MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito

Sistemas de Infraestructura de Red

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Enero 2019

Sobre MILE-SEC

MILE-SEC
Capacitación y Consultoría en
Hacking Ético & Forense Digital

MILESEC E.I.R.L, es una empresa de capitales Peruanos fundada en el año 2017, netamente dedicada a brindar servicios de capacitación a empresas, instituciones, organizaciones y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I.), tales como; Pruebas de Penetracion, Hacking Ético, Evaluación de Vulnerabilidades, Forense de Computadoras y Forense Digital. Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo ha realizado capacitaciones online o virtuales.


http://www.mile-sec.com/

informes@mile-sec.com / mileseceirl@gmail.com

https://www.facebook.com/mileseceirl/

https://twitter.com/mileseceirl

https://www.linkedin.com/in/milesec/

Temario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- Entender las vulnerabilidades en la infraestructura de red
- Seleccionar las herramientas
- Escaners y analizadores
- Evaluar vulnerabilidades
- Escanear, hurgar y estimular la red
- Escanear puertos
- Escanear SNMP
- Capturar banners
- Evaluar reglas del firewall
- Analizar datos de red
- Ataques MAC
- Probar ataques de negación de servicios
- Detectar debilidades comunes en routers, switches y firewalls
- Encontrar interfaces inseguras
- Explotar debilidades IKE
- Descubrir problemas con SSL y TLS
- Implementar defensas generales de red

Introducción

Para asegurar sistemas operativos y aplicaciones, se necesita asegurar la red. Dispositivos como routers, firewalls, e incluso hosts genéricos de red (incluyendo servidores y estaciones de trabajo), deben ser evaluados como parte de un proceso de pruebas de seguridad.

Existen miles de posibles vulnerabilidades de red, igualmente muchas herramientas, e incluso más técnicas para las pruebas. Probablemente no se tenga el tiempo o recursos disponibles para evaluar los sistemas de infraestructura de red, de todas las posibles vulnerabilidades, utilizando cada herramienta y método imaginable. En lugar de ello, es necesario enfocarse en pruebas las cuales producirán un buen resultado global de toda la red.

Se puede eliminar muchas vulnerabilidades bien conocidas relacionadas a las redes, mediante simplemente la aplicación de parches en los hosts de la red, con las más recientes actualizaciones de firmware y software. Se puede también eliminar muchas otras vulnerabilidades siguiendo prácticas sólidas de seguridad en la red.

Entender las vulnerabilidades en la infraestructura de red

- Donde los dispositivos, como firewall o un IPS, están implementados
- Aquello visto por los atacantes externos cuando realicen escaneos
- Diseño de la red, como conexiones a Internet
- Interacción de los dispositivos de seguridad instalados
- Cuales protocolos están en uso
- Puertos comúnmente atacados sin protección
- Configuraciones del host de red
- Vigilancia y mantenimiento de la red

- Un atacante puede lanzar ataques DoS
- Un empleado malicioso utilizando un analizador de red
- Un atacante configurando una puerta trasera
- Un contratista atacando un host específico

- Evaluar los sistemas desde el exterior y el interior.
- Obtener permisos de los propietarios de lar de para verificar vulnerabilidades

Seleccionar las herramientas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Como con todas las evaluaciones de seguridad, las pruebas de seguridad en red requieren las herramientas correctas, se necesitan escáneres de puertos, analizadores de protocolos, y herramientas para la evaluación de vulnerabilidades. Están disponibles excelentes herramientas comerciales, shareware, y freeware. Únicamente se debe tener en mente se necesita más de una herramienta, porque ninguna herramienta realizará todo lo requerido.

Si se busca por herramientas de seguridad fáciles de utilizar, se debe pagar por esto la mayoría de las veces, especialmente en plataformas Windows. Muchos profesionales en seguridad utilizan diversas herramientas de seguridad libres, especialmente aquellas ejecutándose en Linux, u otros sistemas operativos basados en Unix. Muchas de estas herramientas ofrecen mucho valor, si se tiene el tiempo, paciencia, y ansias por aprender sus características y funcionalidades.

Escaners y analizadores

Existe una diversidad de escaners para puertos y la red. Muchos de ellos proporcionan ambas funcionalidades y otras más. Al momento de realizar esta presentación están disponibles algunas de las siguientes herramientas.

- Cain y Abel
- Essential NetTools
- NetScanTools
- GetIf
- Nmap
- Wireshark
- OmniPeek

* http://www.oxid.it/cain.html
* https://www.tamos.com/products/nettools/
* https://www.netscantools.com/
* http://www.wtcs.org/snmp4tpc/getif.htm
* https://nmap.org/
* https://www.wireshark.org/
* https://www.liveaction.com/products/omnipeek/

Evaluar vulnerabilidades

Estas herramientas para evaluar vulnerabilidades, entre otras, permiten evaluar los hosts de la red, de varias vulnerabilidades conocidas, como también potenciales problemas en las configuraciones, lo cual puede conducir a la explotación de seguridad.

- OpenVAS
- Nessus
- GFI LanGuard
- Nexpose

* http://www.openvas.org/
* https://www.tenable.com/products/nessus/nessus-professional
* https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
* https://www.rapid7.com/products/nexpose/

Escanear, hurgar y estimular la red

Realizar un Hacking Ético contra la infraestructura de la red, involucra las siguientes etapas básicas.

1. Obtener información y mapear la red

2. Escanear los sistemas para ver cuales están disponibles

3. Determinar aquello ejecutándose en los sistemas descubiertos

4. Intentar penetrar en los sistemas descubiertos.

Cada controlador de la tarjeta de red e implementación TCP/IP en muchos sistemas operativos, incluyendo Windows y Linux, e incluso firewalls y routers, podrían generar diferentes comportamientos cuando se escanee, hurgue o estimule los sistemas. Esto puede resultar en respuestas diferentes desde los sistemas, incluyendo hallazgos de falsos positivos hasta condiciones DoS.

Escanear puertos

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Un escáner de puertos muestra aquello existiendo en la red, mediante el escaneo la red, para ver cuales host están vivos y funcionando. Los escáneres de puertos proporcionan una visión básica de como está dispuesta la red. Pueden ayudar a identificar hosts no autorizados, o aplicaciones y host de red con errores de configuración, lo cual puede causar serias vulnerabilidades de seguridad.

La gran vista de los escáneres de puertos frecuentemente descubre problemas de seguridad los cuales de otra manera podrían no ser notados. Los escáneres de puertos son fáciles de utilizar, y pueden evaluar los hosts de las redes, sin importar cuales sistemas operativos y aplicaciones están ejecutando. Estas pruebas son usualmente realizadas de manera relativamente rápidas, lo cual de otra manera podría ser muy demandante.

Barridos con Pings (Ping Sweeps)
Nmap (Connect, escaneo UDP, SYN oculto, FIN, Xmas, y Null)
Puertos: TCP 21, TCP 22, TCP 25, UDP 53, TCP, 80, TCP 443, etc.

Escanear SNMP

Simple Network Management Protocol, está incorporado en virtualmente cada dispositivo de red. Programas para la gestión de la red utilizan SNMP para gestión remota de hosts en la red. Desafortunadamente SNMP también presente vulnerabilidades de seguridad.

Vulnerabilidades

El problema es muchos hosts de red ejecutan SNMP habilitado con cadenas de comunidad publica/privada de lectura/escritura. La mayoría de dispositivos de red tiene esto habilitado aunque no lo necesiten.

Si SNMP es comprometido, un atacante puede ser capaz de obtener información de red como tablas ARP, nombres de usuario, y conexiones TCP para atacar más profundamente los sistemas, Si SNMP es mostrado en los escaneos de puertoa, se puede apostar un atacante malicioso intentará comprometer los sistemas.

Herramientas, NetScanTools, Getif, SNMPUTIL.

Capturar banners

Banners son las pantallas de bienvenida, las cuales divulgan números de versión del software, y otra información del sistema sobre los hosts de la red. Esta información del banner podría identificar el sistema operativo, el número de versión, y service packs específicos, lo cual dará a los atacantes maliciosos información valiosa para atacar la red. Se pueden obtener los banners utilizando la clásica herramienta “telnet”, o alguna de las herramientas mencionadas, como Nmap o SuperScan.

Telnet

Se puede hacer telnet hacia un host sobre el puerto por defecto TCP 23, para ver si se presenta algún prompt de login, o cualquier otra información.

Esta misma acción puede ser realizada para otros puertos comunes, como TCP 25, TCP 80, o TCP 110.

Evaluar reglas del firewall

Como parte de un Hacking Ético se puede evaluar las reglas del firewall, para asegurarse están funcionando como se supone lo hagan.

Pruebas

Algunas pruebas pueden verificar el firewall actualmente hace aquello lo cual se supone haga. Se puede conectar a través del firewall sobre puertos abiertos, pero el tema son los puertos abiertos que no deberían estarlo.

netcat

Puede evaluar ciertas reglas del firewall sin deber evaluar directamente los sistemas de producción. Por ejemplo se puede verificar si el firewall permite acceso hacia el puerto TCP 23.

También se tiene un producto comercial como AlgoSec Firewall Analyzer.

* http://netcat.sourceforge.net/
* https://www.algosec.com/firewall-analyzer/

Analizar datos de red

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Un analizador de red es una herramienta la cual permite mirar dentro de la red, y analizar los datos atravesando el cable, para optimización de la red, seguridad o propósitos de solucionar inconvenientes. Como un microscopio es esencial para un científico, un analizador de red es una herramienta crítica para cualquier profesional de seguridad.

- Capturar todo el tráficos de red
- Interpretar o decodificar lo encontrado para poder ser leído
- Mostrar el contenido en orden cronológico

- Visualizar tráfico de red anómalo, o rastrear a un intruso
- Desarrollar una línea base de la actividad de la red y desempeño

- Rastrear y aislar el uso malicioso de la red
- Detectar aplicaciones maliciosas (troyanos)
- Vigilar y rastrear ataques DoS

Herramientas; Savius OmniPeek, Wireshark, Ettercap, etc.

Ataques MAC

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los atacantes pueden utilizar ARP (Address Resolution Protocol) ejecutándose en la red, para hacer a los sistemas aparecer como su sistema u otro host no autorizado en la red.

Spoofing ARP

Un excesivo número de peticiones ARP pueden ser un signo de un ataque de Spoofing ARP, también llamada envenenamiento ARP, en la red.

Spoofing de la dirección MAC

Spoofing de direcciones MAC engaña al switch a creer su computadora es alguien más. Simplemente cambiando la dirección MAC de una computadora y enmascararse como se fuese otra.

Se puede utilizar este truco para evaluar sistemas para el control de acceso, como IPS/firewalls, e incluso controles de login en sistemas operativos verificando direcciones MAC específicas.

Probar ataques de negación de servicios

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los ataques de Negación de Servicio son entre otros, los ataques más comunes. Un atacante malicioso inicia muchas peticiones inválidas hacia un host de la red, con lo cual el host utiliza todos sus recursos respondiendo las peticiones inválidas, e ignora las peticiones legítimas.

- Inundaciones SYN
- Ping de la muerte
- WinNuke

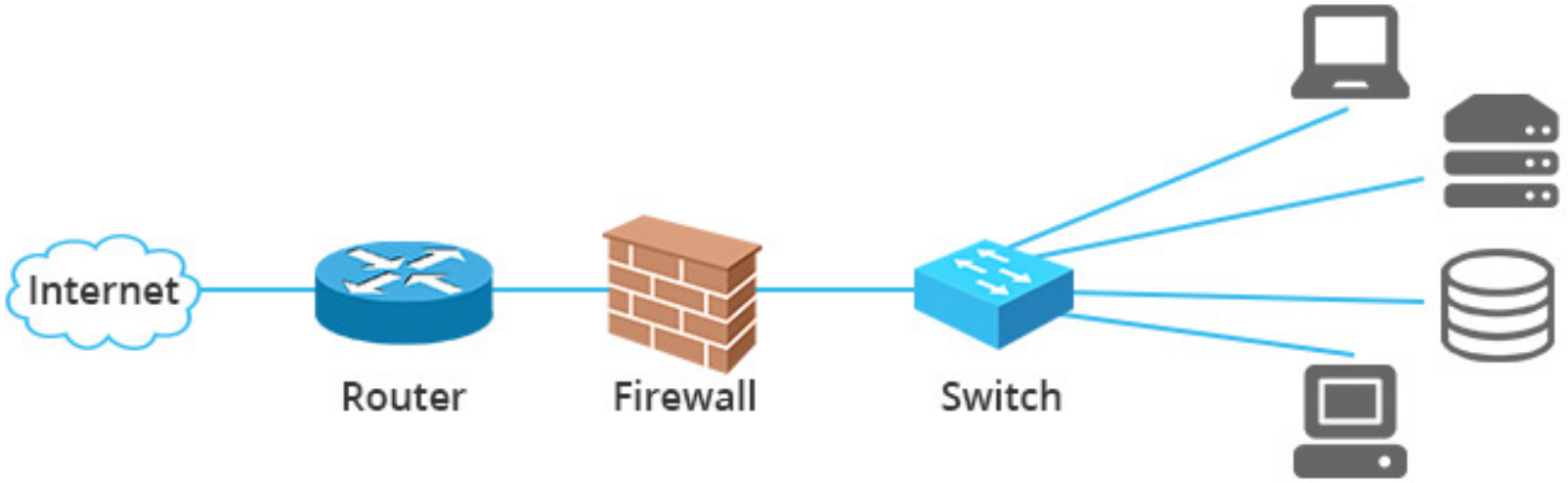
Ataques de Negación de Servicio Distribuido tienen un exponencialmente mayor impacto sobre sus victimas.

Pruebas

Es una de las pruebas de seguridad más difíciles de ejecutar. Una manera de encontrar este tipo de vulnerabilidades es mediante un escaneo de vulnerabilidades utilizando algunas de las herramientas mencionadas.

Detectar debilidades comunes en routers, switches y firewalls

Además de explotaciones más técnicas, se presentarán a continuación algunos vulnerabilidades de un nivel más alto de seguridad, los cuales comúnmente se encuentran en dispositivos de red, y consecuentemente generadores de problemas.



Encontrar interfaces inseguras

Se desea asegurar las interfaces HTTP y telnet hacia los reuters, switches, y firewalls no estén configurados con contraseñas en blanco, por defecto, o fáciles de adivinar. La advertencia puede no sonar muy inteligente, pero es de hecho una de las debilidades más comunes. Cuando un interno malicioso u otro atacante gana acceso hacia los dispositivos de red, se apropia de la red. Él puede entonces desbloquear el acceso administrativo, configurar cuentas de usuario como puertas traseras, reconfigurar puertos, e incluso traer abajo toda al red sin su conocimiento.

Otras debilidades relacionadas con HTTP y telnet, es estar habilitadas y ser utilizadas sobre muchos dispositivos de red. ¿Porqué esto es un problema?. Bueno, cualquiera con algunas herramientas gratuitas y tiempo, podría husmear la red, para consecuentemente capturar credenciales de login para estos sistemas, cuando están siendo enviados en texto plano. Cuando esto ocurre, no es nada bueno.

Explotar debilidades IKE

Las empresas ejecutando VPNs sobre un router o firewall son comunes. Si se está en esta categoría, las probabilidades son buenas de la VPN esté ejecutando el protocolo IKE (Internet Key Exchange). El cual tiene un par de bien conocidas debilidades explotables.

Es posible romper el “modo agresivo” IKE de claves previamente compartidas. Esto se puede automatizar con herramientas.

Algunas configuraciones IKE, como aquellas en ciertos firewalls Cisco PIX pueden ser desactivadas. Todo lo necesario a realizar por el atacante es enviar 10 paquetes por segundo con 122 bytes cada uno, y se tendrá un ataque de negación de servicio.

* http://ikecrack.sourceforge.net/
* https://www.talosintelligence.com/scanner/

Descubrir problemas con SSL y TLS

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

SSL y TLS (Transport Layer Security) fueron proclamados como la solución para asegurar las comunicaciones de red. Sin embargo SSL y TLS también han caído por una serie de explotaciones demostrables, como Heartbleed, POODLE, y FREAK.

Las vulnerabilidades de seguridad generales relacionadas con SSL y TLS son frecuentemente descubiertas por escáneres de vulnerabilidades, como Nexpose, o Nessus. Además a lo mencionado anteriormente, se debe considerar también.

- Versiones de SSL 2 y 3, como también TLS versiones 1.0 o 1.1 en uso
- Cifrados de encriptación débil como RC4 o SHA-1

Si no se está seguro sobre las vulnerabilidades existente en SSL y TLS de los sistemas, y no se tiene un escáner de vulnerabilidades, se puede utilizar un servicio libre de Qualys llamado SSL Labs.

* https://www.ssllabs.com/

Implementar defensas generales de red

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Sin importar los ataques específicos contra los sistemas, algunas pocas y buenas prácticas ayudan a prevenir muchos problemas de red.

- Reglas de inspección de estado, las cuales vigilen las sesiones en firewalls
- Implementar reglas para realizar filtrado de paquetes
- Utilizar proxy para filtrado y NAT o PAT
- Encontrar y eliminar paquetes fragmentados entrando a la red
- Incluir los dispositivos de red en los escaneos de vulnerabilidades
- Asegurarse los dispositivos de red tienen los más recientes firmwares
- Definir contraseñas fuertes, de preferencia frases de paso
- No utilizar IKE en modo agresivo con claves previamente compartidas
- Siempre utilizar TLS (via HTTP, etc), o SSH cuando se conecte
- Deshabilitar SSL y cifrados débiles
- Segmentar la red, y utilizar un firewall

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito

Sistemas de Infraestructura de Red

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Enero 2019