CONCLUSIONES

Seguridad en redes IP

La realización de este trabajo nos ha permitido la obtención de una mayor comprensión de la seguridad existente en las redes IP. No sólo se ha profundizado en el estudio de los protocolos más importantes que permiten el funcionamiento de Internet (IP, UDP, ICMP y TCP) si no que además se han podido observar globalmente, lo que nos ha permitido examinar sus características, relaciones y roles en el transporte de la Información por Internet.

Son numerosos los ataques analizados que se basan en explotar algunas características de los protocolos de comunicación. Estos ataques buscan o bien el cese de las actividades o servicios que presta el ordenador atacado (ataques de denegación de servicio) o bien conseguir un acceso dentro de la máquina que le permita utilizarla a su gusto y conveniencia.

El uso de herramientas de seguridad clásicas basadas en el filtrado simple de los datagramas que circulan por Internet (firewalls) se ha revelado insuficiente ante los ataques organizados. Cuando el atacante es único y está perfectamente identificado (por la dirección IP usualmente) los sistemas básicos de seguridad pueden resultar un muro de defensa relativamente efectivo.

Sin embargo, cuando el atacante no está identificado de una forma explícita o el número de atacantes es desconocido (ataques de denegación de servicio distribuido), estos sistemas no pueden dar la respuesta adecuada.

La proliferación de herramientas automáticas que permiten de una forma sencilla coordinar ataques de cientos o miles de ordenadores simultáneamente, exige sistemas más sofisticados que sean capaces de seguir y entender el flujo de las comunicaciones existentes. El simple filtrado de paquetes aislados del resto del flujo de la comunicación ha dejado de ser efectivo.

También debemos tener en cuenta que muchas veces no basta únicamente con protegernos de las posibles amenazas que provienen de Internet. En el caso de que un sistema fuera comprometido por el motivo que fuese, el resto de ataques que lanzaría el atacante hacia nuestra red serían ataques internos que pasarían desapercibidos.

Los sistemas de detección de intrusos en redes (NIDS) son mecanismos de seguridad pasiva que se encargan de monitorizar todo el tráfico existente en nuestra red, tanto local como remoto. Este tipo de sistemas "inteligentes" nos permitirán incluso la detección de ataques perpetrados por un usuario legítimo de nuestro sistema.

Los sistemas NIDS unen a la capacidad de filtrado del tráfico las posibilidades que brindan la detección por firmas (patrones específicos de ataques conocidos) y el seguimiento de las comunicaciones desde un nivel de flujo de la comunicación.

Las contrapartidas de estos sistemas son principalmente la posibilidad de generar falsos positivos y falsos negativos que pueden desvirtuar la efectividad del sistema. Por otro lado generan una inmensa cantidad de información al tratar con todo el tráfico existente en la red (benigno y maligno) lo que dificulta su post-proceso e interpretación.

Además, para que un sistema de detección de intrusos sea realmente efectivo debe estar perfectamente parametrizado y adaptado a la red en la cual está instalada, lo que implica la existencia de un personal cualificado que regularmente verifique el buen funcionamiento del sistema.

La mejora tecnológica que se produce constantemente en las telecomunicaciones ha llevado a la proliferación de ataques y comportamientos maliciosos que anteriormente eran imposibles. La comprobación de toda una clase A, B o C de direcciones IP empieza a ser factible actualmente en espacios de tiempo cada vez menores. Lo que antes hubiera tardado meses y años, en la actualidad con los anchos de banda mejorando cada día pasa a ser cuestiones de días o incluso horas.

Las antiguas premisas de esconderse tras el anonimato o la falta de documentación pública sobre los aspectos de seguridad o de arquitectura de nuestra red dejan de ser válidos. Los atacantes realizan barridos "ciegos" por toda Internet con el objetivo de conseguir un sistema vulnerable a sus técnicas y métodos.

Los Honeypots son sistemas pasivos que han sido diseñados para ser atacados y/o comprometidos por los atacantes. El cambio de mentalidad que supone la incitación a que ataquen partes concretas de nuestro sistema se basa en la necesidad de conocer y estudiar de una forma fiable los comportamientos y técnicas de los atacantes.

La idea subyacente en el sistema de Honeypot es la de crear un entorno cerrado y acotado dónde los atacantes puedan ser "espiados" con el doble objetivo de conseguir unos nuevos sistemas de protección más seguros y desviar su atención de los sistemas reales. Como el sistema que están atacando está realmente bajo nuestro control, podemos analizar el comportamiento de los atacantes para adoptar las medidas necesarias que nos permitan aplicar una defensa más eficiente de nuestro sistema de producción real.

Las Honeynets son un tipo específico de Honeypots. Estos sistemas persiguen la simulación de una red de ordenadores compuesta de varios equipos y distintos sistemas operativos con el objetivo de que el atacante crea que está atacando una red real.

En la actualidad existen dos generaciones de Honeynets cuya implementación física requiere cada vez de una mayor cantidad de recursos, lo que pueden hacerla inviable para la mayoría de organizaciones. Las Honeynets virtuales permiten abaratar los costes de la arquitectura mediante la instalación de máquinas virtuales en un mismo ordenador que simularán los diferentes sistemas operativos y responderá a tantas direcciones IP como deseemos.

En cuanto a las ventajas añadidas respecto a los sistemas de seguridad tradicionales tenemos que permiten aislar en un entorno controlado a los posibles atacantes y eliminamos la existencia de falsos positivos. Por otro lado, las necesidades de los recursos disminuyen al no existir la necesidad de filtrar o buscar patrones por todo el tráfico y poder crear entornos virtuales en un mismo ordenador.

El riesgo más destacable que introduce el uso de Honeypots y Honeynets es la posibilidad de que un atacante realmente se haga con el control del sistema y lo utilice para atacar a otros ordenadores conectados a Internet, lo que nos obliga a una supervisión constante de estos sistemas.

Parte experimental

El experimento realizado dentro de este trabajo ha consistido en la realización de un estudio estricto del tráfico registrado en una conexión permanente a Internet durante una semana. Nuestro objetivo era el de comprobar si realmente existe en Internet una inseguridad tan grande como las noticias e informes existentes sugieren.

Para llevar a cabo este experimento se realizó un estudio de los diferentes requisitos (software y hardware) necesarios así como de la arquitectura de red a implementar. Se planificaron los distintos servicios que debería proporcionaría nuestra red (SSH, WWW, MAIL…) y se eligieron las diferentes herramientas de monitorización que nos proporcionarían la información deseada.

Del análisis de los datos recogidos durante la semana del 21 al 28 de Agosto de 2003 podemos destacar como prácticamente todo el tráfico existente (83%) hace referencia a los protocolos de servicios de red de Microsoft Windows.

La gran cuota de mercado que posee Microsoft junto con las vulnerabilidades que presentan los sistemas operativos basados en Windows, lleva a que sean los blancos preferidos de los ataques indiscriminados.

Entre el resto del tráfico registrado, hemos podido observar como se recibían distintos tipos de ataques a los servicios que teníamos disponibles en nuestra red. Los ataques más comunes son aquellos que hacen referencia a los servidores WWW y los servicios de MAIL.

La búsqueda de sistemas no actualizados vulnerables a fallos (*bugs*) conocidos es el principal objetivo de los ataques indiscriminados. También se ha observado un cierto número de comprobaciones de la configuración de los distintos servicios de nuestra red (si nuestro servidor WWW ofrece capacidades de *proxy*, si el servidor de MAIL permite enviar correos desde cualquier dirección…) con el objetivo de aprovechar una configuración deficiente de los servicios para sus ataques.

Coincidiendo con este estudio el virus W32/BLASTER tuvo su máximo apogeo, lo que nos permitió observar como recibíamos unos pocos miles de peticiones de ordenadores infectados.

Finalmente y tras analizar todos los resultados obtenidos, llegamos a la conclusión de que si bien sí es cierto que existen una cantidad de peligros que aconsejan siempre la instalación de algún sistema de seguridad en nuestra red u ordenador personal, el volumen y la sofisticación de los ataques distan mucho de crear un Internet caótico.

Líneas futuras de continuación

La realización de este trabajo abarca una gran cantidad de aspectos y conceptos de seguridad de redes relativamente nuevos que presentan una evolución constante.

Los sistemas de detección y bloqueo de ataques DOS/DDOS siguen sin ser efectivos debido a la inexistencia de standares que hayan sido adoptados por sistemas comerciales. La falta de un acuerdo entre fabricantes y organismos internacionales, en parte gracias a la distinta legislación de cada país evita un avance en este campo.

Sin embargo, los sistemas de detección de intrusos en redes (NIDS) es un campo que evoluciona rápidamente y donde más investigadores en seguridad invierten sus esfuerzos. El estudio de nuevas técnicas de detección de intrusos así como la mejora del entendimiento del flujo de las comunicaciones entre ordenadores abre un nuevo campo de estudio denominado IPS (sistemas de prevención de intrusos).

Los Honeypots y Honeynets son técnicas relativamente recientes que últimamente se han convertido en las estrellas de los sistemas de seguridad. Los avances en Honeynets virtuales que permiten la minimización de los recursos destinados así como el refinamiento de sus arquitecturas (generaciones) son un campo de estudio en permanente evolución. La creación y estudio de las Honeynets distribuidas es actualmente una de las líneas futuras con más interés.

En cuanto a la parte experimental, la realización de un estudio más completo, más complejo y con más recursos asociados sobre el tráfico que circula por Internet sería de gran ayuda para observar la evolución de la seguridad en las redes de ordenadores.

Controlar de forma perpetua el tráfico de distintos ordenadores conectados a diferentes puntos de Internet nos permitiría realizar correlaciones y estadísticas más fiables.