

“Sentencia de muerte a los Firewall”.

(por: Alejandro Corletti)

acorletti@wanadoo.es — acorletti@hotmail.com

1. Introducción:

Cuando nacen los primeros sistemas informáticos que emplean la interconexión de computadoras en red, era poco imaginable el potencial peligro que esto implicaba, al comenzar a interconectarse redes entre sí, se inició la era de la seguridad pero inicialmente a través de contraseñas para el acceso a los recursos de los equipos que físicamente podían ser alcanzados. El detonante de la seguridad es si duda Internet, a través de la cual, millones de personas se encuentran analizando día a día mejores técnicas para descubrir y aprovechar las vulnerabilidades de los sistemas que pueden alcanzarse en esta red mundial. Muchos organismos se encuentran estudiando a estas personas, las cuales en muchos casos lo hacen por investigación (realizando acciones muchas veces en los límites de la ley), pero fuera de estas, todo el resto operan ILEGALMENTE. La falta real de protección legal en virtud del anonimato y la dispersión mundial de esta gente, genera que las víctimas comiencen con sus propias técnicas de autoprotección, al igual que en un barrio, ciudad o País donde reina el caos y los vecinos montan en armas. Justamente aquí es donde radica el primer desconcepto: ante un delincuente, uno se defiende o protege; pero ante una fuerza atacante, organizada y con un enorme poderío, uno se enfrenta o se rinde. La actividad de Hacking, intrusión, penetración de sistemas, monitoreo de tráfico, scanneo de sistemas, finger printing, o cualquier indeseable fenómeno de este tipo, no debe ser pensada como realizada por un delincuente, sino por un adversario, términos que difieren radicalmente en el plan de reacción que se desee adoptar. El adversario se lo trata y se lo combate con técnicas militares que poseen experiencia milenaria en enfrentamientos de fuerzas. Sobre estos enfrentamientos podrán cambiar las herramientas y las técnicas, pero la estrategia y las metodologías a seguir se van mejorando a lo largo de la historia y no pueden ser dejadas a un lado, sino que vale la pena poder aprovechar parte de la misma.

2. La Guerra electrónica:

Al descubrirse las ondas Hertzianas hace más de un siglo, comienzan a emplearse para transmitir información y avanzan en forma acelerada, incrementándose notablemente su crecimiento a fines del siglo XX. La facilidad que ofrecen de obtener información al instante independientemente de la distancia las posicionan en un nivel protagónico en todos los ámbitos empresariales, al igual que en la actualidad está sucediendo con Internet pero hace varios años. Se transforman en un instrumento de poder, dejando fuera de mercado a las empresas que no contaban con medios de comunicación ágiles. Al igual que ahora, comienzan a descubrirse facilidades que mal empleadas permitían acceder a la información ajena, obteniendo una ventaja competitiva. En el ámbito militar, este nuevo descubrimiento cambia las técnicas de la guerra (no las estrategias), pues ahora se puede conducir y coordinar esfuerzos muy distantes y controlar la evolución de las operaciones. Se empieza a incluir esta nueva terminología electrónica en las ordenes militares. Se analizan las nuevas vulnerabilidades que ahora se presentan y nace un nuevo concepto de guerra “La guerra electrónica”. Se empieza a hablar de Interferencia, escucha electrónica, triangulación, detección electrónica, radiolocalización, saltos de frecuencia, multitono discreto (una de las bases del hoy ADSL), paquet radio (uno de los precursores del actual GPRS), barrido de frecuencias, radares, etc. Es interesante hasta asociarlo, pues antes de esto, al arma de Infantería se la consideraba la “Reina de las Batallas”, pues era la que en último término conquistaba el terreno (llegaba

materialmente); en lo personal aprecio que este noble título hoy es abdicado a esta nueva guerra, y lo demuestran todos los últimos conflictos donde las fuerzas tecnológicamente equipadas, casi no tienen bajas ni le ven la cara al enemigo.

Hoy, cualquier empresa de magnitud que emplee seriamente sus sistemas de comunicaciones, hace uso de técnicas de guerra electrónica con mayor o menor grado de similitud a las militares.

3. La Guerra Teleinformática:

Para no ser extenso con una historia que se repite en forma muy similar a la desarrollada en el apartado anterior y que todos conocemos o estamos viviendo, simplemente pido que en este momento reflexionemos sobre la situación de este ámbito, en el cual no me refiero sólo al concepto de informática, sino a su integración con las telecomunicaciones:

- La teleinformática creció en estos últimos 15 años de manera análoga a lo que fueron las comunicaciones durante todo el siglo pasado, o más aún.
- Las Empresas dependen en forma incondicional de este medio.
- La teleinformática gobierna todos los sistemas del planeta (y alrededores), sistemas de comunicación, de energía, satélites, centrales nucleares, torres de control aéreo, sistemas de difusión, de cultivos, sistemas de defensa, sistemas, sistemas, sistemas.....
- La complejidad de los sistemas es cada vez mayor.
- Nuevas vulnerabilidades aparecen a diario.
- Aunque aún no es del todo público, ya existe terminología sobre la llamada **“guerra informática o teleinformática”**, lo cual no debería sorprender a nadie, mucho menos en estos momentos de terrorismo.

4. Los Firewalls:

A esta altura ya se estarán preguntando ¿Qué tiene que ver este texto con los Firewall?

Todo lo anterior está íntimamente relacionado con esta sentencia de muerte que vislumbro en estos dispositivos, principalmente por dos razones:

- a. La seguridad de un sistema informático no es una defensa ante delincuentes, es una batalla a ganar o perder.
- b. La historia militar demuestra que las “murallas no sirvieron”.

En el primer punto ya no se puede disociar a un intruso con el concepto de “Enemigo” de las operaciones militares, pues como se trató de aclarar anteriormente, en la actualidad se trata de una fuerza inmensamente superior a la que administra un sistema informático, es desconocida, tiene mayores capacidades y tiempo para analizar técnicas o actualizarse sobre bugs, exploits o vulnerabilidades. El “arte de la guerra” para los conductores es prácticamente un desafío de inteligencia e imaginación, y la historia militar está plagada de ejemplos en los cuales en total inferioridad de condiciones, se logró el triunfo en base a ese juego de engaños, creatividad e inteligencia. Tanto es así que todos los ejercicios de conducción de operaciones militares se llaman “Juegos de guerra”, pues las dos partes intervinientes hacen uso de estas elaboraciones intelectuales para obtener las ventajas sobre las cuales pueda ganar la partida.

En cuanto al segundo punto, se puede decir que durante los primeros siglos de la era cristiana, los pueblos desarrollaban sus defensas construyendo obstáculos que impidan el pasaje de sus atacantes, el obstáculo más poderoso de esa época fue la muralla. Con el descubrimiento de la pólvora, comenzó la “carrera armamentista de la edad media”, pues con el empleo de los cañones, rompían

las murallas. Como contramedida, se construían murallas más grandes, luego aparecían cañones más potentes, murallas más gruesas, cañones más grandes,.....Se firmó una implícita sentencia de muerte.....Las murallas hoy son patrimonio histórico de la humanidad.

5. CONCLUSION:

Ahora sí, tratemos de unir estos dos últimos conceptos.

Los sistemas informáticos actuales, al aparecer Internet, comienzan a ser blanco de ataques (que insisto, a mi juicio no son simples ladrones). La primera herramienta defensiva que sale al mercado es esta muralla llamada, que hasta su nombre la define así "Firewall". Quizás en su inicio puede haber sido efectiva, pero de la misma forma que las murallas anteriores, aparecen formas de romperlas (la NO casualidad hace que justamente una de sus vulnerabilidades se llame Troyano). La forma de defensa de los firewall es que ante una nueva vulnerabilidad, se genera una nueva regla que impide su paso, aparece una nueva vulnerabilidad, una nueva regla, una nueva.....¿Podrá seguir esta historia o ya conocemos como termina?.

Hoy en día ya existen metodologías mucho más eficientes que las murallas, se trata de Sistemas de detección de intrusiones (que reconozco no son ninguna maravilla), Sistemas de monitoreo de tráfico con sus correspondientes alarmas, Honey pots (también llamadas zonas o servidores de sacrificio), listas de control de acceso, el viejo Proxy que sigue en vigencia, etc.

Cómo veo el futuro muy próximo de la seguridad en redes:

- Sin Firewall (en la actualidad el único sentido que les puedo encontrar es a través del análisis de contenidos pero es un cuello de botella que pocos sistemas podrán soportar), considero que su función será reemplazada o asumida por las interfaces de acceso a las distintas zonas del sistema como ya se está haciendo con ACL. Cabe aclarar también que algo novedoso es la posibilidad de creación de reglas "Inteligentes" a través de correlación de eventos que permiten tomar decisiones al Firewall (una nueva moda de los mismos); si se trata de "tomar decisiones inteligentes", apuesto doble contra sencillo hacia los intrusos Vs. los Firewalls, pues no me cabe la menor duda que estas decisiones serán aprovechadas para crear condiciones favorables al intruso, sino fuera así ya deberíamos estar reconociendo la capacidad creadora de las máquinas sobre los humanos.
- Con análisis de contenido en los mismos servidores, que serán quienes en definitiva deberán realizar las operaciones de fragmentación y reensamble y el posible análisis del mal empleo de Unicode.
- Con muy buenas listas de control de acceso en Proxy, access servers y routers, (por favor no se mal interprete) pero con mucho, ¡pero mucho! conocimiento de protocolos de comunicaciones de los administradores a nivel bit de encabezados y campos permitidos o no por las RFC correspondientes.
- Con muy buenos sistemas de alarmas ajustados a cada organización y zona en particular, que permitan la detección temprana de todo intruso que se haga presente, pues se debe tener la certeza que estos accesos tarde o temprano sucederán (pues las murallas quedaron en la edad media).
- Planificando la seguridad de los sistemas, no como una defensa (este es el motivo particular de mi tesis "Estrategia de seguridad informática por Acción Retardante"), sino como un desafío contra un enemigo muy superior al cual sólo se podrá derrotar si se determinan las causas que produjeron esa intrusión. Estas causas no se obtienen gratis, se deberá estar en capacidad de "Jugar con fuego". Estas acciones serán el gran desafío de creatividad, engaño, imaginación, riesgo, voluntad, etc. En concreto, se deberá primero definir zonas con distinto grado de riesgo o impacto para la organización, tomar

medidas de control de acceso a cada una de ellas (Operaciones de seguridad) pero con los mismos dispositivos de acceso, se deberá detectar la presencia enemiga (Alarmas, IDS) la cual existirá, se planificarán zonas en las cuales se pueda derivar el enemigo e interactuar con él (Honey pots), se deberá contar con recursos a “Entregar” al enemigo con un alto grado de credibilidad (Operaciones de engaño o decepción), llegando a ser inclusive información cierta de la empresa que se está dispuesta a sacrificar por un objetivo mayor (Operaciones de información), se analizará cada paso enemigo para determinar sus patrones de conducta (operaciones de inteligencia), se diseñarán contramedidas o contra ataques (Operaciones de reacción y/o contingencia).

- Empleando “Estrategias” de seguridad de sistemas como una batalla muy dinámica y no como una protección policial, de murallas o de centinelas.

Madrid, octubre de 2001.

Alejandro Corletti es militar Argentino, Ingeniero en Informática, cursó un postgrado en Administración y Conducción y en la actualidad se encuentra cursando el Doctorado en Ingeniería de Sistemas Telemáticos en la Universidad Politécnica de Madrid, siendo su tema de investigación “Seguridad en entornos TCP/IP”.

Fue Jefe de Redes del Ejército Argentino durante 3 años. Es docente la Universidad de Ejército Argentino y de la Universidad Tecnológica Nacional de ese País, también se desempeñó como docente en Telefónica de Argentina, CISCO System, CIBSEC. S.A. y como asesor en temas de seguridad en varias Empresas.