TigerWeb viene demostrando una gran utilidad y buena aceptación por parte de las empresas auditadas.

Hasta la fecha, venimos observando que todas las plataformas, tanto Windows como Unix, presentan una nutrida variedad de vulnerabilidades y riesgos, y en todos los casos TigerWeb es de gran ayuda al informar detalladamente y sugerir acciones correctoras concretas.

La solución suele pasar bien por actualizar el software (o firmware) o por configurarlo apropiadamente para garantizar un mayor nivel de seguridad (como el cambio de las contraseñas predeterminadas a contraseñas más fuertes), o bien desactivar servicios no utilizados o servicios que hacen uso de un protocolo inherentemente inseguro (por ejemplo el servicio Telnet, que en caso de ser necesario utilizarlo conviene sustituirlo por el servicio SSH).

En muchos casos se recomienda la deshabilitación del acceso al servicio, no en general sino solo a los potenciales clientes que provengan de Internet, fuera de la Intranet de la empresa.

Las vulnerabilidades por desbordamientos de memoria, un error de programación extremadamente común que conduce a ataques sumamente peligrosos en potencia (pues se puede lograr la ejecución de comandos arbitrarios con privilegios elevados) son resueltas en la casi totalidad de los casos con nuevas versiones que incluyen las modificaciones pertinentes en el código.

Mediante TigerWeb, el administrador de una red IP dispone de una herramienta que le mantiene informado acerca de las vulnerabilidades del perímetro de su red. Cuando desee, tanto de forma puntual como de forma periódica, puede ordenar que se realice un análisis, logrando de esta forma mantenerse informado acerca de los posibles puntos débiles de su red, y delegando la investigación de nuevos defectos en sistemas y sus posibles soluciones a la propia herramienta.

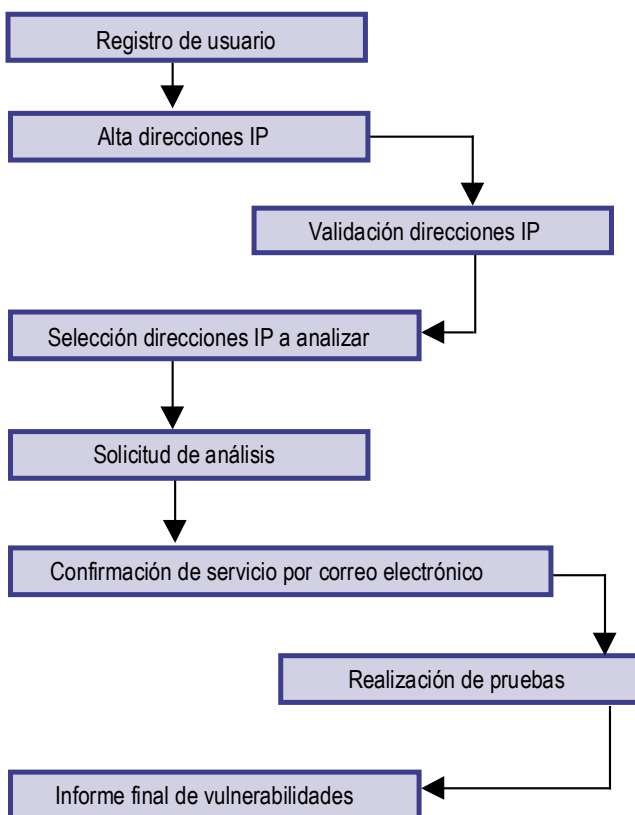


Figura 4: Descripción del servicio.

de análisis preparado para ser iniciado. Dicho proceso consiste en la realización del conjunto de pruebas sobre las direcciones IP que ha seleccionado previamente el usuario, para detectar potenciales fallos o debilidades.

Hay que destacar que es el propio usuario quien inicia el proceso. De esta manera evita el riesgo de posibles problemas que puedan ocasionarse al efectuar el análisis, como podría ser la caída del sistema. Aunque esta situación es poco probable, es conveniente analizar los sistemas en periodos de tiempo de poca actividad, como los fines de semana o durante la noche. De cualquier forma, el usuario

Autores: Yolanda Tomás, Raúl Salinas y Pablo Galdámez
 Para más información sobre TigerWeb:
seguridad@iti.upv.es