Análisis de Seguridad en Redes Wireless Utilizando Dispositivos Móviles

Lic. Paula Venosa - Lic. Nicolás Macia - Lic. Einar Lanfranco - Lic. Alejandro Sabolansky
[pvenosa | nmacia | einar | asabolansky] at linti.unlp.edu.ar

LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas)
Facultad de Informática - UNLP
Calle 50 y 120 – 2do piso – La Plata, Buenos Aires, Argentina

1. Resumen

En la actualidad el mundo es digital y la mayoría de las organizaciones utilizan redes inalámbricas co- mo parte de su infraestructura, extendiendo así sus posibilidades de conectividad, tanto para brindar servicios a sus usuarios como a terceros. Dada es- ta proliferación resulta necesario realizar una eva- luación de las redes Wireless en el marco de una auditoría de la seguridad de una organización.

La implementación de este tipo de redes y su pos- terior interconexión con la infraestructura cableada de la organización en muchos casos es una tarea sen- cilla, incluso realizable por usuarios no administra- dores. Es por esto que al momento de auditar la seguridad de una red no sólo se deben considerar las condiciones en que se brindan los servicios sino también la existencia de redes Wireless "no oficia- les o no declaradas" en el ámbito de la organización en cuestión. Entre los alcances esperados de esta línea de I/D/I se busca adquirir experiencia en lo relacionado al campo de investigación de redes Wi- reless, en particular lo referente a la seguridad de las mismas. Para ello, se pretende identificar y evaluar herramientas de software libre que den soporte a la auditoría de seguridad y que puedan ser utilizados desde dispositivos móviles como un smartphone o

Palabras clave: seguridad de la información, Wireless, Mobile, Smartphone, IoT

2. Contexto

En el Laboratorio de Investigación en Nuevas Tecnologías Informáticas (LINTI) [1] de la Facultad de informática de la Universidad Nacional de La Pla- ta [2], un grupo de docentes/investigadores se dedi- ca a estudiar temas relacionados con la seguridad y privacidad de la información, aplicando los conoci- mientos en los distintos proyectos en los que parti- cipan.

En el marco del proyecto de incentivos "Internet del Futuro: Ciudades Digitales Inclusivas, Innovado- ras y Sustentables, IoT, Ciberseguridad, Espacios de Aprendizaje del Futuro", este grupo investiga vul- nerabilidades de seguridad actuales que afectan a sistemas, redes y servicios.

En líneas anteriores de investigación desarrolladas por el mismo grupo se han tratado las problemáticas relacionadas a dispositivos móviles, principalmente en torno al fenómeno conocido como BYOD [9].

Consideramos que esta línea de investigación re- sulta fundamental en el marco del proyecto ya que, a través de una conexión inalámbrica es, como en la mayoría de los casos, las **cosas** empiezan a conec- tarse a Internet. Se cree que a medida que haya más dispositivos conectados en nuestra red las vulnera- bilidades seguirán apareciendo y lo harán en forma exponencial. Esto hará que la auditoría continua y la investigación asociada en busca de soluciones se vuelvan indispensables.

3. Introducción

En la actualidad el mundo es digital y la mayoría de las organizaciones utilizan redes inalámbricas co- mo parte de su infraestructura, extendiendo así sus posibilidades de conectividad, tanto para brindar servicios a sus usuarios como a terceros.

Las redes inalámbricas son una extensión del

perímetro de la infraestructura de las organizaciones.

Dada esta proliferación se torna necesario realizar una evaluación de las mismas dentro del alcance de las auditorías de seguridad de una organización.

Esta evaluación es importante tanto por lo que los atacantes puedan obtener como valor de activo de información de la propia víctima como lo que estos puedan hacer utilizando los recursos de la organización para afectar a terceros.

Un caso recurrente es la utilización del enlace para realizar ataques de denegación de servicio, denominado habitualmente DoS [3]. Para ejemplificarlo basta simplemente pensar que el atacante logra acceder a la infraestructura de la Empresa X, a través de una vulnerabilidad de alguno de sus activos. Dado que X tiene un enlace con capacidad de 20Mbps, y se decide utilizar a la misma para atacar a la Empresa Y que tiene 5Mbps contratados, no hay que ser un experto para adivinar el resultado; es evidente que la Empresa Y se quedará sin posibilidades de utilizar su enlace, ya que estará saturado por el tráfico entrante.

La superficie a defender incrementa su tamaño, ya que potencialmente hay muchos más objetivos, pudiendo listar entre los factores responsables:

- La disponibilidad de conexión a Internet, sobre todo con la masificación del acceso a través de banda ancha.
- La aparición de dispositivos móviles, en particular los denominados smartphones o teléfonos inteligentes.
- La llegada de Internet de las Cosas (IoT), donde muchos de los dispositivos que se conectan carecen de la posibilidad de ser actualizados sumado al fenómeno denominado Plug It and Forget It [4].
- La necesidad de las personas, tanto técnicos como no técnicos, de contar con acceso a la red en cualquier lugar.
- La facilidad de conectar puntos de acceso de tipo Rogue, es decir no autorizados por la organización, que pueden ser instalados por los empleados sin respetar las normas de seguridad de la organización.

En los procesos de auditoría se suele incluir el análisis de las redes wireless disponibles, tarea que habitualmente se realizan desde un escritorio, una sala de racks o alguna oficina de las instalaciones que se facilita a los analistas para ubicar su computadora y hacer su trabajo.

En este nuevo enfoque y con las necesidades de evaluar todas las secciones de la organización objetivo, entendemos que el camino a seguir es un estudio más parecido al wardriving [5], donde se realiza un recorrido en busca de relevar las redes existentes y no sólo las conocidas por los administradores de la red bajo evaluación. Como objetivos adicionales consideramos minimizar los requerimientos de hardware y aplicar mayor grado de inteligencia al proceso de relevamiento.

Como experiencia previa, en el año 2009 investigadores de este equipo realizamos un wardriving por las calles de la ciudad de La Plata obteniento como resultado un mapa de las redes inalámbricas disponibles halladas al recorrer las calles de la ciudad en un vehículo [6]. En esa oportunidad fue necesario conectar un analizador de redes a un navegador satelital (GPS) y todo ello a una notebook.

En particular, la línea que se presenta en este trabajo se enfoca en proponer mejoras en la metodología y en los procesos para medir los niveles de seguridad de las redes wireless a través del uso de dispositivos móviles.

De esta forma, en nuestro trabajo actual, los dispositivos móviles que hasta ahora han sido un campo de estudio en cuanto a las vulnerabilidades que presentan y las posibles soluciones para mitigarlos [7], [8], adquieren ahora un rol principal ya que en la presente línea aprovecharemos las ventajas de la movilidad que los mismos nos brindan para su utilización en las primeras etapas de la auditoría de redes Wireless.

4. Líneas de Investigación, Desarrollo e Innovación

Sobre los ejes de investigación, inicialmente planteados:

- Realizamos una recopilación de bibliografía para conocer el estado del arte actual.

- Se dirigió alumnos en el desarrollo de sus tesinas relacionada con la temática.
- Asistimos a distintas charlas de seguridad en general; en particular en la conferencia Ekoparty se han realizado diversas presentaciones sobre esta temática.
- En el marco de la operatoria diaria del CERTUNLP, hemos realizado varios pentests en distintas organizaciones.

5. Resultados y Objetivos

5.1. Objetivo General

Se espera continuar adquiriendo experiencia en lo relativo al campo de investigación de la seguridad y auditoría de redes y servicios, aprovechando los beneficios de los dispositivos móviles, en este caso como herramienta para facilitar las tareas de testeo.

Se busca lograr tanto una mejora tanto en el resultado de los tests de penetración como llegar a facilitar la tarea de los analistas.

En esta línea es de investigación es que buscamos que eso mismo pueda realizarse utilizando un solo equipo no especial, es decir un smartphone de uso habitual del investigador agregando otras funciones como ser captura de handshake de autenticación, escaner de puertos o generador de informes.

5.2. Objetivos Específicos

- Abordar un análisis de herramientas preexistentes para auditar la seguridad de las redes wireless a fin de poder identificar y entender los problemas que poseen, poniendo especial énfa- sis en aquellas que sean de software libre.
- Desarrollar una herramienta que permita hacer uso de un smartphone para llevar a cabo la etapa de descubrimiento y relevamiento en el marco de un test de penetración a redes inalámbri- cas.
- Probar la herramienta en campo, utilizándola en pruebas de intrusión reales.
- Formar RRHH que retroalimenten al grupo de investigadores convirtiéndolo en un referente en el tema.
- Fomentar el uso y la mejora continua de la aplicación a partir de las observaciones que se pue- dan realizar en campo y ante la evolución pro- pia de los sistemas operativos.

Algunas de las características no negociables en esta primer versión de la solución a implementar:

- El sistema operativo a utilizar para el desarrollo será Android
- El sistema operativo del equipo a utilizar no deben ser modificado ya que esto podría ocasionar un problema de seguridad en el software mismo. En otros términos, el equipo a utilizar no debe ser rooteado para poder utilizar la aplicación.
- Los resultados obtenidos a partir del uso de la aplicación deben poder utilizarse para complementar el resultado de la auditoria general.
- Se espera obtener más información que simplemente relevamientos de redes disponibles y sus configuraciones de seguridad.
- No es necesario que el dispositivo realice todo el procesamiento de la información, lo que recolecte puede ser trasladado a un un recurso externo de mayor poder de computo, como un servidor. El postprocesamiento permitirá obtener datos adicionales a los procesados insitu.

6. Formación de Recursos Humanos

La línea de investigación seguridad en redes wireless está siendo abordada por los alumnos Juan Ignacio Bernal y Alejandro Zurita en el marco de la realización de su tesina de grado de la Licenciatura en Sistemas, en conjunto con los docentes Alejandro Sabolansky, Nicolás Macia, Einar Lanfranco y Paula Venosa quienes también forman parte del grupo de seguridad del LINTI de la Facultad de Informática de la UNLP, el CERTUNLP y las cátedras de grado y postgrado Seguridad y privacidad en redes.

En cuanto a las experiencias en gestión y despliegue de redes inalámbricas, la Facultad de Informáti- ca de la UNLP cuenta con dos soluciones de administración centralizada, una de las cuales es administrada en forma íntegra por el grupo de investigado- res y la otra es de gestión compartida, ya que parte

del control se realiza vía una controladora alojada en el centro de cómputos de la UNLP.

Esta solución implementada dispone de múltiples SSID que entregan direcciones de red en distintas VLAN, contando actualmente con más de 20 dispositivos conectados. Cada una de estas redes posee diferentes mecanismos de autenticación, entre los cua- les podemos mencionar WPA2 y WPA2 combinado con un portal captivo, similar al que se encuentra en redes públicas como las disponibles en aeropuer- tos o locales de comidas rápidas. El portal captivo fue adaptado para cumplir con la identidad insti- tucional y fue complementado con un software que permite manipular los tokens de acceso en forma automática.

El grupo de seguridad del LINTI de la Facultad de Informática de la UNLP trabaja desde el año 2000 con distintas experiencias relacionadas con la Seguridad de la Información: auditorias de seguridad, implementación de infraestructuras de seguridad, consultoría, desarrollo e implementación de Software Libre y concientización.

Cabe destacar que este grupo de investigadores representa a la UNLP en el Centro de excelencia [10]en el tema “Ciberseguridad” de la UIT, desde el año 2015 [11].

Referencias

[1] Laboratorio de Investigación de Nuevas Tecnologías Informáticas - LINTI.Facultad de Informática: https://www.linti.unlp.edu.ar

[2] Facultad de Informática: https://info.unlp.edu.ar

[3] https://www.us-cert.gov/ncas/tips/ST04-015

[4] Plug IT and Forget IT https://insights.ubuntu.com/2016/12/15/research-consumers-are-terrible-at-updating-their- connected-devices/

[5] Definición de Wardriving: https://es.wikipedia.org/wiki/Wardriving

[6] Wardriving: an experience in the city of La Pla- ta. Autores: Javier Díaz. Matías Robles. Nicolás Macia. Paula Venosa. Germán Vodopivec. CA- CIC 2008. ISBN: 978-987-24611-0-2

[7] Uso de dispositivos moviles y BYOD: Su impac- to en la seguridad. Autores: Nicolás Macia, Ei- nar Lanfranco, Paula Venosa, Alejandro Sabo- lansky, Carlos Damián Piazza Orlando, Sebas- tian Exequiel Pacheco Veliz. WICC 2015. ISBN 978-987-633-134-0.

[8] Dispositivos móviles y el fenómeno del BYOD . Su impacto en la seguridad de las organizaciones Autores: Venosa, Paula; Macia, Nicolás; Piazza Orlando, Carlos Damián; Pacheco Veliz, Sebas- tián. CACIC 2016.

[9] BYOD: https://www.sans.org/reading-room/whitepapers/leadership/managing-implementation-byod-policy-34217

[10] Centro de excelencia en Ciberseguridad. http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0225-BR-COE/Agenda-EN.pdf

[11] ITU. http://www.itu.int