Sistemas Operativos Orientados a la Seguridad Informática

Ayrton Marini, Enrique A. Miranda, Mario Berón, Daniel Riesco

Departamento de Informática/ Facultad de Ciencias Físico Matemáticas y Naturales/
Universidad Nacional de San Luis
Ejercito de Los Andes 950 - San Luis - Argentina
ayrtonmarini10@hotmail.com, {eamiranda, mberon,driesco}@unsl.edu.ar

Resumen

En los últimos años Internet ha ido tomando un rol crucial en la vida moderna de las personas, el comercio, las organizaciones gubernamentales, etc. Este hecho ha convertido a dicho recurso en un medio/herramienta para que se lleven a cabo ataques de diversa índole a los distintos componentes conectados a la red. Esto ha dejado entrever la necesidad de analizar la infraestructura y el software que se utiliza día a día, teniendo como principal objetivo de revisión, aquellas funcionalidades o características de seguridad que los mismos poseen.

El presente trabajo propone una línea de investigación que tiene como principales lineamientos i) el estudio de los Sistemas Operativos orientados a la Seguridad Informática en conjunto con las herramientas que los mismos proveen; y ii) el estudio e inspección de distintos tipos de software maliciosos utilizados en los diversos ataques.

Palabras clave: Seguridad Informática, Software Malicioso, Herramientas de Análisis.

Contexto

La línea de investigación descripta en este artículo se encuentra enmarcada en el contexto del proyecto: *Ingeniería de Software: Aspectos de Alta Sensibilidad en el Ejercicio de la Profesión de Ingeniero de Software* de la Universidad Nacional de San Luis. Dicho proyecto, es reconocido por el programa de incentivos, y es la continuación de diferentes proyectos de investigación de gran éxito a nivel nacional e internacional.

Introducción

En los últimos años Internet ha pasado a ser un pilar fundamental en los distintos ámbitos en done se utiliza. Este rol crucial en la vida moderna de las personas, el comercio, las organizaciones gubernamentales, etc. ha convertido a este valioso recurso en un medio/herramienta para realizar ataques de diversa índole a los distintos componentes conectados a la red. Esto ha dejado entrever la necesidad de analizar la infraestructura y el software que se utiliza día a día, teniendo como principal objetivo de revisión aquellas funcionalidades o características de seguridad que los mismos poseen.

En este contexto, se han ido generando distintas líneas de investigación para: mejorar (o directamente incorporar) determinadas características de seguridad de los sistemas de software actuales, mejorar los procesos de modelado y

desarrollo de nuevos sistemas de software que incorporen funcionalidades o características de seguridad, estudiar los distintos tipos de programas maliciosos que intentan vulnerar los sistemas, mejorar los aspectos relativos a la seguridad de los componentes de la infraestructura de comunicación, entre muchas otras. Teniendo esto en cuenta, es posible afirmar que éstas líneas de investigación son abarcadas por una disciplina denominada la Seguridad Informática [1].

La Seguridad Informática apunta a la protección de los sistemas informáticos en donde generalmente se almacena o transfiere información. Es relevante remarcar que la información no puede ser considerada como segura a menos que los procesos y recursos involucrados en administrar la misma lo sean también. La Seguridad Informática se puede definir como todos los aspectos relativos a definir, obtener y mantener la confidencialidad, integridad, disponibilidad, autenticidad, y confiabilidad de la información administrada en los recursos informáticos [2].

Líneas de Investigación, Desarrollo e Innovación: Seguridad Informática

Al hacer referencia a la Seguridad Informática, es importante comprender el término “malware” o software malicioso. Un malware es todo aquel software que ha sido diseñado para atacar o irrumpir en una computadora o un sistema de información [3,5]. Existen diferentes tipos de acuerdo a su naturaleza y objetivo, entre los más conocidos se pueden mencionar:

Virus: busca alterar el funcionamiento del equipo que infecta. Se caracteriza por atacar documentos digitales, archivos vitales del arranque o incluso, controladores de hardware. Los síntomas más comunes de un ordenador infectado por un virus pueden ser: lentitud, aparición espontánea de accesos directos en los dispositivos de almacenamiento, archivos que se ocultan a sí mismos, entre otros.

Adware: el prefijo “ad” se refiere a “advertisement” que se podría traducir al español como “anuncio”, por lo tanto, es un malware que se encarga de mostrar publicidad mientras el usuario utiliza un navegador. Algunos son más ofensivos e invasivos que otros, pero por lo general, su principal finalidad es promocionar productos o servicios para determinados patrocinadores [7].

Worms (o gusanos): actúan sobre la PC haciéndola extremadamente lenta, replicándose una y otra vez hasta sobrecargarla. A diferencia de un virus, un gusano posee la característica de infectar automáticamente el ordenador, es decir, es auto-ejecutable. A modo de ejemplo, un usuario conecta un dispositivo extraíble (infectado) a su ordenador, si el malware es un gusano, la PC del usuario se verá infectada automáticamente, en cambio, si se trata de un virus, para que logre infectar el ordenador es necesario que se utilice el archivo infectado [8] (por lo general son archivos ejecutables).

Spyware: este tipo de malware, se encarga de recoger información de los movimientos que lleva a cabo el usuario

por la red y enviarlos al interesado. Este puede tener diferentes funcionalidades como robar passwords, IPs, DNS, páginas frecuentadas, temas de interés del usuario, software instalado y demás. Como se puede deducir, este software malicioso presenta una gran amenaza para la seguridad informática. Tiene la particularidad de ejecutarse en segundo plano para no ser detectado. La computadora se infecta cuando se visita un sitio web predeterminado y se descarga algún *cookie* infectado. Un síntoma frecuente de este tipo de infección es la excesiva lentitud en la navegación por Internet [9].

Botnets: cuando un ordenador se ve infectado por un botnet, se dice que dicha máquina es un bot o un zombie y ha caído en una red botnet, este tipo de malware es especialmente peligroso, ya que, le otorga el control total de la PC infectada al autor del botnet, por consiguiente, puede llevar a cabo cualquier tipo de acciones (por lo general, ciberdelitos [4]). Este clase de software malicioso es utilizado, generalmente, para el tráfico de datos ilegales entre hackers o criminales en internet. También se lo ha reconocido como una herramienta poderosa en el contexto de ciberdelitos transnacionales.

Por lo general, los malwares más nocivos para un sistema informático son aquellos que infectan el ordenador mediante un ejecutable o la descarga de un archivo específico. Por otra parte, este hecho se ve agravado mediante la participación involuntaria del usuario, que ejecuta o posibilita que se lleven a cabo las acciones necesarias para que el malware pueda ejecutarse. Sin embargo, también es posible encontrar un gran conjunto de tecnologías y metodologías que promueven la Seguridad Informática. Ciertos sistemas de software como los antivirus, firewalls, sistemas tolerante a las fallas, sistemas operativos seguros, entre otros; son utilizados para garantizar un entorno seguro y controlado.

Teniendo como base lo explicado en los párrafos precedentes, es posible destacar cierto tipo de sistemas operativos frecuentemente referenciados como “orientados a la Seguridad Informática”. Estos incorporan un conjunto de características de seguridad que dificultan en gran medida los distintos tipos de ataques antes descriptos. En muchos casos también brindan herramientas para analizar los distintos recursos fuertemente relacionados con malwares, como los medios de propagación (discos extraíbles, redes, archivos, etc), código fuente del malware, componentes del sistema operativo, entre otros.

Generalmente, el software maligno es desarrollado para ejecutarse en los sistemas operativos más utilizados por los usuarios. Frecuentemente, este tipo de sistemas operativos poseen ciertas características y/o vulnerabilidades que los destacan como objetivos constantes de malwares [6].

Para concluir esta sección cabe destacar que esta línea de investigación se divide en dos temáticas relevantes: i) el estudio de los Sistemas Operativos orientados a la Seguridad Informática y

ii) Inspección de distintos tipos de malwares.

Resultados y Objetivos

A continuación se mencionan los resultados obtenidos hasta el momento dentro del marco de la línea de investigación planteada.

Por un lado, se pudo comprobar que dentro del conjunto de sistemas operativos disponibles, se han desarrollado algunos que proveen varias herramientas para contrarrestar e inspeccionar software malicioso. En este sentido se ha estudiado la distribución *Fedora Linux Security Lab*. Dicho sistema operativo está diseñado para ofrecer un entorno de pruebas estable y seguro para trabajar en auditorías de seguridad forenses, rescate de sistemas y para verificación de seguridad de entidades informáticas, monitoreo de redes, entre otros. De esta manera proporciona muchas herramientas que pueden ser usadas con distinto fines, dentro del contexto de Seguridad Informática. A continuación se mencionan algunas, agrupadas de acuerdo a su principal objetivo:

Análisis de código: *flawfinder, pscan y splint*, analizan código fuente en busca de debilidades o partes de códigos propensas a errores referentes a seguridad informática.

Análisis forense: *dc3dd, ddrescue, disk scruber, driftnet, unhide,* que permiten realizar análisis y operaciones sobre discos rígidos, archivos binarios, procesos ocultos, rootkits, entre otros. Como su nombre lo indica, dichas herramientas están orientadas al análisis forense.

Detección de intrusos: *chrootkkit*, esta herramienta realiza ciertas pruebas estándares para verificar si la computadora ha sido comprometida, es decir afectada por algún tipo de intruso.

Estadística de red: *iftop, iperf, iptraf-ng, nethogs, scampe, Nload,* herramientas destinadas a monitoreo y análisis de tráfico de redes.

Claves (passwords): *john, Medusa brute force, Objetif securite ophcrack, Pwgen, Sucrack,* herramientas de cifrado, detección de falencias en la seguridad de las claves, ataques de fuerza bruta para obtener claves, generación de claves seguras, entre otras.

Reconocimiento: *arp scanner, packet generator, ARGUS, banner grabbing, Ncrack, Siege, Yersinia, tcpjunk,* permiten reconocer atacantes, generar paquetes para congestionar redes locales, testear rendimiento o seguridad de la red, romper la seguridad de la una red local, buscar "griteas" en un servidor HTTP, entre otras funcionalidades.

Testeo de aplicaciones web: *halberd, httping, Ratproxy, Skipfish, Sqlninja,* permiten descubrir balanceadores de carga de aplicaciones HTTP, detección de problemas potenciales respecto la seguridad de una página web, explotación de vulnerabilidades de inyección SQL, entre otras.

Wireless: *airckar -ng, horst, kismet, wavemon,* posibilitan examinar redes inalámbricas en busca de comportamiento intrusivo, recuperar cifrados utilizando protocolos de seguridad WEP, testar la seguridad en las redes, monitoreo general de la red, entre otros.

Por otra parte, actualmente se está haciendo uso de las funcionalidades que proporciona Fedora Security Lab en conjunto con otras herramientas de análisis de código para inspeccionar ciertos módulos escritos en C++ del troyano *Zeus*[1].

[1] https://github.com/Visgean/Zeus

Dentro de los objetivos planteados a corto plazo se pretende: i) identificar las principales fortalezas de dicho malware destacando en cierta manera y de forma semi-automática, la intencionalidad del mismo; ii) analizar otros tipos de malwares con el mismo objetivo que los descriptos en el punto i) y comparar entre sí para identificar patrones en común; iii) realizar un estudio orientado a destacar los lenguajes de programación más utilizados en la construcción de malwares; iv) definir un conjunto de criterios de evaluación que permitan identificar la comprensibilidad de un malware; v) desarrollar un set de herramientas de inspección de malwares.

Formación de Recursos Humanos

Las tareas llevadas a cabo en la presente línea de investigación están siendo desarrolladas como parte de tesis en Ingeniería en Informática en la Universidad Nacional de San Luis. Se pretende que los resultados obtenidos durante el desarrollo de las tesis den origen a estudios de posgrado de los integrantes del proyecto en el que se encuentra enmarcada dicha línea de investigación. Permitiendo, de esta manera, el crecimiento académico de los integrantes de la línea como así también la generación de proyectos de investigación basados en Seguridad Informática.

Referencias

[1] MASROM, Maslin; ISMAIL, Z. Computer Security and Computer Ethics Awareness: a Component of Management Information System. En *Information Technology, 2008. ITSim 2008. International Symposium on*. IEEE, 2008. p. 1-7.

[2] BISHOP, Matt. *Introduction to Computer Security*. Addison-Wesley Professional, 2004.

[3] CHRISTODORESCU, Mihai, et al. Semantics-aware Malware Detection. En *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005. p. 32-46.

[4] GORDON, Sarah; FORD, Richard. On the Definition and Classification of Cybercrime. En *Journal in Computer Virology*, 2006, vol. 2, no 1, p. 13-20.

[5] HANSMAN, Simon; HUNT, Ray. A taxonomy of network and computer attacks. En Computers & Security, 2005, vol. 24, no 1, p. 31-43.

[6] ALHAZMI, Omar H.; MALAIYA, Yashwant K.; RAY, Indrajit. Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems. En *Computers & Security*, 2007, vol. 26, no 3, p. 219-228.

[7] CHIEN, Eric. Techniques of Adware and Spyware. En *Proceedings of the Fifteenth Virus Bulletin Conference*, Dublin Ireland. 2005.

[8] PROVOS, Niels, et al. The Ghost in the Browser Analysis of Web-based Malware. En *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*. 2007. p. 4-4.

[9] MOSHCHUK, Alexander, et al. A Crawler-based Study of Spyware in the Web. *En NDSS*. 2006.