PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

"PROPUESTA DE UTILIZACIÓN DE HERRAMIENTAS DE TELEMETRÍA, PARA IDENTIFICAR TÉCNICAS DE CIBERDELITOS COMO WATERING HOLE, EN REDES DE INFRAESTRUCTURA (CASO DE ESTUDIO NETFLOW DE CISCO)."

AUTOR

DAVID FERNANDO ZAMBRANO MONTENEGRO

DIRECTOR

PHD. GUSTAVO CHAFLA ALTAMIRANNO

Quito – 2015

DEDICATORIA

Dedico la presente tesis:

A Dios por mostrarme día a día que con humildad, paciencia y sabiduría todo es posible. A mis padres, esposa e hija quienes con su amor, apoyo y comprensión incondicional estuvieron siempre a lo largo de este proyecto; a ellos que siempre tuvieron una palabra de aliento en los momentos difíciles y que han sido incentivos de mi vida.

AGRADECIMIENTO

Agradezco en primer lugar a Dios quien me dio la vida y la ha llenado de bendiciones en todo este tiempo, a él que con su infinito a amor nos ha dado la sabiduría suficiente para culminar la maestria. Quiero expresar mis más sincero agradecimiento, reconocimiento y cariño a mis padres por todo el esfuerzo que hicieron para darnos una profesión y hacerme una persona de bien, gracias por los sacrificios y la paciencia que demostraron todos estos años. Gracias a todas aquellas personas que de una u otra forma me ayudaron a crecer como profesionales. Agradezco también de manera especial a mi director de tesis quién con sus conocimientos y apoyo supo guiar el desarrollo de la presente tesis desde el inicio hasta su culminación.

RESUMEN

El presente trabajo de investigación presenta la propuesta de utilización de herramientas de telemetría, para identificar técnicas de ciberdelitos como watering hole en redes de infraestructura, caso de estudio Netflow de cisco. Para simular este ciberataque se diseñó una red de infraestructura con la herramienta GNS3, en este caso una topología vulnerable que consta de dos redes LAN, conectadas entre sí a través del internet. El área LAN de los clientes será denomina como LNCL y el área de los servidores como LNSR. El área atacada fue la de los servidores donde se explotaron las vulnerabilidades de los navegadores y de la bases de Datos utilizando la herramienta Kali Linux. Para realizar el monitoreo de nuestra red se utilizó la herramienta Solarwinds Real-time Netflow Analyzer misma que permitió capturar flujos de datos de los routers previamente configurados con Netflow, para luego mostrar gráficamente el tráfico de nuestra red una manera rápida y sencilla.

SUMMARY

This research presents the proposed use of telemetry tools to identify cybercrime techniques like watering hole in infrastructure networks, case study Cisco Netflow. To simulate this cyber network infrastructure was designed with GNS3 tool, in this case a vulnerable topology consisting of two LANs interconnected via the internet. The LAN area customers will be referred to as LNCL and area servers as LNSR. The attacked area was the server where browser vulnerabilities were exploited and data bases using the Kali Linux tool. The Solarwinds Real-time NetFlow Analyzer tool that allowed it to capture data streams routers configured using Netflow, then graphically display network traffic our quick and easy way was used to monitor our network.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

CAPITULO I: INTRODUCCIÓN Y OBJETIVOS

1.1. INTRODUCCIÓN

La presente investigación se refiere al tema de identificar técnicas de ciberdelitos como Watering Hole (pozo de agua), que se puede definir como el ataque contra empresas u organizaciones en el cual el hacker o atacante selecciona un sitio web para insertar un fragmento de software conocido como exploit, con el fin de aprovechar una vulnerabilidad de seguridad, obteniendo como resultado la infección del sitio con código malicioso (malware) que tiene como objetivo infiltrarse o dañar una computadora .

La característica principal de este tipo de ataques es que mientras el exploit se aprovecha de las vulnerabilidades de la red, las víctimas que visitan el sitio web hackeado, involuntariamente descargan el malware al equipo. El malware puede ser en forma de un troyano de acceso remoto, que permite a los atacantes acceder a datos sensibles y tomar el control del sistema.

Para analizar esta problemática es necesario de mencionar las causas. Una de ellas es la vulnerabilidad de seguridad que existe actualmente en las redes de infraestructura. Se entiende por vulnerabilidad a una falla en un sistema o en una red que permite a un usuario no autorizado el acceso y el robo de datos confidenciales.

Para prevenir este tipo de ataque existen herramientas de detección de tráfico de red. Aunque los atacantes pueden incorporar diferentes exploits, el tráfico generado por el programa malicioso se mantiene constante cuando se comunica con los servidores de

comando y control. Mediante la detección de estas comunicaciones, las organizaciones o empresas pueden implementar las respectivas medidas de seguridad para prevenir el ataque.

La tecnología Netflow es utilizada por dispositivos de red Cisco, para coleccionar la información del tráfico de la red, este protocolo puede ayudar a los administradores a detectar el tráfico sospechoso. El monitoreo de la red puede ser realizado a diferentes escalas. Desde una red local, hasta un conjunto de estas.

1.2. JUSTIFICACIÓN

La seguridad de la red se está convirtiendo en uno de los principales problemas para el desarrollo de las nuevas tecnologías y servicios de telecomunicaciones, los hackers están en constante evolución hacia nuevas técnicas de ataque, lo que hace muy difícil la tarea de construir mecanismos de defensa eficientes para prevenir o evitar dichos ataques, por tal motivo esta investigación se profundizó en el análisis estadístico de ciberdelitos o ataques contra redes de infraestructura, específicamente el ataque Watering Hole.

En la actualidad no hay ningún método de detección perfecto, inevitablemente algunas amenazas son lo suficientemente sofisticadas e indetectables como para penetrar todas las capas de defensa de una red, frente a este escenario se presenta la solución utilizando herramientas de telemetría que le permite a los responsables de seguridad tener visibilidad en todos los puntos de la red y control preciso sobre las amenazas avanzadas.

Para realizar este análisis se utilizó la tecnología CISCO NETFLOW, que permite obtener informes en los que se muestra toda la información que consumen los recursos de la red, además detecta y previene cuellos de botella y ayuda a tomar acciones preventivas o correctivas al administrador de la red.

1.3.OBJETIVOS

1.3.1. OBJETIVO GENERAL:

Analizar las herramientas de telemetría, para identificar técnicas de ciberdelitos como Watering Hole, en redes de infraestructura (caso de estudio Netflow de Cisco).

1.3.2. OBJETIVOS ESPECÍFICOS:

1 Identificar las principales vulnerabilidades de seguridad en redes de infraestructura.

2 Reconocer cuales son las herramientas de telemetría más utilizas para identificar técnicas de ciberdelitos.

3 Determinar las características más importantes de los ataques Watering Hole.

4 Análisis estadístico de ataques Watering Hole con el protocolo Netflow de Cisco.

CAPÍTULO II: VULNERABILIDADES DE SEGURIDAD EN REDES DE INFRAESTRUCTURA

2.1. INFRAESTRUCTURA DE RED

> "Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos.
>
> No obstante, no podemos pasar por alto tampoco que una red de datos se pone también en funcionamiento con otros dos objetivos primordiales: compartir tanto el software como el hardware y otorgarle soporte y centralización a la administración pertinente."*[1] Definiciones.de (2015)*

Los sistemas y aplicaciones requieren uno de los más fundamentales sistemas de comunicaciones de la organización. Esta red se compone de dispositivos como routers, firewalls, e incluso hosts genéricos que se debe evaluar como parte del proceso de hacking (piratería) ético.

Hay miles de posibles vulnerabilidades de la red, igual tantas herramientas, y aún más las técnicas de prueba. Es probable que no se tenga el tiempo o los recursos disponibles para poner a prueba los sistemas de infraestructura de red para las vulnerabilidades posibles, utilizando todas las herramientas y técnicas imaginables. En su lugar, deben centrarse en las pruebas que producirán una buena evaluación general de la red.

Se pueden eliminar muchas vulnerabilidades conocidas, vulnerabilidades relacionadas con la red con solo remendar los hosts con el software más reciente de proveedores y parches de firmware. Dado que la mayoría de la infraestructura de red

hosts no son públicamente accesibles, las probabilidades son que los hosts de red no serán atacados desde el exterior e incluso si lo son, los resultados no son propensos a ser perjudicial. Se puede eliminar muchas otras vulnerabilidades siguiendo algunas prácticas sólidas de seguridad en la red. Cuanto mejor se conozcan los protocolos de red, las pruebas de vulnerabilidad de red será más fácil, porque los protocolos de red son la base para la mayoría de los conceptos de seguridad de la información.

2.1.1. VULNERABILIDADES DE LA INFRAESTRUCTURA DE RED

Vulnerabilidades de la infraestructura de red son la base de todos los problemas de seguridad técnicas en los sistemas de información. Estas vulnerabilidades de nivel inferior afectan todo lo que funcione en la red. Es por eso que se necesita para poner a prueba para ello y eliminarlos siempre que sea posible.

El enfoque para las pruebas de hacking ético en la infraestructura de red debe ser encontrar los puntos débiles que otros puedan ver en la red para que pueda cuantificar el nivel de la red de exposición.

Muchos problemas están relacionados con la seguridad de la infraestructura de red. Algunos temas son más técnicos y requieren el uso de diversas herramientas para evaluar de manera adecuada. Se puede evaluar a los demás con un buen par de ojos y un poco de pensamiento lógico. Algunos problemas son fáciles de ver desde fuera de la red, y otros son más fáciles de detectar desde el interior de la red.

Al evaluar la seguridad de la red de infraestructura de una empresa, se tiene que mirar en áreas tales como:

- ✓ Cuando los dispositivos tales como un firewall o IPS se colocan en la red y cómo están configurados
- ✓ Lo que los hackers ver cuando realizan escaneos de puertos, y cómo pueden aprovechar las vulnerabilidades en los hosts de la red
- ✓ Diseño de la red, tales como las conexiones a Internet, capacidades de acceso remoto, defensas por capas, y la colocación de las máquinas de la red
- ✓ Interacción de los dispositivos de seguridad instalados, tales como firewalls, IDS y antivirus, etc.
- ✓ ¿Qué protocolos están en uso?
- ✓ Puertos comúnmente atacadas no protegidas
- ✓ Configuración de host de red
- ✓ Supervisión y mantenimiento de la red

Si un hacker explota la vulnerabilidad en uno de los elementos anteriores o en cualquier lugar en la seguridad de la red, pueden pasar cosas que perjudiquen como:

- ❖ Un hacker puede usar un ataque de denegación de servicio, que puede acabar con su conexión a Internet - o incluso toda su red.
- ❖ Un empleado malicioso utilizando un analizador de red puede robar información confidencial en los correos electrónicos y los archivos que se transfieren en la red.
- ❖ Un hacker puede crear puertas traseras en la red.
- ❖ Un hacker puede atacar hosts específicos mediante la explotación de vulnerabilidades locales a través de la red.

Figura 1: Proceso Explotar las vulnerabilidades en la red. Año 2015

Fuente: [2] http://blog.trendmicro.es/wp-content/uploads/2010/09/vulnerabilidadADOBE.bmp, (2015)

Elaborado por: Trend Micro Incoporated

2.1.2. RECOMENDACIONES DE SEGURIDAD PARA LA INFRAESTRUCTURA DE RED

Para la seguridad de LA infraestructura de red, se debe realizar los siguientes pasos:

- ✓ Poner a prueba los sistemas desde el exterior, el interior, y en el interior (es decir, entre los segmentos de la red interna y DMZ).

  Obtener el permiso de las redes de socios que están conectados a la red para comprobar si hay vulnerabilidades en sus extremos que pueden afectar a la seguridad de la red, como los puertos abiertos y la falta de un firewall o un router mal configurado.

2.1.3. HERRAMIENTAS PARA PROBAR LAS INFRAESTRUCTURA DE RED

Las pruebas requieren las herramientas adecuadas que necesitan escáneres y analizadores, así como herramientas de evaluación de la vulnerabilidad. Great Commercial, Shareware y herramientas de software libre están disponibles son algunas de las herramientas más utilizadas en las siguientes secciones. Se ha de tener en cuenta que se necesita más que una herramienta, y que ninguna herramienta tiene todo lo que necesita.

Si estás buscando herramientas de seguridad fácil de usar con todo en un solo paquete, para obtenerlo se tiene que pagar esto ocurre la mayor parte del tiempo especialmente para la plataforma Windows. Toneladas de profesionales de la seguridad confían en muchas herramientas de seguridad gratuitas, especialmente las que se ejecutan en Linux y otros sistemas operativos basados en UNIX. Muchas de estas herramientas ofrecen una gran cantidad de valor si se tiene el tiempo, la paciencia y la voluntad de aprender sus pormenores.

2.1.3.1. ESCÁNER Y ANALIZADORES

Estos escáneres ofrecen prácticamente todos los puertos de exploración y de la red de pruebas de herramientas que se necesitará:

- Para preguntas en la red de búsquedas de DNS a traceroutes (Trayectos de Información) se puede utilizar Sam Spade para Windows
- Para barridos de ping y escaneo de puertos se puede utilizar SuperScan.
- Para una amplia variedad de funciones de escaneado de red se puede utilizar NetTools Esenciales.
- Para docenas de funciones de evaluación de seguridad de red, incluyendo los barridos de ping, escaneo de puertos, y las pruebas de retransmisión SMTP se puede utilizar NetScanTools Pro
- Para la enumeración SNMP se puede utilizar Getif
- Para sondear host-puerto y las huellas dactilares del sistema operativo se puede utilizar Nmap o NMapWin para Nmap
- Para los controles de seguridad, tales como la exploración de puertos y pruebas de firewall se puede utilizar Netcat
- Para el análisis de redes se puede utilizar LanHound ó WildPackets EtherPeek

2.1.3.2. EVALUACION DE VULNERABILIDADES

Estas herramientas de evaluación de la vulnerabilidad permiten probar los hosts de red para diferentes vulnerabilidades conocidas, así como posibles problemas de configuración que podrían conducir a agujeros de seguridad:

- Security Scanner GFI LANguard Network para el escaneo de puertos y otras pruebas de vulnerabilidad
- Inspector de Seguridad de Sunbelt de red para las pruebas de vulnerabilidad

- Nessus como una herramienta libre todo en uno para pruebas como redadas de ping, escaneo de puertos, y las pruebas de vulnerabilidad
- Qualys QualysGuard como un gran todo en uno la herramienta para las pruebas de vulnerabilidad en profundidad

2.1.3.3. ESCANEAR, HURGAR Y PINCHAR

Para realizar hackeo en la infraestructura de una red implica realizar los siguientes pasos básicos de hacking:

1. Recopilar información y el mapa de la red.
2. Analizar los sistemas para ver que están disponibles.
3. Determinar qué está funcionando en los sistemas descubiertos.
4. Tratar de penetrar los sistemas descubiertos, si se lo desea.

Cada controlador de la tarjeta de red y la implementación de TCP / IP en la mayoría de sistemas operativos, incluyendo Windows y Linux, e incluso en sus firewalls y routers, tiene peculiaridades que dan lugar a comportamientos diferentes cuando se escanea, hurga y pinchar sus sistemas. Esto puede dar lugar a diferentes respuestas dependiendo de los sistemas.

2.1.3.4. ANALIZADORES DE RED

Un analizador de red es una herramienta que le permite buscar en una red y analizar los datos que van a través del cable con fines de optimización de redes, seguridad, y / o solución de problemas. Al igual que un microscopio para un científico de

laboratorio, un analizador de red es una herramienta imprescindible para cualquier profesional de la seguridad.

Los analizadores de red a menudo se denominan genéricamente como sniffers, aunque eso es en realidad el nombre y la marca comercial de un producto específico de Network Associates, Sniffer (la herramienta original análisis de la red comercial).

Al evaluar la seguridad y respuesta a incidentes de seguridad, un analizador de red puede ayudar a ver el tráfico de red anómalo e incluso localizar a un intruso y desarrollar una línea de base de la actividad de la red y el rendimiento, tales como protocolos en uso, las tendencias de uso, y las direcciones MAC, antes de que ocurra un incidente de seguridad.

Cuando la red se comporta de forma errática, un analizador de red puede ayudar a:

- Seguir y aislar el uso de red maliciosa
- Detectar aplicaciones maliciosas de caballo troyano
- Monitorear y rastrear a los ataques de denegación de servicio

2.1.4. ATAQUES

2.1.4.1. DENEGACIÓN DEL SERVICIO (D.O.S.)

2.1.4.1.1. PRUEBA DE ATAQUES DE DENEGACIÓN DE SERVICIO

De denegación de servicio (DoS) son algunos de los ataques de piratas informáticos más comunes. Un hacker inicia tantas solicitudes no válidas a un host de red que

utiliza todos sus recursos en respuesta a ellos y hace caso omiso de las peticiones legítimas.

2.1.4.1.2. LOS ATAQUES D.O.S.

Son posibles en contra de su red y hosts los siguientes tipos de ataques de denegación de servicio y pueden provocar que determinados sistemas se estrellen, la pérdida de datos, y que cada usuario se pregunte cuándo se restablecerá el acceso a Internet.

2.1.4.1.3. ATAQUES INDIVIDUALES

Aquí están algunos ataques DoS comunes:

- ✓ Inundaciones SYN: El atacante inunda un host con paquetes TCP SYN.
- ✓ Ping de la Muerte: El atacante envía paquetes IP que exceden la longitud máxima de 65.535 bytes, lo que en última instancia, pueden bloquear la pila TCP / IP en muchos sistemas operativos.
- ✓ WinNuke: Este ataque puede desactivar redes en más antiguas de Windows 95 y NT computadoras.

2.1.4.1.4. ATAQUES DISTRIBUIDOS

Distribuidos DoS (DDoS) tienen de manera exponencial un mayor impacto en sus víctimas. El más famoso fue el ataque DDoS contra eBay, Yahoo!, CNN, y docenas

de otros sitios Web por un hacker conocido como MafiaBoy. Estos son algunos de los ataques distribuidos comunes:

- ✓ **Ataque Smurf:** Un atacante falsifica la dirección de la víctima y envía peticiones de eco ICMP (paquetes ping) a la dirección de difusión. El ordenador de la víctima queda inundado con toneladas de paquetes en respuesta a esas peticiones de eco.
- ✓ **Trinoo y Tribe Flood Network (TFN) ataques:** Conjuntos de programas basados en el cliente y servidor lanzan inundaciones de paquetes contra un equipo de la víctima, efectivamente sobrecargarlo y provocando que se bloquee.

Los ataques DoS y DDoS pueden llevarse a cabo con las herramientas que el hacker ya sea escribe o descargas de Internet. Estas son buenas herramientas para probar de la red IDS / IPS y firewalls. Se puede encontrar programas que permiten a ataques actuales y programas reales, como de Karalon Traffic IQ Pro, que le permiten enviar ataques controlados.

2.1.4.1.5. PRUEBAS

Su primera prueba DoS debe ser la búsqueda de vulnerabilidades de denegación de servicio desde una perspectiva de búsqueda de puertos y el análisis de redes.

No se debe pasar por DoS a menos que tenga sistemas de prueba o puede realizar pruebas controladas con las herramientas adecuadas. Las pruebas de DoS mal planificadas es una búsqueda de trabajo en la fabricación, es como tratar de borrar los

datos de un recurso compartido de red de forma remota y con la esperanza de que los controles de acceso en su lugar vayan a impedirlo.

2.1.4.1.6. MEDIDAS CONTRA LOS ATAQUES DE DENEGACIÓN DE SERVICIO

La mayoría de los ataques de denegación de servicio son difíciles de predecir, pero pueden ser fáciles de prevenir:

- ✓ Probar y aplicar parches de seguridad tan pronto como sea posible para los hosts de la red, tales como routers y cortafuegos, así como para los sistemas operativos para servidores y estaciones de trabajo.
- ✓ Usar un IDS o IPS para monitorear regularmente los ataques de denegación de servicio. Se puede ejecutar un analizador de red en el modo de captura continua si no se puede justificar el costo de un todo-fuera IDS o solución IPS.
- ✓ Configurar firewalls y routers para bloquear el tráfico con formato incorrecto. Se puede hacer esto sólo si los sistemas soportan.
- ✓ Reducir al mínimo la suplantación de IP, ya sea:
  - ➢ Uso de la autenticación y el cifrado, como una infraestructura de clave pública (PKI).
  - ➢ El filtrado de paquetes externos que provengan de una dirección interna, el host local (127.0.0.1), o cualquier otra dirección privada y no direccionable, como 10.xxx, 172.16.xx-172.31.xx o 192.168.xx

- Bloquear todo el tráfico entrante ICMP a la red a menos que específicamente lo necesite. Incluso entonces, se debe permitir que venga sólo a hosts específicos.
- Desactivar todos los pequeños servicios que no sean necesarios TCP / UDP, como eco y chargen.

Establecer una base de referencia de los protocolos de red y los patrones de tráfico antes de un ataque DoS se produce. De esa manera, conoces qué buscar. Y analizar con regularidad para tales potenciales vulnerabilidades de denegación de servicio DoS como software bribón instalado en máquinas de la red.

2.1.4.2. ATAQUES IMPLEMENTADOS

Los ataques ejecutados como una prueba de concepto para el marco NETA, por cada ataque implementado describimos:

- El comportamiento del ataque
- Los parámetros que se pueden modificar para configurar el ataque.

2.1.4.2.1. ATAQUE IP DROPPING

En el ataque IP Dropping, los nodos que exhiben este comportamiento caen intencionalmente, con una cierta probabilidad, recibieron paquetes de datos IP en lugar de transmitirlos, lo que altera el funcionamiento normal de la red. Dependiendo de la aplicación, se puede convertir la red mucho más lenta debido a la existencia de retransmisiones; hacen los nodos desperdicien mucho más recursos energéticos, etc. El parámetro principal de la aplicación del ataque de goteo es:

- Soltando Probabilidad de ataque: la probabilidad de descartar un paquete, definido entre 0 y 1. De forma predeterminada, se establece en 0, lo que hace que al nodo atacante comportarse normalmente (sin soltar en absoluto).

2.1.4.2.2. ATAQUE IP DELAY

En este ataque, un nodo malicioso retrasa paquetes de datos IP para una cierta cantidad de tiempo. Esto puede afectar a diferentes parámetros de QoS (retardo de extremo a extremo, fluctuación de fase, etc.), lo que resulta en un rendimiento de la red. La lista de parámetros en la implementación del ataque retraso es:

- Probabilidad Ataque Delay: la probabilidad de retrasar un paquete de datos, definido entre 0 y 1. De forma predeterminada, se establece en 0, lo que implica un comportamiento normal para el nodo atacante (sin retardo adicional para cualquier paquete).

- Retraso Ataque Valor: El tiempo de retardo específico aplicado al paquete. Tenga en cuenta que este parámetro podría ser especificado por una distribución estadística. Por esta razón, se define como volátil, es decir, se modifica cada vez que se accede. Por defecto, se sigue una distribución normal con media 1 segundo y una desviación estándar de 0,1 segundos.

2.1.4.2.3. ATAQUE SINKHOLE

En un ataque de sumidero, un nodo malicioso envía la información de enrutamiento falsa, alegando que tiene una ruta óptima y causando otros nodos a los paquetes de datos a través de la propia ruta. Aquí, el atacante forja respuestas de enrutamiento

(RREP) para atraer tráfico. La lista de los parámetros de ataque Sinkhole (Sumideros) es:

- Probabilidad de ataque Sumidero: La probabilidad de responder un mensaje RREQ con una respuesta de ruta falsa (RREP), definida entre 0 y 1. Por defecto se establece en 0, lo que implica el comportamiento normal del protocolo AODV.

- Sólo hundirse cuando la ruta esté en la Tabla: Si se establece como verdadero, el sumidero sólo envía RREP falsa a las peticiones de aquellos que el nodo atacante tiene una ruta válida, es decir, las rutas existentes en su tabla de enrutamiento. En caso contrario (valor falso), el nodo envía RREP falsa para cualquier mensaje RREQ que llegue, incluso si no sabe una ruta válida.

- Seqno Añadido: el número de secuencia falsa generada por el nodo atacante. Se añade al número de secuencia observada en la solicitud. Puede ser diferente cada vez, si se especifica como una distribución estadística. Por defecto, se sigue una distribución uniforme con valores entre 20 y 30 años.

- Saltos núm.: El número falso de saltos devueltos por el atacante. De forma predeterminada, se establece en 1, lo que indica que el atacante llega al final de la comunicación en un solo salto.

2.1.5. DETECTAR ROUTES COMUNES, INTERRUPTORES Y DEBILIDADES EN EL FIREWALL

Algunas vulnerabilidades de seguridad de alto nivel se encuentran comúnmente en dispositivos de red y pueden crear muchos problemas.

2.1.5.1. ENCONTRAR LAS INTERFACES NO SEGURAS

Se tiene que asegurar de que el HTTP y las interfaces de telnet a tu routers, interruptores y cortafuegos no se configuran con un espacio en blanco, por defecto, o de otra manera con una contraseña fácil de adivinar. Este consejo parece una obviedad, pero es para una de las debilidades más comunes. Cuando una persona maliciosa u otros atacantes obtienen acceso a los dispositivos de red, él ya es el propietario de la red. Entonces el puede bloquear el acceso administrativo, configurar cuentas de usuario de puerta trasera, volver a configurar los puertos, e incluso hacer caer toda la red sin que ni te des cuenta.

Otra debilidad está relacionada con HTTP y telnet está activado y utilizado en muchos dispositivos de red, cualquier persona con algunas herramientas gratuitas y de algunos minutos de tiempo puede oler la red y capturar las credenciales de inicio de sesión para estos sistemas cuando están siendo enviadas en texto plano y cuando eso sucede, todo vale.

2.1.5.2. LA EXPLOTACIÓN DE LAS DEBILIDADES DE IKE

Las empresas que ejecutan una VPN en un router o firewall son comunes. Si se pertenece a esta categoría, es muy probable que el VPN esté ejecutando el protocolo Internet Key Exchange (IKE), que tiene un par de debilidades explotables conocidas:

✓ Es posible romper IKE "modo agresivo" claves pre-compartidas utilizando Cain & Abel y la herramienta IKECrack

✓ Algunas configuraciones IKE, como las que en ciertos firewalls Cisco PIX, se pueden tomar fuera de línea. Todo el atacante tiene que hacer es enviar 10 paquetes por segundo a 122 bytes cada uno y usted tiene un ataque de denegación de servicio en sus manos.

2.1.6. DEFENSAS GENERALES DE LA RED

Independientemente de los ataques específicos contra un sistema, algunas buenas prácticas pueden ayudar a prevenir muchos problemas de la red:

- Utilizar las reglas de inspección de estado que supervisa las sesiones de tráfico de cortafuegos. Esto puede ayudar a asegurar que todo el tráfico que pase por los cortafuegos es legítimo y puede prevenir ataques DoS y otros ataques de suplantación.
- Implementar reglas para realizar el filtrado de paquetes basado en el tipo de tráfico, TCP / UDP, las direcciones IP y las interfaces específicas incluso en sus routers antes de que el tráfico es cada vez permitió entrar en su red.
- Filtrado de Proxy y Network Address Translation (NAT).
- Encontrar y eliminar paquetes fragmentados que entran en su red (de Fraggle u otro tipo de ataque) a través de un sistema IDS o IPS.

- Segmento de la red y el uso de un firewall en la red interna en general y en los departamentos críticos, tales como contabilidad, finanzas, recursos humanos, y la investigación.

CAPÍTULO III: HERRAMIENTAS DE TELEMETRÍA – MONITOREO DE RED

3.1.TELEMETRÍA

3.1.1. DEFINICIÓN DE TELEMETRIA

La telemetría es una de herramientas más utilizadas en la actualidad y según la Diccionario de la Real Academia de la Lengua Española (DRAE) se define como: "Medida de distancias mediante el telémetro; o; Sistema de medida de magnitudes físicas que permite transmitir esta a un observador lejano."*[3]DRAE (2015) – Telemetría, recogido de Pág. Web: http://lema.rae.es/drae/?val=TELEMETRIA.*

La definición anterior es una descripción global del término en todas las áreas en la que puede ser aplicada, pero en informática se la define como: "La telemetría es una tecnología que permite la medición remota de magnitudes físicas, datos, entre otros y el posterior envío de la información hacia el operador del sistema."*[4]Wikipedia la enciclopedia libre (2015), Telemetría, Recogido de Pagina Web: http://es.wikipedia.org/wiki/Telemetr%C3%ADa.*

3.1.2. TIPOS DE PROTOCOLOS DE RED

3.1.2.1.NETFLOW

3.1.2.1.1. DEFINICIÓN

> NetFlow es un protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP. NetFlow se ha convertido en un estándar de la industria para monitorización de tráfico de red, y actualmente está soportado para varias plataformas además de Cisco IOS y NXOS, como por ejemplo en dispositivos de fabricantes como Juniper, Enterasys Switches, y en sistemas operativos como Linux, FreeBSD, NetBSD y OpenBSD. *[5]Wikipedia enciclopedia libre (2015)*

Netflow fue desarrollado originalmente para ayudar a los administradores de red a obtener una mejor comprensión de lo que su tráfico de red parecía. Una vez se habilita en un enrutador, simplemente hace un seguimiento de las sesiones IP, sin almacenar ninguno de los datos reales utilizados en esa sesión. Debido a que el contenido de la sesión no se almacena en los registros de Netflow, profesionales de la seguridad a veces se consideran esto un factor limitante en su uso. Sin embargo, ese mismo comportamiento permite a los administradores de seguridad para instalar y utilizar en lugares donde Sniffer de red no podría manejar el ancho de banda, los requisitos de almacenamiento o sobrecarga de la CPU. Debido a los muchos usos diferentes para Netflow, hay varias versiones de protocolo y aplicaciones disponibles para el análisis.

Al momento de decidir qué herramienta de Netflow implementar para la recolección y el análisis, hay que tener en cuenta que hay varias ventajas y desventajas de cada herramienta. Flujo-herramientas es popular porque era una de las primeras herramientas de libre disposición para apoyar Netflow, y tiene una base de característica rica que incluye el análisis, informes estadísticos, y un fácil manejo en el método para ejecutar consultas en archivos ACL nombradas estándar.

3.1.2.1.2. VENTAJAS Y DESVENTJAS DE NETFLOW

3.1.2.1.2.1.VENTAJAS DE NETFLOW

- ✓ Una solución de muy bajo costo:
  - ❖ Cisco NetFlow es parte integral de IOS (aunque se requiere una licencia de imagen y / o función correspondiente).
  - ❖ No requiere ningún hardware sonda externa costosa.
- ✓ Las estadísticas se reunieron antes de la compresión y / o cifrado, lo que proporciona datos sobre los flujos que no serían accesibles para sondas externas.
- ✓ Compatible con la mayoría de las interfaces del router, incluyendo WAN, MAN, LAN y las interfaces de túnel.
- ✓ Trabajos sobre subinterfaces ejemplo frame relay
- ✓ La mejor solución para el detalle granular sobre los flujos de paquetes IP
- ✓ No se requiere de votación, la información es "empujado" cuando esté disponible
- ✓ El tráfico puede ser agregado en el router antes de la exportación reduciendo los volúmenes de tráfico.
- ✓ Provee duración y marcas de tiempo absolutos para cada flujo.
- ✓ Amplio soporte para plataformas de router de Cisco, y en 5500 con NFFC y 6000 con MSFC.
- ✓ Hace reembolso según el uso y la facturación posible.
- ✓ Ampliamente desplegado (estado de Cisco que se ha desplegado por más de 15.000 clientes).

3.1.2.1.2.2.DESVENTAJAS DE NETFLOW

- ✓ IP única - no monitorea IPX u otros protocolos.
- ✓ Monitores solamente de tráfico de ingreso
- ✓ Al tener un impacto en la CPU del router, que impone un límite en el número total de flujos que pueden ser monitoreados en cualquier dispositivo único.
- ✓ Sólo admite el tráfico unicast hasta IOS 12.3.

3.1.2.1.2.3.COMPARACIÓN DE NETFLOW CON OTROS PROTOCOLOS

Cuadro 1: Tabla comparativa de Netflow con otros protocolos.

TECNOLOGIA / PARAMETROS	NETFLOW	SFLOW	IPFIX
Tipo de información	Flujos	Parcialmente paquetes seleccionados por muestreo	Flujos
Cantidad de datos	Desde pequeñas hasta grandes cantidades (depende de la tasa de muestreo y de las condiciones de creación de flujos)	Grandes cantidades (depende de la tasa de muestreo)	Desde pequeñas hasta grandes cantidades
Colección de información	Datos de la capa de enlace de datos y de la capa de transporte	Datos de la capa de enlace de datos	Datos de la capa de enlace de datos y de la capa de transporte y otros datos que se recoge por medio de extensiones del vendedor
Estado de estandarización	RFC3954 (Información dada por Cisco)	RFC3411(Información dada por InMon)	Etapa inmediata de publicación del FRC (estándar)
Enfoque de recolección	Almacenamiento en cache basado en "traps", y recolección de estadísticas	Basada en la muestra	Basado en un muestreo aleatorio (muestreo probabilístico)
Desarrollo de las tecnologías	Basada en software	Utiliza un chip dedicado que está incorporado en el hardware	Basada en software

Fuente: *[6] Castro A, Estrella A (2009)*

Elaborado por: Castro A, Estrella A.

Las empresas buscan hardware de red comparan y seleccionan sus equipos en base a las capacidades de reenvío, los bits de supremacía, opciones de expansión, servicios integrados, redundancia, capacidad de gestión y más.

NetFlow, debido a su enfoque en los flujos, captura información acerca de todas las conversaciones de tráfico IP que pasan a través de una interfaz e informa todo el tráfico de la interfaz. Proporciona detalles sobre el 100% del tráfico mientras que sFlow a menudo pierde el tráfico que se necesita mirar, lo que hace que sFlow sea casi inutilizable para la detección de amenazas a la red y el análisis forense. NetFlow es una mejor elección para la detección de anomalías de la red, debido a su capacidad para capturar todas las conversaciones. sFlow también puede ser utilizado para la detección de anomalías, pero la posibilidad de que falte un flujo crítico es alta debido a su naturaleza de muestreo. Si la detección de anomalías está en el borde donde cada conversación es crítica, sFlow puede dejar de cumplir con las expectativas.

Netflow permite informar sobre los componentes tales como el reconocimiento de aplicación basada en la red (NBAR), Medianet, enrutamiento rendimiento y la visibilidad de las aplicaciones y el control (AVC) con las mismas herramientas que ya está utilizando para sus datos de tráfico. Además, admite las nuevas tecnologías como el tráfico IPv6, etiquetas MPLS, el tráfico multicast, direcciones de control de acceso de medios de comunicación, la identificación de VLAN, jitter y el tiempo de ida y vuelta de tráfico de medios.

Una de las ventajas sFlow es que puede capturar todo el tráfico de la red, incluyendo IP e incluso protocolos heredados como IPX, AppleTalk, etc., mientras que NetFlow se limita al tráfico IP y no puede capturar información de protocolo legado. Esto no

es una gran ventaja, pero es posible que haya algunos entornos en los que esos protocolos heredados aún representan una parte significativa del tráfico. La escalabilidad es una ventaja para sFlow porque no consume recursos adicionales como el número de conversaciones aumenta. NetFlow, debido a ser manejado por el software, puede causar problemas de rendimiento cuando está habilitado en los dispositivos de manipulación de grandes volúmenes de tráfico. sFlow teóricamente se puede habilitar en incluso 100 redes Gb y todavía no afecta al rendimiento.

Las ventajas deñ sFlow incluyen la ausencia de una memoria caché de flujo, que permite a los dispositivos de encaminamiento se concentren en su núcleo y funciones de conmutación. Por otro lado, NetFlow es más preciso, permite a los usuarios profundizar en cada flujo IP (que permite un mejor ámbito para el análisis de causa raíz) y está bien adaptado para detectar cualquier anomalía en el comportamiento de la red.

Netflow e IPFIX son muy parecidos entre sí, este tiene algunas ventajas contra netflow pero también algunas desventajas y limitaciones. Una de estas desventajas es el aumento de la sobrecarga de procesamiento, puesto que IPFIX se configura en los dispositivos de red a sí mismos, la utilización de la CPU de los dispositivos se incrementa en 1% al 2%. Ademas es Limitado sólo al IP Tráfico, los protocolos IPFIX son capaces de capturar y reportar el solo el tráfico IP.

Por estos motivos netflow es el protocolo para el análisis de redes más completo que existe en la actualidad, teniendo muchas ventajas significativos contra otros protocolos que permite un mejor análisis de datos en las conversaciones de trafico IP,

lo cual es necesario para saber cuándo un intruso se está robando información y poder detenerlo a tiempo.

3.1.2.1.3. RECOLECCION DE NETFLOW

Hay varias cosas que se deben considerar al decidir cuál va a ser la arquitectura de colección de Netflow. Estos factores incluyen el espacio colector de disco, energía de la CPU, los paquetes exportados por segundo, y la topología de la red. Si el entorno es bastante simple, un solo colector puede ser suficiente.

El espacio en disco y la velocidad es siempre una de las principales preocupaciones cuando se preparan para desplegar Netflow. Debido a la naturaleza, es difícil predecir lo que una red específica requerirá para el almacenamiento. Una regla general es de 1 MB de almacenamiento para los 2Gb de tráfico de red. Esto puede no parecer mucho, pero en una red empresarial que esto puede aumentar rápidamente, especialmente teniendo en cuenta el hecho de que una sola transacción red podría potencialmente pasar varios dispositivos exportadores de Netflow.

Hay varias herramientas de código abierto y comercial que tendrán alimentos Netflow y escribir los datos directamente a una base de datos. Hay que tener en cuenta que debido a la compresión incorporada realizado por los daemons del colector de flujo, esto requerirá mucho más espacio para almacenar la misma cantidad de datos. Además, también puede ser más fácil de presentar un registro Netflow prima como evidencia cuando sea necesario.

Debido a estos problemas, si una base de datos se utiliza para almacenar los flujos, a menudo es útil disponer de tablas con capacidad limitada para almacenar una pequeña cantidad de los flujos, y mantener los registros de Netflow originales como un archivo. Esta solución también permitirá utilizar cualquiera de las herramientas ya escritos para analizar archivos de registro Netflow a su discreción.

Una manera fácil de perfeccionar las estimaciones sobre los requisitos de almacenamiento para la recolección de Netflow es la creación de un colector temporal y comenzar los flujos de exportación. Basado en el tamaño de los registros y el número de registros por día (esta es una configuración de colector específico que vamos a cubrir en los ejemplos), es fácil de obtener una estimación de las necesidades de almacenamiento diarias.

La topología de red también debe tenerse en cuenta al momento de elegir dónde desplegar físicamente su colector. Envío de registros desde un dispositivo WAN remoto a un colector central puede poner presión adicional sobre un enlace sin necesidad, especialmente durante un ataque de denegación de servicio. Paquetes Netflow se basan UDP, así que usar conexiones gran ancho de banda puede conducir a flujos exportados perderse. Aunque la colección de la propia Netflow requiere poca CPU, muchas de las herramientas disponibles para analizar archivos de datos va consumir grandes cantidades de energía del procesador. El uso de la infraestructura recogida existente para ejecutar consultas sobre datos Netflow aprovecha la CPU adicional, así como disco I / O.

Si hay varios routers exportadores de flujos a un único colector, puede ser beneficioso tener varios daemons de recogida que se ejecutan en diferentes puertos

de escritura a diferentes estructuras de directorios. La segmentación de los datos de este modo permitirá a las consultas que se ejecutan específicamente para el segmento de red asociado con un router específico.

Muchos dispositivos también tienen un número limitado de destinos Netflow disponible para exportación. Este factor, junto con el hecho de que muchos productos requieren su propia corriente de Netflow, significa que los flujos a menudo deben replicarse. Esto también permitirá que seleccione el tráfico que se redistribuye a aplicaciones adicionales "fanning out" los flujos.

3.1.2.1.4. EXPORTACIÓN DE NETFLOW

Netflow se puede exportar desde una variedad de dispositivos, incluyendo pequeños routers de oficina, aparatos dedicados, así como monitores pasivos que funcionan de la misma manera como un sniffer de red. Este debe exportarse desde dispositivos ubicados en los puntos de convergencia, muy parecidos a un sensor IDS. Tener exportadores bien colocados reduce el número de dispositivos necesarios para cubrir toda la red y reduce los requisitos de almacenamiento.

Es recomendable usar NTP y una zona horaria común para la sincronización de tiempo. Ajustar la zona horaria de todos los dispositivos de red a un formato común como UTC toma muy poco esfuerzo pero previene la necesidad de conciliar los problemas de fecha y hora durante un incidente.

El muestreo de flujo se utiliza a menudo para la utilización de la red y la tendencia. Muestreo funciona mediante la selección de un subconjunto de paquetes que pasan a

través de una interfaz. El muestreo se configura como una relación. Si el muestreo se establece en 100, la relación es de 1 a 100. Debido a que no todos los flujos se recogen, el muestreo no debe ser utilizado para la configuración de Netflow en la detección de incidente.

Registros de Netflow de "timed out" en un dispositivo de exportación basado en el estado de la corriente, los flujos se clasifican como "activo" o "inactivo". Un flujo se desactiva cuando se termina una conexión IP. El ajuste de tiempo de espera inactivo determina el tiempo (en segundos) se mantiene un flujo en el caché después de que se desactiva.

El ajuste de tiempo de espera activo determina cuando se quita un flujo activo de la memoria caché y se exporta a un colector. Una vez que el flujo se exporta desde la caché, se crea un nuevo flujo tan pronto como un paquete de la sesión atraviesa el dispositivo de exportación. Debido a este comportamiento, una sola sesión IP puede tener varios flujos. La herramienta “nfdump” tiene una función de agregar los flujos y ensambla los registros Netflow separados debido a los tiempos de espera activa.

3.1.2.1.5. ANALIZADOR NETFLOW

Netflow puede ser utilizado para determinar cuándo se ha producido una transacción de red específica, como una conexión a un destino malicioso, o el tráfico que no cumpla con ciertos criterios. Puede incluir los servicios IP que no fueron autorizados, así como las transferencias de archivos grandes y conexiones de botnet servidores de comando y control.

Tener múltiples colectores permite consultas globales que se ejecutan directamente en cada colector en paralelo. Esta opción se aprovechará de la CPU adicional y el disco "I / O" de cada colector, y aumentará la velocidad de la consulta. Además, si el tráfico sólo pasa a través de un único colector (tal como un único host interno que tengan una conexión de salida) sólo eso colector tiene que ser consultado, reduciendo la cantidad de registros Netflow que necesitan ser procesados.

Casi cualquier herramienta en la que se puede consultar la base de los campos contenidos en las cabeceras de Netflow puede ser utilizado para detectar los mismos incidentes. Los campos más frecuentemente utilizados para la respuesta a incidentes son el tiempo, la fuente IP / puerto, destino de IP / puerto, número de paquetes y bytes.

3.1.2.1.5.1. NETFLOW TRAFFIC ANALYZER

> "Orion NetFlow Traffic Analyzer (NTA) le permite capturar datos desde secuencias continuas de tráfico de red y convertir esos valores sin procesar en cuadros y tablas fáciles de interpretar que cuantifican exactamente cómo se está utilizando la red corporativa, quién la utiliza y con qué fin. Y con la supervisión de CBQoS, puede estar seguro de que las políticas que ha establecido le dan a su tráfico esencial el más alto nivel de prioridad. Hacemos que sea fácil obtener una visión integral de su tráfico de red, buscar los cuellos de botella y terminar con los excesos de banda ancha.
>
> Puntos destacados de NetFlow Traffic Analyzer:
>
> - Identifica cuáles usuarios, aplicaciones y protocolos están consumiendo la mayor cantidad de banda ancha de la red y destaca las direcciones IP de los principales conversadores de la red.
> - Supervisa el tráfico de red al capturar los datos de flujo desde los dispositivos de red, incluidos Cisco® NetFlow v5 o v9, Juniper® J-Flow, IPFIX y sFlow®.
> - Asigna el tráfico que llega desde puertos designados, IP de origen, IP de destino e incluso protocolos a nombres de aplicaciones que puede reconocer fácilmente.

- Proporciona una notificación de alerta instantánea, que incluye una lista de los principales conversadores, cuando una interfaz supera su umbral de utilización.
- Realiza supervisión de calidad de servicio basado en la clase (CBQoS) para asegurar que sus políticas de priorización de tráfico sean efectivas.
- Le permite obtener rápidamente detalles del tráfico en elementos de red específicos, utilizando vistas simples para obtener la perspectiva que busca.
- Genera informes de tráfico de red con solo un par de clics.
- Facilita la investigación de problemas de fallas, rendimiento y configuración gracias a la completa integración con Orion NPM y Orion NCM".*[7]SolarWinds Inc. (2012)*

3.1.2.1.5.2.CARACTERÍSTICAS DE NETFLOW TRAFFIC ANALYZER

"Análisis detallado de tráfico.

NetFlow Traffic Analyzer (NTA) le proporciona vistas sin precedentes del tráfico de red, lo cual le permite asegurar de manera proactiva que esté optimizando los recursos de red. Al examinar los datos de flujo en los enrutadores y conmutadores de proveedores líderes, NTA determina el tráfico según el usuario, la aplicación, el departamento, la conversación, la interfaz, el protocolo y el tipo de servicio.

La integración con Orion proporciona a los usuarios amplios análisis de los patrones de tráfico y del rendimiento de los dispositivos, lo cual genera una visibilidad profunda de las estadísticas de uso, rendimiento y disponibilidad.

NetFlow problemas forenses

NTA hace que sea rápido y fácil investigar y aislar la utilización excesiva del ancho de banda y el tráfico inesperado de las aplicaciones, además de analizar el rendimiento de calidad de servicio por usuario, grupo, aplicación, país o protocolo.

Asignación avanzada de aplicaciones

Saber que el 98% de su ancho de banda es "tráfico web" es bueno. ¡Pero saber qué porcentaje es utilizado por YouTube™, Facebook® o Amazon® en comparación con las aplicaciones empresariales críticas como Salesforce. com® es realmente útil! Orion NTA correlaciona el tráfico que llega desde puertos designados, IP de origen, IP de destino e incluso protocolos a nombres de aplicaciones que puede reconocer fácilmente.

Generador de vista de tráfico de red

Con Orion NetFlow Traffic Analyzer, puede crear y compartir vistas personalizadas del tráfico de red. Puede ser lo específico que usted desee; si desea ver el tráfico de dominio generado durante el horario de atención estándar desde una dirección IP específica, no hay problema. ¡Con su propia vista personalizada del tráfico de red, puede aislar rápidamente y supervisar continuamente esas aplicaciones y usuarios problemáticos!

Optimización de principal conversador

La optimización de principal conversador le permite enfocar su análisis de tráfico en los usuarios y las aplicaciones que consumen la mayor parte del ancho de banda de la red. Orion NTA determina cuáles flujos son representativos de la mayor parte del uso del ancho de banda y almacena estos flujos mientras que no tiene en cuenta los datos de flujo de los usuarios y las aplicaciones que tienen un impacto insignificante en el ancho de banda general. Esta elegante solución mejora el rendimiento general de Orion NTA hasta 10 veces al capturar los flujos que representan el 95% del tráfico de red total.

Alertas de interfaz con detalles de principal conversador

Con Orion, puede configurar fácilmente una alerta de utilización de interfaz para notificarlo cada vez que el consumo de banda ancha exceda su umbral definido y también determinar rápidamente quién la está consumiendo. Por lo tanto, la próxima vez que Ann de Finanzas vea videos de Justin Bieber en Youtube y que ataque la interfaz primaria de puerta de enlace de Internet, obtendrá una notificación de alerta por correo electrónico que le informará que la utilización del ancho de banda para esa interfaz se está acercando a su capacidad con una lista de los principales conversadores para que pueda quitar prioridad instantáneamente al tráfico de Youtube de Ann.

Vistas de rendimiento de CBQoS

Con NTA, puede ver el tráfico de red segmentado por métodos de clase de servicio, como tipo de servicio o DSCP. Además, puede cuantificar rápidamente la cantidad de ancho de banda que está consumiendo cada uno de sus niveles críticos de calidad de servicio, incluidos los datos de voz y video, para determinar si su red está configurada para satisfacer los objetivos de su compañía.

Grupos de direcciones IP

¡Cree sus propios grupos de direcciones IP para ver el tráfico de red en la forma en que USTED desea verlo! Con la función de grupos de direcciones IP, puede ver el tráfico de red por rangos múltiples de direcciones IP (incluso direcciones IP superpuestas), por geografía, departamento o incluso tipos de dispositivos como servidores de seguridad, enrutadores, conmutadores y servidores.

Integración con Orion NPM

Orion NTA es parte de la familia Orion, que proporciona todos los beneficios de escalabilidad y estabilidad empresarial que ya conoce y aprecia. Orion NTA incorpora supervisión de tráfico de NetFlow, J-Flow, sFlow®, IPFIX y CBQoS en los cuadros, gráficos, tablas, listas de los 10 principales e informes basados en la web familiares e intuitivos de Orion.

Informes basados en el flujo

Los informes de estilo Orion pueden ejecutarse y programarse con NTA, lo cual hace que sea rápido y simple crear informes profundos de tráfico de red con solo algunos clics del mouse, o programar la entrega semanal automática a su equipo de administración. Los informes instantáneos incluyen lo siguiente:

- ✓ Tráfico por principales recursos xx basados en porcentajes de los 100 principales elementos
- ✓ Tráfico por principales aplicaciones xx, extremos, protocolos y dominios en "y" días
- ✓ Tráfico por grupo de direcciones IP en y días.**"***[7]SolarWinds Inc. (2012)*

3.1.2.2. SNMP

3.1.2.2.1. DEFINICIÓN DE SNMP

La definición del Protocolo SNMP la podemos encontrar en Microsoft y nos dice:

> "El Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) es un estándar de administración de redes utilizado en redes TCP/IP.
>
> SNMP proporciona un método de administración de hosts de redes como concentradoras, puentes, enrutadores y equipos de servidor o estaciones de trabajo desde un equipo central donde se ejecuta software de administración de redes. SNMP realiza servicios de administración mediante una arquitectura distribuida de sistemas de administración y agentes."*[8]Microsoft (2015).*

Es un protocolo de capa de aplicación, facilita el intercambio de información sobre la gestión de los dispositivos de red, tales como nodos y routers. Comprende parte de la suite TCP / IP. Los administradores del sistema pueden administrar de forma remota rendimiento de la red, encontrar y resolver problemas de red, y panificar el crecimiento de la red mediante el uso de SNMP.

3.1.2.2.2. UTILIDAD DEL PRORTOCOLO SNMP

"Puesto que la administración de redes es fundamental para la administración de recursos y auditoría, SNMP puede utilizarse para:

- **Configurar dispositivos remotos.** La información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración.

- **Supervisar el rendimiento de la red.** Puede hacer un seguimiento de la velocidad de procesamiento y el rendimiento de la red, y recopilar información acerca de las transmisiones de datos.

- **Detectar errores en la red o accesos inadecuados.** Puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos. Cuando se dispara una alarma, el dispositivo envía un mensaje de suceso al sistema de administración. Entre las causas más frecuentes de alarma se incluye el cierre y reinicio de un dispositivo, un error de un vínculo detectado en un enrutador y un acceso inadecuado.

- **Auditar el uso de la red.** Puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario, y los tipos de uso de servicios y dispositivos de la red."*[8]Microsoft (2015).*

3.1.2.3. RMON

3.1.2.3.1. DEFINICIÓN DE RMON

"RMON protocolo para la monitorización remota de redes. Es un estándar que define objetos actuales e históricos de control, permitiendo que usted capture la información en tiempo real a través de la red entera. El estándar de RMON es una definición para Ethernet, además de formar parte del protocolo TCP/IP.

El MIB de RMON proporciona un método estándar para vigilar las operaciones básicas de Ethernet. RMON también proporciona un mecanismo para notificarle de cambios en el comportamiento de la red."*[9]EcuRed (2015)*

Supervisión de red remota (RMON) es el estándar de cómo controlar el tráfico de Internet. Esta es una norma que supuestamente está implementado por los proveedores de dispositivos de Internet para que una red utilizando dispositivos RMON compatibles puede ser monitoreado utilizando el software. Por lo general, se define de modo que se puede implementar en una red genérica. Pero alguna especificación es creado para el seguimiento de las redes de monitoreo de red Ethernet, ya que es una de la red más popular en internet

3.1.2.3.2. UTILIDAD DEL PROTOCOLO RMON

> "Usted puede utilizar RMON para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite que usted detecte, aísle, diagnostique, y señale problemas potenciales y reales de la red antes de que se extiendan a las situaciones de crisis. Por ejemplo, Ethernet DCM puede identificar los ordenadores principales en una red que generan la mayoría del tráfico o los errores.
>
> RMON permite que usted instale las historias automáticas, que el agente de RMON recoge durante todo el tiempo, proporcionando datos en la estadística básica tal como la utilización, colisiones. RMON automatiza esta colección de datos y proporciona a otros datos del proceso las hojas de operación (planning), el proceso es más fácil y el resultado más exacto."*[9]EcuRed (2015)*

El objetivo general de RMON consiste en permitir que los dispositivos de vigilancia de red sean construidos. Estos dispositivos son generalmente, mencionados como monitores o sondas, que miden aspectos específicos de la red sin interferir las operaciones normales. Estos dispositivos son generalmente dispositivo independiente y situado en zona remota de la red o incluso a través de fronteras de la red. El estándar RMON permite que estos dispositivos se comuniquen a través de la red que están monitoreando.

3.2. MONITOREO DE RED

3.2.1. DEFINICIÓN DE MONITOREO DE RED

> "Se conoce con el nombre de monitoreo de red a un sistema que realiza un control constante de una red de ordenadores, intentando detectar defectos y anomalías; en caso de encontrar algún desperfecto, envía un informe a los administradores. El monitoreo de red se diferencia claramente de los sistemas diseñados para detectar intrusos: este último se encarga de buscar intentos no autorizados de ingresar en la red, mientras que el primero trabaja sobre los potenciales errores internos de los servidores."*[10]Definición.de (2015).*

El Monitoreo de red es la función de recogida de información de gestión de red. Las aplicaciones de monitoreo de red sirve para recopilar datos para aplicaciones de gestión de red. El objetivo es la recolecta de información útil de varias partes de la red para que esta pueda ser gestionada y controlada utilizando la información recopilada. La mayoría de los dispositivos de red están ubicados en lugares remotos. Estos dispositivos no suelen tener terminales conectados directamente, por lo que la aplicación de gestión de red no puede controlar sus estados fácilmente. Por lo tanto, las técnicas de monitorización de red se desarrollan para permitir que las aplicaciones de gestión de red puedan comprobar los estados de sus dispositivos.

3.2.2. HERRAMIENTAS

3.2.2.1. WHIRESHARK

> "Es un programa de software libre y multiplataforma, que podremos instalar tanto en Windows, como en Mac o Linux. Para capturar tramas directamente de red es necesario ejecutarlo con permisos de súper usuario, razón por la cual es recomendable utilizarlo con mucho cuidado y establecer la configuración de forma adecuada para los propósitos de nuestra empresa.

> Para sacarle todo el partido deberemos saber realizar filtros para la información recibida de forma que no nos veamos desbordados por la información que nos proporciona Para muchos el principal programa de referencia en su sector. Se trata de un analizador de protocolos que permite realizar análisis y solucionar problemas en redes de comunicaciones. Posee una interfaz gráfica que nos permitirá interpretar mejor la información que nos proporciona. Nos permite analizar todo el tráfico de una red ethernet, aunque también se puede utilizar en redes de otro tipo, estableciendo la configuración en modo promiscuo lo que le permite capturar todo el tráfico de la LAN."*[11]Pymesyautonomos (2015).*

Wireshark es una herramienta de código abierto para crear perfiles de tráfico de la red y el análisis de los paquetes. Tal herramienta se refiere a menudo como un analizador de red, analizador de protocolo de red o sniffer. Muchos desarrolladores de redes de todo el mundo han contribuido a este proyecto con el análisis de redes, resolución de problemas, desarrollo de software y protocolos de comunicación. Wireshark se usa en muchas instituciones educativas y otros sectores industriales Anteriormente, este tipo de herramientas eran muy caras, sin embargo con el llegada de Wireshark, todo ha cambiado. Este actualmente se considera como un de los más completos analizadores de paquetes con código abierto disponibles.

3.2.2.1.1. COMPONENTES DE WIRESHARK

Los menús de comando son menús desplegables estándar situados en la parte superior de la ventana. De interés para nosotros son los menús de archivo y captura. El menú Archivo permite guardar datos en paquetes capturados o abrir un archivo que contiene datos de paquetes previamente capturados, y salir de la aplicación Wireshark. El menú Captura le permite comenzar la captura de paquetes.

La ventana de paquetes listado muestra un resumen en una línea por cada paquete capturado, incluyendo el número de paquetes (asignado por Wireshark, lo que no es un número de paquetes que figura en la cabecera de cualquier protocolo), el momento en que fue capturado el paquete, la fuente del paquete y las direcciones de destino, el tipo de protocolo, e información específica del protocolo contenida en el paquete. La lista de paquetes se puede clasificar de acuerdo a cualquiera de estas categorías haciendo clic en un nombre de columna. El campo de tipo de protocolo enumera el protocolo de nivel más alto que envía o se recibe este paquete, es decir, el protocolo que es la fuente o sumidero final para este paquete.

La cabecera de detalles de la ventana del paquete proporciona detalles sobre el paquete seleccionado (resaltado) en la ventana de paquetes listado. Estos detalles incluyen información sobre la trama de Ethernet y de datagramas IP que contiene este paquete. La cantidad de Ethernet y detalle IP-capa visualizada se puede ampliar o minimizar haciendo clic en el botón derecho del puntero o la punta de flecha que apunta hacia abajo a la izquierda de la trama Ethernet o línea de datagramas IP en la ventana de detalles del paquete. Si el paquete se ha realizado a través de TCP o UDP, TCP o UDP detalles también se mostrará, que de igual forma se puede ampliar o minimizado. Por último, también se proporcionan detalles sobre el protocolo de más alto nivel que envió o recibió este paquete.

La ventana de paquetes de contenido muestra todo el contenido del fotograma capturado, tanto en formato ASCII y hexadecimal.

Hacia la parte superior de la interfaz gráfica de usuario Wireshark, es el campo de filtro de visualización de paquetes, en la que un nombre de protocolo u otra

información se pueden introducir con el fin de filtrar el información que se muestra en la ventana de paquetes listado.

3.2.2.2. NAGIOS

> "Nagios es un sistema de monitorización en software libre, bajo licencia GPL2, que nos permite conocer en todo momento el estado de nuestros sistemas, monitorizando nuestra granja de servidores y los servicios que en éstos se alojan, generando alertas y alarmas cuando el comportamiento de los mismos no sea el esperado. Esta monitorización permite a los administradores de sistemas abstraerse de la vigilancia continua, permitiéndoles desempeñar otras funciones y tareas sin tener que estar constantemente revisando que todo está funcionando. Para la recepción de alarmas, la aplicación es bastante flexible puesto que éstas pueden recibirse mediante correo electrónico. SMS, a través de un servidor de mensajería Jabber o utilizando un plugin para Thunderbird. Dentro de las capacidades de la aplicación se encuentra la de monitorizar servicios de red, la gestión vía SNMP (que quizás sea uno de los aspectos más importantes) o la monitorización de recursos hardware (carga del procesador, espacio en disco, memoria, estado de los puertos, etc.). Cualquier sistema que soporte SNMP es susceptible de ser monitorizado con Nagios (switches, routers, puntos de acceso, servidores de cualquier tipo, etc.)."*[12]Hipertextual (2015).*

Nagios es una herramienta de código abierto distribuido bajo los términos de la Licencia Pública General de GNU (GPL). No hay costo alguno para utilizar el software, a menos que se tenga que pagar por ayuda profesional. Nagios fue escrito originalmente para ejecutarse en Linux, pero debería funcionar bajo casi cualquier variante de Unix con un compilador C. Además, la máquina debe tener un servidor HTTP y una pila TCP disponible.

3.2.2.2.1. CARACTERISTICAS DE NAGIOS

Programación de tiempo inactivo.- Es posible, usando la interfaz web de Nagios, para programar el tiempo de inactividad de hosts o servicios individuales. Esto

significa que los controles de los hosts y los servicios serán suspendidos hasta que termine el tiempo de inactividad programado.

Controladores de eventos.- Un controlador de eventos es una escritura automática que se inicia cuando un servicio supervisado entra en un estado particular.

Por ejemplo, si una máquina es propensa a tener su accidente de instalación de Apache, un script puede ser escrito que intentará reiniciar los daemon y sólo el administrador de este no se realiza correctamente.

Las escaladas de notificación.- Nagios apoya escaladas de notificación, un método de alertar a grupos adicionales o diferentes de los administradores cuando un problema queda sin resolver.

Dependencias de servicio.- En un caso como éste, los servicios en el servidor Web serán inalcanzables desde el servidor Nagios si hay algo mal con el router de frontera. Este permite Dependencias de servicio que se añade a la configuración, por lo que en una situación así, el servidor Web no estaría controlado hasta que el router Frontera esté funcionando correctamente de nuevo.

3.2.2.3. WINDUMP

> "Es la versión para sistemas Windows de TCPDump, un paquete disponible en Linux y Unix, entre otros sistemas para capturar los paquetes de datos que circulan por la red de nuestra empresa. Tiene una gran funcionalidad, pero muchos pensarán que le falla el aspecto gráfico, puesto que funciona por línea de consola, algo cada día más en desuso sobre todo en sistemas Windows, donde muchos prefieren disponer de una interfaz gráfica aún a costa de un rendimiento algo menor. Es una herramienta de análisis muy potente, que para utilizar correctamente debemos dominar los comandos básicos y saber

> extraer la información necesaria en la que estamos interesados. De igual modo que en el caso anterior, establecer filtros para tratar de segmentar el filtrado de paquetes es fundamental para poder analizar la información y no vernos desbordados."*[11]Pymesyautonomos (2015).*

Es un software que nos permite ver dentro de la actividad del tráfico que se produce en una red. Es una herramienta de Unix utilizado para recoger datos de la red, descifrar los bits, y mostrar la salida en un formato legible para las personas. El tráfico de red viaja en paquetes de datos; cada paquete de datos contiene la información que necesita para viajar a través de la red. Esta información está contenida en un encabezado TCP. Un encabezado TCP contendrá el destino y la dirección de origen, información de estado y los identificadores de protocolo. El resto del paquete contiene los datos que se está enviando. Los dispositivos que se encargan de enrutamiento leen la información de estos paquetes y los envía a su destino correcto. Sniffing es un proceso que supervisa de forma pasiva y captura estos paquetes. Es una herramienta de paquetes sniffer que es utilizado por los administradores de red para rastrear y analizar el tráfico en una red.

3.2.2.4. PRTG

> "PRTG Network Monitor es una herramienta de monitoreo de tráfico en la red establecido, popular y asequible que le permite gestionar su red como usted lo quiere. Gracias a su soporte de SNMP, packet sniffing, y NetFlow / sFlow / jFlow, el software muestra los datos de tráfico en gráficos y tablas claras. Puede acceder a estos datos a través de su navegador, o exportarlos como informes. Así, es muy fácil monitorear el tráfico de la red. Si monitoriza el tráfico de la red se puede: Prevenir cuellos de botella de la banda ancha y del rendimiento de sus servidores; Descubrir qué programas causan más tráfico de red**;** Actuar de forma proactiva y dar un servicio mejor a sus usuarios**;** Reducir costes comprando el ancho de banda y hardware

según sus necesidades reales**;** Resolver problemas de conectividad con facilidad.”*[13]Paessler AG (2015).*

PRTG es la solución de supervisión de red de gran alcance. Asegura la disponibilidad de los componentes de red, mide el tráfico y el uso. Se ahorra costes al evitar interrupciones, optimizando las conexiones, el ahorro de tiempo y control de los acuerdos de nivel de servicio. Es la herramienta de monitoreo de última generación que combina el interfaz basada en la web y un nuevo estado de la supervisión técnica adecuado para redes de cualquier tamaño. Es una aplicación de monitoreo de red de gran alcance para los sistemas basados en Windows. Es adecuado para pequeñas, medianas y grandes redes, capaz de LAN, WAN, WLAN, y la supervisión de VPN. También puede supervisar web físico o virtual, electrónico y servidores de archivos, sistemas Linux, los clientes de Windows, routers, y muchos más. PRTG supervisa disponibilidad de la red y la utilización de ancho de banda, así como otros parámetros de red, tales como la calidad de servicio, carga de memoria, y usos de la CPU. Proporciona a los administradores de sistemas con lecturas en vivo y las tendencias de uso periódicas para optimizar la eficiencia, el diseño y la configuración de líneas arrendadas, routers, firewalls, servidores y otros componentes de la red.

El software es fácil de instalar y de usar, supervisa una red utilizando Simple Network Protocolo de administración (SNMP), Windows Management Instrumentation (WMI), analizador de paquetes, Cisco NetFlow (así como IPFIX, sFlow y jFlow), y muchos otros protocolos estándar de la industria. Se ejecuta en una máquina con Windows en su red durante 24 horas todos los días. Parámetros PRTG

Network y la disponibilidad de los sistemas de red. Los datos registrados se almacenan en una base de datos interna para su posterior análisis.

3.2.2.4.1. CARACTERISTICAS DE PRGT

Monitorea la red y no requiere software de terceros. La realización de una descarga ad-hoc rápida, no es necesario llenar los formularios web y no tiene ningún tipo de molestias de registro. El proceso de instalación requiere sólo unos pocos minutos, así como la primera configuración que se realiza principalmente de forma automática. La configuración inicial se logra mediante una guía interactiva por el software.

Alto rendimiento: propio sistema de base de datos rápida y eficiente de PRTG almacena los resultados brutos de vigilancia, así como los registros, toplists y boletos (supera a servidores SQL para los datos de vigilancia), accesibles a través de la interfaz de programación de aplicaciones (API). Puede distribuir las altas cargas sobre múltiples sondas.

Bajos requerimientos de sistema: Un promedio de PC desde el año 2007 es suficiente e incluso un netbook puede supervisar más de mil sensores.

Los altos estándares de seguridad: Cifrado SSL para las conexiones y servidor web, y múltiples cuentas de usuario con sensores privadas y compartidas, así como de gestión de derechos, y muchos más.

Además es construido en SSL de servidor web segura con HTTP y HTTPS, ayuda para la interfaz de usuario, el interfaz web rápido, trabaja como "Single Page Application" (SPA) para evitar la recarga de tiempo extenso la página, el servidor de correo tiene para la entrega automática de correo electrónico y maneja los diferentes idiomas como el Inglés, alemán, español, francés, portugués, holandés, checo, japonés y chino simplificado.

3.2.2.5. CACTI

> "Con Cacti podremos monitorizar cualquier equipo de red que soporte el protocolo SNMP, ya sea un switch, un router o un servidor Linux. Siempre que tengan activado el protocolo SNMP y conozcamos las MIBs con los distintos OIDs (identificadores de objeto) que podemos monitorizar y visualizar, podremos programar la colección de gráficas con las que queramos realizar el seguimiento. Cacti es una aplicación que funciona bajo entornos Apache + PHP + MySQL, por tanto, permite una visualización y gestión de la herramienta a través del navegador web. La herramienta utiliza RRDtool, que captura los datos y los almacena en una base de datos circular, permitiendo visualizar de forma gráfica los datos capturados mediante MRTG.
>
> El funcionamiento de Cacti es bastante sencillo, la aplicación sondea a cada uno de los hosts que tiene configurados solicitando los valores de los parámetros, OIDs, que tiene definidos y almacenando el valor. El período de sondeo es configurable por el administrador, éste determinará, entre otros factores, la precisión de la información a visualizar, ya que un período bajo aumentará la cantidad de datos capturados y, por tanto, la resolución de la representación gráfica. Sin embargo, un período corto de muestreo aumentará la carga del sistema."*[14]Hipertextual (2015).*

CACTI utiliza un conjunto de aplicaciones de hacer web visual graficando los resultados extraídos a través de SNMP. Estos valores pueden variar de las tasas de entrada / salida en las interfaces de red / servidor a la cantidad de direcciones MAC asociada a un punto de acceso dado. Usando SNMP para administrar una red puede

proporcionar un punto central no técnico de consolidación y vigilancia de la salud de su infraestructura, es algo que ya es o puede ser fácilmente activado en muchos dispositivos con capacidad IP. Usando SNMP para sacar constantemente información estadística y graficar esa información puede ser útil en el seguimiento de las cosas, como la utilización del disco, la actividad de red y mucho más. La aplicación CACTI requiere varias utilidades para ser configurados para trabajar juntos con el fin de presentar la información en una interfaz GUI web. Estas utilidades incluyen un servidor web, una base de datos, PHP y RRDTOOL, todo lo cual es de libre acceso para el sistema operativo Linux.

3.2.2.5.1. CARACTERÍSTICAS DE CACTI

- Cacti se escribe como un grupo de scripts PHP.
- El guion clave en "poller.php", que se ejecuta cada 5 minutos (por defecto).
- Cacti usa RRDtool para crear gráficos para cada dispositivo y los datos que se recaba sobre ese dispositivo. Se puede ajustar todo esto desde la interfaz web Cacti.
- Los ficheros RRD se encuentran en "/var/lib/cacti/rra" cuando cactus se instala desde los paquetes.

Ventajas

- Se puede medir Disponibilidad, carga, errores y más, todo con la historia.
- Cacti puede ver las interfaces de router y conmutación y su tráfico, incluyendo todo el tráfico de error también.

- Cacti puede medir la capacidad del disco, la carga de la CPU (red h / w y servidores) y mucho más. Puede reaccionar a las condiciones y enviar notificaciones sobre la base de los rangos especificados.
- Permite utilizar toda la funcionalidad de rrdgraph para definir gráficos y automatizar la forma en que se muestran.
- Permite organizar la información en estructuras de árbol jerárquico.
- Permite que usted pueda utilizar todas las funciones de rrdcreate y rrdupdate incluyendo la definición de varias fuentes de información para cada archivo RRD.

Desventajas

- La configuración de interfaces es tediosa
- Configuración del Plugin Arquitectura no es sencillo
- Actualización de las versiones pueden ser complejas

CAPÍTULO IV: WATERING HOLE ATTACK

4.1.GENERALIDADES

4.1.1. DEFINICIÓN

> "Agujero de riego es un ataque informático estrategia identificada en 2012 por RSA Security, en el que la víctima es un grupo en particular (organización, industria o región). En este ataque, el atacante adivina u observa los sitios web que el grupo utiliza a menudo e infecta a uno o más de ellos con el malware. Eventualmente, algún miembro del grupo objetivo se infecta. Basándose en los sitios web que los fideicomisos de grupo hace que esta estrategia eficiente, incluso con grupos que son resistentes a spear phishing y otras formas de phishing."*[15]Wikipedia (2015), Watering Hole, recogido de: http://en.wikipedia.org/wiki/Watering_Hole*

Una forma de agentes maliciosos intentan entregar software malicioso a organizaciones en industrias verticales específicas es mediante el uso de ataques "watering hole" (abrevadero). Al igual que el cazador está viendo a sus presas, los cyber delincuentes buscan dirigirse a un grupo en particular, supervisan los sitios web que frecuenta el grupo, infectan uno o más de estos sitios con malware, luego toca sentarse y esperar al menos que un usuario en el grupo objetivo visite ese sitio y se vea afectado por el ataque.

Figura 2: Realizar el Ataque Watering Hole. Año 2015

Fuente: *[16]Cristhian Borguello (2015)* http://www.mug-it.org.ar/343019-Watering-Hole-Attack-Metodo-de-espionaje-contra-las-empresas.note.aspx

Elaborado por: MUG

4.1.2. INCIDENCIA DEL WATERING HOLE ATTACK

A finales de abril de 2013, un ataque al watering hole fue lanzado desde las páginas específicas alojamiento de contenido relacionado nuclear en la web del Departamento de Trabajo de Estados Unidos. Luego, a partir de principios de mayo de 2013, se observa otro ataque watering hole que emana de varios otros sitios centrados en el sector de la energía y el petróleo. Similitudes, incluyendo la elaboración específica de un exploit utilizado en ambos ataques, dar credibilidad a la posibilidad de que los dos ataques estaban relacionados. La investigación Cisco TRAC / SIO también indicó que muchos de los sitios utilizan el mismo diseñador de

páginas web y el proveedor de hosting. Esto podría dar a entender que el compromiso inicial se debió a las credenciales de phishing o robo de ese proveedor.

La técnica de ingeniería social utilizada en ataques watering es estratégica. A diferencia de un ataque habitual de ingeniería social, los actores de amenazas que emplean la técnica de watering hole seleccionan cuidadosamente los sitios legítimos más adecuados para comprometer, en lugar de apuntar a sitios al azar. Debido a que los objetivos de la técnica es visitar sitios de confianza y sitios frecuentados, entonces confiando en los únicos sitios de confianza para evitar las amenazas en línea puede no ser una práctica efectiva.

En los casos en que los ataques abrevadero llevan a una RAT, los atacantes también pueden ejecutar comandos en los servidores infectados. Estos incluyen el espionaje y la vigilancia de las actividades de la organización de destino. Debido a que un atacante fue capaz de infiltrarse en la red de una organización específica, también pueden iniciar ataques que son perjudiciales para las operaciones de la organización, que incluyen la modificación o eliminación de archivos con información crucial.

4.1.3. FUNCIONAMIENTO DEL ATAQUE

Un ataque watering hole normalmente funciona de esta manera:

- ✓ Los atacantes se reúnen información estratégica que pueden utilizar para poder entrar en su organización específica. Este paso se puede comparar a una misión de reconocimiento militar. La información recopilada puede incluir ideas sobre los sitios web de confianza a menudo visitados por los empleados o miembros de

su entidad de destino. El proceso de selección de sitios web a compromiso se denominó inicialmente " compromisos web estratégicos.

- ✓ Los atacantes insertar un exploit en los sitios seleccionados.
- ✓ Una vez que las víctimas dirigidas visitan el sitio comprometido, el exploit se aprovecha de las vulnerabilidades del software, ya sea viejo o nuevo, para caer malware. El malware caído puede ser en forma de un troyano de acceso remoto (RAT), que permite a los atacantes acceder a datos sensibles y tomar el control del sistema vulnerable

Un ataque watering hole es esencialmente un fideicomiso exploit porque se emplean sitios web legítimos. También es una forma de Spear Phishing (lanza de pesca de contraseñas). Sin embargo, mientras Spear Phishing está dirigido a individuos selectos, watering hole está diseñado para comprometer a grupos de personas con intereses comunes. Los ataques watering hole no están discerniendo acerca de sus objetivos, cualquier persona que visita un sitio infectado está en riesgo.

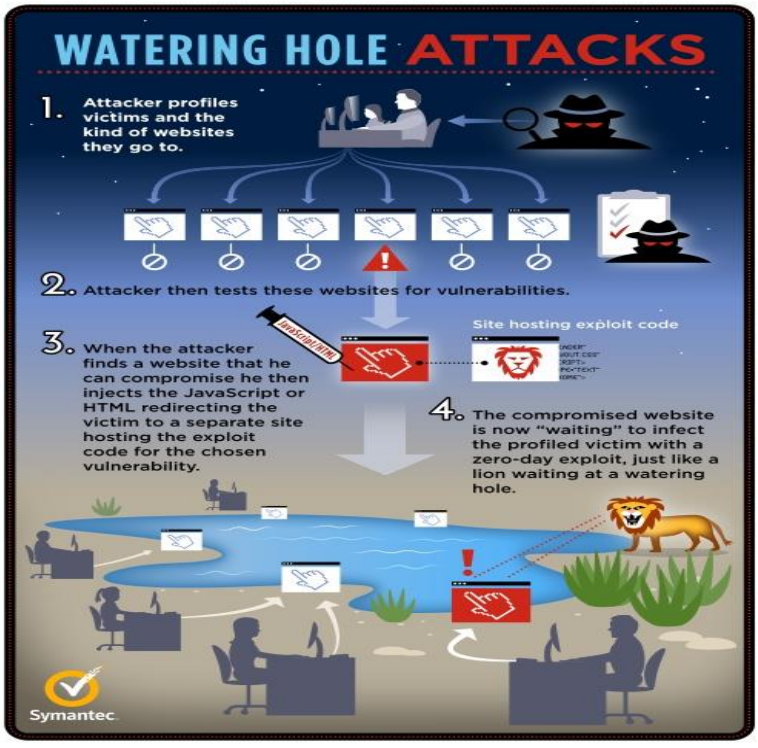
4.1.4. EFECTIVIDAD DEL ATAQUE

Los atacantes incorporan estrategias para eludir las defensas de las organizaciones específicas con el fin para que te ataque para ser eficaz. Estos pueden venir en forma de sistemas obsoletos o simplemente error humano. En el watering hole, el objetivo no es servir de software malicioso a tantos sistemas posibles. En cambio, los atacantes se ejecutan en bien conocidos y sitios de confianza que puedan ser

visitados por sus víctimas específicas. Esto hace que la técnica sea efectiva en la entrega de su carga útil prevista.

Aparte de elegir cuidadosamente los sitios frecuentes de los objetivos, el ataques es conocidos por incorporar exploits de día cero que se dirigen a las vulnerabilidades sin parches. Por lo tanto, las entidades objeto se quedan con poca o ninguna defensa contra estos exploits. Esto no significa que los atacantes no se dirigen a las vulnerabilidades del sistema parcheado. Debido a las dificultades de gestión de parches en un entorno empresarial, los administradores de TI pueden retrasar el despliegue de actualizaciones críticas. Esta ventana de exposición puede conducir a un ataque dirigido aprovechando de edad, pero las vulnerabilidades fiables.

Figura 3: Efectividad del ataque Watering Hole. Año 2015



Fuente: http://seguinfo.blogspot.com/2012/09/que-son-son-los-ataques-water-hole.html*[17]Symantec(2015)*

Elaborado por: Symantec

4.1.5. PREVENCIÓN DEL ATAQUE

Para tener un poco más de seguridad contra estos tipos de ataques se deben realizar las siguientes recomendaciones:

- **Actualización de software oportuna.** Para regar ataques agujero que emplean vulnerabilidades antiguas, la mejor defensa de una organización es actualizar los sistemas con los últimos parches de software ofrecidos por los vendedores.
- **Protección de vulnerabilidades.** También conocido como "parches virtuales", que opera en la premisa de que explota tomar una ruta de red definidos por el fin de utilizar una vulnerabilidad. Protección de vulnerabilidades ayuda a los administradores analizan el tráfico sospechoso, así como cualquier desviación de los protocolos típicos utilizados. Por lo tanto, este seguimiento permite a los administradores de sistemas para evitar exploits.
- **Detección de tráfico de red.** Aunque los atacantes pueden incorporar diferentes exploits o cargas útiles en su ataque, el tráfico generado por el programa malicioso definitiva cuando se comunica con los servidores de comando y control se mantiene constante. Mediante la detección de estas comunicaciones, las organizaciones pueden implementar fácilmente las medidas de seguridad para prevenir el ataque de una mayor escalada. Tecnologías como Trend Micro profundo descubrimiento puede ayudar a los administradores en la detección de tráfico de red sospechoso.

Las organizaciones también deben considerar la construcción de su propia inteligencia local para documentar los casos anteriores de ataques dirigidos dentro de

la empresa. Estos permiten a las organizaciones detectar posibles correlaciones y conocimientos necesarios para crear un plan de acción o una recuperación efectiva.

La protección de los usuarios frente a estos ataques consiste en mantener las máquinas y los navegadores web con todos los parches para reducir al mínimo el número de vulnerabilidades que un atacante puede explotar. Garantizar el tráfico web es filtrado y se comprueba en busca de malware antes de su entrega al usuario del navegador es algo esencial. Este tipo de ataques "watering hole" son cada vez más comunes como las campañas en línea dirigidas a grupos específicos en busca de la inteligencia, en oposición a los ataques masivos que todavía se producen a menudo, pero se centran principalmente en la ganancia financiera.

4.2. EXPLOITS Y MALWARE

4.2.1. EXPLOITS

4.2.1.1. DEFINICIÓN

> "Si bien no existe una definición universal de exploit, esencialmente el término se refiere a cualquier código diseñado para exponer las vulnerabilidades de otras aplicaciones, o aprovecharse de ellas. Los exploits de la red trabajan aprovechándose de las fallas de los navegadores o sus complementos, y de otros programas con acceso a Internet, incluyendo Microsoft Word, Adobe Acrobat y otras aplicaciones de uso habitual. Estas amenazas pueden tomar muchas formas diferentes: descargas forzadas, instalación de códigos maliciosos ocultos, infecciones silenciosas o automatizadas, pero todas tienen el mismo resultado: el ordenador se infecta solamente navegando por Internet, sin que sea necesario hacer nada especial como, por ejemplo, descargar un archivo. Los exploits permiten que los códigos maliciosos se instalen silenciosamente en el sistema, sin el conocimiento del usuario. Esto puede tener como consecuencia el robo de información, el mal funcionamiento del ordenador o su incorporación a una botnet, y otros problemas serios."*[18]*

Agnitum (2015), Exploits en la red, Recogido de pág. web: http://www.outpost-es.com/download/docs/security_insight/2007-10.pdf

Un exploit es un término general para cualquier método utilizado por los hackers para obtener acceso no autorizado a las computadoras, el acto mismo de un ataque informático, o un agujero en la seguridad de un sistema que abre un sistema para un ataque. El término es muy flexible y puede ser utilizado tanto como un sustantivo como un verbo. Como sustantivo, el exploit es el agujero en el sistema que el hacker utiliza para hacer el ataque. Muy a menudo, se trata de una vulnerabilidad desde un servidor sin parchear. Como verbo, se refiere al acto. Por ejemplo, podría escuchar "el hacker publicó detalles de sus exploits en su blog para mostrar lo fácil que era para entrar en servidores de XYZ."

4.2.1.2. CICLO DE VIDA

El siguiente grafico muestra cómo se encuentran las vulnerabilidades en un sistema, producto o aplicación y cómo actúan los exploits en el proceso, a esto se lo llama ventana de oportunidad

Figura 4: Ventana de Oportunidad - Ciclo de vida Exploits en la red

Fuente: [18]http://www.outpost-es.com/download/docs/security_insight/2007-10.pdf

Elaborado por: Agnitum

“1. La aplicación es lanzada al público.

2. Un investigador corrupto, o un delincuente informático descubre una vulnerabilidad en el programa, pero no da aviso al desarrollador. En lugar de esto, entrega esta información a los escritores de códigos maliciosos a cambio de dinero u otro tipo de recompensa. Se crea entonces una aplicación que se aprovecha de dicha vulnerabilidad.

Los desarrolladores de soluciones de seguridad aún no conocen estos programas dañinos, de modo que no pueden detectarlos. Generalmente, este tipo de amenazas se conoce como código malicioso de día cero.

3. El desarrollador de la aplicación vulnerable se entera del error a través de canales públicos. Esto puede ocurrir de varias formas. La más común es que información sobre el hallazgo se filtre en foros clandestinos que los piratas comparten.

También puede tomar conocimiento por medio de los propios usuarios, por comunicaciones de otros desarrolladores, o por trabajos de investigación paralelos realizados por investigadores honestos.

4. El código de prueba de concepto no lleva una carga maliciosa. Su función es, simplemente, probar la viabilidad de los hallazgos, y demostrar que, sin el parche adecuado, la vulnerabilidad realmente podría ser explotada. Un POC (Proof-of-concept, código de prueba de concepto) se usa principalmente para convencer de esto al desarrollador del programa en riesgo.

5. Una vez que el desarrollador evalúa el informe de vulnerabilidad, y concluye que es necesario crear un parche, comienza a trabajar en ello.

6. El desarrollador crea un parche para corregir la vulnerabilidad detectada. Posteriormente se distribuye la actualización de seguridad, usando el procedimiento estándar de la aplicación en cuestión.

7. El usuario instala el parche del fabricante, para proteger la aplicación contra posibles explotaciones de la vulnerabilidad.

En algún punto entre las etapas dos y siete, el exploit sale a la luz y comienza a infectar usuarios vulnerables.

Este período se denomina ventana de oportunidad, ya que los piratas informáticos pueden adueñarse de los sistemas de los usuarios sin que estos lo sepan, aprovechándose de las vulnerabilidades que no fueron detectadas o solucionadas.”[18]*Agnitum (2015), Exploits en la red, Recogido de pág. web: http://www.outpost-es.com/download/docs/security_insight/2007-10.pdf*

4.2.1.3. FUNCIONAMIENTO DE LOS EXPLOITS

"En ocasiones, se lanzan a la venta en el mercado clandestino paquetes de herramientas para crear exploits. Estos conjuntos de herramientas contienen un grupo de exploits que se aprovechan de las vulnerabilidades conocidas en complementos desarrollados por otras compañías, o en funciones del navegador (las cuales van desde la vulnerabilidad del cursor animado de Microsoft, hasta la sobrecarga de la memoria intermedia de QuickTime de Apple, o múltiples errores descubiertos en los controles ActiveX, JavaScript, y otras extensiones de Internet Explorer).

Una vez que los atacantes obtienen un exploit, necesitan esconderlo de forma tal que los usuarios que visitan ciertos sitios —ya sea de manera deliberada, o accidentalmente— sean infectados automáticamente, y sin que tomen conocimiento de esto.

Existen varias formas de atraer víctimas a un sitio malicioso, pero típicamente los piratas usan uno o más de los siguientes recursos:

- ✓ Envían mensajes de correo electrónico no solicitados para hacer que los usuarios visiten un sitio mantenido por el delincuente informático. Para conseguir este objetivo también se utilizan otras técnicas sofisticadas, como la suplantación de direcciones DNS (Domain Name Service, servicio de nombres de dominio), los ataques de ingeniería social y otras tácticas predatorias.
- ✓ Crean una serie de sitios infecciosos cuyos nombres sean similares a los de entidades legítimas, registrando direcciones en Internet que apenas se diferencien de las originales (por ejemplo, microsooft.com o dowload.com).
- ✓ Infectan sitios web pertenecientes a entidades legítimas, infiltrando los códigos maliciosos antes de que sus administradores puedan bloquear la intrusión. El Banco de la India sufrió un ataque de este tipo recientemente.
- ✓ Ponen enlaces a elementos multimedia en sitios de encuentros sociales, tales como FaceBook o MySpace, que en realidad apuntan a códigos maliciosos externos. Estos se aprovechan de las vulnerabilidades de los complementos desarrollados por otras empresas y que son necesarios para ejecutarlos"[18]*Agnitum (2015), Exploits en la red, Recogido de pág. web: http://www.outpost-es.com/download/docs/security_insight/2007-10.pdf*

Los cibercriminales están siempre buscando maneras más fáciles de lograr sus objetivos de hacer dinero. Una de las herramientas que ha tenido más éxito ha sido

los kits de herramientas exploits. Estas Conjuntos de herramientas consisten en una serie de exploits, un panel de control para configurar varios aspectos del kit, qué exploits se va a utilizar, las direcciones IP a la lista negra, cómo ver estadísticas, entre otros y también la configuración de la base de datos donde se almacena toda la información, la guía de instalación mediante archivo de texto se incluye a menudo.

Los kits son vendidos y entonces los sitios vulnerables focalizados y en peligro realizan la redirección a sitios que alojan el código principal del kit exploits. El código fuente tiende a ser difícil de conseguir debido a los archivos PHP que se codifican utilizando el codificador ioncube, un codificador de PHP comercial diseñado para ayudar a los autores de software proteger su código fuente PHP. Los fabricantes de estos kits manejan sus negocios de manera similar a unas empresas de software legítimo.

Por lo general tienen paneles de control que proporcionan opciones estadísticas, de configuración y administración. Para los investigadores, las páginas de estadísticas tienden a ser la pieza más interesante, ya que ofrecen información sobre el éxito que tendrán en su explotación. Incluso hacer su propio marketing en foros clandestinos anunciando estos lanzamientos y en ocasiones acusa a sus competidores de robar componentes tales como aspecto y estilo o exploits específicos del kit.

Los autores de los kits hacen afirmaciones inverosímiles acerca de las tasas de infección y restan importancia a las de sus competidores en un intento de reunir más ventas. Los índices de infección en los kits de exploits jóvenes bajas son característicos para la mayoría de los exploits mayores incluidos en los kits, mientras exploits más recientes experimentan significativamente más altas tasas de infección.

4.2.1.4. PROTECCIÓN CONTRA EXPLOITS

"Existe una serie de pasos muy sencillos que los usuarios pueden seguir para proteger sus ordenadores de la amenaza de los exploits:

1. Mantener actualizados los parches del sistema, y utilizar siempre la última versión del navegador.

2. Desactivar funciones de programación innecesarias, como códigos ActiveX, o permitir solamente que estas sean usadas en sitios previamente revisados y confiables.

3. No visitar sitios desconocidos, o que puedan resultar poco confiables.

4. Usar programas que examinan el contenido de los sitios web en tiempo real, antes de permitir que el usuario acceda a ellos. Programas como Link Scanner Pro, revisan el código HTML del sitio de destino, para asegurarse de que no tiene amenazas ocultas. La extensión Finian SecureBrowsing realiza una evaluación del código y de la reputación del sitio, para estimar así la amenaza potencial.

5. Utilizar un cortafuego que proteja el sistema contra códigos maliciosos del tipo día cero, bloqueando cualquier actividad inadecuada dentro de la red o de las aplicaciones locales. Outpost Firewall Pro 2008 incluirá la posibilidad de armar y personalizar una base de datos de sitios peligrosos cuyo acceso estará bloqueado."[18]*Agnitum (2015), Exploits en la red, Recogido de pág. web: http://www.outpost-es.com/download/docs/security_insight/2007-10.pdf*

4.2.2. MALWARE

4.2.2.1. DEFINICIÓN

Malware, también conocido como código malicioso, es la abreviatura de software malicioso y se utiliza para referirse ampliamente a cualquier software que no está autorizado y secretamente se inserta en un sistema informático con la intención de poner en peligro la confidencialidad, integridad de la información o datos de la

víctima, las aplicaciones, sistemas operativos u otro modo molesto de interrumpir la víctima.

En la década de 1980, el malware era ocasionalmente una molestia o molestias a las personas y organizaciones, en la actualidad el malware es la amenaza externa más importante para la mayoría de los sistemas, causando daños y trastornos generalizados que requieran esfuerzos de recuperación amplios dentro de la mayoría de las organizaciones.

4.2.2.2. CICLO DE VIDA

- **Creación.-** La creación de un malware requiere de un conocimiento de lenguaje de programación. Hoy en día cualquier persona con conocimientos de programación básica con acceso a Internet puede crear un malware. Hay muchos sitios web ofrecen descargas de malware con códigos fuente e instrucciones que muestran a las personas interesadas de cómo crear y difundir códigos maliciosos. También animan a las personas a desarrollar su propia versión nociva de un malware ya existente, y son programas maliciosos probados y comprobados. Estos kits son aplicaciones que generan malware y a menudo ofrecen a los usuarios la opción de crear malware personalizado, la mayoría de los kits pueden producir múltiples variaciones de un malware, muchos se han utilizado para generar nuevas variantes de gusanos existentes.

- **Replicación y Propagación.-** Los Malware se propagan en varias formas. Los gusanos pueden propagarse a través de correo electrónico, mensajería instantánea, o partes de la red. Los virus se replican dentro de un sistema, mientras que algunos virus también tienen las técnicas de propagación automáticas similares a gusanos. Los Troyanos si bien no tiene una forma automática de la replicación y propagación, son sin embargo disponibles en todo el Internet, y pueden ser incluidos en los enlaces para descargar en mensajes de correo electrónico u otros sitios Web.
- **Activación.-** La mayoría de los malware realizan sus actividades maliciosas en ejecución. Algunos tienen ciertas cargas útiles que se activan sólo a una cierta fecha de activación, o con el inicio de una condición de activación específica.
- **Descubrimiento.-** Esta fase no siempre sigue después de la activación (pero típicamente así sucede). Cuando un malware es detectado y aislado, se envía a la ICSA en Washington, DC, para que este sea registrado e informado a los desarrolladores del antivirus. Sin embargo, con el rápido desarrollo de la tecnología, y la facilidad con la que los autores de malware crean sus programas, la mayoría del malware se lanza a los usuarios desprevenidos incluso antes de que sean descubiertos por las "autoridades". Esta es una razón más para proteger su sistema contra las amenazas que rodean el mundo de la computación en la actualidad.
- **Asimilación.-** En este punto, los desarrolladores de software antivirus cambian su software para que pueda encontrar el nuevo malware. Esto puede tomar desde varias horas hasta varios días, todo en relación del desarrollador y el tipo de malware.

- **Erradicación.-** Si suficientes usuarios aplican un software de defensa antivirus actualizado, cualquier malware puede ser aniquilado. En la actualidad ningún malware han sido eliminado en su totalidad, pero ciertos malware ya no se consideran una amenaza importante.

4.2.2.3. CLASIFICACION DEL MALWARE

4.2.2.3.1. VIRUS

Un virus informático, comúnmente conocido como un virus, es un programa o una pieza de código ejecutable que tiene la capacidad de replicar su propio código (de auto-replicación) uniéndose a otros archivos ejecutables (infección archivo de host) y se propagan cuando los archivos se copian y envían de un individuo a otro. En tal forma que se ejecuta el código del virus cuando se ejecuta el archivo ejecutable infectado.

4.2.2.3.2. GUSANOS

Un gusano informático es un programa autónomo o conjunto de programas que es capaz de propagar copias funcionales de sí mismo o de sus segmentos a otros sistemas informáticos. La propagación suele efectuarse a través de conexiones de red o archivos adjuntos de correo electrónico. Por lo general, el gusano no requiere la interacción humana para propagarse. Gusano se propaga a través de vulnerabilidades o errores de configuración en los sistemas de destino. Sin embargo, para un pequeño

número de gusanos, alguna interacción de usuario es necesaria para la propagación (por ejemplo, la apertura de un visor de correo electrónico). Gusanos bien conocidos incluyen Code Red, Gusano Morris, SQL Slammer, Sasser y Netsky.

4.2.2.3.3. CABALLO TROYANO

Un troyano es un malware que realiza una acción malintencionada, pero no tiene capacidad de replicación. Acuñado de caballo de Troya de la mitología griega, un troyano puede llegar como un archivo de utilidad o aplicación y aparentemente inofensivo, pero en realidad tiene algo de mala intención oculta dentro de su código. Troyano suele tener una carga útil. Cuando se ejecuta un troyano, puede experimentar problemas del sistema no deseados en la operación, y en ocasiones la pérdida de datos valiosos. Troyanos bien conocidos incluyen Hydan y Setiri.

4.2.2.3.4. SPYWARE

Spyware es un término general usado para describir el software que ha diseñado para capturar información de o tomar el control de la computadora del usuario sin obtener el consentimiento de los usuarios por primera vez. Este software se divide en un número de categorías:

MONITOREO DE SEGURIDAD

El software que puede ser instalado legítimamente para proporcionar la supervisión de seguridad o lugar de trabajo.

PUBLICIDAD

Software que rastrea las actividades en línea de los usuarios con fines de marketing y muestra publicidad a través de ventanas emergentes o pop-under ventanas mientras se navega por la Web se suele llamar adware.

Adware es una aplicación publicitaria centrada en que ellos mismos se instala en sistemas con poca o ninguna interacción con el usuario.

Esto no significa que todo el software que proporciona anuncios o seguimiento de sus actividades en línea es malo. Por ejemplo, es posible suscribirse a un servicio de música gratuita, pero el usuario "paga" por el servicio al aceptar recibir los anuncios orientados. Si el usuario entiende los términos y está de acuerdo con ellos, es posible que haya decidido que es una compensación justa. También se puede acceder a que la empresa tenga seguimiento de sus actividades en línea para determinar qué anuncios que mostrar.

RECOPILACIÓN DE INFORMACIÓN PERSONAL O INFORMACIÓN SENSIBLE

Software que se instala con malicia, ya sea como una violación general de la privacidad de un usuario o de recoger información para permitir que nuevos ataques contra el ordenador o transacciones en línea. El software que recopila información personal o información sensible se llama spyware. Spyware es potencialmente bestia más peligrosa que Adware porque puede registrar las pulsaciones del teclado, historia, contraseñas y otra información confidencial y privada.

CAMBIO DE LA CONFIGURACIÓN DE SU ORDENADOR

Algún tipo de software, que modifican la computadora de los usuarios que pueden ser molestos y pueden causar ordenador ralentice o se bloquee. Estos programas pueden cambiar la página de inicio o de búsqueda la página de navegador web, o añadir componentes adicionales al navegador que los usuarios no necesitan o desean. Estos programas también hacen que sea muy difícil de cambiar la configuración de nuevo a la configuración original.

4.2.2.3.5. CODIGO MALICIOSO MOVIL

Código móvil malicioso es un término general para cualquier programa ligero ejecutable que se descarga desde un sistema remoto y ejecutado localmente con mínima o ninguna intervención del usuario para hacer algo que su sistema no quiere que haga. Código móvil malicioso puede ser una manera eficaz de los sistemas, así como un buen mecanismo para la transmisión de virus, gusanos y caballos de Troya a los usuarios atacar. Código móvil malicioso se diferencia de los virus y gusanos en que no infecta archivos o intentar propagarse. En lugar de explotar vulnerabilidades particulares, a menudo afecta a los sistemas de aprovechamiento de los privilegios predeterminados concedidos al código móvil. Lenguas populares para código móvil malicioso incluyen Java, ActiveX, JavaScript y VBScript. Uno de los ejemplos más conocidos de código móvil malicioso es Nimda, que utiliza JavaScript.

CAPÍTULO V: ANALISIS ESTADISTICOS NETFLOW CISCO

5.1. ANÁLISIS DE ASPECTOS GENERALES DE LA RED

5.1.1. PROBLEMAS Y NECESIDADES DE LA RED

Todas las redes son vulnerables a los ataques internos y externos, por lo que uno de los grandes problemas que presentan las redes son las seguridades, las cuales pueden ser vulneradas de diferentes maneras, debido a esto se debe auditar las redes para poder identificar usuarios ajenos a la red, también usuarios infiltrados en la redes capturando datos de la misma, robando datos sensibles e importantes de servidores o clientes conectados a servidores que contienen código malicioso para los ataques.

Generalmente las redes son expuestas a diferentes problemas de seguridad como:

- Ataque internos de la red
- Intercepción de correos electrónicos
- Estafas electrónicas
- Phishing
- Código malicioso
- Robo de contraseñas
- Ataques de hackers
- Explotación de vulnerabilidades conocidas
- Infección de servidores y equipos terminales con virus
- Pinchazos a la red
- Robos de información a bases de datos

- Desencriptar contraseñas de redes WiFi
- Robo de información de bases de datos

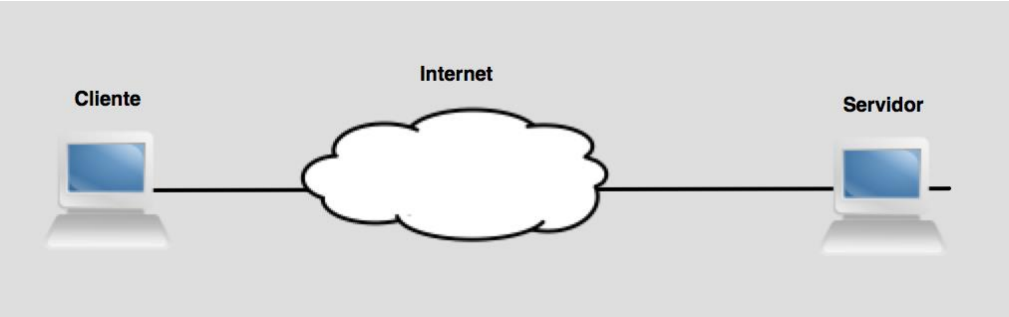
Existen una serie de problemas de seguridades que se presentan en cualquier topología de red. Una de las maneras de mitigar estos problemas que se pueden dar por las seguridades es aplicando medidas preventivas como firewalls, haciendo captura de datos con sniffers, usando políticas de seguridad interna, limitando el número de puertos de acceso a la red.

5.2. ESCENARIO A EJECUTAR

Se ha escogido un entorno simulado para analizar los problemas de las redes, en este caso se ha diseñado una topología vulnerable que nos permitirá obtener resultados cuando se exploten estas vulnerabilidades con equipos preparados para realizar estas acciones.

Se ha diseñado dos redes LAN, conectadas entre sí a través del internet.

Figura 5: Conexión LAN a través de internet. Año 2015



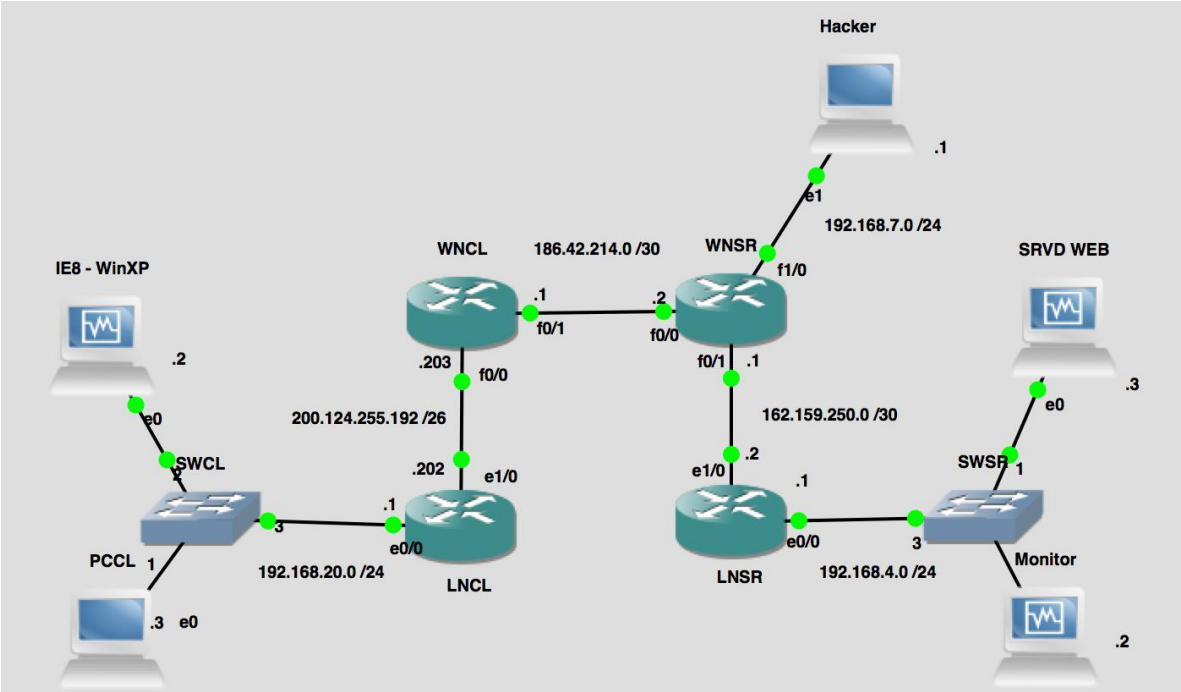
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

El área LAN de los clientes será denomina como LNCL y el área de los servidores como LNSR.

El área atacada será la de los servidores donde se explotarán las vulneranilidades de los navegadores y de las bases de Datos.

Figura 6: Topología de La Red. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

La topología presenta las siguientes características:

- Un cliente con sistema operativo Windows XP el que se encuentra en el área de clientes.
- El área LAN la que contiene a todos los clientes que soliciten servicios, los clientes pueden salir de la red mediante el router LNCL.

- El área WAN que permite el intercambio de datos entre las redes controlada por los routers WNCL y WNSR.
- El área LAN que contiene los servidores limitados por el router LNSR.
- En el área LAN tenemos un servidor web SRVD WEB con sistema operativo Linux preparado para ser explotado llamado Metasploitable 2, el que nos proporciona algunos servicios, especialmente servicios WEB y de Bases de Datos, los que serán vulnerados.
- Un equipo con monitor que es el que se encargará de hacer el análisis de los flujos de datos que se presenten.

5.3. OBJETIVOS DEL MONITOREO

- Analizar el flujo de paquetes dentro de la rede, para identificar cuando la red sea atacada por agentes externos.
- Recaudar datos para mostrar datos estadísticos de la red.
- Realizar un ataque a la base de datos de un servidor web.
- Simular el Watering hole attack mediante el uso de herramientas de hacking ethical.

5.4. SELECCIÓN DE EQUIPOS

Para la selección de equipos se tenemos que se requiere simular un ataque muy utilizado actualmente que se denomina Watering Hole Attack. Esta forma de ataque es uno de los más exitosos que fue identificado por RSA Security enfocado al robo información de usuarios sin que ellos se den cuenta que es lo que está pasando realmente. Este modo de ataque se presenta en servidores vulnerables, donde el

atacante elige su objetivo que en este caso es un servidor en el Internet o dentro de una LAN.

Esta forma de ataque se da de la siguiente manera:

- El atacante modifica un sitio web agregando scrips maliciosos sin que el usuario se dé cuenta.
- La víctima ingresa a la página web.
- El sitio infectado re direcciona a la víctima a un sitio de descarga con un malware, es decir que el sitio web real es usado como un trampolín, de esta manera se llevan a cabo los ataques.
- El malware comprueba las vulnerabilidades de navegadores, aplicaciones javas obteniendo así la información de cuál es la vulnerabilidad y que malware específico será descargado para cada sistema operativo.
- Generalmente la victima realiza todo este proceso sin darse cuenta que ha sido infectado, por lo que debemos acotar que la mayoría de veces son los mismos usuarios en su mayoría inexpertos los que infectan los computadores.

En nuestra simulación se asume que las victimas ya han instalado el malware que permite explotar las vulnerabilidades, en este caso específico la vulnerabilidad explotada será hacia la base de datos, la cual podremos acceder desde nuestro equipo atacante.

Debido a que el usuario no es capaz de darse cuenta cuando los equipos estar infectados, es importante tener un software que nos permita capturar paquetes de red y que nos permita obtener resultados de que flujos están pasando por la misma, por lo que el enfoque no es hacia la instalación de malware, sino el enfoque del resultado final es analizar los flujos de datos presentes al momento de los ataques y también

cuando no existan, de esta manera podríamos identificar cuando existan infección de equipos en nuestra red.

Para la Simulación se ha elegido los siguientes equipos:

- GNS3
- Cliente con sistema operativo Windows XP con virtualBox
- Kali Linux con Script de Ataque
- Servidor Linux Metasploit2
- Equipo con Windows XP dedicado a la captura de paquetes Netflow Analizer
- Router 3640
- Router 7200
- Ethernet Switch

GNS3

Es una herramienta de simulación para redes el cual nos permite diseñar ambientes de red o topologías, facilitando y optimizando el diseño de una red, puede ser utilizado como una herramienta para el diseño de topologías y configuración de equipos debido a que permite configurar los mismos como si fueran un equipo físico, por lo que además de ser utilizado para el aprendizaje y diseño de redes, también se usa para simular entornos de red reales sin necesidad de tener los equipos físicos, es decir, que en la parte empresarial podríamos mostrar a nuestros clientes como quedaría la topología de red y cuáles son los equipos más adecuados para solventar sus requerimientos.

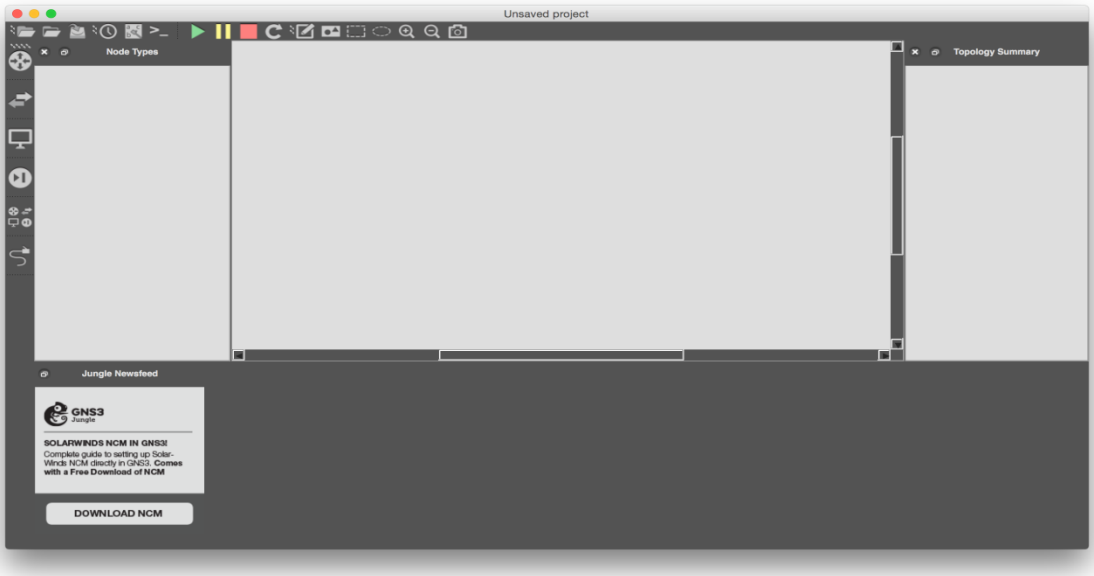
El GNS3 puede ser instalado en OSX, Linux y Windows, brindando los elementos necesarios para poder crear las simulaciones. GNS3 está enfocado a el uso de

equipos cisco, por lo que debemos trabajar con equipos de red de esa marca y sus diferentes modelos, nos permite tener conectividad con máquinas virtuales y equipos físicos. Las limitaciones dependerán más del hardware de equipo donde se realice la simulación más que del mismo software GNS3.

GNS3 es una herramienta profesional que actualmente cuenta con soporte técnico y con foros donde podemos despejar dudas y exponer soluciones al resto de usuarios, es decir que contaremos con todo el apoyo tanto de usuarios expertos como aquellos que puede tener la habilidad de resolver problemas enfocados a las redes.

La instalación es muy sencillas solamente debemos crear una cuenta de usuario y bajar directamente el software desde http://www.gns3.com, luego de esto podemos empezar la instalación la que nos mostrará un asistente de instalación de forma rápida y sencilla, el resultado final será el ambiente de simulación de GNS3.

Figura 7: Ambiente de simulación de GNS3. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Cliente IE8-WinXp

El cliente IE8 se encuentra en la LAN LNCL, y se trata de un cliente con sistema operativo Windows el cual será virtualizado. GNS3 nos permite virtualizar sistemas operativos completos para poder utilizar todas las funcionalidades, es decir, que no solamente podemos probar la conectividad de la red sino que también podemos utilizar servicios, aplicaciones, funcionalidades completas de cualquier sistema operativo que pueda ser simulado.

Para agregar esta máquina virtual necesitamos instalar previamente el virtualBox que lo podemos conseguir de forma gratuita desde https://www.virtualbox.org, una vez instalado descargamos desde la página de Microsoft el archivo .ova, esta extensión es compatible con virtualBox la que trabajará sin ningún problema y podrá ser importada por virtualBox.

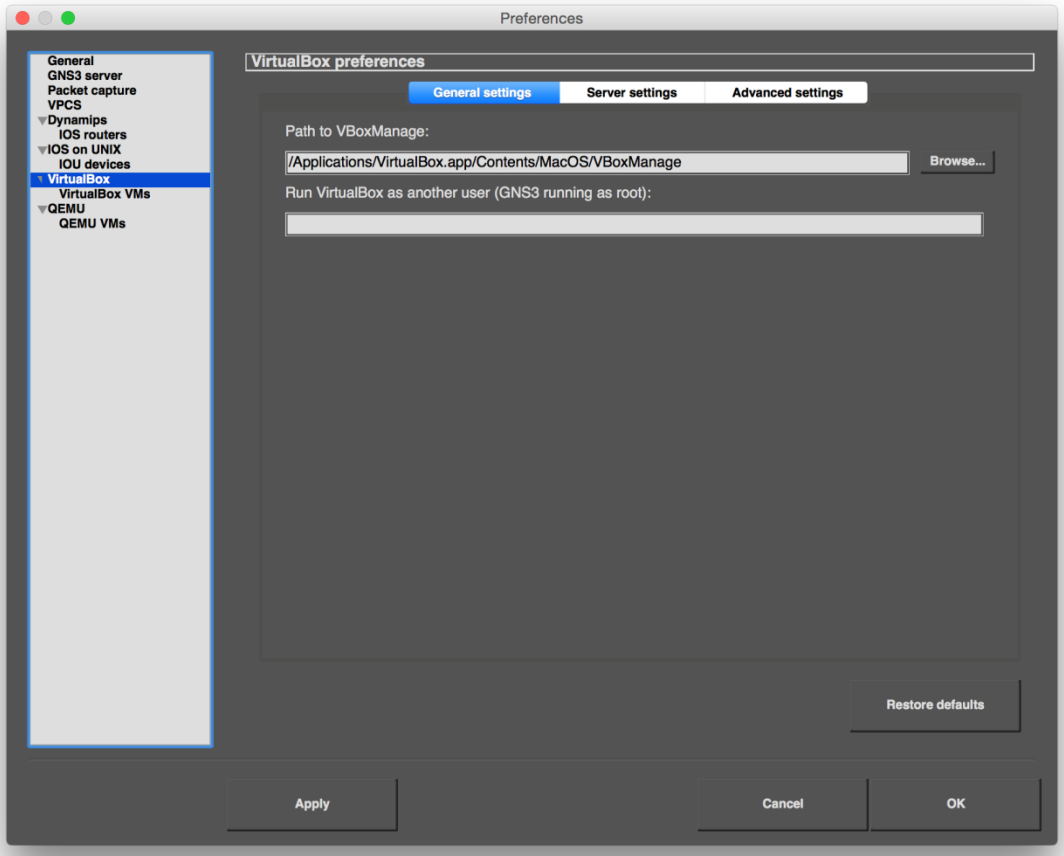
Figura 8: Agregar máquina virtual con VirtualBox. Año 2015

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Una vez instalada la imagen .ova debemos abrir el GNS3 dentro de sus preferencias.

Figura 9: Preferencias en VirtualBox del GNS3. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

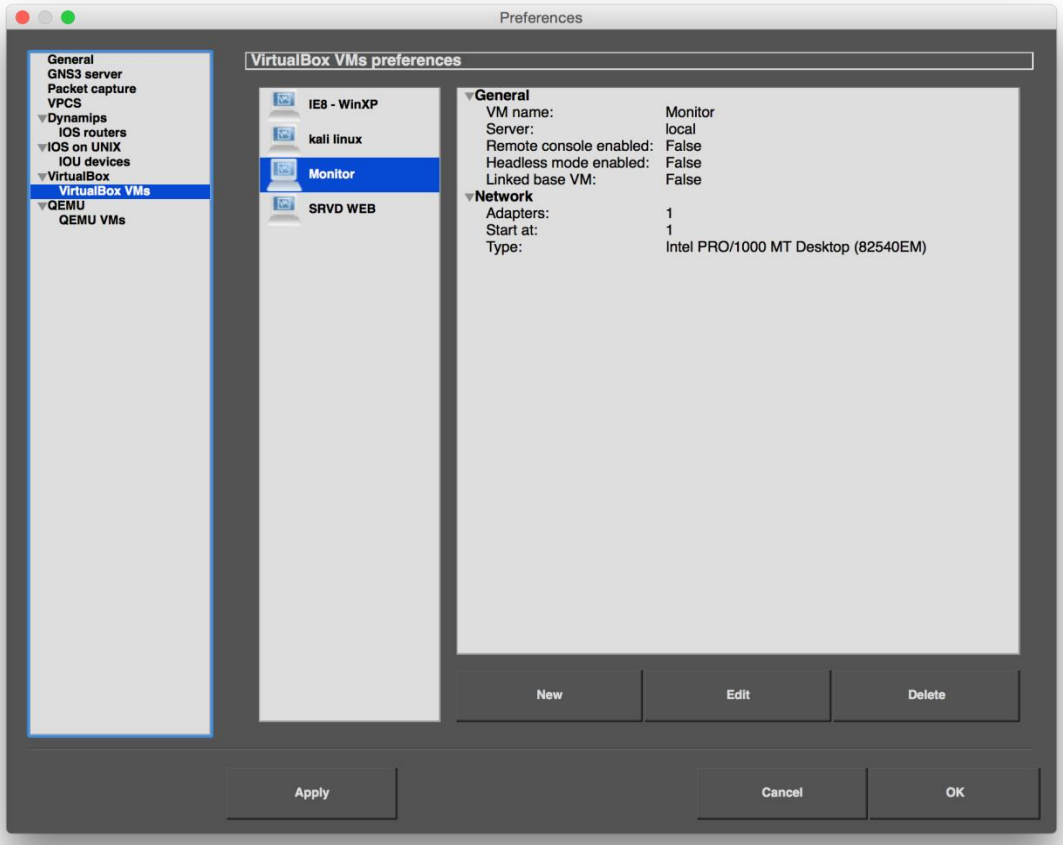
Nos dirigimos a VirtualBox y dentro de él agregamos la máquina virtual para que podamos más adelante arrastrarle a nuestro entorno de simulación.

Al final de agregar todos los equipos nos debe aparecer todas las máquinas virtuales disponibles, cabe destacar que solamente se pueden usar una vez al mismo tiempo, es decir que si necesitamos máquinas virtuales con similares características debemos

incluir todas las que necesitemos ya que no se podrá usar la misma dos veces en el mismo ambiente de simulación.

El resultado final de agregar las máquinas virtuales es:

Figura 10: Resultado de la instalación de todas las máquinas virtuales. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

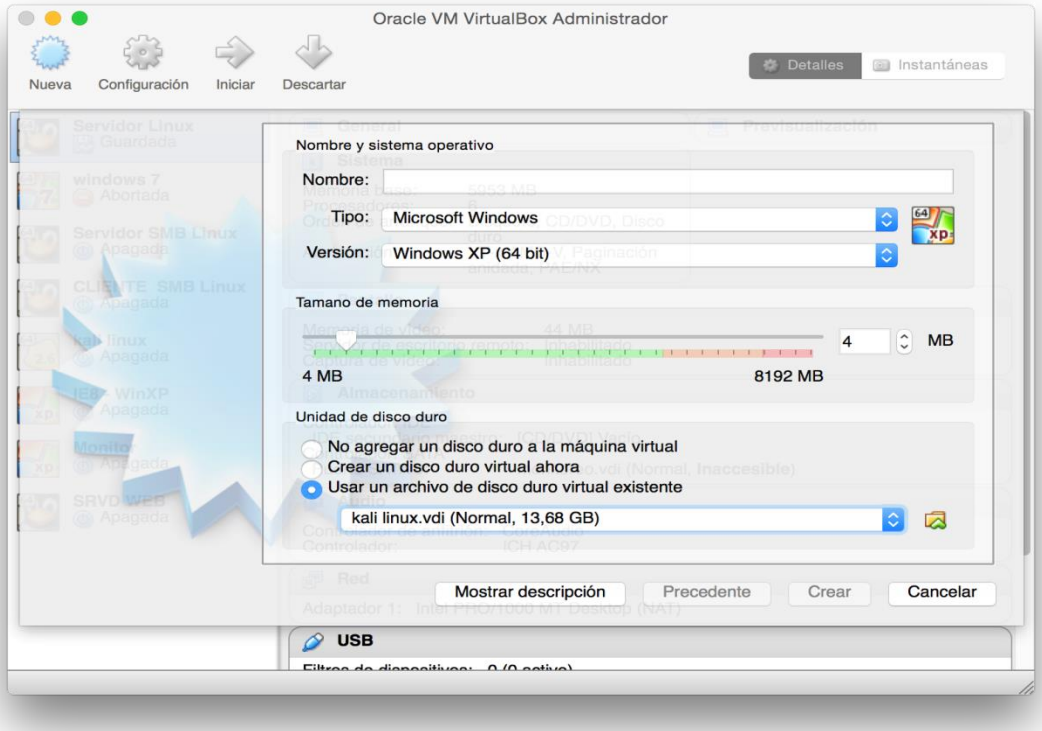
Kali Linux

Kali Linux es una distribución de Linux prepara especialmente para explotar vulnerabilidades de sistemas operativos, redes inalámbricas, bases de datos, con el fin de hacer ataques de manera ética, es decir que Kali Linux es orientado al

aprendizaje de explotación de vulnerabilidades ya reportadas como encontradas, por ningún motivo se debe utilizar los exploits y herramientas incluidas para realizar ataques a servidores y redes para obtener información que no nos pertenece, es decir que no solamente funciona con fines educativos sino que se pueden realizar ataques reales a las redes.

Por esta razón con Kali Linux es la herramienta perfecta para nuestra simulación, esta herramienta se encargará de hacer el ataque a nuestro servidor. De la misma manera podemos virtualizar este sistema operativo utilizando VirtualBox, simplemente bajaremos la imagen .iso y la cargaremos en nuestro VirtualBox.

Figura 11: Virtualizar herramienta Kali Linux mediante VirtualBox. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

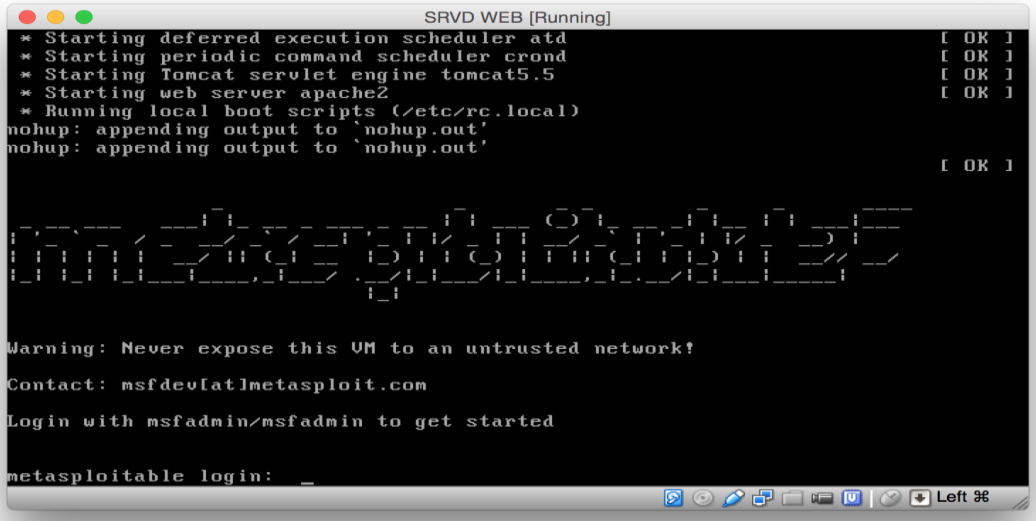
Metasploit2 SRVD WEB

Metasploit es una imagen de código abierto preparada con vulnerabilidades en el sistema operativo, está basado en Linux y presenta únicamente modo consola, carga servicios web y de base de datos, esta imagen viene lista para hacer pruebas de penetración y al mismo tiempo nos permite identificar intrusos que pretendan vulnerar los sistemas operativos.

Para descargar la imagen .iso podemos hacerlo desde http://www.metasploit.com/ la cual contiene algunas imágenes preparadas para este tipo de eventos.

Al añadir al virtual box tendremos un servidor Web y de Base de Datos al cual se pueden hacer inyecciones SQL directamente de la página web para acceder como usuario o por línea de comandos, podemos explotar las vulnerabilidades de la base de datos.

Figura 12: Virtualizar Metasploit mediante VirtualBox. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Netflow Analizer (Monitor)

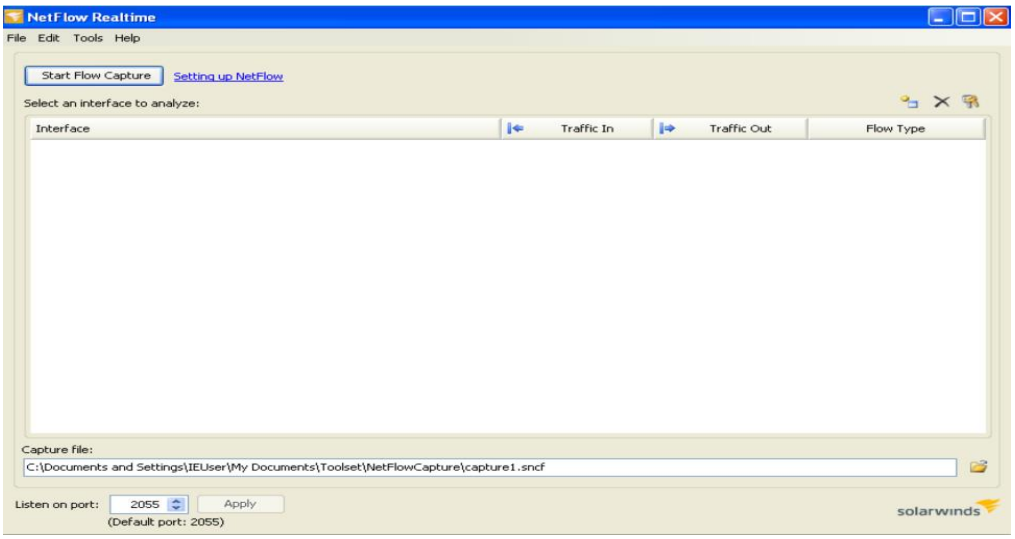
Netflow Analizer es una herramienta que permite la captura de paquetes a manera de sniffer pero con ventajas adicionales ya que no solamente puede capturar paquetes, sino que también podemos hacer una análisis de paquetes en la red, los flujos que se presentan en períodos de tiempo, el protocolo Netflow fue creado por cisco el cual se encarga de obtener paquetes en períodos de tiempo en el router y los puede exportar a aplicaciones como Netflow Analizer.

Netflow Analizer es soportado en:

> "Cisco 2600 series, Cisco 3600 series, Cisco 7100 series, Cisco 7200 series, Cisco 7300 series, Cisco 7400 series, Cisco 7500 series, Cisco 12000 series."*[19]Cisco Systems (2003).*

Para la simulación utilizaremos router 3600 y router 7200, y la captura de datos se hará desde un sistema operativo virtualizado Windows Xp llamado Monitor, el que contará con Netflow Analizer, para mostrar gráficamente los resultados.

Figura 13: Captura de datos con Netflow Analizer. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

5.5. CONFIGURACIÓN DE EQUIPOS

Cada equipo pertenece a un segmento de red distinto y llevan sus nombres codificados de acuerdo a donde pertenecen.

IE8-WinXp cliente de Windows el que recibirá el ataque por parte del servidor en el momento que empiece la comunicación entre los dos.

PCCL Computador personal del área de Clientes.

LNCL Router de la LAN del área de Clientes.

WNCL Router WAN del área de Clientes.

WNSR Router Wan del área de Servidores.

LNSR Router LAN del área de servidores

SRNVR servidor NVR para video vigilancia referencial.

SRVD WEB servidor WEB y de Bases de Datos

Hacker Servidor con script de ataque.

Monitor equipo para el análisis del flujo de datos

La configuración de cada interfaz por equipo es la siguiente:

Cuadro 2: Configuración de cada interfaz por equipo. Año 2015

EQUIPO	INTERFACE	RED	IP
IE8-WinXp	Eth0	192.168.20.0/24	.2
PCCL	Eth0	192.168.20.0/24	.3

LNCL	e0/0	192.168.20.0/24	.1
LNCL	e1/0	200.124.255.192/26	.202
WNCL	f0/0	200.124.255.192/26	.203
WNCL	f0/1	186.42.214.0/30	.1
WNSR	f0/0	186.42.214.0/30	.2
WNSR	f0/1	162.159.250.0/30	.1
LNSR	e1/0	162.159.250.0/30	.2
LNSR	e0/0	192.168.4.0/24	.1
SRVD WEB	e0	192.168.4.0/24	.3
MONITOR	e0	192.168.6.0	.2
Hacker	e1	192.168.7.0/24	.1

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

5.5.1. CONFIGURACIÓN DE NETFLOW

Se han definido 14 pasos básicos para la configuración de Netflow

Figura 14: Configuración de la Capa 2 de NetFlow y las Exportaciones de Monitoreo de Seguridad parte 1/2. Año 2015

	Comando o acción	Propósito
Paso 1	**enable** **Example:** `Router> enable`	Habilita el modo EXEC privilegiado. • Ingrese su contraseña si se le pide que lo haga.
Paso 2	**configure terminal** **Example:** `Router# configure terminal`	Ingresa en el modo de configuración global.
Paso 3	**ip flow-capture fragment-offset** **Example:** `Router(config)# ip flow-capture fragment-offset`	Los permisos que capturaban el valor del campo de desplazamiento del fragmento IP del primeros hicieron fragmentos del IP datagram en un flujo.
Paso 4	**ip flow-capture icmp** **Example:** `Router(config)# ip flow-capture icmp`	Le permite para capturar el valor del tipo ICMP y el código coloca del primer datagrama ICMP en un flujo.
Paso 5	**ip flow-capture ip-id** **Example:** `Router(config)# ip flow-capture ip-id`	Le permite para capturar el valor del campo IP-ID del primer IP datagram en un flujo.
Paso 6	**ip flow-capture mac-addresses** **Example:** `Router(config)# ip flow-capture mac-addresses`	Le permite para capturar los valores de los MAC Address de origen y destino de la primera trama de la capa 2 en un flujo.

Paso 7	`ip flow-capture packet-length`
	Example:
	`Router(config)# ip flow-capture packet-length`
		Le permite para capturar el mínimo y los valores máximos del campo de la Longitud del paquete de los datagramas IP en un flujo.

Fuente: [20]Cisco Systems (2009)

http://www.cisco.com/cisco/web/support/LA/107/1073/1073894_nf_detct_analy_thrts_ps6922_TSD_Products_Configuration_Guide_Chapter.html?bid=0900e4b1820934bc

Elaborado por: Cisco Systems

Figura 15: Configuración de la Capa 2 de NetFlow y las Exportaciones de Monitoreo de Seguridad parte 2/2. Año 2015

Paso 8	**ip flow-capture ttl** **Example:** `Router(config)# ip flow-capture ttl`	Le permite para capturar el mínimo y los valores máximos del campo del Tiempo para vivir (TTL) de los datagramas IP en un flujo.
Paso 9	**ip flow-capture vlan-id** **Example:** `Router(config)# ip flow-capture vlan-id`	Le permite para capturar el 802.1q o el campo ISL VLAN-ID a partir de la trama encapsulada primera VLA N de la capa 2 en un flujo que se reciba o se transmita en un puerto troncal.
Paso 10	**interface** *type interface-type interface-number*] **Example:** `Router(config)# interface ethernet 0/0`	Ingresa en el modo de configuración de la interfaz del tipo de interfaz especificado en el comando.

Paso 11	**ip flow ingress**
	y/o
	`ip flow egress`
	Example:
	`Router(config-if)# ip flow ingress`
	y/o
	Example:
	`Router(config-if)# ip flow egress`
		Habilita la entrada de recolección de datos de NetFlow en la interfaz.
		y/o
		Habilita la salida de recolección de datos de NetFlow en la interfaz.

Paso 12	`end`
	Example:
	`Router(config)# end`
		Vuelve al modo EXEC privilegiado.

Fuente: [20] Cisco Systems (2009) http://www.cisco.com/cisco/web/support/LA/107/1073/1073894_nf_detct_analy_thrts_ps6922_TSD_Products_Configuration_Guide_Chapter.html?bid=0900e4b1820934bc

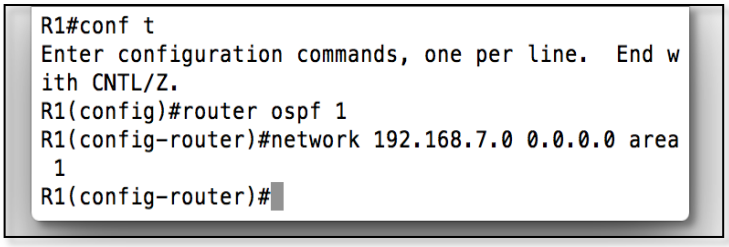
Elaborado por: Cisco Systems

Los pasos que usaremos para configurar Netflow de la simulación son:

- “En la configuración Global
- Ip flow-export source loopback
- Ip flow-export version 5
- Ip flow-cache timeout active 1
- Ip flow-export destination [IP] 9996
- Para cada interfaz a monitorizar
- Ip route-cache flow”*[21]Fluke Networks (2015)*

Los Router usarán el protocolo OSPF para tener conectividad en la red, debido a que se necesita agilidad en el proceso de rutas se utilizará este método dinámico para la configuración de las tablas de ruteo.

Figura 16: Configuración de router con protocolo OSPF. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

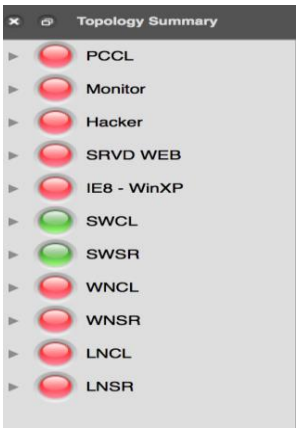
Elaborado por: Autor de la Tesis

Uniremos a cada router a OSPF 1 y luego publicaremos las redes aledañas y su wildcard mask en el AREA 1, una vez configurado esto en todos los routers tendremos conectividad.

Una vez terminada la configuración de los dispositivos podemos imprimir la configuración de runnig-config y obtendremos el siguiente resultado para cada router. (Anexos A: Configuraciones del Router)

Como resultado de la configuración de la topología de red tendremos los siguientes equipos:

Figura 17: Resumen de equipos en la topología de red. Año 2015

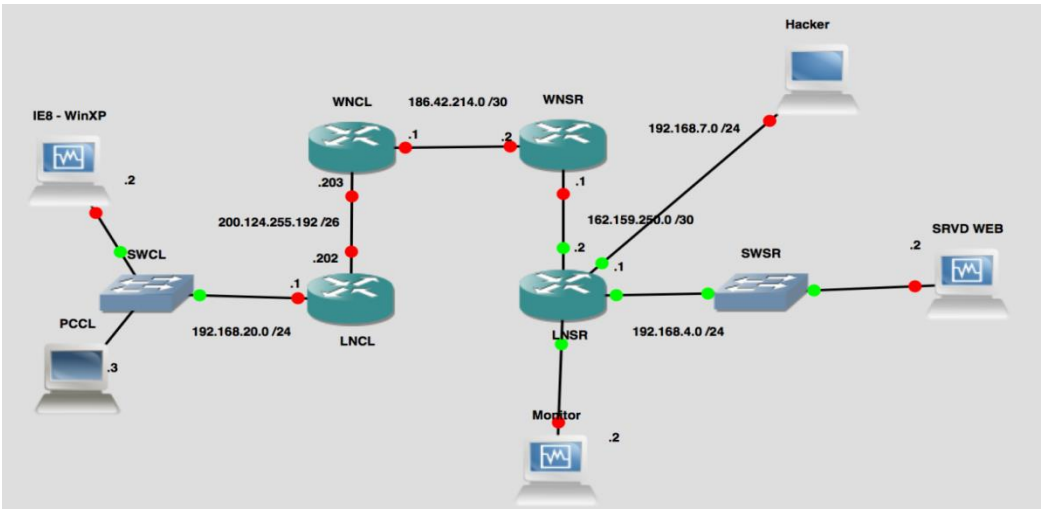


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

5.5.2. CONFIGURACIÓN DEL EQUIPO A UTILIZAR PARA EL MONITOREO

Figura 18: Configuración del equipo a utilizar para el monitoreo. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

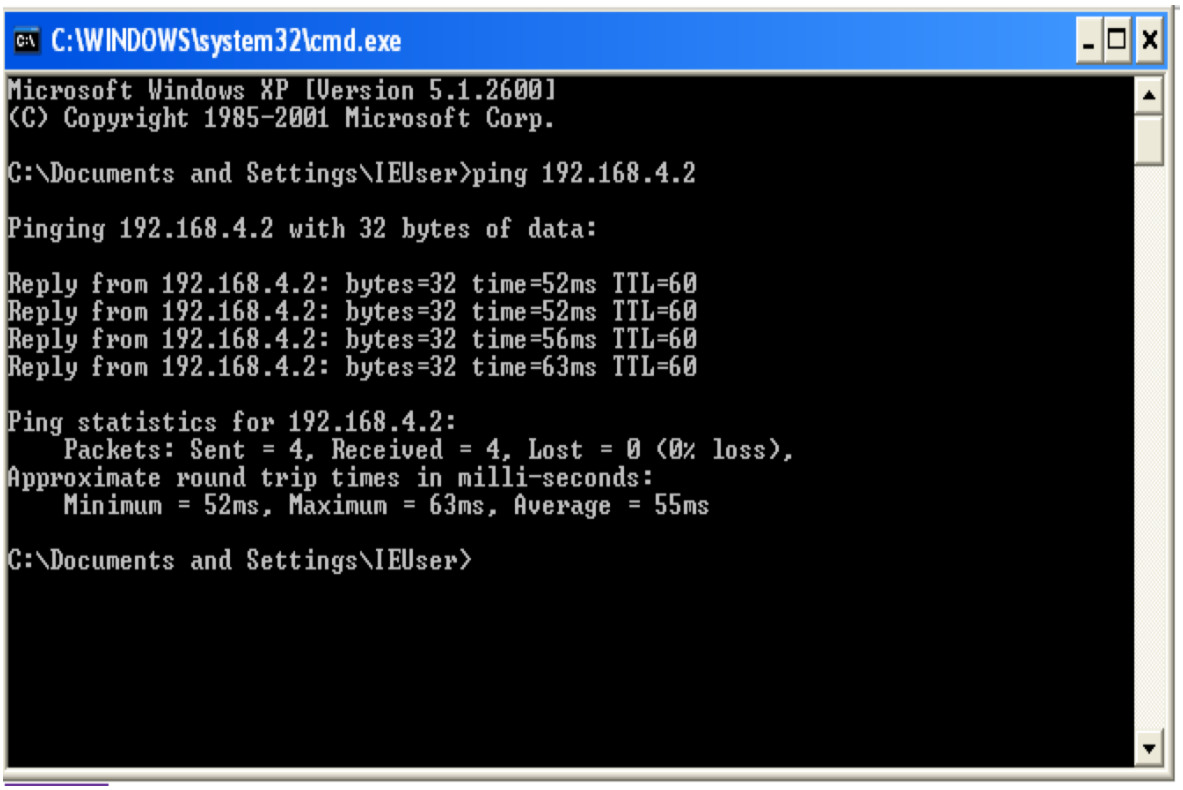
Elaborado por: Autor de la Tesis

5.6. PRUEBAS REALIZADAS

5.6.1. PRUEBAS DE LABORATORIO

Una de la primeras pruebas que debemos hacer son las de conectividad, por lo que en un terminal utilizaremos el comando ping para probar conectividad en la red, utilizaremos este comando para hacer un ping desde el cliente IE8-WinXp hacia el servidor SRVD WEB.

Figura 19: Prueba de conectividad utilizando el cliente IE8-WinXp. Año 2015



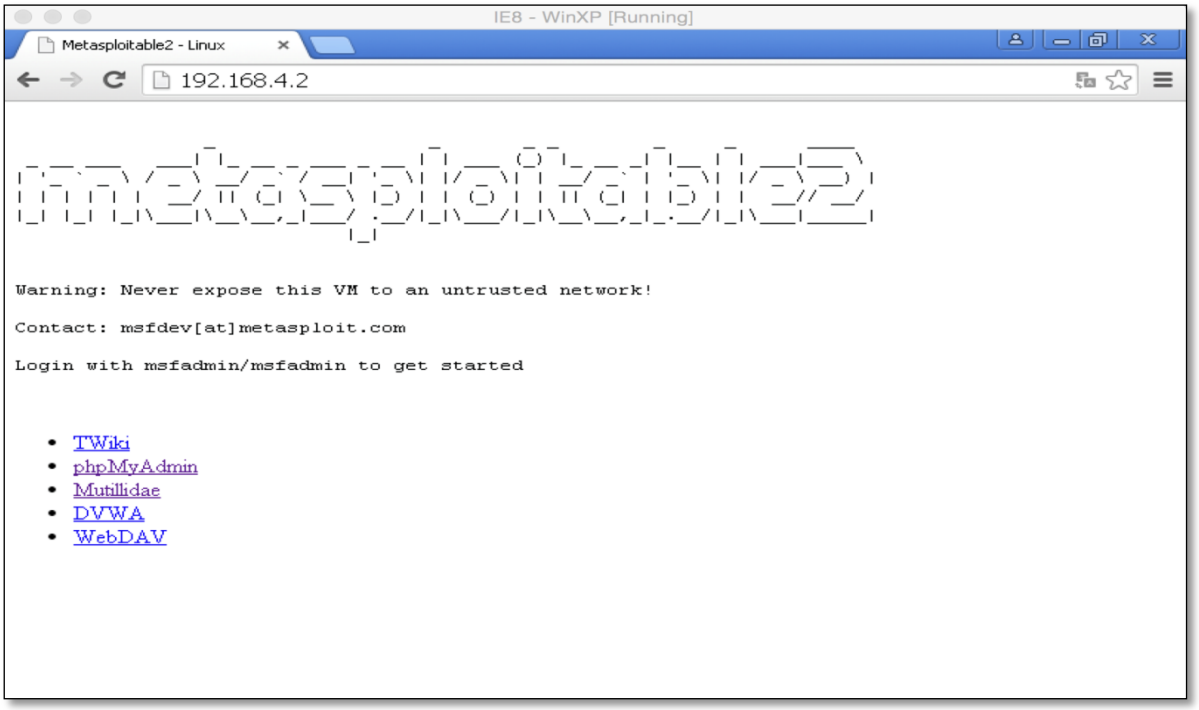
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

El resultado es exitoso por lo que podemos asegurar que tenemos conectividad a través de todos los routers involucrados en la red. También podemos acceder a uno

de los servicios mediante un navegador web, al poder acceder a los servicios de la red podemos constatar que los enlaces se encuentran correctamente configurados.

Figura 20: Constatar los enlaces correctamente configurados. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

AL poder cargar los servicios Web del servidor Metasploitable2, hemos comprobado que la red se encuentra correctamente configurada.

5.7. ESCENARIO EN EJECUCIÓN

El requerimiento principal de la simulaciones analizar los datos de nuestra topología al momento que se produzca un ataque o cuando un intruso se encuentre atacando a nuestro servidor, debido a que esta información no es transparente para los usuarios comunes, se utilizará la herramienta netflow analyzer, se debe tomar en cuenta que el ambiente simulado se encuentra en condiciones ideales, es decir que tenemos un

servidor completamente vulnerable, permitiendo realizar ataques de manera más sencilla y utilizamos herramientas de ethical hacking las que se encuentran disponibles de manera gratuita en la web listas para ser usadas con fines educativos.

El escenario a ejecutar nos permitirá encontrar resultados en la red es decir, cuando las redes son vulneradas por agentes externos o intrusos, en nuestro caso se accederá a la base de datos del Servidor WEB mediante la explotación de la misma, hay varias maneras de lograr esto, mediante la inyección Sql o con sqlmap hacia las páginas web con php, es decir existen actualmente varias manera de atacar vulnerabilidades de los sitios web.

Los que realizaremos en esta simulación es un ataque desde Kali Linux hacia el servidor SRVD WEB, para acceder a la base de datos y hacia sus tablas, además utilizaremos el cliente IE8-winXP para ingresar datos al a base de datos vía web.

Para analizar los datos existe un tercer agente que actúa dentro de la red que es el Monitor quien se encuentra trabajando conjuntamente con el router cisco LNSR, quien se encuentra configurado con el protocolo netflow.

Al final analizaremos los resultados obtenidos cuando se realice el ataque, debemos tomar en cuenta que el Netflow Analyzer nos es un snnifer común y que nos permitirá encontrar nuestro atacante.

Inicialmente podemos crear usuarios en nuestra base de datos, por default la base de datos de mysql en metasploitable se encuentra con algunos usuarios pre configurados, para nuestra simulación ingresaremos los siguientes usuarios.

Cuadro 3: Información para la base de datos de usuarios. Año 2015

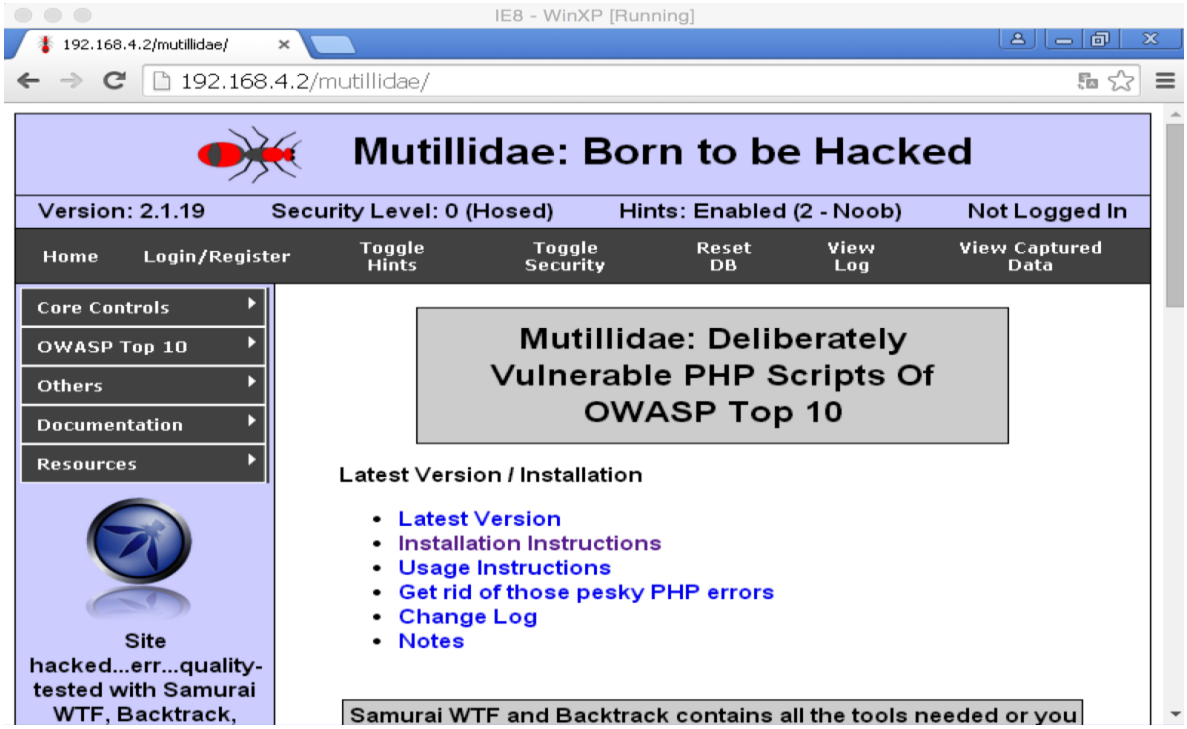
Usuario	Password
maestria	maestria
redes	redes
comunicaciones	comunicaciones

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Ingresamos al URL: http://192.168.4.2/mutillidae/ desde el cliente IE8 – WinXp el que nos direccionará a la página de Mutillidae.

Figura 21: Ingreso de URL en el Cliente IE8-WinXp, re-direccionando a Multillidae. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Esta página nos permitirá ir a la página de logeo y creación de usuarios, luego damos clic en el link Login/Register y abriremos la página para loguear y crear usuarios.

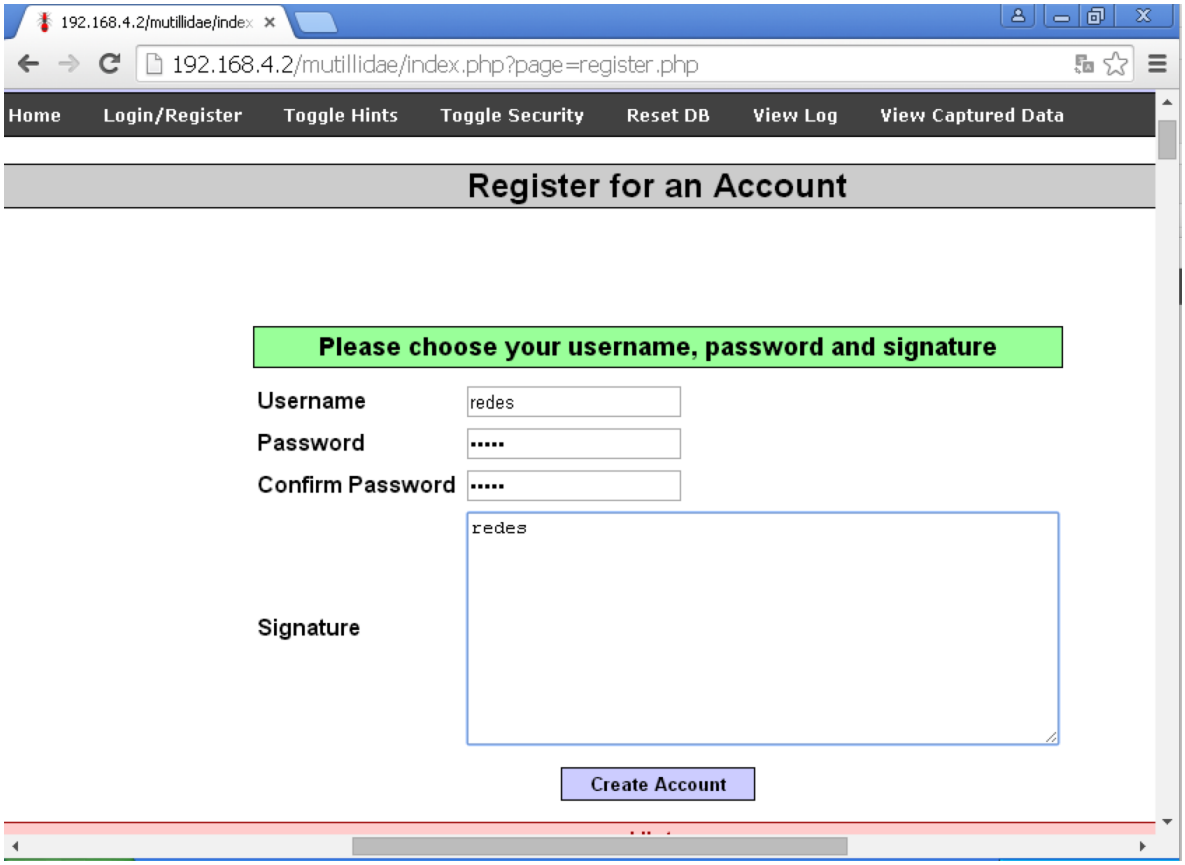
Figura 22: Página para loguear y crear usuarios en Mutillidae. Año 2015

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Abrimos el link para crear usuarios e ingresamos uno a uno los usuarios que ya se describieron en la tabla anterior.

Figura 23: Ingreso de datos y creación del usuario. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Luego de ingresar los usuarios tenemos lista la base de datos para ser explotada, al momento de realizar el ataque nuestra base de datos presentará estos usuarios y password correspondientes.

Ahora estamos listos para loguearnos desde nuestro cliente con los nuevos usuarios, en este caso ingresaremos con el usuario redes y la página nos muestra con que usuario estamos logueados.

Figura24: Ingresos desde nuestro cliente con el nuevo usuario. Año 2015

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

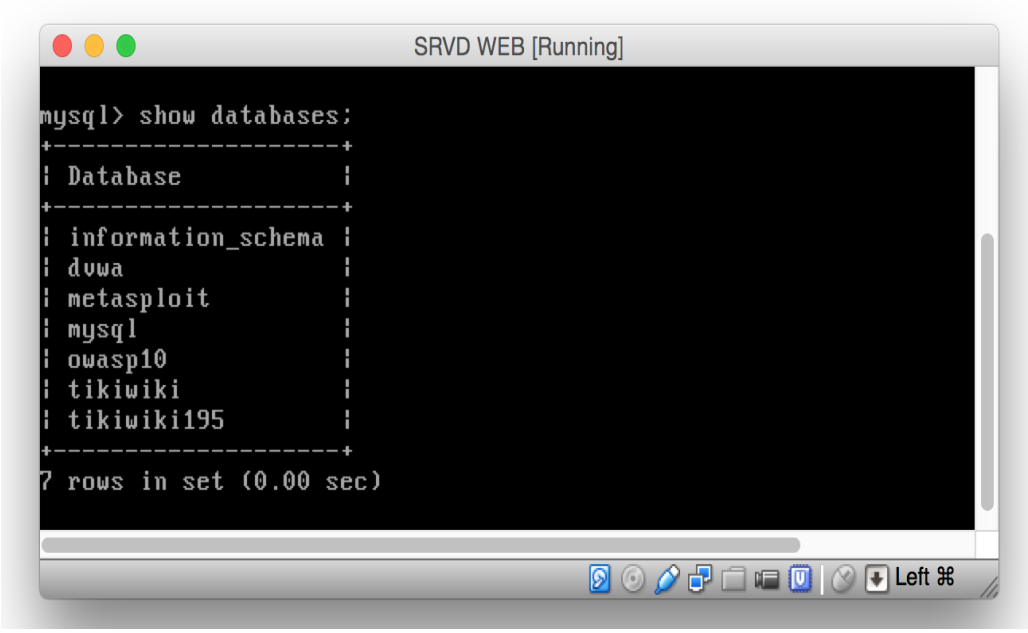
Como administradores de la base de datos antes de hacer el ataque podemos constatar que los datos han sido ingresados en las tablas, de esta manera nos aseguramos que cuando hagamos el ataque los datos estén ingresados y comparemos al final de la simulación.

Usaremos ahora la máquina virtual Metasploitable2 que es una distribución de Linux modo línea de comandos preparada para recibir estos ataques y también configurada con algunos servicios como ftp, base de datos y web.

El usuario y password por default es msfadmin el cual viene pre configurado una vez logueados podremos acceder a nuestra base de datos de mysql y verificaremos que los usuarios ingresados se encuentren en la misma.

Figura 25: Máquina virtual Metasploitables2 verificacion de usuarios ingresados.

Año 2015



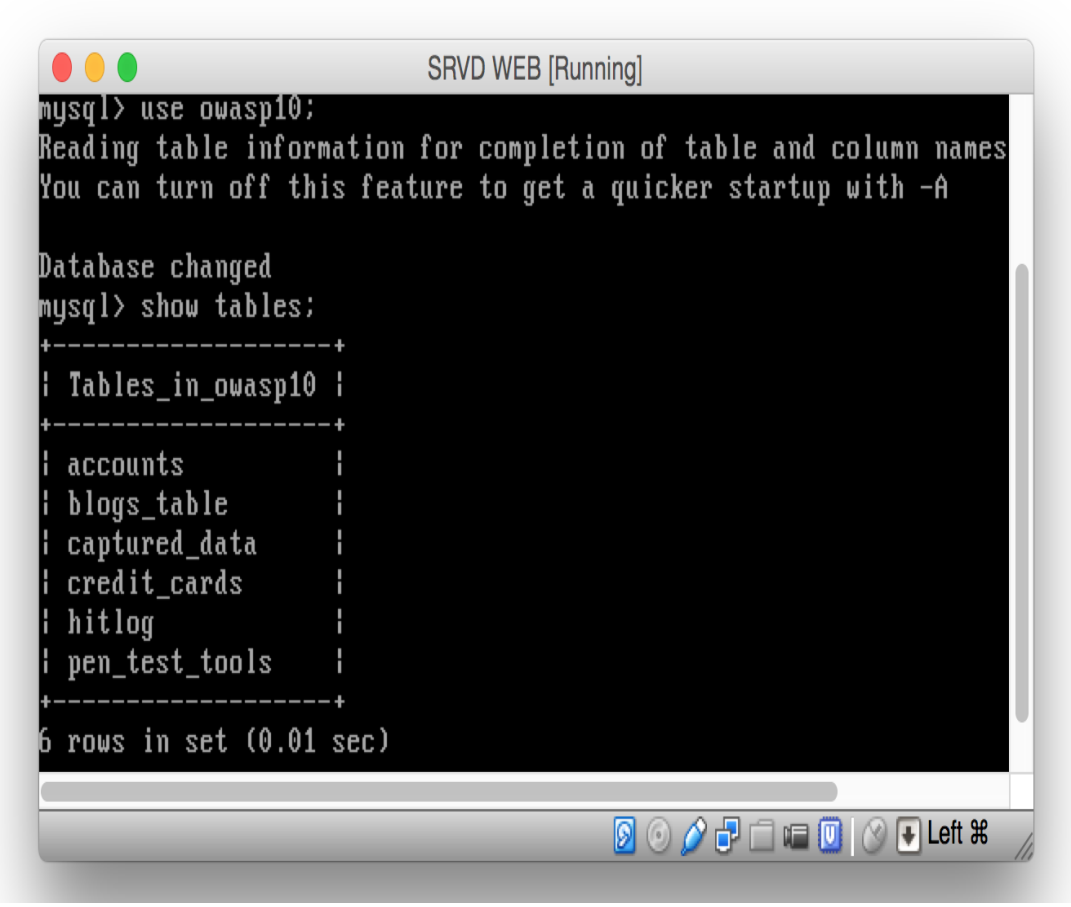
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Al ingresar a la base de datos de Metasploitable2 podemos listar el esquema de las bases de datos que están contenidos en mysql, la base de datos que pertenece a la web mutillidae es owasp10.

Con el comando use owasp10; podemos seleccionar las base de datos y luego con el comando show tables; listamos todas las tablas

Figura 26: Ejecutar comando Show Table en Máquina virtual Metasploitables2. Año 2015



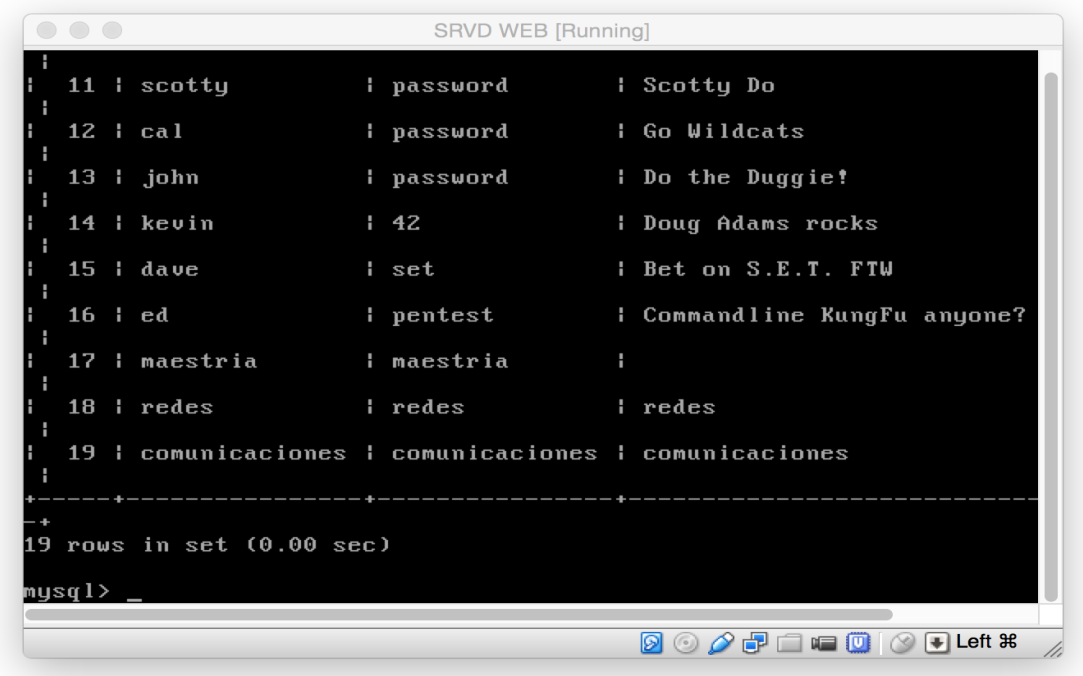
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Usando un query muy sencillo podemos listar los elementos de la tabla, con: Select * from accounts;

Podemos verificar en las últimas posiciones de la base de datos los usuarios que hemos ingresado.

Figura 27: Listar los elementos de la tabla. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Con esta información nuestra simulación está lista para el siguiente paso que es el ataque mediante un intruso infiltrado en la red, en este caso usaremos a Kali Linux, el cual consta con herramientas para lanzar ataques a sistemas vulnerables.

Ingresamos a Kali Linux con el usuario y password creado al momento de la instalación, para nuestro caso es:

Usuario: root

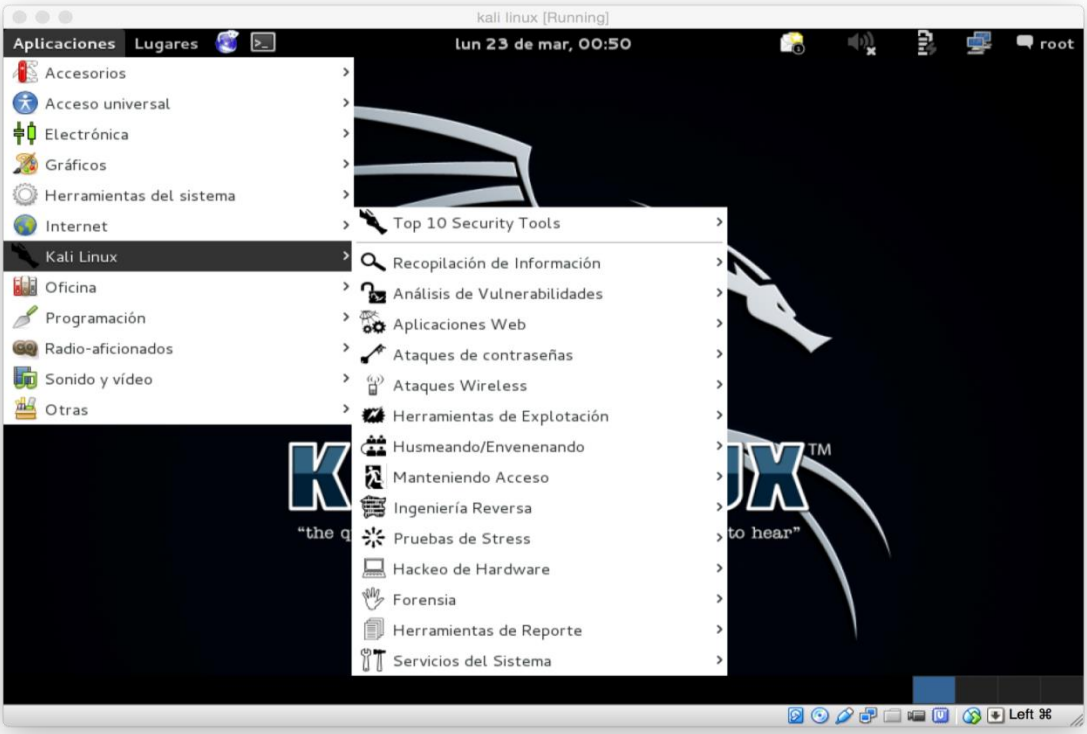
Password: kali

Kali Linux es una herramienta muy utilizada por hackers pero para solventar problemas de seguridades, se usa normalmente al hacer ataques controlados a redes y

poder encontrar problemas de seguridad, son ataques de carácter ético, educativo y también profesional sin ánimo de causar daños. La recomendación al momento de usar este tipo de herramientas es usarlas con el propósito para lo que fueron creadas, ya que también pueden ser utilizadas para causar daño.

Con el ataque que se muestra a continuación ponemos al descubierto una de las vulnerabilidades que se tiene al momento de estar expuesto a una red que no tiene seguridades, que no sea administrada.

Figura 28: Herramientas que posee Kali Linux. Año 2015



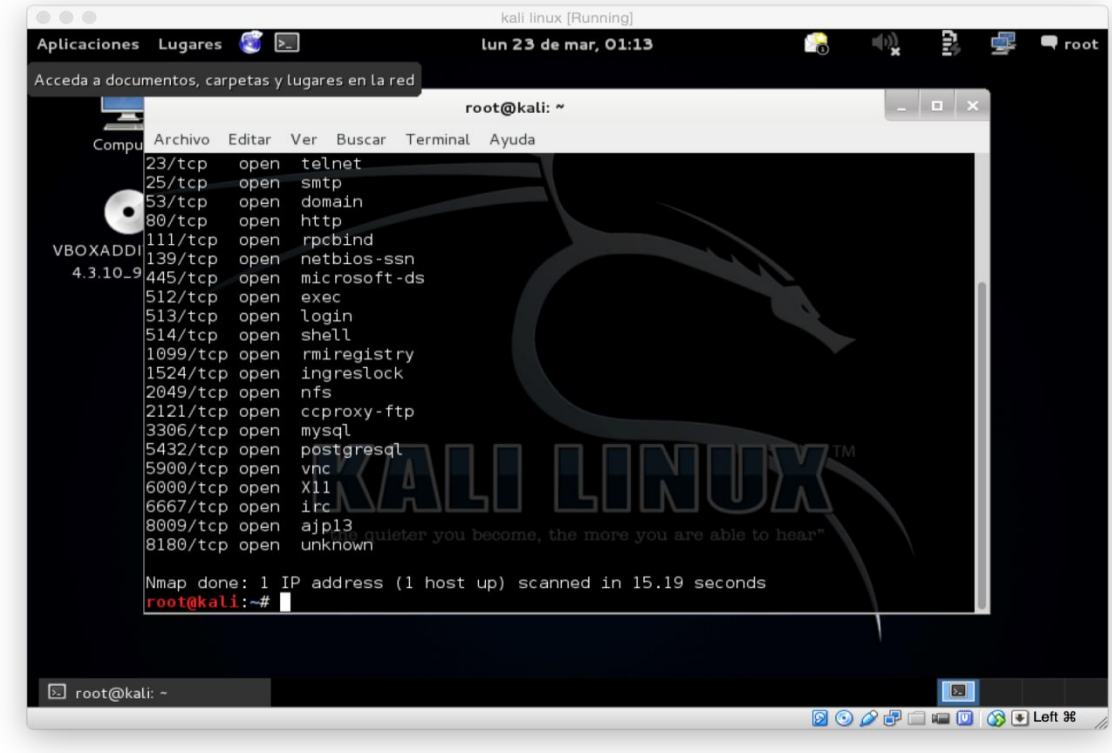
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Como se muestra en la figura Kali Linux posee algunas herramientas muy útiles para poner a prueba las redes, se puede manejar lo que es línea de comandos y mediante interfaz gráfica.

Para realizar el ataque iniciamos el terminal y verificamos los puertos abiertos del servidor desde nuestra consola.

Figura 29: Verificación de puertos abiertos del servidor desde la consola. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

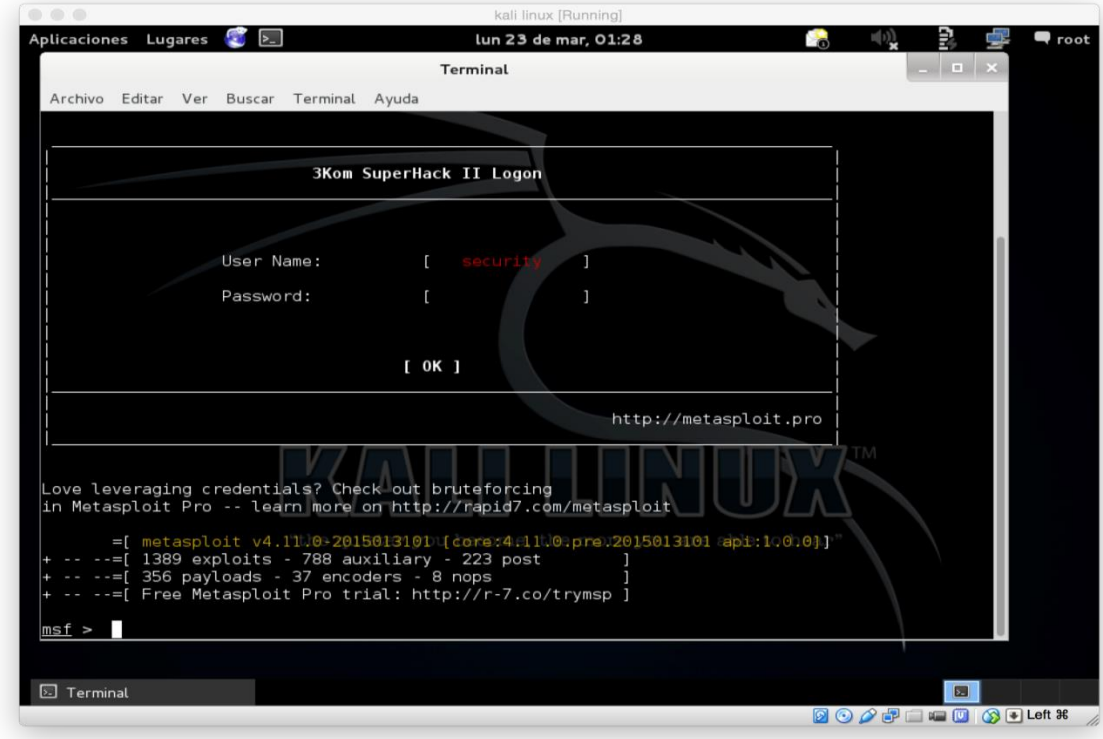
Elaborado por: Autor de la Tesis

Utilizamos el comando nmap 192.168.4.2, debido a que el servidor Metasploit2 se encuentra preparado para los ataques todos los puertos se encuentran abiertos,

observamos que el puerto 3306 se encuentra abierto por lo que el ataque será más sencillo de realizar.

Ejecutamos el metasploit framework esta herramienta nos permitirá hacer el ataque a la base de datos para obtener los usuarios y sus respectivos password, con esta herramienta vamos a sustraer toda esta información y toda la que necesitemos de la base de datos.

Figura 30: Ataque a la base de datos para robo de información. Año 2015

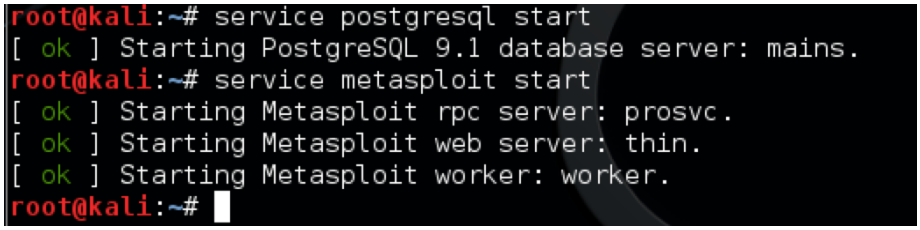


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Previamente debemos arrancar en Kali Linux postgre y metasploit, iniciamos los servicios

Figura 31: Arranque en Kali Linux y Metasploit. Año 2015

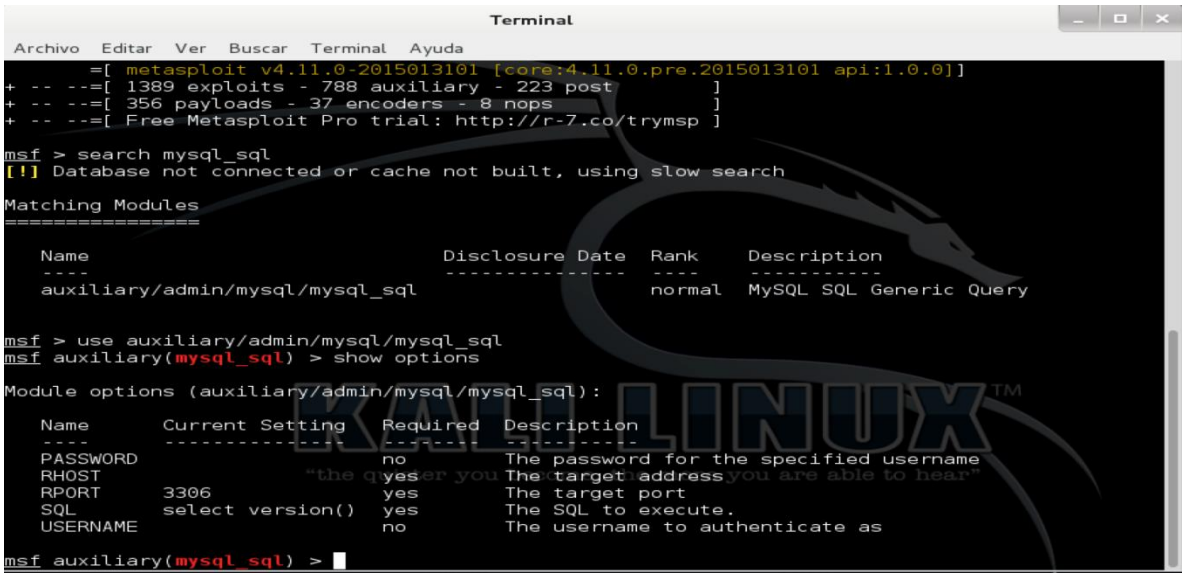


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

En el terminal con metasploit framework msf buscamos e indexamos a las bases de datos disponibles utilizando search mysql_sql para buscar los módulos de ataque, el módulo utilizado es auxiliary/admin/mysql/mysql_sql que nos permitirá hacer el ataque a la base de datos deseada y finalmente estamos listos para hacer el ataque, simplemente debemos utilizar los parametros de msf, para listarlos hacemos un show options y se lista los parámetros que necesitamos para el ataque.

Figura 32: Buscar e Indexar base de datos disponibles. Año 2015

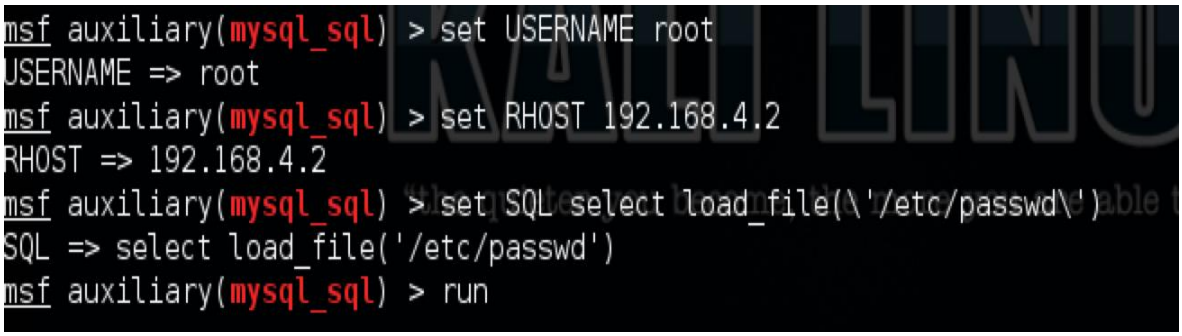


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Utilizamos los siguientes parámetros para el ataque y corremos el script de ataque

Figura 33: Utilizar los parámetros mysql y correr el script de ataque. Año 2015

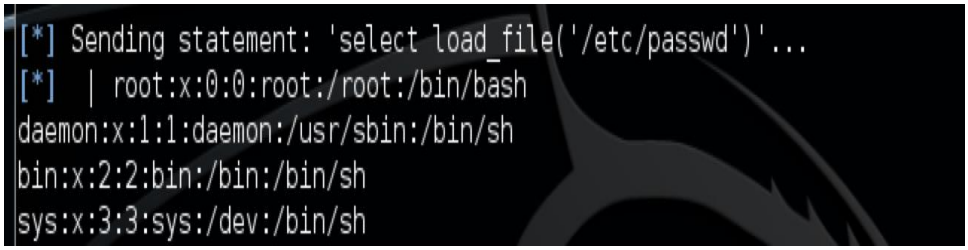


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Elegimos un usuario root y el host a ser atacado en este caso 192.168.4.2, y por último seteamos una sentencia SQL direccionando al archvo ubicado en /etc/passwd. El resultado del ataque se muestra con el archivo ejecutando.

Figura 34: Elección de usuario y el host a ser atacado inyectado SQL. Año 2015

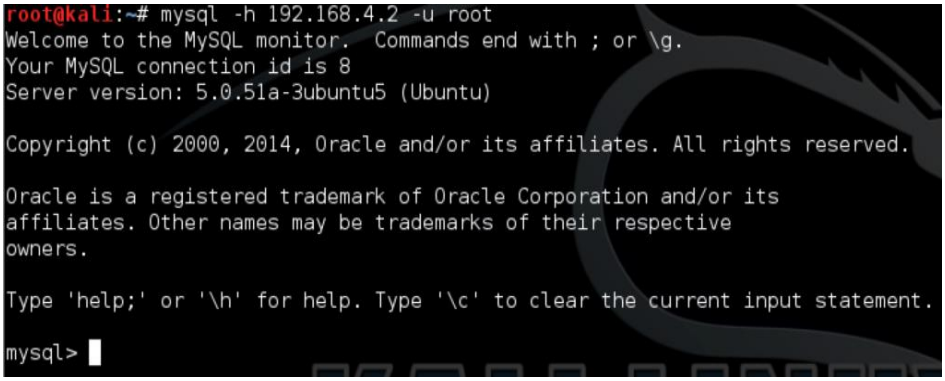


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Cuando ya se ha ejecutado esta inyección SQL podemos ingresar a la base de datos desde Kali Linux como usuario root.

Figura 35: Ingreso desde Kali Linux como usuario root. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

A pesar de que se desconoce el usuario debido a el exploit que hemos ejecutado ahora podemos loguearnos como usuario root y ver toda la información requerida.

Podemos ahora dentro de mysql desde Kali empezar a obtener la información.

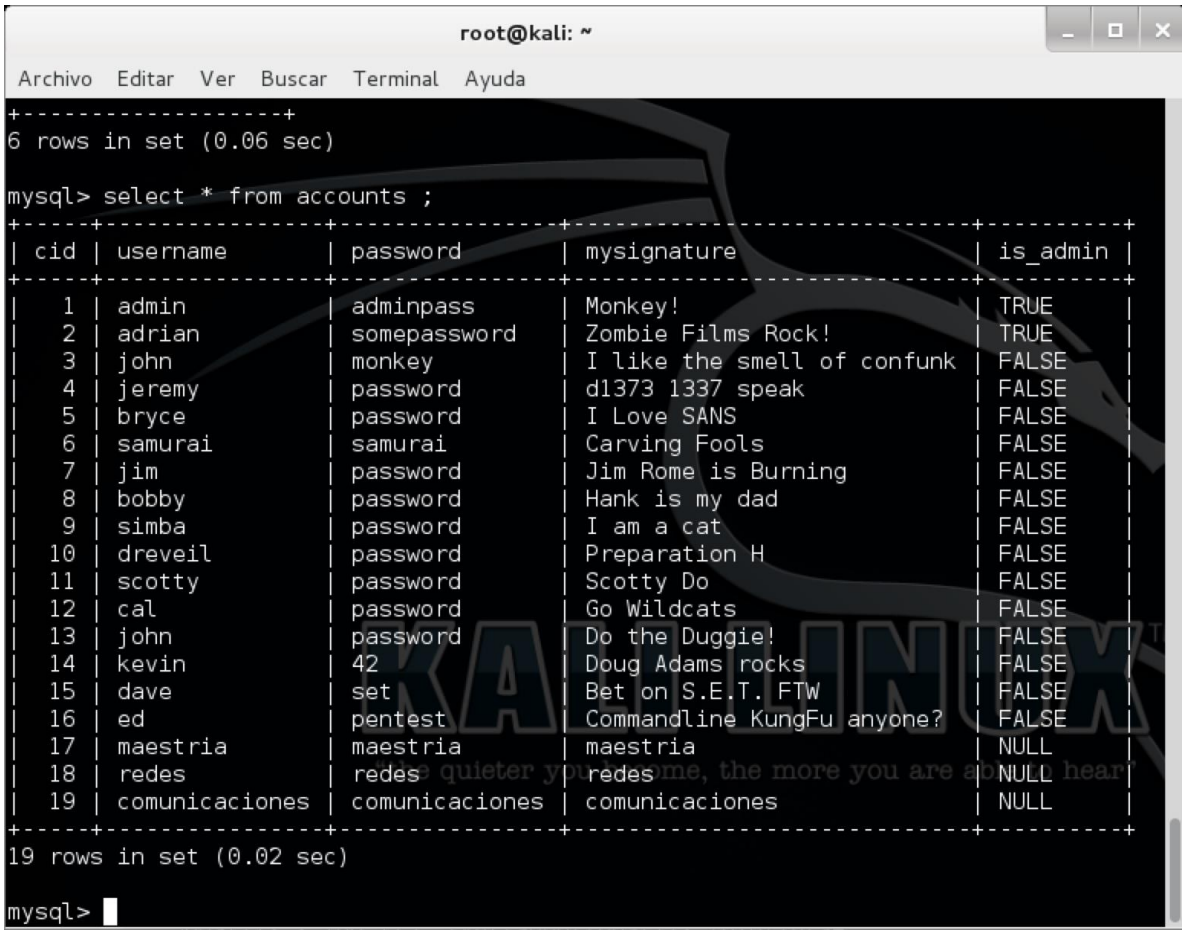
Figura 36: Dentro de mysql desde Kali obtención de información. Año 2015

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

La tabla que contiene la información para acceder a los usuarios es accounts, ejecutamos ahora un consulta sql para obtener el listado de la información.

Figura 37: Ejecución de consulta SQL y obtener listado de información. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

El resultado final de la consulta a la base de datos es la obtención de todos los usuarios y passwords tal cual se lo había propuesto, podemos visualizar a los usuarios maestria, redes y comunicaciones que fueron ingresados mediante la página web anteriormente. De esta manera hemos concluido el ataque a el servidor y hemos podido aprovechar las vulnerabilidades que presentaba.

Una de las piezas fundamentales de la simulación es el análisis de los datos ayudados de la herramienta Solardwinds Real-time NetFlow Analyzer, la que nos permitirá capturar flujos de datos de cualquier router configurado con netflow.

Se ha elegido el router LNSR debido a que concentra toda la actividad de flujos, tanto de servidores, clientes, hackers, y routers, por este motivo se ha configurado el protocolo netflow dentro de este router, podemos hacer una vista de ip flow export.

Figura 38: Vista de ip flow export de actividad de flujo de Netflow. Año 2015

```
LNSR#show ip flow export
LNSR#show ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 192.168.6.2 (9996)
  Exporting using source interface Ethernet3/0
  Version 5 flow records
  157 flows exported in 43 udp datagrams
  0 flows failed due to lack of export packet
  1 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
LNSR#
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

En la figura se muestra la versión 5 de netflow, los flujos de paquetes serán exportados a el equipo con IP 192.168.6.2 y puerto 9996 que corresponde a nuestro equipo Monitor que tiene instalado el Netflow Analyzer, además, indica a que interface van ha ser exportados los flujos de datos y un resumen de flujo de datos que fueron exportados.

Luego de configurar netflow también podemos ver los flujos que son capturados aquí podemos observar todo lo que pasa a través del router.

Figura 39: Observar los flujos capturados que pasan por el router. Año 2015

```
LNSR#show ip cache flow
IP packet size distribution (1332 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .425 .108 .004 .002 .003 .019 .033 .006 .000 .002 .000 .003 .002 .011

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .009 .003 .002 .015 .345 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  0 active, 4096 inactive, 160 added
  2912 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 160 added, 160 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             41      0.0        24   744      0.3      11.5       5.2
TCP-other           21      0.0         4   155      0.0       5.1      14.0
UDP-DNS             42      0.0         1    64      0.0       0.2      15.5
UDP-NTP              3      0.0         1    76      0.0       0.0      15.7
UDP-other           53      0.0         3   140      0.0       4.0      15.5
Total:             160      0.0         8   588      0.4       5.0      12.6

SrcIf_        SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
```

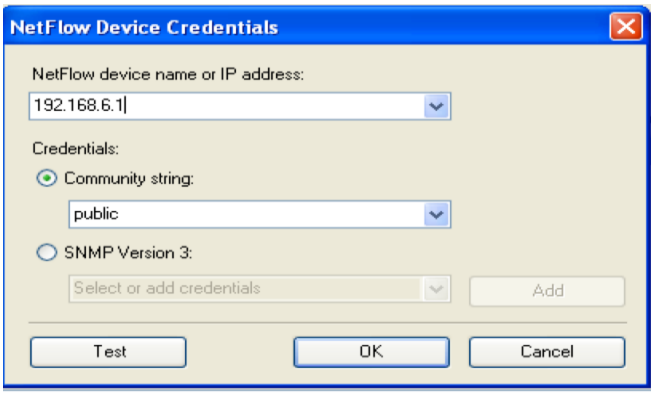
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Se puede observar que la red interactúa de manera normal que existe conectividad, pero a pesar de tener estos datos es bastante complejo interpretarlos, por esta razón los datos serán exportados a Netflow Analyzer.

Nuestra PC denominada Monitor tiene instalado Netflow Analizer, ejecutamos y agregamos la interfaz de donde queremos recibir los flujos.

Figura 40: Ejecución y agregación de interfaces para recibir flujos. Año 2015

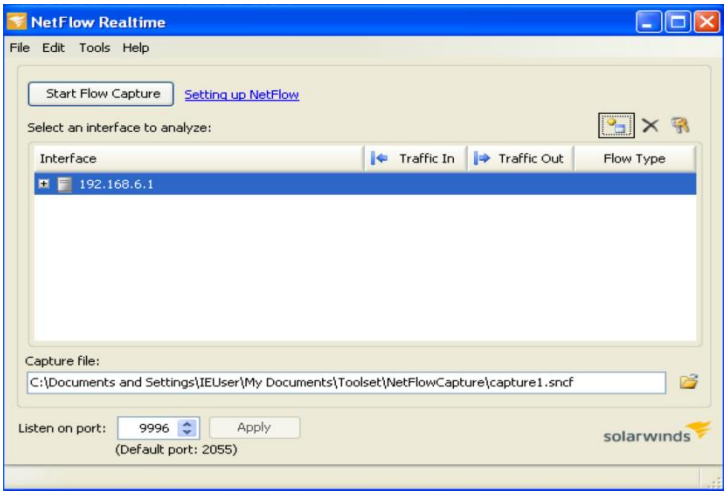


Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Añadimos la interfaz 192.168.6.1 que es por la cual estamos conectados al router, una vez hecho esto se agrega la interfaz al Netflow Analyzer y podemos empezar la captura, es importante tomar en cuenta que el puerto que se configuro en el router en netflow debe corresponde al de Netflow Analizer.

Figura 41: Agregar interfaz al Netflow Analyzer para captura. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

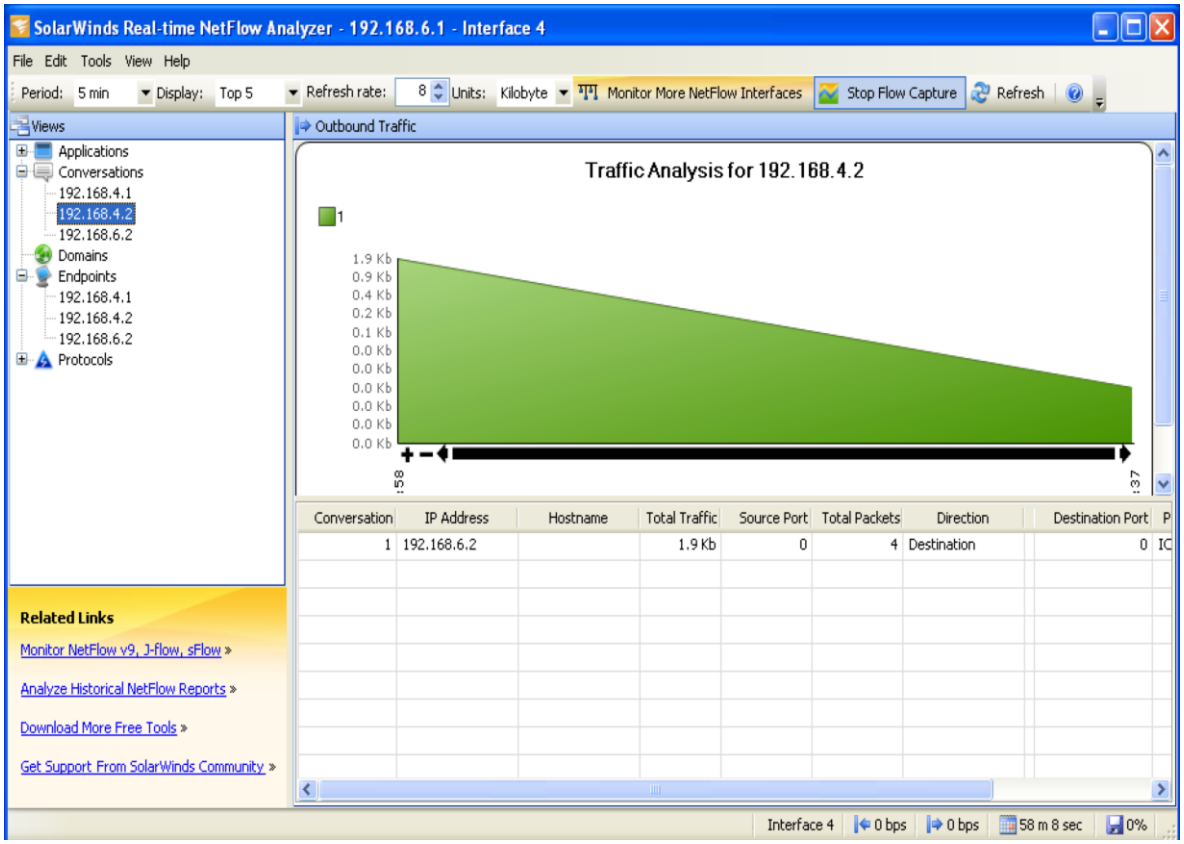
Elaborado por: Autor de la Tesis

Una vez configuradas todas las opciones iniciamos la captura de flujos.

5.8. RESULTADOS OBTENIDOS

Uno de los primeros resultados obtenidos utilizando el protocolo ICMP, es decir haciendo un ping a 192.168.4.2 es:

Figura 42: Flujos exportados de diferentes direcciones IP. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

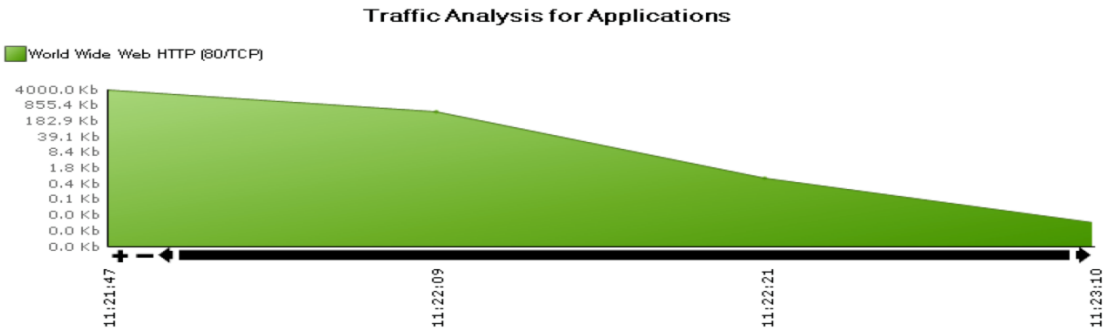
Elaborado por: Autor de la Tesis

En la figura se muestra los flujos exportados de diferentes direcciones IP, por tanto ahora tenemos ya lista toda la configuración para poder obtener resultados de flujos.

5.8.1. ANÁLISIS DE LOS RESULTADOS

Mientras navegamos en la Web podemos ver uno de los primeros resultados

Figura 43: Cantidad de información que pasa a través del tiempo. Año 2015



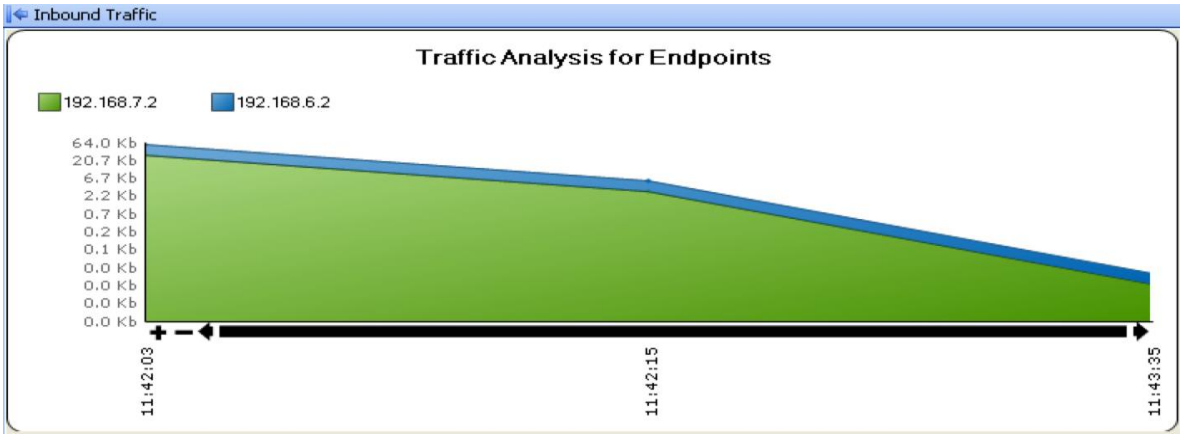
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

En la figura se muestra que se usa el protocolo http para este flujo y la cantidad de información que pasa a través del tiempo

Mientras la red este en uso y no existan novedades se mostraran todos los flujos para las interfaces de todas las intefaces.

Figura 44: Herramienta Netflow captura flujos de salida y entrada. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Tanto flujos de salida como de entrada se muestran en los gráficos estadísticos.

La herramienta netflow nos permite monitorear todas las interfaces que deseemos y exportar a un solo controlador.

En este punto podemos iniciar el ataque nuevamente para identificar el momento que se produce, el dato que sabemos previamente es que se va atacar a la base de datos o se va a acceder de manera remota a la base de datos con herramientas de ataque y un host externo.

Luego de ejecutar el comando run, hacia el SRVD WEB inyectando el archivo SLQ, tenemos acceso a la base de datos remotamente y lo que se obtuvo en el router LNSR es lo siguiente:

Figura 45: Direcciones que están interactuando, protocolo y cantidad de flujos. Año 2015

```
LNSR#show ip cache flow
IP packet size distribution (16304 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .382 .396 .001 .002 .003 .005 .007 .001 .000 .001 .001 .000 .001 .007

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .003 .002 .003 .010 .166 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  11 active, 4085 inactive, 2311 added
  44577 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  11 active, 1013 inactive, 2311 added, 2311 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW            213      0.0        29   715      0.6       8.8       6.6
TCP-other           46      0.0         5   144      0.0       2.7      10.6
UDP-DNS           1786      0.1         1    62      0.3       0.0      15.5
UDP-NTP              3      0.0         1    76      0.0       0.0      15.7
UDP-other          135      0.0         3   127      0.0       4.5      15.5
ICMP               117      0.0        48    81      0.5      47.5       4.1
Total:            2300      0.2         7   326      1.5       3.5      14.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.4.2     Et2/0         192.168.7.2     06 0CEA 884E     1
Et0/0         192.168.4.2     Et2/0         192.168.7.2     01 0000 0000    50
Et0/0         192.168.4.2     Local         192.168.4.1     11 BC9C 0035     1
Et0/0         192.168.4.2     Et2/0         192.168.7.2     06 0CEA 8505     1
Et0/0         192.168.4.2     Local         192.168.4.1     11 DDA2 0035     1
Et0/0         192.168.4.2     Local         192.168.4.1     11 BEF5 0035     1
Et0/0         192.168.4.2     Et2/0         192.168.7.2     06 0CEA B0B5     1
Et0/0         192.168.4.2     Local         192.168.4.1     11 AAD8 0035     1
Et0/0         192.168.4.2     Local         192.168.4.1     11 9B28 0035     1
Et2/0         192.168.7.2     Et0/0         192.168.4.2     01 0000 0800    54
Et0/0_        192.168.4.2     Local         192.168.4.1     11 ABA4 0035     1
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

En la tabla se muestra las direcciones que están interactuando, en este caso es claro ver que la dirección 192.168.7.2 que es la de Kali Linux y la 192.168.4.2 que corresponde a el SRVD WEB tienen una interacción e intercambio de paquetes, además podemos ver los protocolos que se están usando y la cantidad de flujos de cada uno.

En primera instancia podemos darnos cuenta que hay una dirección IP ajena a nuestra configuración de red, si bien sabemos que Kali Linux fue configurado de manera manual para esta simulación, las redes en condiciones normales no tienen agentes externos o direcciones extrañas a nuestras configuraciones, por lo que podemos determinar que la IP 192.168.7.2 es un intruso en la red que se encuentra intercambiando flujos con el servidor. Uno de los puntos débiles de netflow en el router cuando nos muestra resultados a manera de texto es que no nos muestra toda la información de manera transparente, podemos notar que en la figura nos muestra un flujo TCP-other, el cual nos puede estar ocultando información ya que no sabemos exactamente que flujo es el que se está presentando y podría ser este un elemento clave del análisis del ataque.

Para solventar este inconveniente que el modo texto del router donde el netfow fue activado, se utiliza las herramientas gráficas compatibles con el protocolo, es este caso el Netflow Analizaer será quien se encargue de mostrar los flujos que el netflow solo no ha podido.

Al ejecutar la herramienta también elegimos por donde recibiremos el flujo de datos en este caso la interface que interactúa entre el atacante y SRVD WEB es la interfaz correspondiente a Ethernet e2/0.

Figura 46: Configuración de Netflow. Año 2015

```
Flow export v5 is enabled for main cache
  Exporting flows to 192.168.4.3 (9996)
  Exporting using source interface Ethernet2/0
  Version 5 flow records
```

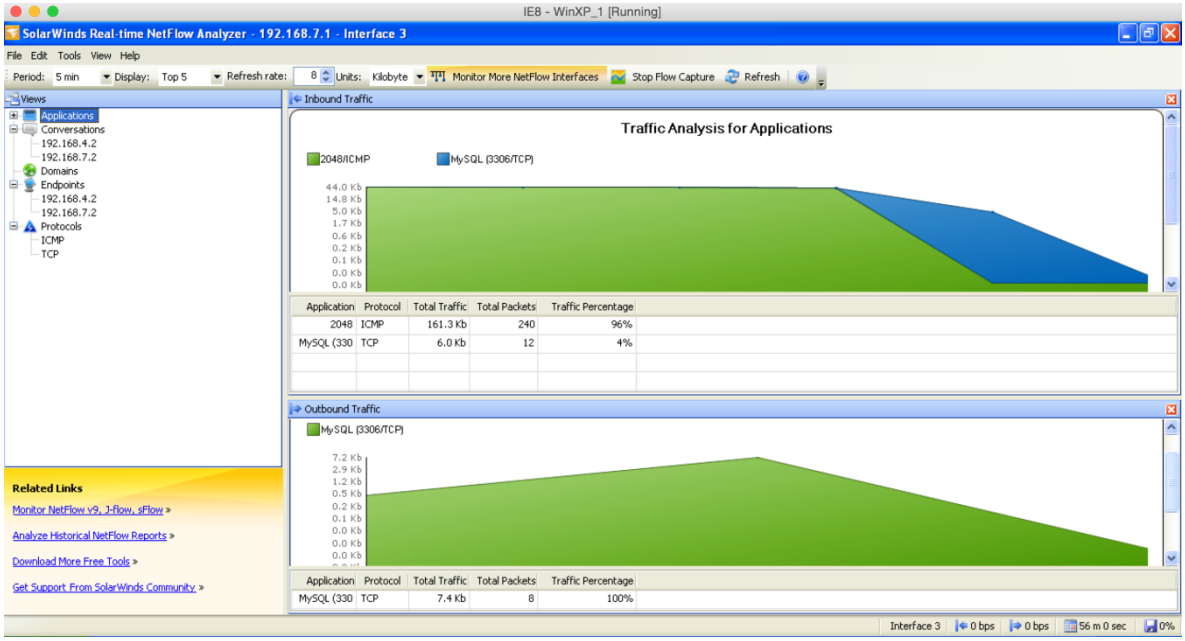
Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

En la captura podemos ver la configuración que hemos hecho a netflow.

Una vez que arranca la herramienta gráfica el resultado de los flujos es el siguiente:

Figura 47: Resultados de la Herramienta Netflow Analyzer. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

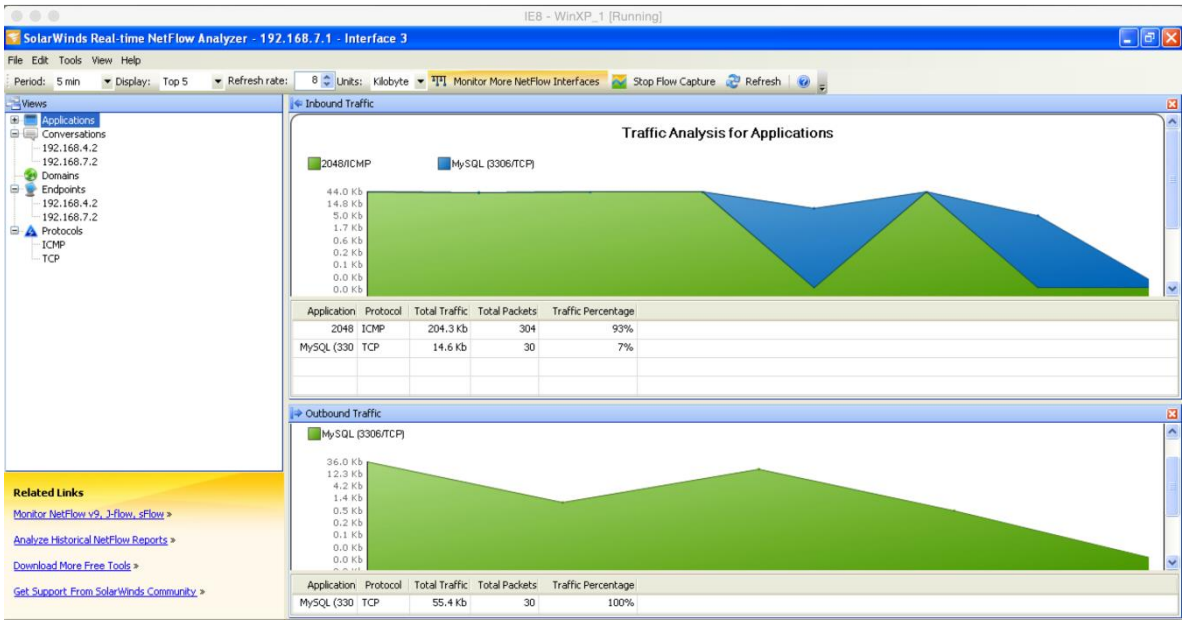
Elaborado por: Autor de la Tesis

En la primera captura gráfica al lado de la izquierda de la interfaz podemos ver que equipos están intercambiados flujos, de la misma manera que en el router y también los protocolos activos en los flujos en este caso ICMP y TCP. En el lado izquierdo

tenemos la gráfica correspondiente a los flujos y cantidad de ancho de banda que ocupan a medida que pasa el tiempo, aquí podemos identificar que en primera instancia todo lo que corresponde al color verde es para el protocolo ICMP, el cual prueba conectividad, pero también tenemos un área color azul la que nos dice que esa parte corresponde a flujos MYSQL (3306/TCP), donde nos muestra que se está usando el protocolo 3306 de MYSQL y que los flujos corresponden a base de datos.

De esta manera podemos rápidamente deducir primero que ningún equipo con esa dirección IP 1928.168.7.2 pertenece a nuestra red y que los flujos que mantiene con nuestro servidor son de bases de datos, anque no sabemos que tipo de información intercambian en cuanto al contenido, es decir, no podemos saber si el intruso esta simplemente probando las seguridades de nuestra red o realmente sustrayendo información de nuestra base de datos.

Figura 48: Incremento de intensidad de flujos y robo de información. Año 2015



Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

En la última figura podemos ver que la intensidad de flujos se ha aumentado por lo que podemos deducir que se ha incrementado el lujo de paquetes TCP de MYSQL y de que efectivamente se trata de un robo de información por parte de un intruso a nuestra base de datos.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- La mejor manera de auditar redes es usando este tipo de protocolos en nuestro caso Netflow de cisco porque nos permiten identificar todos los flujos de las redes y host conectados a las mismas en un intervalo de tiempo, debemos usar siempre las versiones Pro, las que tienen muchas más funcionalidades para el análisis adecuado de la red.

- Se identificó uno de los puntos débiles de Netflow, es cuando nos muestra los resultados en modo de texto, debido a que no muestra toda la información de manera transparente y esto podría ser este un elemento importante del análisis en el momento del ataque.

- Es importante el uso de herramientas gráficas y visuales, debido a que nos permiten el control estadístico de los flujos de datos, si bien Netflow es un protocolo manejado por routers de cisco y nos muestra resultados a manera de texto, también podemos utilizar los interpretes de estos datos como Netflow Analyzer, de esta manera seremos capaces de identificar flujos de una manera más sencilla y rápida.

- Se comprobó que la herramienta GNS3 ofrece una manera fácil de diseñar y construir redes de cualquier tamaño, sin la necesidad de tener el hardware,

ahorrando costos y tiempo en este caso implementando una red de infraestructura para la simulación de un ataque de watering hole.

- Se demostró que Kali Linux es una herramienta que puso en evidencia las vulnerabilidades tanto de la red como de los sistemas operativos. Esta simulación mostró el grado de vulnerabilidad que tienen los equipos dentro de una red sino se usan políticas, hardware y software para implementar seguridades.

- Se identificó tres puntos sensibles para que un ataque se realice, sistemas operativos con puertos siempre abiertos, uso de bases de datos que permiten ejecutar inyecciones SQL ya identificadas, y routers que permiten el paso de flujos sin ninguna restricción, en estos puntos debemos aplicar políticas de seguridad para evitar los ataques.

- Finalmente, se pudo concluir que el ataque watering hole es uno de los más efectivos en la actualidad, con la desventaja que necesita la intervención directa del usuario para desencadenar todos los procesos que se ejecutan en este ataque.

6.2. RECOMENDACIONES

- Configurar el servidor web apache con los mejores parámetros de seguridad para que no se muestre la información de sistema operativo, puertos abiertos y bases de datos disponibles cuando se ejecuta un escaneo con nmap-sql.

- Mantener actualizado a las últimas versiones los sistemas operativos para tener más protección contra ataques, debido a que se encuentran bugs en las últimas versiones y estas serán parchadas por los desarrolladores para evitar posibles violaciones a la seguridad de nuestro sistema.

- No es recomendable usar motores de distribución libre por que se puede exponer información a intrusos, es mejor utilizar un motor de Bases de Datos que garantice un alto nivel de seguridad como ORACLE.

- Visitar frecuentemente la página web: http://www.exploit-db.com/platform/?p=php, la misma que recoge exploits en la red para concentrarlos en una base de datos y poder conocer la información de los mismos.

- Implementar políticas de seguridad a todos los dispositivos de red, es decir, sistemas operativos protegidos con antivirus y firewalls, routers con control de

flujo, servidores configurados que no permitan acceso a usuarios no autorizados, monitoreo de flujos en cualquier punto de la red con protocolos de seguridad como netflow trabajando conjuntamente con el netflow Analyzer para evitar todo tipo de ataques.

BIBLIOGRAFÍA:

[1] Definiciones.de (2015), Redes de Datos, Recuperado de página web: http://definicion.de/red-de-datos/#ixzz3T5Ghew50

[2]TrendMicro (2015), Vulnerabilidades Adobe, Recuperado de página web: http://blog.trendmicro.es/wp-content/uploads/2010/09/vulnerabilidadADOBE.bmp

[3]DRAE (2015) – Telemetría, Recuperado de Pág. Web: http://lema.rae.es/drae/?val=TELEMETRIA.

[4]Wikipedia la enciclopedia libre (2015), Telemetría, Recuperado de Página Web: http://es.wikipedia.org/wiki/Telemetr%C3%ADa.

[5]Wikipedia enciclopedia libre (2015), NetFlow, Recuperado de Pág. Web: http://es.wikipedia.org/wiki/Netflow

[6] Castro A, Estrella A (2009), Estudio de las técnicas de análisis de flujos IP y su aplicación en el monitoreo de redes de datos, recogido de página web: http://dspace.espoch.edu.ec/bitstream/123456789/98/1/18t00375.pdf

[7]SolarWinds Inc. (2012), NetFlow Traffic Analyzer Modulo Orion, Recuperado de:http://web.swcdn.net/creative/pdf/datasheets/ES/1201_orionnta_v3.6_datasheet_0810-spanish.pdf

[8]Microsoft (2015), Definición de SNMP, recuperado de Pág. Web: https://msdn.microsoft.com/es-es/library/cc780057(v=ws.10).aspx

[9]EcuRed (2015), RMON, Reccuperado de pág. Web: http://www.ecured.cu/index.php/RMON

[10]Definición.de (2015) - Definición de monitoreo, Recuperado de Pág. Web: http://definicion.de/monitoreo/#ixzz3UZ8D1T3W

[11]Pymesyautonomos (2015), Tres alternativas para monitorizar el tráfico de red, recuperado de pág. web: http://www.pymesyautonomos.com/tecnologia/tres-alternativas-para-monitorizar-el-trafico-de-red

[12]Hipertextual (2015), Nagios te alerta del estado de tus servidores, recuperado de: http://hipertextual.com/archivo/2010/09/nagios-te-alerta-del-estado-de-tus-servidores/

[13]Paessler AG (2015), Monitorear el tráfico de la red con PRTG, recuperado de: http://www.es.paessler.com/info/network_traffic_monitor

[14]Hipertextual (2015), Monitoriza el estado de tu red con Cacti, recuperado de: http://hipertextual.com/archivo/2010/09/monitoriza-el-estado-de-tu-red-con-cacti/

[15]Wikipedia (2015), Watering Hole, recogido de: http://en.wikipedia.org/wiki/Watering_Hole

[16]Cristhian Borguello (2015), recuperado de: http://www.mug-it.org.ar/343019-Watering-Hole-Attack-Metodo-de-espionaje-contra-las-empresas.note.aspx

[17]Symantec (2015), Waterhole Attack, recuperado de: http://seguinfo.blogspot.com/2012/09/que-son-son-los-ataques-water-hole.html

[18]Agnitum (2015), Exploits en la red, Recogido de pág. web: http://www.outpost-es.com/download/docs/security_insight/2007-10.pdf

[19]Cisco Systems (2003), NetFlow v9 Export Format, recuperado de: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/nfexpfv9.html

[20]Cisco Systems (2009), Detección y Análisis de Amenazas de Red con NetFlow, recuperado de: http://www.cisco.com/cisco/web/support/LA/107/1073/1073894_nf_detct_analy_thrt

s_ps6922_TSD_Products_Configuration_Guide_Chapter.html?bid=0900e4b1820934bc

[21]Fluke Networks (2015), Cisco IOS NetFlow, recuperado de: http://www.upv.es/upl/U0260972.pdf

ANEXOS

ANEXOS A: CONFIGURACIONES DEL ROUTER

Referencia: Configuración runnig-config del router WLNC – Parte 1/9.

Configuración WNCL
Current configuration : 947 bytes ! version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname WNCL ! boot-start-marker boot-end-marker ! ! ! no aaa new-model no ip icmp rate-limit unreachable ip cef ! ! ! ! !

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WLNC – Parte 2/9.

```
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name  authenticated
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
ip ssh version 1
!
!
!
!
!
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WLNC – Parte 3/9.

```
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 200.124.255.203 255.255.255.192
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 186.42.214.1 255.255.255.252
 speed auto
 duplex auto
!
router ospf 1
 network 186.42.214.0 0.0.0.3 area 0
 network 200.124.255.192 0.0.0.63 area 0
!
ip forward-protocol nd
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

d

Referencia: Configuración runnig-config del router WLNC – Parte 4/9.

```
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WLNC – Parte 5/9.

```
end


WNCL#show running-config
Building configuration...


Current configuration : 947 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname WNCL
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WLNC – Parte 6/9.

```
!
!
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name  authenticated
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
ip ssh version 1
!
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WLNC – Parte 7/9.

```
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 200.124.255.203 255.255.255.192
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 186.42.214.1 255.255.255.252
 speed auto
 duplex auto
!
router ospf 1
 network 186.42.214.0 0.0.0.3 area 0
 network 200.124.255.192 0.0.0.63 area 0
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

h

Referencia: Configuración runnig-config del router WLNC – Parte 8/9.

```
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WLNC – Parte 9/9.

```
 login
!
!
end
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config de WNSR – Parte 1/5.

Configuración WNSR
Current configuration : 1149 bytes ! version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname WNSR ! boot-start-marker boot-end-marker !

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WNSR – Parte 2/5.

```
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name  authenticated
!
!
!
!
!
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

k

Referencia: Configuración runnig-config del router WNSR – Parte 3/5.

```
!
!
ip tcp synwait-time 5
ip ssh version 1
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 186.42.214.2 255.255.255.252
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 162.159.250.1 255.255.255.252
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router WNSR – Parte 4/5.

```
 speed auto
 duplex auto
!
interface FastEthernet1/0
 ip address 192.168.7.1 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 network 162.159.250.0 0.0.0.3 area 0
 network 186.42.214.0 0.0.0.3 area 0
 network 192.168.7.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

m

Referencia: Configuración runnig-config del router WNSR – Parte 5/5.

```
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

n

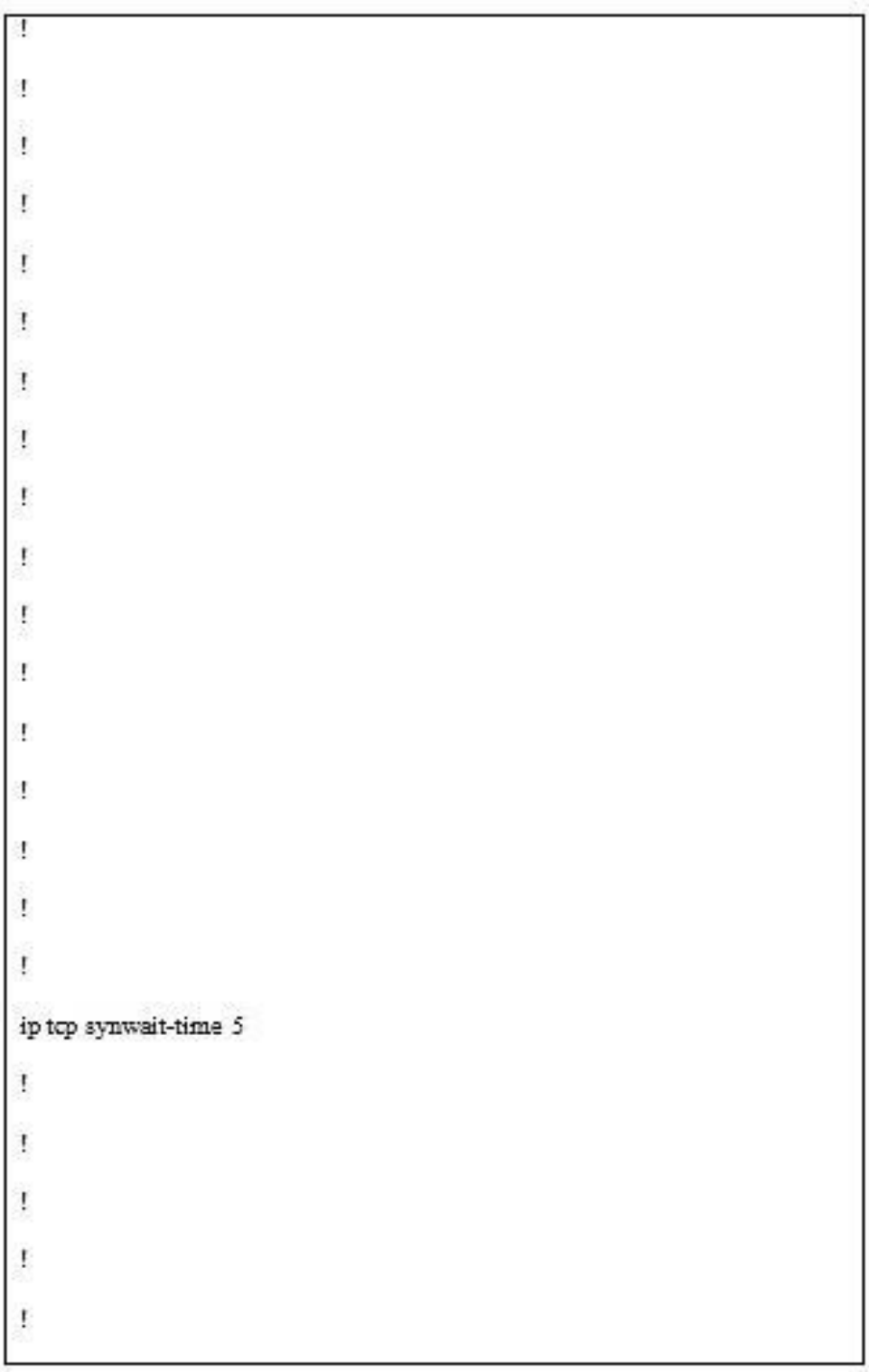
Referencia: Configuración runnig-config del router LNCL– Parte 1/4.

Configuración LNCL
Current configuration : 912 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname LNCL ! boot-start-marker boot-end-marker ! ! no aaa new-model memory-size iomem 5 no ip icmp rate-limit unreachable ! ! ip cef no ip domain lookup !

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router LNCL– Parte 2/4.



```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

p

Referencia: Configuración runnig-config del router LNCL– Parte 3/4.

```
interface Ethernet0/0
 ip address 192.168.20.1 255.255.255.0
 half-duplex
!
interface Ethernet1/0
 ip address 200.124.255.202 255.255.255.192
 full-duplex
!
router ospf 1
 log-adjacency-changes
 network 192.168.20.0 0.0.0.255 area 0
 network 200.124.255.192 0.0.0.63 area 0
!
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
!
control-plane
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router LNCL– Parte 4/4.

```
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

r

Referencia: Configuración runnig-config del router LNSR– Parte 1/5.

Configuración LNSR
Current configuration : 1377 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname LNSR ! boot-start-marker boot-end-marker ! ! no aaa new-model memory-size iomem 5 no ip icmp rate-limit unreachable ip flow-cache timeout active 1 ! ! ip cef

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router LNSR– Parte 2/5.

```
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

t

Referencia: Configuración runnig-config del router LNSR– Parte 3/5.

```
!
!
!
interface Ethernet0/0
 ip address 192.168.4.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
interface Ethernet1/0
 ip address 162.159.250.2 255.255.255.252
 ip route-cache flow
 full-duplex
!
interface Ethernet2/0
 ip address 192.168.7.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
interface Ethernet3/0
 ip address 192.168.6.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

u

Referencia: Configuración runnig-config del router LNSR– Parte 4/5.

```
router ospf 1
 log-adjacency-changes
 network 162.159.250.0 0.0.0.3 area 0
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
!
no ip http server
no ip http secure-server
ip flow-export source Ethernet3/0
ip flow-export version 5
ip flow-export destination 192.168.6.2 9996
!
!
!
snmp-server ifindex persist
no cdp log mismatch duplex
!
!
!
control-plane
!
!
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis

Referencia: Configuración runnig-config del router LNSR– Parte 5/5.

```
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Fuente: Análisis Estadístico Cisco Netflow en ataque Watering Hole

Elaborado por: Autor de la Tesis