Revista Digital Universitaria
10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

ARTICULO

HONEYPOTS Y EL MONITOREO DE SEGURIDAD DE REDUNAM

David Jiménez Domínguez
Líder del Proyecto Honeynet UNAM
de Septiembre del 2004 a febrero del 2008.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Resumen

En el presente articulo se describe la arquitectura del Proyecto Honeynet UNAM, que es parte fundamental del monitoreo de seguridad de RedUNAM, realizado por el equipo de respuesta a incidentes del Departamento de Seguridad en Cómputo UNAM-CERT. Se hace énfasis en la captura pasiva de la actividad maliciosa en la red y cómo esta información es utilizada en la tarea diaria de la atención de incidentes de seguridad en la máxima casa de estudios, además de la tecnología y las herramientas utilizadas, así como los retos que se presentan en el monitoreo de la actividad maliciosa de red de una de las infraestructuras de red más robustas en la académica de México.

Palabras clave: incidentes, Monitoreo de seguridad de la red, Honeynets, Honeypots, Malware, Hackers.

http://www.revista.unam.mx/vol.9/num4/art21/int21.htm

INICIO

En la actualidad, la mayoría de las instituciones que proveen un servicio de red no sólo se preocupan por el monitoreo del cumplimiento y disponibilidad de los mecanismos que proporcionan conectividad a los usuarios, sino también se han interesado por el monitoreo de seguridad de la red. Sin embargo esta tarea representa varios retos en la industria privada, en el gobierno y en la academia, ya que desde su inicio las redes de computadoras son diseñadas con el objetivo de proporcionar un desempeño óptimo, para la cantidad de usuarios dependientes de este servicio, así como la disponibilidad del mismo.

Cuando una institución tiene la tarea de monitorear su red en busca de las amenazas y ataques que pueden comprometer su servicio y la información que viaja a través de ella, se encuentra con problemas como: la falta de infraestructura para el monitoreo, la diversidad de tipos de usuario e información que consultan desde la red, así como recursos limitados para cumplir con esta labor.

El equipo de respuesta a incidentes del Departamento de Seguridad en Cómputo UNAM-CERT, a través de la Dirección General de Servicios de Cómputo Académico, se encarga de proveer servicios a sitios que han sido víctimas de algún ataque, de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole, así como la realización de investigaciones del área de cómputo para ayudar a mejorar la seguridad en los sitios. Por medio del monitoreo pasivo de seguridad de RedUNAM, el UNAM-CERT, a través del Proyecto Honeynet UNAM, busca obtener información que permita identificar tendencias en la actividad maliciosa observada en la red de la máxima casa de estudios.

El Proyecto Honeynet UNAM tiene como objetivo ser un recurso de seguridad pro-activo que ayude a identificar las amenazas existentes dentro de la red de la Universidad, así como un recurso de investigación en seguridad computacional que permita conocer las herramientas, motivos y las tácticas de la comunidad blackhat (hackers no éticos) que tiene como objetivo las redes mexicanas.

El interés de los intrusos por las redes de información de las universidades ha existido desde tiempo atrás, las amenazas van desde la propagación de malware, hasta la explotación de vulnerabilidades asociadas no solamente con una debilidad de hardware o software, sino a los procedimientos administrativos, como por ejemplo: el uso de contraseñas débiles o la exposición de servicios innecesarios para cumplir con el objetivo de la institución.

Las redes académicas cuentan con un ancho de banda necesario para que los intrusos lleven a cabo acciones maliciosas, en el cual es difícil el control de todas las actividades en la red por medio de políticas y buenas practicas de seguridad, lo que les permitiría pasar desapercibidos al encontrar segmentos de red cuya administración y monitoreo sea completamente inexistente.

En un nota titulada "Experts map out future malware creation hotspots"[1] la firma de seguridad finlandesa F-Secure, realiza un comparativo de la actividad maliciosa en los últimos 20 años relacionada con malware, y pronostica que a partir del 2008 se empezará a observar un incremento en México y países de África del número de grupos con actividades delictivas en la red. Este problema llega a tener nexos socioeconómicos, ya que existen pocas oportunidades de empleo para egresados de carreras relacionadas con las tecnologías de información, por lo que muchos profesionistas optan por unirse a grupos delictivos, los cuales cuentan con un nivel de conocimiento más avanzado que hace 20 años.

1 "Experts map out future malware creation hotspots". Enero 2008 http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080117_1_eng.html Consultado el 28/03/08

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

En los últimos dos años hemos leído titulares acerca del incremento de ataques a diferentes instituciones así como a la infraestructura de TI en diferentes dependencias del país.[2]

Honeypots

Una manera de identificar las vulnerabilidades utilizadas por los intrusos y aquella actividad no identificada como un ataque por nuestros sistemas de monitoreo, es instalar computadoras en la red y observar el tráfico que se dirige a ellas. El equipo no debe tener uso en producción alguna, por lo que nadie debe utilizarlo. Una vez conectado a la red, todo el tráfico que se dirija al mismo será sospechoso por naturaleza, si el sistema es atacado, aprenderemos algo nuevo y tendremos la evidencia para analizar el incidente. Esta es la idea central de un honeypot. Un honeypot es un sistema de información cuyo valor reside en el uso no autorizado o ilícito de este, ya que será un equipo con el cual los intrusos podrán interactuar e incluso comprometer, permitiéndonos reunir tanta información como sea posible sobre los mismos.

Los honeypots se clasifican por el nivel de interacción que tendrá con el intruso, nuestra elección dependerá del tipo de información que deseemos obtener; a mayor interacción mayor será la información que obtendremos de las actividades del intruso.

Honeypots de baja interacción

Este tipo de honeypots se caracteriza por la emulación de servicios que permiten al intruso interactuar de manera limitada con el honeypot, sin afectar al sistema por completo. Son fáciles de implantar, configurar y mantener debido a su funcionalidad reducida. Cuando un intruso intente utilizar uno de los servicios que el sistema de baja interacción emula, obtendrá una respuesta a sus solicitudes, esto podría ser un inicio de sesión o una página Web de error; sin embargo dependiendo de la programación de la aplicación, estas respuestas podrían ser limitadas e incluso podrían permitir la identificación del honeypot como una herramienta de monitoreo, alejando al intruso en el peor de los casos.

El objetivo principal de este tipo de sistemas es la detección de escaneos, la captura de malware y de intentos de inicio de sesión no autorizados (Honeyd y Kojoney). El administrador sólo configura el programa que simulará los servicios, por lo que la implantación y el mantenimiento son sencillos. El administrador podrá enfocarse más tiempo al monitoreo de los mecanismos de alerta del honeypot.

El riesgo existente en este tipo de software es mínimo, debido a que la funcionalidad es reducida; no hay un sistema operativo con el cual el intruso pueda interaccionar, de manera que el honeypot no puede ser utilizado para atacar a otros sistemas. La cantidad de información que podemos obtener con este trabajo es reducida, a saber:

- Fecha y hora del ataque.
- Dirección IP y puerto origen del ataque.
- Dirección IP y puerto destino del ataque.

2 "Agrada a dirigente de PRI Tamaulipas su PRISimpson". Agosto 2007 http://www.eluniversal.com.mx/notas/442730.html

"Hackean página de ALDF con mensaje contra el aborto". Marzo 2007 http://movil.eluniversal.com.mx/notas/413730.html

"Hackean portal de San Lázaro". Febrero 2008 http://www.eluniversal.com.mx/grafico/vi_75302.html

"Hackean página web de Turismo estatal". Julio 2006 http://www.eluniversal.com.mx/grafico/53922.html

"Hackean página web de AMLO". Julio 2006 http://estadis.eluniversal.com.mx/notas/358856.html

"Hackean portal de Profeco, tras "ventilar" a gasolineras". Agosto 2006 http://www.eluniversal.com.mx/notas/369610.html

Es posible que si el honeypot permite un cierto grado de interacción con el intruso se puedan capturarar algunos comandos HTTP, FTP, SMTP, etc., esto depende de los servicios emulados.

Honeypots de alta interacción

Son los que proporcionan más información sobre los intrusos, su implantación y mantenimiento requiere tiempo, además son de alto riesgo ya que de ser comprometidos, el intruso tendrá control total de un equipo desde el cual puede hacer lo que desee, incluso atacar otros sistemas de cómputo. En este tipo de honeypots nada es emulado, el intruso tendrá un sistema operativo por completo con el cual interaccionar, nada está restringido. La información de la cual podemos aprender es muy valiosa; herramientas, nuevas vulnerabilidades, cómo es que se comunican los intrusos entre si, etc.

Los equipos destinados a ser de alta interacción, se diferencian de los sistemas de producción, porque no tienen valor alguno en la producción de la organización; su único valor reside en ser escaneados, atacados o comprometidos. El valor de la de información capturada está ligado al alto riesgo que implica tener un honeypot de este tipo. Para mitigar estos riesgos, los sistemas de alta interacción suelen colocarse dentro de un ambiente controlado, como por ejemplo detrás de un firewall, cuya función será permitir todo el tráfico de entrada hacia los honeypots, e impedir que desde este se ataque a otros equipos de la red, lo cual se torna complicado especialmente cuando se desea que el intruso no se entere que está siendo monitoreado.

El compromiso de este equipo nos permite estudiar la debilidad utilizada para infiltrase en el sistema y analizar las actividades del intruso una vez que tiene control remoto del equipo. El honeypot puede trabajar bajo cualquier sistema operativo y ejecutar cualquier servicio que deseemos. Los servicios que configuramos en estos equipos determinan el vector de ataque que proporcionamos a los intrusos. Una vez identificada la vulnerabilidad explotada, podemos buscar otros sistemas en RedUNAM que proporcionen el mismo vector de ataque, con la finalidad de prevenir agresiones futuras o localizar equipos comprometidos de la misma forma que nuestro honeypot.

Otras tecnologías de monitoreo pasivo de red

Una de las tecnologías de monitoreo de seguridad de red más utilizadas son los Sistemas Detectores de Intrusos (IDS por sus siglas en ingles). Estos sistemas monitorean uno o más segmentos de red en busca de indicadores de ataque mediante la inspección del tráfico de red. Los IDS cuentan con problemas de exactitud en sus alertas, que permiten a este tipo de dispositivos identificar un ataque cuando éste es inexistente, a esto se le conoce como falso positivo. Un falso negativo sucede cuando un IDS falla en la identificación de un ataque real. Este tipo de fallas es común no sólo en los IDS, también en firewalls que soportan la inspección de tráfico. En las tecnologías de monitoreo descritas a continuación no existe este problema ya que están basadas en la idea de funcionamiento de un honeypot. Todo el tráfico de entrada o salida desde estas arquitecturas son sospechosas por naturaleza, lo que ayuda a minimizar tiempos de respuesta a la hora de analizar una cantidad de alertas importante en un IDS.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Honeynet

Una honeynet consiste de una red de honeypots de alta interacción que pueden estar en diferentes plataformas (Windows, Unix, Linux, etc.). Esto nos permite capturar información sobre diferentes tipos de actividad maliciosa en la red, es una de las soluciones honeypot mas complejas, ya que requiere de dedicación en su implantación, administración y monitoreo por el riesgo que representa el contar con honeypots de alta interacción en ella.

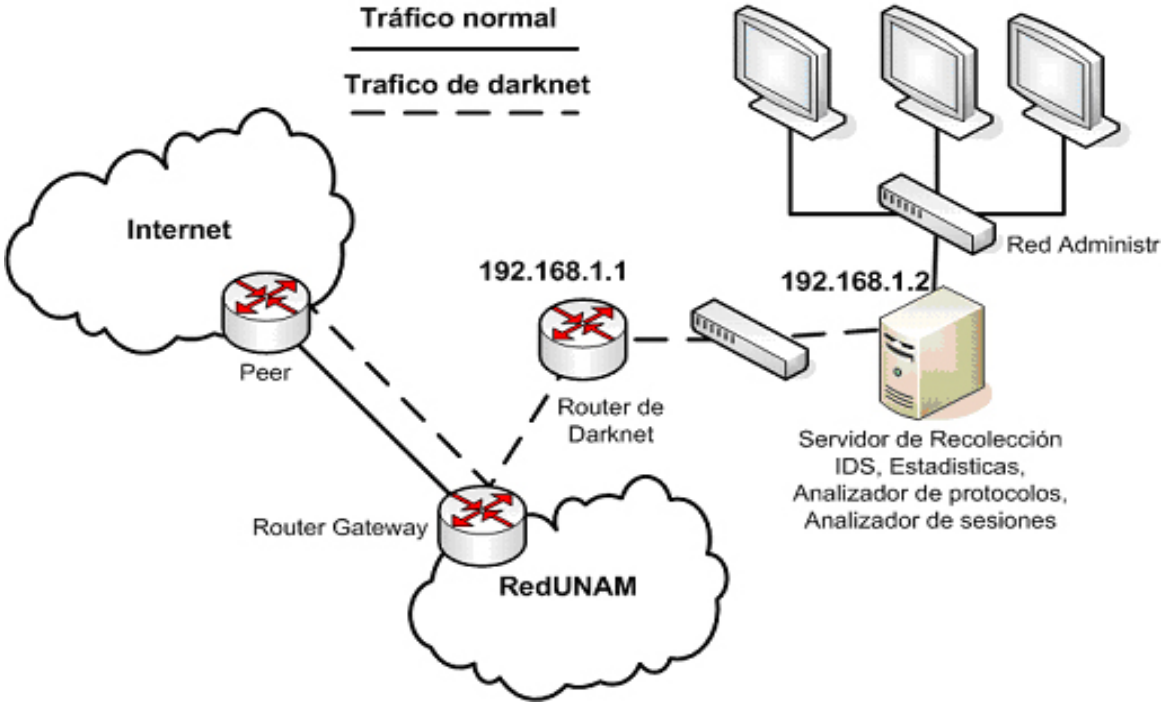

Figura 1. Arquitectura de una Honeynet

Una honeynet proporciona la información de mayor valor en las arquitecturas de monitoreo pasivo de red. Cualquier persona que trabaja en secreto, no tendrá miedo de ser identificada o capturada, pero sí de ser monitoreada de cerca y de que los detalles de sus actividades lleguen a otra persona sin su conocimiento, ese es el objetivo de una honeynet. La información capturada por esta red puede ser desde un nuevo malware que se propaga en la red, hasta organizaciones criminales tratando de obtener acceso a los recursos de la institución.

Cabe recordar que una honeynet no es una solución de software, es una arquitectura de alta interacción en donde nada es simulado por una aplicación, toda la arquitectura consta de sistemas reales dedicados al monitoreo pasivo de red dentro de un ambiente controlado por la misma. La razón por la cual una honeynet es un ambiente controlado se debe a que proporciona los mecanismos de control y monitoreo necesarios para que los honeypots dentro de ella, no sean utilizados para lanzar un ataque a sistemas que no se encuentran en la red, como pueden ser sistemas en producción.

Existen dos requerimientos importantes a la hora de implantar una honeynet, el control de los datos y la captura de estos. Todas las arquitecturas basadas en la idea de este tipo de redes deberán contar con las dos propiedades. Estos elementos de la la red residen en un sólo equipo llamado honeynet gateway (figura 1).

Control de datos

Es el elemento más importante de una honeynet, se encarga de contener la actividad originada desde la estación. Su objetivo es mitigar el riesgo, por riesgo. Entendemos que existe la posibilidad de que un intruso comprometa una honeynet y la utilice para atacar sistemas que no pertenecen a ella. Esto es mas difícil de lo que aparenta, ya que debemos brindar un cierto grado de libertad al intruso para actuar, mientras más libertad tenga el intruso de actuar, más aprenderemos de el, sin embargo a mayor libertad del intruso mayor es el riesgo de que burle el mecanismo de control, y así pueda atacar a otros sistemas que no pertenecen a la honeynet. Además necesitamos controlar las actividades del intruso sin que se de cuenta que está siendo monitoreado y controlado.

El honeynet gateway canaliza todo el tráfico de entrada y salida por el firewall y por el sistema para la prevención de intrusos (IPS por sus siglas en ingles). El firewall registra todas las conexiones, si el número de conexiones originadas desde la honeynet rebasa un umbral establecido bloquea cualquier intento de conexión entre el honeypot y el equipo externo por un periodo de tiempo definido. Esta es la primer capa de protección. El IPS inspecciona todo el tráfico de salida de la red en busca de patrones de ataque, cuando los detecta en curso puede bloquear el tráfico e impedir su transito a través del honeynet gateway, o modificarlo de manera que sea inofensivo a la hora de llegar al equipo destino externo. Cuando el IPS analiza el tráfico y este no tiene similitud con algún patrón de ataque conocido lo deja pasar a través del honeynet gateway.

Caputara de datos

Consiste en capturar y almacenar todas las actividades realizadas por el intruso en la honeynet. Estos datos son analizados posteriormente para aprender de las herramientas, tácticas y motivos de la comunidad blackhat. El reto es capturar la información como sea posible, sin que el intruso se de cuenta que está siendo observado.

La captura de datos se realiza en el honeynet gateway por medio del firewall y del IDS. Las bitácoras del firewall de los intentos de conexión y las alertas originadas por el IDS, representan el primer indicio en el radar sobre la actividad observada en la honeynet. Además es el mismo IDS, en modo sniffer, el que realiza la captura de todo el tráfico de red observado en la honeynet, el cual es utilizado para un análisis más detallado de la actividad.

Darknet

Una darknet es un espacio de direcciones IP, en el cual no residen equipos o servicios válidos que respondan a solicitudes de los usuarios de la red. Este espacio de direcciones, también conocido como blackhole, no cuenta con registros en algún servidor de nombres de dominio, sin embargo tienen entradas válidas en las tablas de ruteo de la universidad. El tráfico que entre en este espacio de direcciones es sospechoso por naturaleza, siendo un escaneo, una prueba o un ataque en curso. Es útil en la identificación de tendencias en las amenazas a la infraestructura de red de la Universidad ya que es información libre de falsos positivos.

El tráfico malicioso generado por escaneos o la propagación de malware no utiliza nombres de dominio para localizar a sus víctimas, seleccionan un rango de direcciones y lo escanean en busca de equipos vulnerables a ciertos exploits. Sin embargo en este tipo de monitoreo también podemos identificar equipos con una configuración de red errónea y cuyos mensajes de broadcast son enviados a un segmento al cual no pertenecen.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

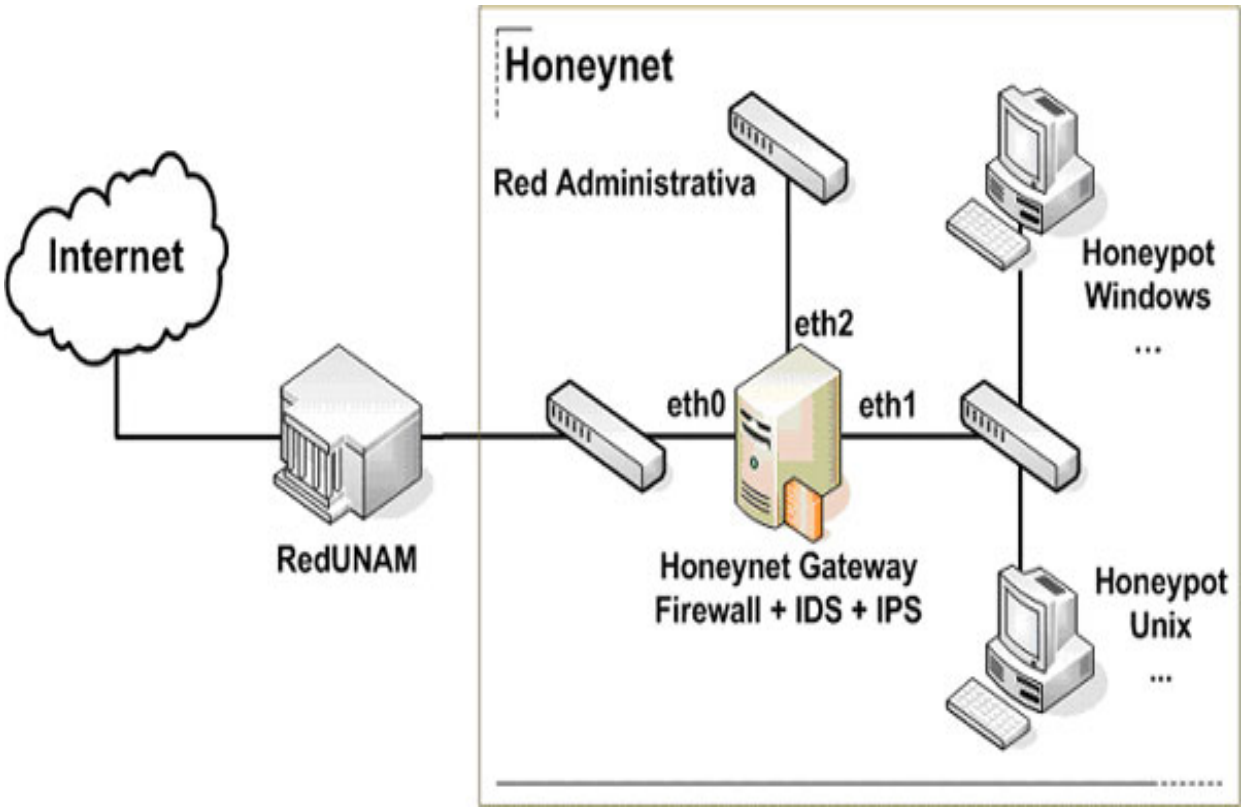

Figura 2. Arquitectura de darknet

Se puede incluir en este espacio de direcciones un equipo que cuente con un sniffer o un sistema detector de intrusos (figura 2), con los que se captura información para un posterior análisis forense e incluso para la generación de estadísticas y la identificación de tendencias. El tamaño de este rango de direcciones no impacta considerablemente en la calidad de la información capturada, un número mayor de direcciones proporcionará una mayor precisión de la actividad maliciosa en la red académica. Existen proyectos que monitorean redes de clase B, útiles en la detección de nuevos ataques y en el monitoreo de tráfico backscatter.

El tráfico de tipo backscatter es una respuesta a solicitudes que no fueron enviadas previamente; como mensajes de error sobre ICMP, terminación o confirmación de sesiones TCP. El monitoreo de este tipo de tráfico es útil en la detección temprana de ataques de negación de servicio y del uso de IP spoofing.

Sink hole por DNS

El concepto de sink hole en la seguridad de redes se refiere a la capacidad de redirigir tráfico IP específico, con la finalidad de realizar un análisis forense de red, detectar tráfico anómalo o mitigar el riesgo de un ataque en curso. Cuando un ISP cuenta con la capacidad de actuar ante el ataque contra uno de sus clientes, este puede modificar las tablas de ruteo, indicando una ruta mas especifica para el rango de direcciones afectado por el ataque, y redirigiendo este tráfico, ya sea a una red de cuarentena en donde es analizado o simplemente es descartado en el perímetro del ISP (también conocido como null routing).

Utilizando esta técnica podemos detectar de forma pasiva, equipos que han sido vulnerados por virus, gusanos, spyware o que pertenecen a una botnet, redirigiendo el tráfico desde los servidores de nombres de dominio de la Universidad.

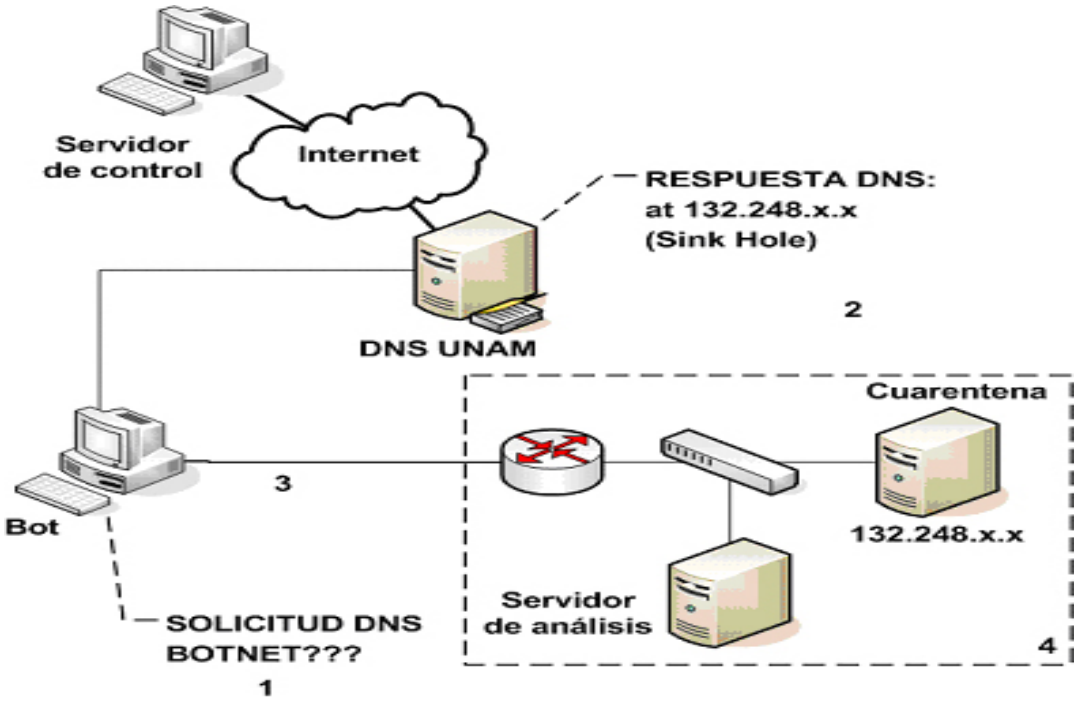

Figura 3. Arquitectura de un sink hole por DNS

Los servidores de nombres de dominio son parte fundamental de la Internet, si no se cuenta con ellos la conectividad con la mayor parte de la red sería mínima. Su tarea principal es el traducir nombres a direcciones IP y viceversa, sin ellos, los usuarios tendrían que recordar la dirección IP de cada sitio al que deseen conectarse en lugar de utilizar un nombre común como google.com o yahoo.com. Un sink hole de DNS consiste en la redirección de tráfico IP mediante las respuestas del servidor de nombres de dominio a solicitudes específicas. Un equipo que intente resolver un nombre de dominio que ha sido identificado, como un sitio malicioso con anterioridad, puede ser redirigido mediante la respuesta proporcionada por el DNS a una red de cuarentena para su monitoreo de forma pasiva (figura 3).

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Experiencias en Red UNAM

El proyecto cuenta con una honeynet, dos darknets y varios honeypots de baja interacción para la captura de malware, instalados en diferentes segmentos de la red universitaria. La información proporcionada por estos sensores, permite identificar a los equipos infectados por malware y con actividad maliciosa hacia el interior de la misma red. Como parte de las tareas de atención de incidentes realizadas por el UNAM-CERT esta información es canalizada directamente a los administradores de red de cada dependencia de la UNAM, y en casos externos al personal responsable de la administración del segmento de red o al CERT correspondiente.

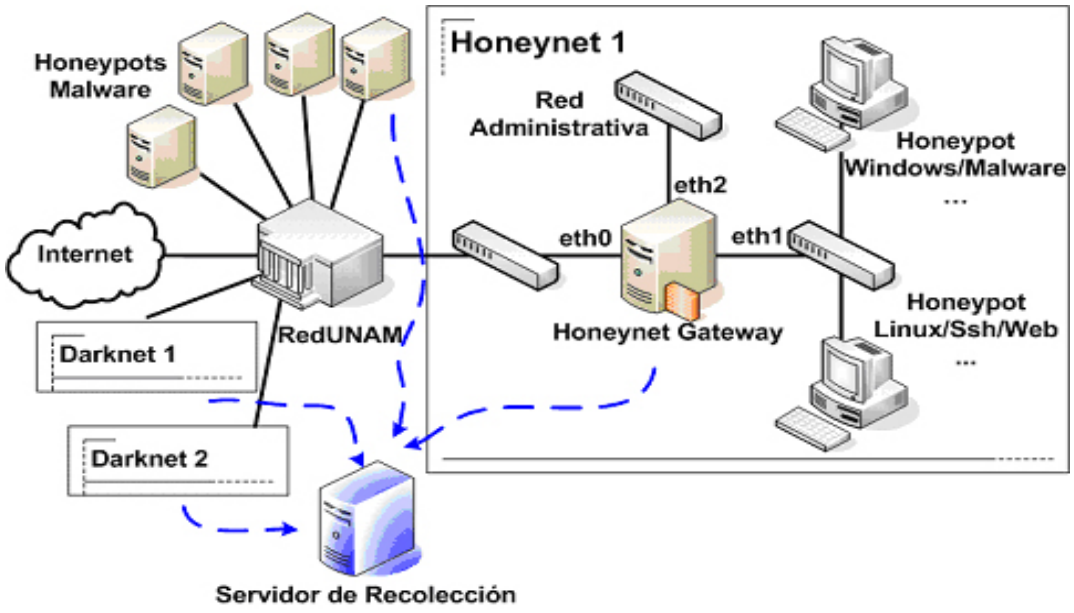

Figura 4. Arquitectura Proyecto Honeynet UNAM

Todas las herramientas utilizadas en el control de tráfico se basan en software libre. La recolección de información de cada honeynet y cada darknet se realiza de forma cifrada, asegurando la confidencialidad de los datos. La información de los honeypots dedicados para la captura de malware, es recolectada de forma similar a la de cualquier honeynet, mientras que cada muestra de malware capturada, es canalizada al equipo de análisis, quienes por medio de la ejecución en un laboratorio de pruebas controlado y en caso necesario un análisis de ingeniería inversa, obtienen la información relevante al espécimen capturado y al incidente que es atendido por el equipo.

Resultados

En el año 2007 identificamos 4242 muestras de malware diferentes propagándose en RedUNAM, se analizaron 4 incidentes en la honeynet, los cuales afectaron principalmente a sistemas operativos Unix, siendo el uso de contraseñas débiles la vulnerabilidad más explotada por los intrusos en este sistema operativo, mientras que en sistemas Windows los ataques son mas automáticos, y fueron realizados en su totalidad por medio de la propagación de código malicioso. Se identificaron 1900 IPS diferentes de RedUNAM con actividad maliciosa, donde el 92.15% se identifico por medio del monitoreo de escaneos y pruebas realizadas por las darknets y honeynets, mientras que el resto se identificó por el monitoreo con honeypots de baja interacción para la captura de malware así como de equipos comprometidos por medio de los servidores DNS de la UNAM a través del sink hole por DNS.

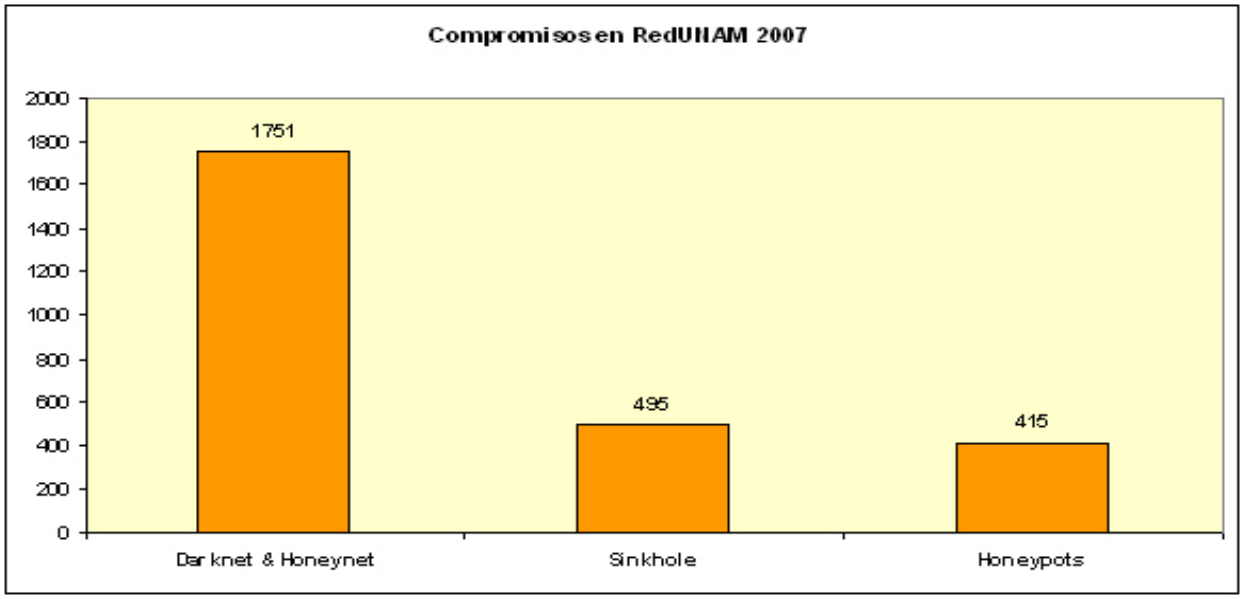

Figura 5. Equipos en RedUNAM identificados como comprometidos por tecnología de monitoreo en el 2007.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Desventajas

Una de las desventajas de los honeypots es el fingerprinting, el cual se refiere a la identificación de la identidad de un honeypot, debido a ciertos patrones y características que delatan su propósito. Si un intruso detecta la presencia de un honeypot en alguna organización, éste podría utilizar la identidad de otro equipo en la organización para atacarlo, de esta manera, cuando el administrador de la red se dé cuenta, iniciará una investigación interna, mientras el atacante se concentra en equipos reales. Además, si un intruso identifica un honeypot de alta interacción, éste podría generar datos que desvíen la investigación y resulten en conclusiones erróneas sobre su comportamiento.

El uso de honeypots puede agregar un riesgo adicional al ambiente de toda organización, esto quiere decir que cuando uno de ellos sea comprometido, puede ser utilizado para atacar o perjudicar a otros sistemas en la organización. Entre más simple sea el honeypot, menos riesgo existe, de manera que un equipo que sólo simula servicios, será difícil de comprometer con la finalidad de atacar a otros equipos; sin embargo, en sistemas que ofrecen todo un sistema operativo, un atacante podría comprometer el sistema y utilizarlo para realizar ataques pasivos o activos en contra de otros sistemas en la misma organización. El riesgo es variable, dependiendo de cómo se implementa y utiliza el honeypot.

La utilización de un honeypot dentro de la organización proporcionará información valiosa sobre la actividad maliciosa de la red; no obstante, es una muestra pequeña del trabajo, , dependiendo del tamaño de la red de la organización, y mucho más pequeña en comparación con el tamaño de la Internet.

Una desventaja del uso de sink holes de DNS es que la red en cuarentena podría ser objeto de ataques y pruebas aleatorias realizadas por otros equipos en la red. Además el número de equipos comprometidos que serán identificados por este método, dependerá del porcentaje de equipos que utilizan como servidor de nombres primario, el utilizado en este esquema de monitoreo.

Tendencias

Conforme surgen nuevas técnicas y vectores de ataques, el concepto de honeypot ha sido extendido a otras tecnologías en las que hace una década era impensable que se pudiera incursionar. Actualmente existen desarrollos interesantes en las siguientes áreas de investigación:

Honeypots cliente

Cada vez mas intrusos explotan vulnerabilidades en aplicaciones cliente (p.e. Internet Explorer o la suite de Office). Esto ha dado pauta a la creación de un concepto nuevo basado en la idea de honeypots llamado honeyclients. En lugar de esperar por un intruso de forma pasiva, este sistema busca activamente el contenido malicioso en la red. La idea detrás de todas estas herramientas es simular el comportamiento humano y averiguar si tal comportamiento puede ser explotado por un intruso. Por ejemplo, un honeyclient podría ser un mecanismo para controlar un navegador Web. El honeyclient viaja por la red a través del navegador (en pocas palabras una aplicación cliente), simula el comportamiento humano, visitando paginas resultado de patrones de búsqueda definidos con anterioridad; por medio de herramientas y técnicas, el honeypot es observado, las anomalías creadas en el sistema a partir de la visita de un sitio Web son detectadas. No podemos analizar toda la Internet en busca de sitios web maliciosos, pero podemos basar nuestra búsqueda en sitios sospechosos o presumiblemente maliciosos: sitios warez, de intercambio de torrents, foros, páginas con contenido erótico, sitios promocionados por medio de correo spam, etc.

Honeypots Wifi

La idea del monitoreo de seguridad de redes inalámbricas por medio de honeypots ha estado en el aire desde hace un par de años. Ha surgido una solución exitosa que puede aportar información sobre las amenazas en este tipo de tecnologías.
Honeypots Bluethoot

En el 2006 la firma de seguridad F-Secure publicó en su blog la utilización de un prototipo de honeypot sobre bluetooth que se anuncia como un teléfono celular, es capaz de aceptar transferencias de archivos y analizarlos en busca de patrones de malware. No se publicó más sobre este prototipo, sin embargo conforme las amenazas en telefonía móvil se incrementen y se aproximen al continente americano, el uso de esta tecnología será una opción para incursionar en el monitoreo de seguridad sobre estos dispositivos.

Conclusiones

Las redes académicas cuentan con una diversidad de ambientes y de usuarios que en ocasiones limitan la capacidad de implantar una política de seguridad restrictiva en la protección perimetral, sobre todo cuando se cuenta con una administración descentralizada de la red. El monitoreo de la seguridad de la red siempre se ha visto afectado por el falseo en la generación de alertas, omitiendo ataques que son exitosos, o alertando sobre supuestos ataques de forma errónea. Las técnicas de monitoreo descritas en este documento no son víctimas del falseo en la detección de actividad maliciosa, pueden ser utilizadas para la captura de información útil para la defensa de la organización así como para la investigación de la actividad maliciosa observada en la red.

Actualmente los honeypots han dejado de ser herramientas geek, utilizadas por algunos académicos, para convertirse en opción tanto en la investigación como en la defensa en contra de ataques que buscan vulnerar la infraestructura de TI de cualquier organización. Son el mejor medio para conocer las tácticas del enemigo, lo cual puede llegar a ser nuestra mejor arma para ganar una guerra que se proyecta para muchos años más.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Bibliografía

The Honeynet Project (2004), Know your Enemy. Learning about security Threats, 2nd Ed,. Addison Wesley

Neils Provos, Thorsten Holz (2008), Virtual Honeypots. From Botnet Tracking to Intrusion Detection, Addison Wesley.

Victor Oppleman, Oliver Friedrichs (2005), Extreme Exploits. Advanced Defenses Against Hardcore Hacks, McGraw Hill

Richard Bejtlich (2006), Extrusion Detection. Security Monitoring for Internal Intrusions, Addison Wesley.

Richard Bejtlich (2005), The Tao of Network Security Monitoring. Beyond Intrusion Detection, Addison Wesley.

"Know Your Enemy Whitepapers" (en linea) http://www.honeynet.org/papers/kye.html