UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Ciberseguridad:
Un enfoque práctico

Integrantes:

Javier Ahumada

Rodolfo Cruz

Cristian Vega

Fecha:

13/09/2019

Resumen

Ante la necesidad de hacer conciencia sobre el impacto que han generado los frecuentes ataques a las redes de comunicaciones, creemos necesaria la propia enseñanza de las técnicas disponibles en el entorno para acercarnos a estos ataques y poner un pie sobre el mundo de la ciberseguridad. Comenzando la búsqueda de información para responder a la pregunta de cómo nos podemos defender si no sabemos cómo nos pueden atacar, se establece la estructura principal de la investigación. Por lo tanto, el siguiente informe presentará una idea clara sobre cómo nace la necesidad de ofrecer servicios de seguridad, como también un enfoque práctico con el fin de asimilar una perspectiva del funcionamiento de estos ataques. Finalmente, los resultados de la investigación han generado en la propia conciencia del grupo, la idea de “vulnerabilidad en la red”, comprendiendo que para defendernos de un ataque debemos acumular la mayor cantidad posible de perspectivas en que una persona puede atacar una red.

Introducción

Ante la creciente evolución de las redes de comunicaciones, como futuros ingenieros civiles telemáticos, debemos hacer frente a las futuras problemáticas que abundarán en la red y lograr presentar soluciones eficientes a los accesos no autorizados de información tanto a nuestros seres queridos como a grandes empresas. El área en que se encuentra inserto el tema a presentar gira entorno a la ciberseguridad y, en efecto, nuestro rol es generar un conocimiento lo más cercano a la realidad para así poder actuar ante ataques en la red. Por lo tanto, esperamos que el lector pueda asimilar el contexto general de la idea con la ayuda de un ejercicio práctico de ataque en una red.

Hacking Ético

Ante la creciente evolución de las redes de computadoras se hicieron más fluidas las comunicaciones interpersonales, intersucursales y las transacciones o flujos digitales dejando muchos datos expuestos a terceros. Por lo tanto, se hizo necesaria la falta de servicios que imitaran a esos ataques o capacitara a su personal con las mismas metodologías que utilizaba el intruso con el fin de evaluar las reales

condiciones de seguridad a las que se encontraban las redes de las organizaciones. (Tori, 2008:11). Según Tori, cuando las organizaciones comenzaron a brindar este tipo de servicios a modo de proveedores externos o contratados, se le denominó “ethical hacking”. El término anterior hace referencia explícitamente al escaneo de vulnerabilidades y pruebas de penetración, mejor denominado a este conjunto como a la evaluación de seguridad de redes.

A razón de lo anterior, como futuros ingenieros debemos hacer conciencia de cómo funcionan los ataques a las redes, al igual como evidencia Tori, para aprender a hacer evaluaciones más eficientes de un sistema de redes. Sin embargo, con respecto al tema ético, podemos darnos la libertad de expresar nuestro más alto grado de conocimiento en ejercer nuestra profesión en función de un bien común de la sociedad. Lo anterior incluye a nuestra motivación de proteger tanto a nuestros seres queridos como también inclinar la balanza hacia la justicia.

Malware

Para hacer conciencia sobre cómo ocurren los ataques, hacemos referencia a un caso de Malware detectado en la aplicación CamScanner. La noticia explica que “se ha detectado código malicioso en la versión gratuita de CamScanner, una aplicación de Android destinada a crear documentos PDF que posee más de 100 millones de descargas. Google ha retirado la aplicación de su tienda hasta que se resuelva el incidente.” (Oficina de Seguridad Internauta, 2019)

En esta noticia aparece el concepto Malware, el cual se define como “todo aquello que se cataloga como código malicioso o programas. Generalmente, estas amenazas son detectadas por los antivirus, se trate de gusanos, spyware, troyanos, virus o scripts malintencionados.” (Tori, 2008:11)

Por lo tanto, como futuros ingenieros de las redes debemos conocer cómo funcionan la mayor cantidad Malware posible para así definir una tabla esquemática de cómo defenderse ante ciertos ataques específicos.

Herramientas prácticas: Kali Linux

Considerando la existencia de los constantes accesos no autorizados a información en una red o usuarios, se introduce a la investigación planteando la pregunta principal que refiere a ¿Cómo defenderse si no sabemos cómo nos pueden atacar?

Investigando en la red nos encontramos con Kali Linux de Offensive Security, que se describe como una distribución de Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoría de seguridad. Lo importante de esta distribución es su variada cantidad de herramientas orientadas a diversas tareas de seguridad de la información. (Offensive Security, 2019)

A continuación, la imagen n°1 muestra las herramientas disponibles en Kali Linux ordenadas en 14 secciones según su función.

Imagen n°1: Herramientas de Kali Linux. Se muestra sección 09 “Husmeado/Envenenado” para observar que existe Wireshark como opción a utilizar. Wireshark fue una herramienta utilizada para realizar nuestras tareas del curso ELO322.

Herramientas de explotación: Metasploit Pro

En la sección 08 “Herramientas de Explotación” de la imagen n°1 se encuentra “Metasploit Pro” de Rapid7 que se describe como una herramienta de explotación y validación de vulnerabilidades. Este facilita el flujo de trabajo de las pruebas de penetración en tareas más pequeñas y manejables. Con esta herramienta nos

encontramos con Metasploit Framework que, con su base de datos de exploits, ayuda a realizar evaluaciones de seguridad y validación de vulnerabilidades eficientes. Entre sus funciones encontramos la búsqueda de puertos y servicios abiertos, explotación de vulnerabilidades, pivoteo de más en una red, recopilación de evidencia y creación de informes como resultados de la prueba. (Rapid7, 2019)

Investigando en Internet, nos impacta la gran cantidad de tutoriales disponibles para aprender a utilizar las distintas herramientas de Kali Linux, por lo tanto, para evidenciar un aprendizaje sobre cómo utilizar Metasploit Pro de Kali Linux, aprenderemos a realizar una conexión fuera de nuestra red de área local (WAN).

Conexión WAN

Para hacer expedita la comprensión del tutorial, se utiliza la imagen n°2 para formalizar la idea. En el escenario propuesto, existe una terminal Kali Linux al lado izquierdo y una terminal Windows 10 al derecho, donde cada terminal está conectada a internet a través de un router en su domicilio. Cuando la terminal Windows se conecta a su router se le asigna una IP personal, lo mismo ocurre con nuestra terminal Kali Linux con nuestro router de VTR, la cual es (192.168.0.23). Ahora, cada vez que un router se conecta a internet se le asigna una IP pública, en nuestro caso, es la 190.46.5.241, esta IP cambia regularmente. En nuestro router VTR debemos configurar el Port Forwarding o Redirección de puertos, donde debemos habilitar un puerto aleatorio con los protocolos TCP/UDP (Transmission Control Protocol / User Datagram Protocol) habilitados, de modo que cuando se establezca la conexión con la terminal de Windows, todo el tráfico TCP/UDP se redirija a la IP de la terminal de Kali Linux. En la imagen n°3 se muestra la interfaz de configuración del Router VTR. Ahora se debe crear un backdoor con Veil-evasion, es decir, un tipo de troyano que permite el acceso al sistema infectado y su control remoto. Con esto, el atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas. Antes de enviar el backdoor será enviado a la terminal Windows, tendremos que abrir una sesión de Metasploit abierta preconfigurada con el backdoor, de manera que cuando este se active en la terminal Windows 10, se

buscará la IP publica de nuestro terminal en la red y nos llegara aviso para aceptar la conexión. Dentro de la terminal del usuario uno tiene varias opciones, como por ejemplo: grabar audio, espiar la webcam, cargar y descargar archivos de terminal a terminal.

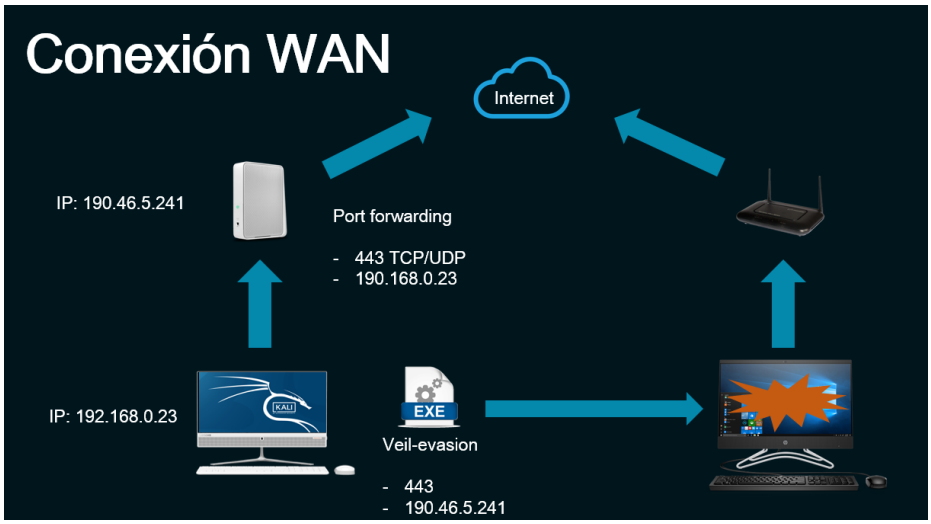

Imagen n°2: Conexión WAN, desde Kali Linux a la izquierda y Windows 10 a la derecha.

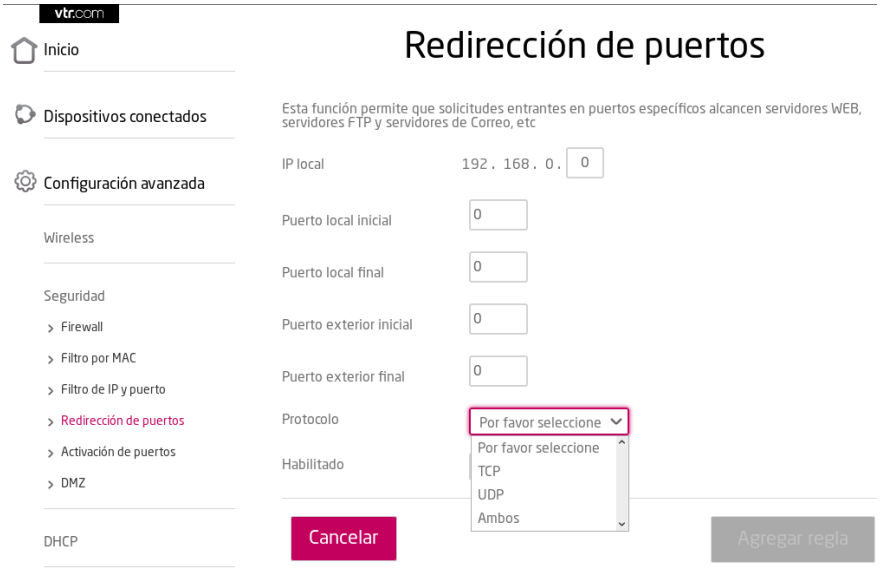

Imagen n°3: Redirección de puertos VTR. La interfaz permite modificar la IP y puerto origen / puerto destino.

Conclusión

Lo más relevante de la investigación es la asimilación de un contexto tan complejo como lo es la ciberseguridad. Gracias a la investigación teórico-práctico se nos hace más fácil pensar en cómo funciona el mecanismo de un ataque de red tras bambalinas, para así dar posibles proyecciones a la defensa. El problema de responder a la pregunta de cómo defendernos ante ataques que no conocemos, se responde a la acumulación de diversas perspectivas sobre el funcionamiento de los malware posibles y así generar un esquema general de defensa. Hemos solucionado nuestra necesidad obteniendo conciencia sobre lo que puede ocurrir en una red cuando recibamos un ataque tanto de manera personal como a nivel organizacional. En cuanto a la parte práctica, no solo hemos realizado una conexión WAN no autorizada, si no que en nuestro tiempo libre hemos extendido esta concepción y hemos abarcado otras formas de ataques para abrirnos paso sin problemas al mundo de la ciberseguridad. Finalmente, ante la reflexión de hacer conciencia del uso de las redes y sus posibles accesos no autorizados de información, es menester plantearnos a la proyección de que ante la inconsistencia del carácter humano debemos observar el comportamiento de los usuarios en las redes y, durante todo ese tiempo, acumular la mayor cantidad de perspectivas de ataque posibles para así defendernos ante ataques más evolucionados acorde a los tiempos en que nos encontremos. En síntesis, se trata de que si queremos ejercer el oficio de la ciberseguridad, debemos aprender desde ya todas las variantes posibles de ataques y estar atento a las nuevas formas de malware.

Referencias

Offensive Security. (2019). Kali Linux Documentation. Recuperado el 08 de septiembre de 2019, de: https://docs.kali.org/category/introduction

Oficina de Seguridad Internauta. (2019). Malware detectado en la aplicación CamScanner. Recuperado el 10 de Septiembre de 2019, de: https://www.osi.es/es/actualidad/avisos/2019/08/malware-detectado-en-la-aplicacion-camscanner

Rapid7. (2019). Metasploit Documentation. Recuperado el 09 de Septiembre de 2019, de: https://metasploit.help.rapid7.com/docs/metasploit-basics

Tori, C. (2008). Hacking Ético. Buenos Aires, Argentina: Mastroianni Impresiones.