REVISTA CIENTÍFICA RETOS DE LA CIENCIA
http://retosdelacienciaec.com
mcrevistas@gmail.com

Enero – junio, 2017
Vol. 1, No. 1
ISSN 2602-8247

EVALUACIÓN DE TIPOS DE CLIENT SIDE EXPLOITS EN UNA RED LAN COMO PLATAFORMA EXPERIMENTAL: VULNERACIÓN A LA PRIVACIDAD DE INFORMACIÓN

EVALUATION OF TYPES OF CLIENT SIDE EXPLOITS IN A LAN NETWORK AS AN EXPERIMENTAL PLATFORM: VULNERATION TO INFORMATION PRIVACY

Aldrin Marcel Espín León[1]
Daisy Astrid Valdivieso Salazar[2]
Carlos Santiago Buenaño Armas[3]

Recibido: 2016-06-05 / **Revisado**: 2016-08-19 / **Aceptado**: 2016-10-20 / **Publicado**: 2017-01-01

Forma sugerida de citar: Espín-León, A. M., Valdivieso-Salazar, D. A. y Buenaño-Armas, C. S. (2017). Evaluación de Tipos de Client Side Exploits en una red LAN como plataforma experimental: Vulneración a la privacidad de información. *Retos de la Ciencia*, 1(1), pp. 20-35.

RESUMEN

A pesar que las tecnologías están en constante cambio, la falta de seguridad de la información sigue siendo un factor crítico. Los ataques a la seguridad en las organizaciones utilizando técnicas Client Side se han incrementado en los últimos años. Con el desarrollo y evolución de la ingeniería social las empresas son cada vez más vulnerables a sufrir este tipo de ataques, lo que ocasiona que el contenido que reciban no siempre sea beneficioso a sus intereses, sin darse cuenta que los usuarios internos pueden proporcionar las facilidades para que el atacante tengan éxito. Los resultados de este experimento realizado en un ambiente controlado evalúan la efectividad de los ataques efectuados y determina cómo influye la ingeniería social sobre los usuarios, puesto que dichas personas son las que contribuyen activa, pero inconscientemente con los intrusos. Haciendo una síntesis general del experimento, se demostró que los usuarios de una organización tienen mayor grado de confianza y accesibilidad a los archivos PDF que a las direcciones URL, cuando se utiliza correos electrónicos anónimos; de igual forma cuando se utiliza e-mails conocidos, los usuarios acceden de igual forma a los archivos PDF y las direcciones URL, siendo este el preferido de los atacantes.

Palabras Clave: vulnerabilidades, seguridad, ingeniería social.

[1] Magíster en Gerencia en Sistemas, Profesor Titular en la Universidad Central del Ecuador, Ecuador: E-mail: amespin@uce.edu.ec
[2] Doctora en Ciencias Internacionales, Profesora Titular en la Universidad Central del Ecuador, Ecuador: dagus36@yahoo.com
[3] Magíster en Ingeniería Industrial, Profesor Titular en la Universidad Central del Ecuador, Ecuador: sbuenanio@uce.edu.ec

ABSTRACT

Even though that technologies are changing constantly, the lack of information security continues being a critical factor. The organization's security attacks using Client Side techniques has been increasing in the last years. With the development and social engineering's evolution the companies are each time more vulnerable to suffer this kind of attacks which is causing that the content they get is not always useful to their interests, without being aware that internal users can provide the facilities to attacker's success. The results of this experiment which was done in a controlled environment assesses the effectiveness of the performed attacks and determines how social engineering influence over users, because people are who actively but unconsciously contribute with intruders. In summary it has been demonstrated that organizations users have more confidence and accessibility to PDF files than to URL addresses when anonym emails are used, in the same way when known emails are used the users access in the same way to PDF files than URL addresses, being this the preferred one by the attackers.

Keywords: vulnerabilities, security, social engineering.

INTRODUCCIÓN

El presente trabajo surge como consecuencia del gran interés por la seguridad informática y la dependencia de Servidores que proveen los servicios con los cuales las aplicaciones cliente puedan interactuar. Estos servicios son accesibles por parte de los clientes que deseen hacer uso de ellos, lo que los expone a diversas vulnerabilidades que pueden ser atacados. En la actualidad, una de las técnicas de ataque más frecuentes que logro captar total atención de la comunidad científica y que está tomando cada vez más fuerza es: Client Side Attacks; que a través del envío de direcciones URL o de **archivos PDF** maliciosos permite al atacante tomar control sobre el sistema de la víctima.

Con los "exploit del lado del cliente", se evalúa los accesos que tiene el cliente para determinar el grado de desconfianza que tiene un usuario al acceder a una dirección web o abrir un archivo, el cual proporciona al atacante información necesaria para delinquir o poder acceder a la terminal. La experimentación se lo realizó utilizando dos tipos de ataque: a través del envío de una dirección URL y del envió de un archivo PDF malicioso, utilizando ingeniería social, la cual trata de engañar, distraer y manipular las mentes y acciones de un colectivo de personas de forma sutil para obtener información necesaria para un ataque [1]

Para la detección y prevención de los ataques client-side, en el 2012 Syed Inran Ahmed Qadri [16] en base al análisis de los ataques, crea un framework de seguridad para los ataques del lado del cliente y de servidor, además proporciona algunos métodos de prevención, los cuales se aplicarán para el lado del servidor y replicaciones de alerta en el lado del cliente, esto actúa sobre archivos embebidos con direcciones web maliciosas, contenidos JavaScript o simplemente archivos HTML, en este framework el cliente accede a sus datos que están encriptados desde el lado del servidor.

Como resultados del experimento se evidenció que las debilidades explotadas no son nuevas, sino que lo nuevo es la manera de llevarlas a la práctica de una forma creativa e innovadora, la misma que se puede evidenciar en los distintos

temas tratados en este documento. Por otro lado, en cada sección temática se encontrará una línea de investigación clara y definida, que permite apreciar la metodología aplicada y elementos que confirman este tipo de experimento. Es así que la distribución del presente documento es la siguiente: Fundamento teórico, configuración del experimento, análisis de datos, conclusiones, trabajo futuro y bibliografía.

Un gran porcentaje de exploits del lado del cliente día a día están apareciendo relacionados con software de escritorio, los cuales se utilizan para realizar ataques a los ordenadores personales del cliente, estos pueden utilizarse como pívot y acceder a otros equipos de la red local “LAN” que no son accesibles desde internet. [3] . Según CVE-Details, Oracle sufrió unas 2581 vulnerabilidades en los distintos software que posee y ya para el año 2015 lleva 114 [4] .

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entries) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. [5] .

Exploit del lado del Cliente

Tiene como objetivo explotar la vulnerabilidad en el lado del cliente, aprovechando de las debilidades de uno de los equipos más débiles en la cadena de la seguridad de la información, como lo es el “usuario final”. Las fases de un ataque que un delincuente informático utiliza para explotar las diversas vulnerabilidades en los sistemas de usuarios finales son:

1. Reconocimiento. El atacante obtiene toda la información de la víctima antes de realizar el ataque o escaneo de la red, es cuando se crea una estrategia para su ataque. Dentro de esta fase se pueden aplicar diversos métodos de obtención de información por ejemplo: Ingeniería Social, puertos abiertos, routers que utilizan la red, host más vulnerables de la red; esta fase puede tomar mucho tiempo, pero para el atacante puede “garantizar un éxito”. Para realizar el test se intenta recopilar la mayor cantidad de información posible, para ello se utiliza Internic, IANA/RIPE, Whois (herramienta para footprinting y reconocimiento: http://www.allwhois.com/), Google/ Usenet, páginas privadas de empleados, direcciones de correo electrónico, números de teléfono. Por ejemplo para conocer información sobre el URL xxx.com se utiliza: http://reports. internic.net/cgi/whois?whois_nic=xxx.com&type=domain.[6] .
2. Escaneo. En esta fase el atacante utiliza la información que obtuvo en la primera fase de reconocimiento para identificar vulnerabilidades específicas, se puede identificar el sistema operativo que utiliza la víctima además se pueden escanear puertos y utilizar herramientas automatizadas para poder vulnerar dichos puertos. Se utilizan técnicas como:

(i) Quering System e información de DNS. Se pueden utilizar:

(a) TraceRoute. Especifica la ruta de red, da información acerca del proveedor y del tipo de conexión que puede ser simple, redundante o con

carga balanceada, también permite saber en qué salto o hop el ICMP[4] se bloquea.

(b) Transferencia de Zona DNS. El servidor DNS debería configurarse para no permitir Transferencias de Zona salvo a correspondientes específicos. Las Zonas DNS nos dicen qué máquinas existen en la Zona y se obtiene información acerca de la estructura de la red IP. Se utiliza nslookup.

(ii) Exploración de puertos y Fingerprinting. El escaneo de puertos da información acerca de que puertos escucha una máquina. Cada puerto abierto es potencialmente vulnerable. Scaners más avanzados descubren la clase de software del sistema operativo está instalada (fabricante y versión). Los scanners más populares son SuperSacan y Nmap. También se puede conectar con NetCat[5] o Telnet a un servicio para obtener información detallada, esta técnica se denomina "banner grabbing".

(iii) Exploración y explotación de vulnerabilidades. Se pueden utilizar scanners automatizados que dan más información para investigar las vulnerabilidades. Existen en Internet bases de datos de vulnerabilidades y exploits: (a) SecurityFocus (http://www. securityfocus.com/bid/vendor). (b) Packet Store (http://packetstormsecurity.org). Entre los scanner de puertos más populares están: Nmap (http://www.insecure.org/nmap) y SuperScan (http://www.foundstone. com).

3. Ganar y mantener el acceso. El atacante explota las vulnerabilidades encontrada en la fase de escaneo. La explotación puede ocurrir en forma local o de forma remota por medio de Internet y puede incluir técnicas como denegación de servicios, desbordamiento de buffer, y romper claves de seguridad o acceso. El atacante usa sus propios conocimientos en informática y redes, usa el sistema objetivo como plataforma de ataque, puede tener además la habilidad de subir, alterar programas o datos. En esta fase el hacker desea ser indetectable y para eso elimina evidencia de su seguridad al sistema y utiliza métodos como puertas traseras

4. Cubrir las huellas. En esta fase el atacante elimina toda evidencia de sus accesos realizados a equipos con eso puede seguir manteniendo el acceso al sistema víctima. Las herramientas y técnicas que usa para esto suelen ser caballos de Troya, Steganography, Tunneling, Rootkits y la alteración de los "log files"[6]

Los ataques de lado de cliente presentan facilidades, porque la mayor atención en las tecnologías de protección actualmente se enfoca más de servidores expuestos a ataques remotos. Los clientes están protegidos en entornos donde el acceso de clientes internos a servidores en el Internet está restringido por técnicas de defensa tradicional como firewalls o proxies, sin

[4] ICPM, Es un protocolo de control de mensajes en internet con número STD 5, comunica errores e información entre sistemas principales. La aplicación PING utiliza funciones de eco y respuesta de eco de ICMP y nos ofrece una manera fácil de determinar si se puede llegar a un equipo mediante una dirección de la red

[5] http:// www.atstake.com/research/ tools/network_utilities /nc11nt.zip

[6] Archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios

embargo, un firewall, a menos que se combine con otras tecnologías como IPS, solamente restringe el tráfico de la red, una vez que el tráfico está permitido, un cliente interactuando con un servidor está en riesgo, existen también soluciones de filtrado corporativas, pero estas típicamente solo protegen un conjunto de tecnologías cliente. [7]

La explotación de las vulnerabilidades busca casi siempre introducir un pedazo de código en la máquina de la víctima, de modo que se pueda lograr un objetivo de ataque a largo plazo, en la actualidad existen un sinnúmero de código malicioso instalado a través de exploits para navegador, incluyendo virus que infectan archivos, puertas traseras que abren puntos de entrada para un acceso no autorizado futuro, en ambos casos lo que se busca es obtener el control de la red comprometiendo los sistemas que puedan ser vulnerables al ataque. [8]

Metodologías de Ataque usando sitios web Maliciosos

Un sitio web que expone al menos un exploit, es llamado un sitio web malicioso, dichos web site realizan ataques en contra de los usuarios en 4 fases: Ofuscación, Configuración del sitio web malicioso, Engaño a la víctima, y Control de la máquina de la víctima. [9] .

i. **Ofuscación** El atacante oculta el exploit usando varias opciones de encriptamiento, para hacer que el código sea difícil de interpretar, esta técnica apunta a evadir las herramientas estáticas de detección como IDS, herramientas anti virus, y filtros de firewall. El atacante usa el código del exploit en JavaScript y VBscript que sea ilegible en el transporte desde el servidor web al navegador del cliente, el atacante usa múltiple capas para codificar el código lo que lo hace difícil de decodificar.

ii. **Configuración del servidor web malicioso.** El atacante crea una red de sitios web maliciosos, los cuales no hospedan el código de ataque directamente, en su lugar el código del exploit es importado en la página que es expuesta al usuario usando iframes, o el usuario es redireccionado al código del ataque. Los atacantes intentan explotar los sitios web insertando un iframe o un script de redireccionamiento, el código del ataque contiene referencias a un servidor de malware donde una variación de malware está alojado, luego de que el código del exploit ha sido ejecutado por una aplicación del cliente, automáticamente se descarga e instala el malware.

iii. **Engaño a la víctima.** Una vez que el sitio malicioso está listo, el atacante debe incitar o tentar a las víctimas para visitarlo usando técnicas de ingeniería social o usando mensajes instantáneos, emails masivos, redes sociales, etc.

iv. **Control de la máquina de la víctima.** Luego que el cliente visita el sitio malicioso y el sistema es explotado, el atacante usualmente quiere el control del sistema del cliente, una manera de lograr este propósito es mediante una descarga guiada donde los servidores pueden cambiar el estado de un cliente, sin su consentimiento, lo que significa que un servidor malicioso descarga e instala un programa en el sistema del cliente sin que éste se entere, y puede ser mediante la instalación de malware, proxy, key-logger, objetos de ayuda de navegador y varios tipos de adware.

Configuración del Experimento

a. Herramientas

Para la implementación del experimento se utilizó diferentes herramientas, las mismas que se detallan a continuación:

1. **Sistema de virtualización:** Se utilizó Oracle VM Virtual Box, para configurar varias máquinas virtuales interconectadas entre sí, implementando un escenario virtual de red.
2. **Firewall:** En las máquinas cliente se utilizó el firewall propio de Microsoft Windows.
3. **Kali Linux:**
   a. Línea de Comandos (msfcli): Se ejecutó metasploit como parte de un script externo.
   b. Consola Interactiva (msfconsole): Básicamente se ejecutó el framework, y se obtuvo una línea de comandos donde se seleccionó los exploits que se ejecutaron, el payload, las opciones y se lanzó el ataque.
   c. Interfaz Gráfica de Usuario (msfgui): Es atractiva, rápida e intuitiva y se consideró por sobre la versión de la consola.
   d. Aplicación Web (msfweb): Cómoda y versátil manera de ejecutar Metasploit en forma remota o local, sólo se apuntó un navegador a su Servidor Web y Aplicación embebidos.
4. **Herramienta para envío del link para interactuar con el servidor malicioso:** se utilizó el correo electrónico para enviar el link que permita interactuar con el servidor malicioso.

b. Diseño de la Topología Experimental

Para efectos del presente caso la metodología que se planteó permitió definir un conjunto de reglas, prácticas, procedimientos y métodos a seguir e implementar durante la realización de cualquier programa de auditoría en seguridad de la información. Es importante indicar que al momento que se estableció una metodología de pruebas de penetración se definió una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales fueron manejadas cuidadosamente y, que permitió evaluar correctamente los sistemas de seguridad.

La metodología aplicada para el experimento fue la Prueba de Caja Gris, la misma que permitió al equipo de pruebas simular un ataque realizado por un miembro de la organización inconforme o descontento. El equipo de pruebas fue dotado con los privilegios adecuados a nivel de usuario y una cuenta de usuario, además de permitirle acceso a la red interna.

Desde dentro de la organización.- Si de alguna manera se obtuvo acceso desde dentro de la organización a los objetivos; es decir, teniendo por ejemplo el control de alguna estación de trabajo con o sin permiso, desde donde se accede al sistema vía red por ejemplo, las probabilidades de éxito aumentan considerablemente. No es casual que el 80% de los ataques exitosos provengan de una red interna al servicio que se compromete [HACK_BASICS]. La ventaja está dada en que el sistema debe permitir el acceso a este nodo, a diferencia de los que residen fuera de la red de la organización. Además de las posibilidades de obtener información del punto anterior, aquí las posibilidades se amplían sustancialmente, entre las más comunes se encuentran:

● Escuchar tráfico de otros componentes de la red.

● Acceso a la información del equipo y la que se encuentra disponible en volúmenes compartidos de la red: e-mails, documentos, contraseñas, listados de

usuarios, archivos, bases de datos, registros, cualquier dato que proporcione maneras de ingresar al sistema objetivo.

La red que se planteó para el Diseño Experimental es la comúnmente aplicada en empresas medianamente pequeñas y en producción. Se tomó como prototipo la empresa EQUILAR S.A ubicada en la Av. Bartolomé Álvarez 1252 y Bobonaza, Quito-Ecuador.

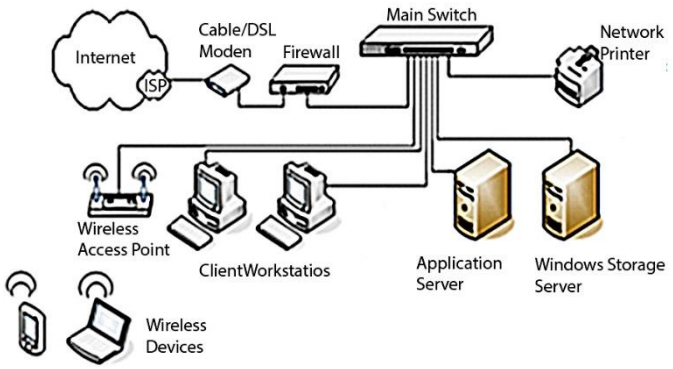

Fig. 1. Topología Experimental

La generación de ataques Social Engineering, utilizando Client Side Attacks (Ataques del Lado del Cliente) que para efectos de este caso se aplicaron los ataques tradicionales y servidores web maliciosos, requirieron de la creación de una infraestructura de red similar a la utilizada por la empresa anteriormente mencionada o a su vez cualquier red en producción. Fig. 1.

c. Implementación de plataforma experimental.

Para la realización del experimento, se configuró un archivo malicioso PDF y un servidor malicioso sobre el ordenador con Linux distribución Kali, una vez configurados y afinados los Client Side Attacks, se realizó un envío a través de dos correos electrónicos: a) Conocido “cuenta@dominio_victima.com”. b) Anónimo “cuenta@anónimo.com”. Dicho envío disponía de ciertas características como: archivo malicioso PDF y dirección URL maliciosa.

Es importante resaltar que los dos ataques tienen el mismo objetivo, y es tener acceso y control a la terminal de la víctima a través de la ingeniería social y la explotación de la vulnerabilidad de una aplicación que será ejecutada por el recurso humano.

Uno de los primeros ataques configurado es el archivo malicioso PDF, puesto que al ser uno de los Client Side tradicional y uno de los más documentados, se omite la descripción del mismo para dar lugar a unos de los ataques más efectivos en sus distintas aplicaciones “Client Side Attack Web Server Malicious”; el cual, a través del envío de una dirección URL permitió la interacción entre el servidor malicioso y las terminales de la red, alcanzando así la intrusión a las máquinas.

A continuación se detalla el procedimiento realizado respecto al ataque mencionado:

1.Se creó la máquina virtual utilizando el programa VirtualBox, en esta máquina se instaló Linux distribución Kali para que sea utilizado como el servidor malicioso, se configuraron las interfaces de red, y se procedió a configurarlo

utilizando la consola de metasploit, interactuando con los comandos de msfconsole, se procedió a cargar el exploit malicioso para que use las vulnerabilidades del navegador web, se configuró las opciones del meterpreter utilizando la IP del servidor en la misma y finalmente se procedió a levantar el servidor malicioso como se observa en la Fig. 2, con lo cual se obtuvo la URL que se debe enviar a las máquinas que van a ser atacadas, la cual aparece en la Fig. 3.

2. Se creó una máquina virtual utilizando el programa VirtualBox, en la cual se instaló el sistema operativo Windows 7 Enterprise Edition, se configuró la interfaz de red, se verificó que el firewall de Windows esté activo y que la máquina cuente con las más recientes actualizaciones.

3. Se creó una máquina virtual utilizando el programa VirtualBox, en la cual se instaló el sistema operativo Windows XP Professional, se verificó la configuración de red, se verificó que el firewall de Windows esté activo y que la máquina tenga las últimas actualizaciones.

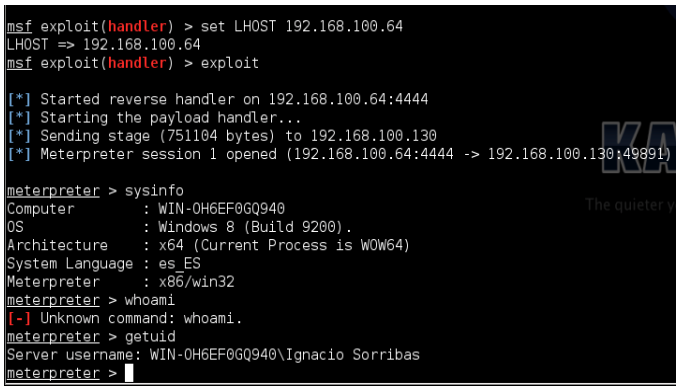

Fig. 2. Configuración de servidor malicioso

d. Generación de ataques.

La generación de Client Side Attacks (Ataque del lado del cliente) se realizó ejecutando ataques tradicionales y levantando un servidor web malicioso, con el objetivo de tener acceso y tomar control de una o varias máquinas víctima, explotando una vulnerabilidad de una aplicación que será ejecutada por el o los usuarios víctima (Windows XP y/o Windows 7). Las técnicas aplicadas consisten en crear e infectar un archivo malicioso "Ataque *Tradicional"* con el fin de obtener acceso a la computadora víctima ya sea por red LAN o WAN. Así mismo para el segundo caso "*Ataque mediante un Servidor Web Malicioso*" el cual consiste en configurar un servidor malicioso, con el objetivo de obtener el control de la computadora víctima, a través el envío de un link, el mismo que al ser pulsado por el o los usuarios víctimas, permitirá que el atacante obtenga acceso y pueda tomar el control de la máquina víctima.

El archivo malicioso PDF y el link generado a través del servidor web malicioso, fueron creados utilizando la herramienta Metasploit 4.9 que viene incorporada en Kali Linux 64 bit V. 1.1.0

Al utilizar una metodología de caja gris y disponer del esquema de red LAN y WAN se procedió con el ataque de la siguiente forma: Aplicando ingeniería social básica y levantando ciertos patrones repetitivos en la información disponible, se

obtuvo el listado de correos electrónicos de todo el personal, permitiendo así la ejecución de Client Side Attacks (Tradicional y servidor web malicioso). Dentro de la planificación del ataque se planteó dos tipos de vulnerabilidades: 1) Envío de archivo malicioso “PDF”. 2) Envío de una dirección URL desde servidor web malicioso. Ambos contienen exploits que permitirán el acceso y control de la terminal.

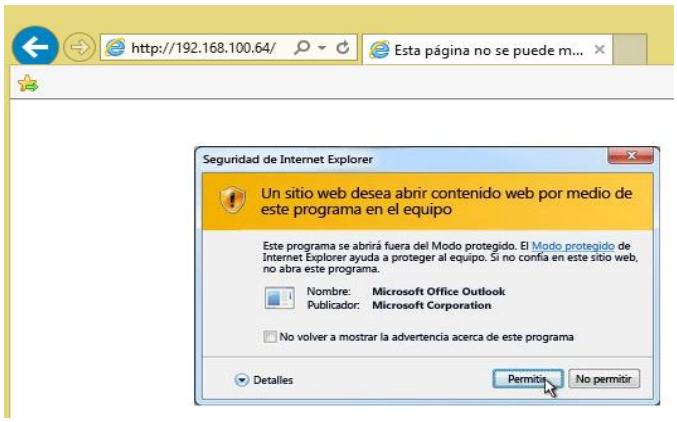

Fig. 3. Dirección URL del servidor

Los tipos de ataque fueron enviados desde una cuenta de correo conocida y otra cuenta anónima “*pero con sentido lógico hacia el negocio*”, para evitar un mayor número de repudio al mail. Es así que se enviaron a todos los correos electrónicos con el archivo infectado PDF y la URL que apunta a un servidor web malicioso en distinta fecha y horario.

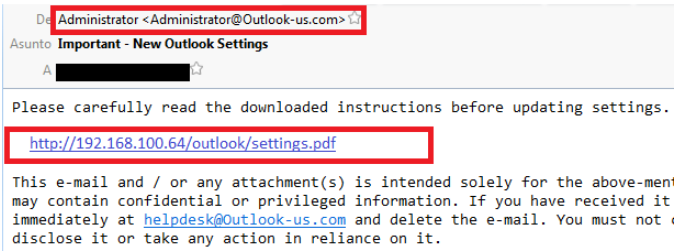

Fig. 4. Envío correo malicioso con URL del servidor

RESULTADOS

Basado en los 2 tipos de ataques efectuados, el propósito fue poder medir el grado de afectación, es decir, medir el número de clientes en los que el ataque pudo llegar a realizarse exitosamente, para lo cual se llevó a cabo un ataque controlado dentro de la red de la empresa EQUILAR S.A, a 20 usuarios de la red, de lo cual se obtuvieron los siguientes resultados:

CUADRO DE RESULTADOS						
No.	Tipo Ataque	Correo Electrónico	Correos Enviados	Fecha Envío	Correos Abiertos	Terminal(es) Atacado(s)
1	PDF Malicioso	Mail Conocido	20	Lunes	20	16
2	PDF Malicioso	Mail Anónimo	20	Miércoles	15	11
3	Link Malicioso	Mail Conocido	20	Viernes	20	15
4	Link Malicioso	Mail Anónimo	20	Martes	12	7
		Total	80	Total	67	49

DETALLE Y SIGNIFICADO DEL CUADRO DE RESULTADOS		
Tipo Ataque		
1	PDF Malicioso	Client Side Attack archivo malicioso
2	Link Malicioso	Client Side Attack servidor web malicioso

Correo Electrónico			
1	Conocido	gerencia@dominio.com	Servidor de correos habilitado puerto SFP
2	Desconocido	nombre_compania@dominio_falso.com	Envio a través de software Mini Relay

Correos Abiertos	Aquellos correos que han sido abiertos a través de un CLIK
Terminal(es) Atacado(s)	Aquella terminal que se logró tener acceso y control

Fig. 5. Cuadro de Resultados

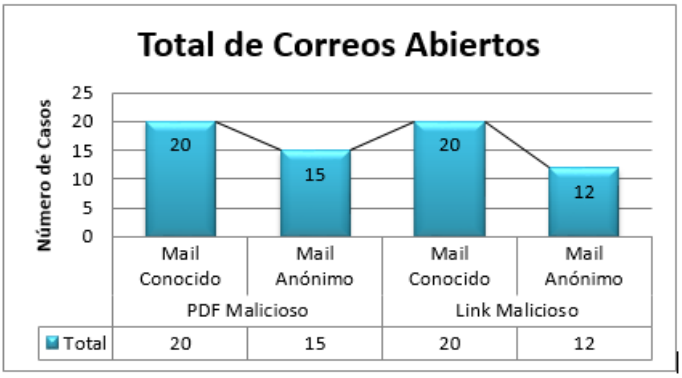

Fig. 6: Total de Correos Abiertos

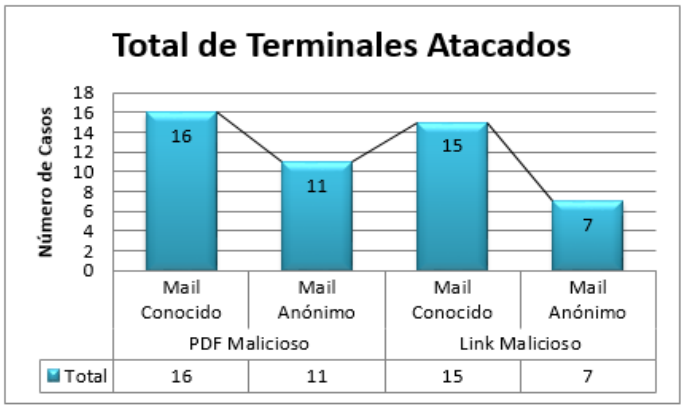

Fig. 7.: Total de Terminales Atacados

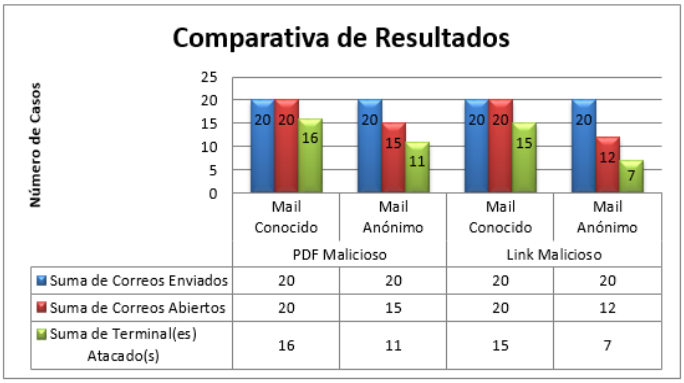

Fig. 8. Comparativa de Resultados

Trabajo relacionado

Con la diversificación del uso de la web, los ataques del lado del cliente, se han ido incrementando considerablemente, y de la misma manera, la investigación para entenderlos y combatirlos es también importante en el ámbito de las tecnologías de la información. Como se menciona en [2] las vulnerabilidades en los componentes client-side de las aplicaciones se han incrementado, lo cual resulta en un amplio espectro de ataques, a través de técnicas de análisis dinámico se estudió e implementó un prototipo de herramienta para descubrir este tipo de vulnerabilidades.

En el 2010, Hossain Shahriar [9] analiza los ataques client-side los cuales le permiten al atacante realizar actividades no autorizadas sin el conocimiento del usuario final. El ataque obtiene ventaja en el hecho de que el browser envía información en cada petición que realiza, por lo tanto es el primer lugar para observar síntomas de un ataque y poder tomar medidas para mitigarlo.

En el 2012, Usman Shaukat Qurashi [11] discute sobre ataques client-side basados en AJAX, el cual maneja las peticiones HTTP request, además del uso de scripts del lado del cliente, los cuales trabajan en múltiples diferentes capas, por lo que cada en cada capa se van agregando vulnerabilidades, se mencionan prácticas de seguridad que se enfocan en el aseguramiento de HTM a través del uso de las mejores prácticas. En [12] se analiza un tipo de ataque client-side

basado en la infección por la descarga de archivos, en el cual sin el consentimiento del usuario, cuando éste se descarga un programa, viene junto con este otro tipo de programa malicioso que se instala en el computador de la víctima y comienza a causar daño en el sistema operativo, en este paper se analiza un plugin para los navegadores, de modo tal que el archivo se envía a una zona segura en disco donde no puede ser ejecutado.

Los ataques del lado del cliente se analizan significativamente en [13] para emular el comportamiento de las aplicaciones de cliente en una red controlada, en la cual puede ser explotado el contenido de la web por los atacantes, usando análisis dinámico, se puede remover la ofuscación de varias páginas maliciosas, proporcionando para esto un framework modular para el estudio de páginas maliciosas y entender vulnerabilidades y ataques modernos.

No todas las investigaciones se basan solamente al contenido de las páginas web, en [14] se analiza el contenido de los correos usando Outlook Express a través de scripts externos para descubrir amenazas que pueden llegar a afectar a las víctimas mediante el uso del correo electrónico, se analiza un conjunto de operaciones ilegales, como cambios en el registro de Windows, creación de archivos o el tráfico de red específico que puede estar afectando a los usuarios.

Para la detección y prevención de los ataques client-side, en el 2012 Syed Inran Ahmed Qadri [15] en base al análisis de los ataques, crea un framework de seguridad para los ataques del lado del cliente y de servidor, además proporciona algunos métodos de prevención, los cuales se aplicarán para el lado del servidor y replicaciones de alerta en el lado del cliente, esto actúa sobre archivos embebidos con direcciones web maliciosas, contenidos JavaScript o simplemente archivos HTML, en este framework el cliente accede a sus datos que están encriptados desde el lado del servidor.

Como parte del análisis a los ataques client side, se analizan scripts en páginas web como una práctica común [16] para lo cual se refuerza el lado del cliente a través del uso de un framework, en los sitios web que lo utilizan, de modo tal que en base a las políticas aplicadas a los recursos web, se logra asegurar a los usuarios que acceden al contenido web. En [17] se analiza a través del historial de navegación de los usuarios, el uso de sitios web maliciosos, y como a través del acceso a los mismos se compromete la seguridad del usuario, sin el conocimiento del mismo, además se identifica que algunas medidas de seguridad fallan al prevenir este tipo de ataque client side. Para que un ataque client side llegue a perpetrarse la comunicación de datos entre el cliente y el servidor es fundamental como se menciona en [18] y es exactamente ahí donde reside el peligro de que los atacantes puedan agregar contenido malicioso, para mitigar esto se plantea el uso de diferentes técnicas como el sniffing de contenido para la detección de ataques.

Las herramientas que pueden ser usadas para la realización de los ataques client side, además de las que se analizan en el presente paper pueden ser: hojas de estilo (CSS), en combinación con otras técnicas como HTML plano, imágenes SVG inactivas o archivos fuente, a estos se los llama scriptless attacks y se los analiza a detalle en [19] .

Una forma más avanzada de ataques client side se analiza en [20] donde el propósito es primeramente robar las credenciales de los usuarios para luego redireccionarlos a un sitio fraudulento usando técnicas basadas en DNS, y haciendo el ataque imperceptible para el usuario. La cual difiere con el presente trabajo, por el tipo de ataque que se realiza y por la forma en la que a través del

uso de la ingeniería social, se crea un escenario en el cual los usuarios finales ni siquiera sospechan que estén siendo víctimas de un ataque informático que puede comprometer seriamente la información que usan.

DISCUSIÓN

De los resultados obtenidos se pudo concluir que el ataque que logró mayor efectividad al contaminar a un número mayor de máquinas de los usuarios, fue en el que se envió el archivo PDF malicioso, como se observa en la Fig. 8, ya que a través de la ingeniería social y de la construcción de un mensaje de correo electrónico que despierte algún interés o inquietud en los usuarios, se podrá conseguir que ellos al abrirlo contribuyan inconscientemente a que el ataque sea exitoso.

Es importante mencionar que sí existen mecanismos de defensa para que el ataque no llegue a concretarse, es así que del número de usuarios que abrieron el mensaje de correo enviado, no en todos los casos fue posible obtener el acceso a sus máquinas a través del ataque, esto se evidencia en la Fig. 6 y Fig. 7, y esto se debe básicamente a las medidas de seguridad que cada uno de los usuarios tengan en sus máquinas, además de poseer en ellas las más recientes actualizaciones liberadas por parte de la empresa que comercializa el sistema operativo.

Por otro lado, se pudo evidenciar que los usuarios tienen un mayor grado de confianza para abrir correos electrónicos de remitentes conocidos, lo cual se puede comprobar en la Fig. 5, lo cual se puede constatar en la tabla de resultados, esto es un punto a favor importante para la seguridad, ya que en la actualidad el correo electrónico no deseado o spam, circula con una frecuencia significativa con todo tipo de ofertas, promociones e información para los usuarios, por esto mientras menos de estos correos desconocidos se lleguen a abrir, existirá un menor riesgo de que su contenido tenga algún tipo de código malicioso que busque atacar a los usuarios.

La ingeniería social va más allá de los conocimientos técnicos, por esta razón es una grave amenaza que puede ocasionar enormes pérdidas sin precedentes, ya sea a grandes o pequeñas empresas e igualmente a cualquier persona. No se puede afirmar que el hecho de tener una buena estructura tecnológica garantiza la seguridad informática. Por esta razón se debe disminuir el riesgo de ser víctimas de la ingeniería social, teniendo claro que es fundamental la capacitación del usuario ya que el desconocimiento de este tema es la mayor ventaja que tiene el atacante, y puede ser contrarrestada creando conciencia sobre los riesgos y daños potenciales frente a estos ataques.

CONCLUSIONES

La falta de creación y cumplimiento de políticas de seguridad, educación y prevención de los usuarios y la no actualización de software, son algunos de los motivos que hacen vulnerable un sistema de información, pero en gran medida el elemento humano es el más crítico ya que este constituye uno de los problemas más importantes de toda organización, puesto que tiene la capacidad de decidir voluntaria o involuntariamente, romper las reglas y normas impartidas en las políticas de seguridad, permitiéndole a un atacante obtener información y

acceder a un sistema informático eludiendo los mecanismos y las tecnologías de seguridad aplicadas. Un gran número de personas del experimento realizado, fueron vulnerables a la ingeniería social, utilizando como medio de acceso direcciones de correos electrónicos anónimos y conocidos con el objetivo de enviar un archivo malicioso o una dirección web.

El acceso a archivos PDF o a direcciones URL por parte del usuario sin verificar su procedencia, ayuda a los atacantes a ingresar a las terminales para obtener acceso o control de la misma. Es así que la falta de capacitación al personal permitió demostrar que los usuarios de una organización tienen mayor grado de confianza y accesibilidad a los archivos PDF que a las direcciones URL, cuando se utiliza correos electrónicos anónimos; de igual forma cuando se utiliza e-mails conocidos, los usuarios acceden de igual forma a los archivos PDF y las direcciones URL, siendo este el preferido de los atacantes. La ingeniería social es asunto de extremado cuidado, no existe sistema informático que no dependa de algún dato ingresado por un usuario, se puede decir que la mejor manera de estar protegido contra la ingeniería social y sus técnicas, es el conocimiento.

TRABAJO FUTURO

Como las protecciones de los clientes a los accesos de malware por medio de su servicio web son relativamente débiles y, los atacantes están aplicando varias técnicas de acceso malicioso, siendo una de ellas por medio de correos electrónicos y mensajería, se debería intensificar estudios sobre detección de códigos maliciosos a través de exploit mediante servidores web, controles y seguridades aplicando ingeniería social, trabajos e investigaciones que apunten a que herramientas estáticas de detección como IDS, herramientas anti virus, y filtros de firewall detecten códigos encriptados y poder mitigar los accesos que no tengan consentimiento de la víctima. Accesos a los servidores empresariales por medio de usuarios en redes LAN que no tiene protección y están expuestas a código malicioso.

Realizar estudios sobre la cultura informática que tienen los usuarios especialmente en las tecnologías de redes sociales y mensajería en la actitud y la resistencia que deben tener ante la tentación de acceder a un file o dirección sospechosa.

Un escenario futuro para fortalecer un sistema informático estará en el empoderamiento y capacitación a los usuarios/as, sobre los riesgos de manipulación en la información, fortalecer su capacidad de prevención teniendo una conciencia crítica que permita al usuario determinar una posible violación a la seguridad del sistema a través de spam, ficheros o URL's enviadas a sus cuentas personales, actos que carentes de ética y de respeto por el ser humano y por la propiedad privada, transformado la utilidad científica objetivo fundamental de la informática.

Actualmente la tecnología aplicada a la informática, telemática, telecomunicaciones, es considera una de las formas de inter relacionamiento directo con la sociedad ya sea a través de internet mediante el uso de redes sociales, sitios web para realizar transacciones en línea o simplemente para conocer las actividades de una organización; o, utilizado para el desarrollo de sistemas informáticos que faciliten el manejo y control de una organización, ésta

debe responder a la demanda del conocimiento que hace posible que el enfoque social se fusione en su concepción desde parámetros del fortalecimiento de la ética en el ejercicio personal y profesional y el respeto por el derecho a la privacidad, además de la seguridad personal que cada usuario debe mantener hacia sus datos, factores que limiten el mal uso de la información contenida en los sistemas y se prevenga la transgresión de la norma que se convierta en un delito contra la seguridad de los activos de los sistemas de información y comunicación establecidos en el Código Orgánico Integral Penal (COIP) el cual establece penas de privación de la libertad con lo que se intenta castigar a la persona que hizo un mal uso de la tecnología en beneficio propio, sin embargo se está dejando de un lado algo muy importante como la capacitación a los usuarios y las medidas de seguridad informática aplicadas a las empresas factores que permitirán una disminución drástica de los ataques a los sistemas.

La utilización de la web 3.0 con las redes sociales en los lugares de trabajo está provocando que gran cantidad de empresas consideren a la seguridad de información online en alta prioridad sobre la cual investigar, para mantener la relación clientes - usuarios protegiendo el servicio que se brinda, y no detenerse en la evolución informática de acceso a servicios en línea o en la nube. Estudios para la implementación generalizada de dispositivos llamados tokens para identificar a los usuarios cuando acceden a la empresa en forma remota. Un token genera un código aleatorio, único y distinto que deben ingresar con su nombre de usuario y contraseña. De esta manera el servidor determina que se trata del empleado correcto porque conoce su usuario y contraseña, y porque tiene presente el token que lo identifica. Es así como el servidor empresarial identifica al empleado de dos formas: por lo que conoce y por lo que tiene.

Como trabajo futuro se plantea realizar el análisis de dispositivos llamados tokens y la aplicación de filtros de firewall que detecten códigos encriptados, con el fin de mitigar los ataques a una red corporativa mediante ingeniería social.

REFERENCIAS BIBLIOGRÁFICAS

[1] Areitio, Javier; Areitio Ana, Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red, 2009

[2] Detecting Malicious Web Servers with Honeyclients - Mahmoud T. Qassrawi, Hongli Zhang, disponible en: http://www.ojs.academypublisher.com/index.php/jnw/article/viewFile/0601145152/2559

[3] Sorribas, Ignacio http://es.linkedin.com/in/nachosorribas, http://www.at4sec.com

[4] *Un Informatico en el lado del mal*. (11 de 2014). Recuperado el 06 de 02 de 2015, de Un Informatico en el lado del mal: http://www.elladodelmal.com/2014/11/shellshock-client-side-scripting-attack.html

[5] http://www.cvedetails.com/vendor/93/Oracle.html

[6] Areitio, Javier Dr, ; Areitio Ana Dra., Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red, tomado de http://www.redeweb.com/_txt/653/36.PDF

[7] C. Seifert, R. Steenson, T. Holz, Y. Bing, and M. A. Davis, “Know your enemy: Malicious web servers.” The Honeynet Project, 2007, http://www.honeynet.org/papers/mws/

[8] Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities disponible en:http://research.microsoft.com/en-us/um/redmond/projects/strider/honeymonkey/NDSS_2006_HoneyMonkey_Wang_Y_camera-ready.PDF

[9] FLAX: Systematic Discovery of Client-side Validation Vulnerabilities in Rich Web ApplicationsPrateek Saxena§ Steve Hanna§ Pongsin Poosankam‡§ Dawn Song§ {prateeks, sch,ppoosank,dawnsong}@eecs.berkeley.edu §University of California, Berkeley ‡Carnegie Mellon University

[10] Hossain Shahriar and Mohammad Zulkernine, "Client-Side Detection of Cross-Site Request Forgery Attacks", 2010 IEEE 21st International Symposium on Software Reliability Engineering.

[11] Usman Shaukat Qurashi, Zahid Anwar, "AJAX Based Attacks: Exploiting Web 2.0", IEEE 2012.

[12] BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections Long Lu† Vinod Yegneswaran‡ Phillip Porras‡ Wenke Lee††College of Computing, Georgia Institute of Technology ‡SRI International {long, wenke}@cc.gatech.edu {vinod, porras}@csl.sri.com

[13] PhoneyC: A Virtual Client Honeypot Jose Nazario jose@monkey.org April 1, 2009

[14] J. Rocaspana. SHELIA: A Client HoneyPot for Client-ide Attack Detection, 2009. http://www.cs.vu.nl/˜herbertb/misc/shelia/.

[15] Syed Imran Ahmed Qadri, Prof. Kiran Pandey, "Tag Based Client Side Detection of Content Sniffing Attacks with File Encryption and File Splitter Technique", International Journal of Advanced Computer Research (IJACR), Volume-2, Number-3, Issue-5, September-2012.

[16] JSand: Complete Client-Side Sandboxing of Third-Party JavaScript without Browser Modifications Pieter Agten†, Steven Van Acker†, Yoran Brondsema†, Phu H. Phung‡, Lieven Chalmers University of Technology, Gothenburg, Sweden

[17] Timing Attacks on Web Privacy Edward W. Felten and Michael A. Schneider Secure Internet Programming Laboratory Department of Computer Science Princeton University Princeton, NJ 08544 USA

[18] International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-2 Issue-10 June-2013 7 Content Sniffing Attack Detection in Client and Server Side: A Survey Bhupendra Singh Thakur1, Sapna Chaudhary2

[19] Scriptless Attacks – Stealing the Pie Without Touching the Sill Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk Horst Görtz Institute for IT-Security Ruhr-University Bochum, Germany

[20] A dual approach to detect pharming attacks at the client-side Sophie Gastellier-Prevost, Gustavo Gonzalez Granadillo, and Maryline Laurent