PROYECTO MODELO LÍNEA DE BASE

El proyecto consiste en elaborar el modelo de línea de base para la plataforma informática de una empresa de su elección.

Para dicho propósito, conformarán equipos de trabajo de 3 personas, y realizarán el trabajo de elaboración del modelo, de acuerdo con la metodología vista en clase.

El proyecto se presentará en una serie de entregas, como sigue:

- 20 de febrero: Caracterización de la organización y relevamiento de la red.
- 5 de marzo: Usuarios y servicios, y mapa de las aplicaciones.
- 2 de abril: Ficha técnica de la captura de información
- 16 de abril: Resultados y recomendaciones

Los informes respectivos deben presentarse en papel, en la clase correspondiente a la fecha de la entrega a más tardar.

No se ha intentado realizar esta tarea

Por este enlace deben subir el ejercicio de análisis de riesgos, realizado empleando la metodología de matrices vista en clase.

Disponible en: Tuesday, 26 de May de 2009, 14:20
Fecha de entrega: Thursday, 28 de May de 2009, 12:00

Moodle Docs para esta página

Usted se ha autentificado como Juan Manuel Madrid Molina (Salir)

09666_1

UNIVERSIDAD ICESI
INGENIERÍA TELEMÁTICA
PLANEACIÓN Y GESTIÓN DE REDES
LABORATORIO #1 – MONITOREO A NIVEL DE HOST

Una de las labores claves que debe realizar todo administrador de un servidor es la de revisar periódicamente parámetros de funcionamiento del mismo, tales como el nivel de utilización de la CPU, la memoria y los discos. Existen en el mercado herramientas de software que pueden facilitar este trabajo. Sin embargo, no siempre es posible usarlas, por razones como las siguientes, entre otras:

- Existe muy poco espacio en disco para almacenar los ejecutables
- Por política de seguridad, no se desea habilitar servicios adicionales en el servidor
- No se dispone de compilador, o de una versión compilada de la herramienta para la plataforma en cuestión.

En este caso, sistemas operativos como Unix y Linux permiten emplear las poderosas capacidades de su shell para escribir herramientas de administración a la medida. Para ello, se emplea el shell como lenguaje de programación, y los comandos de procesamiento de texto de Unix, tales como gawk, grep, head, tail, cut y otros. En el sistema operativo Windows, se pueden lograr prestaciones parecidas empleando las herramientas Cygwin.

El objetivo de esta práctica es construir una herramienta que permita reportar periódicamente datos críticos de operación de un servidor al administrador del sistema. La herramienta deberá reportar cada 10 minutos, a una cuenta de correo electrónico que se definirá en un archivo de configuración, las siguientes estadísticas de utilización del servidor:

- Porcentaje de uso de la CPU
- Porcentaje de utilización de los discos
- Porcentaje de utilización de la memoria RAM y del espacio de swap.
- Número de procesos creados, activos y suspendidos en la máquina.
- Número de conexiones de red activas (TCP)
- Número de usuarios en sesión en el sistema, y número de procesos que cada uno tiene corriendo en la máquina.

Algunos de los comandos que puede emplear para esta tarea son: top, ps, df, vmstat, who, w, netstat, mail y cron.

Tenga en cuenta lo siguiente:

- Las herramientas que muestran el uso de la CPU demoran un poco en estabilizar su lectura. Ejecute una de estas herramientas y revise las primeras lecturas que arroja. ¿Habría algún dato que tuviera que descartar?
- Las herramientas que reportan el uso de disco muestran una gran cantidad de información innecesaria. Su herramienta de gestión debe tener un archivo de configuración, que permita especificar cuáles discos y/o filesystems serán monitoreados.

- Algunos de los comandos de monitoreo corren en forma interactiva, lo cual imposibilita capturar la información a un archivo. Debe verificarse si el comando tiene una modalidad de ejecución no interactiva, para poder extraer los datos.
- El proceso de monitoreo debe ejecutarse periódicamente, reportar sus resultados, y ser limpio, en el sentido de dejar la máquina en el estado en que la encontró.

Deberán conformarse grupos de 2 personas para la realización del trabajo.

La herramienta deberá empaquetarse en un archivo .tar.gz, y subirse por Moodle (basta con que uno de los integrantes del grupo lo haga). La herramienta debe estar correctamente documentada, de modo que cualquier persona con conocimientos de Unix pueda montarla y entender cómo funciona. El código debe documentarse adecuadamente, y en la distribución debe incluirse un archivo README que contenga las instrucciones de instalación. Todos los archivos de documentación deben ser legibles con herramientas estándar de Unix.

La calificación del laboratorio se hará conforme a la siguiente guía:

Funcionalidad de la herramienta.....50%
Documentación del código y archivo README 40%
Ortografía y redacción del archivo README 10%

El profesor actuara como usuario de la herramienta, y contestará preguntas relacionadas con la misma en horario de oficina.

Como se pudo apreciar en la clase pasada, el empleo de un sniffer como herramienta de diagnóstico puede ayudar a la solución de un problema relacionado con la red, mediante la correlación de los datos capturados en la red con el comportamiento de los equipos conectados a ella.

En el presente laboratorio, se presenta una serie de desafíos a resolver empleando análisis de paquetes y flujos de red con Wireshark. Las respuestas a los diferentes casos deben estar estructuradas de la siguiente manera:

- Especificar dónde se haría la captura de la información (en el equipo involucrado o en algún punto cercano), así como que método se emplearía (hub out, port mirroring…).
- Hacer una descripción del problema y de los indicios que le llevaron a concluir que ése era el problema.

1. Anatomía de una descarga lenta en la red.
Analice el archivo slowdownload.pcap, que corresponde a una descarga lenta en la red. Empleando las opciones Expert Infos e IO Graphs, y empleando sus conocimiento del protocolo TCP, encuentre la evidencia de que la descarga es lenta. En este problema, no hace falta especificar dónde haría la captura.

2. Análisis de una ruta lenta
Su departamento de helpdesk recibe una llamada de un usuario, quien informa que su conexión a Internet está muy lenta. Tras ir a visitar al usuario, se verifica que el problema de lentitud persiste, sin importar el sitio web que se visite. Además, el problema se presenta no solamente en el computador del usuario que puso la queja, sino en todos los computadores de la subred asociada.

Para verificar el funcionamiento de la red, usted decide emplear un traceroute desde el computador del usuario que puso la queja. La captura del tráfico generado está en el archivo icmp-tracert-slow.pcap

AYUDA: Estudie la forma en la que funciona el comando traceroute.

3. Servicio negado
Otro usuario llama al helpdesk, quejándose de que su conexión a la Internet es muy lenta. El usuario se queja de que no puede acceder a cierta parte del sitio web de Novell, para bajar cierto software que necesita. Cada vez que accede al sitio, su browser se queda cargando, pero no ocurre nada.

Después de revisar la red, usted determina que el acceso a Internet es normal para todas la máquinas, exceptuando la del usuario en cuestión. El computador de dicho usuario corre Windows, y está con todos los parches y actualizaciones al día. Navegando desde el equipo afectado, usted descubre que el problema ocurre únicamente con una determinada sección del sitio web de Novell.

La captura de la visita a dicho sitio se encuentra en el archivo http-client-refuse.pcap.

4. Congestión torrencial
Un usuario llama al helpdesk, quejándose de que la red está funcionando en forma extremadamente lenta. No puede acceder la Internet ni ninguna aplicación basada en red a una velocidad decente.

Después de preguntar a otros usuarios, usted se da cuenta de que el problema es general. Todos los usuarios se quejan de lentitud en la red. Además, el enrutador de frontera de la red indica una alta utilización de CPU, mostrando que está manejando una cantidad sustancial de tráfico, tanto hacia adentro como hacia fuera de la red.

El archivo de captura de esta situación se denomina torrential-slowness.pcap

5. Servidor de correo caído
En esta ocasión, todos los usuarios de la red se quejan de que el e-mail está demorándose demasiado en llegar a su destino. Debe partirse de la base de que todo el e-mail de la empresa se maneja a través de un único servidor. Después de verificar algunos computadores, usted concluye que el problema se presenta con todos los clientes de correo de la compañía. Un correo entre empleados de la empresa, que normalmente llega instantáneamente, se está demorando entre 10 y 15 minutos. Lo mismo pasa con el correo externo.

El archivo de captura de esta situación se denomina email-troubles.pcap

6. Problemas con un servidor FTP
En su compañía se emplea un servidor FTP interno para mantener diferentes versiones de software y documentos. En los últimos días, el técnico de sistemas de información que administra el servidor ha notado que el tráfico hacia el servidor se ha incrementado mucho, en horas no laborales. Por desgracia, el servidor FTP no tiene servicio de logging. Se desea encontrar la causa del incremento el uso de la red por parte del servidor, y eliminar la fuente.

Todos los usuarios de la compañía tienen username y password en este servidor, y el servidor es accesible desde el exterior de la empresa, de manera que los empleados pueden accederlo desde sus casas.

La captura de este caso puede encontrarse en el archivo ftp-crack.pcap

7. Información encubierta
En este caso, usted es el oficial de seguridad de la red de una multinacional. Un superior suyo acaba de avisarle que un empleado escuchó a otros dos empleados haciendo planes de robarse parte de los activos de la compañía. Su tarea consiste en monitorear los computadores de los dos sospechosos, para tratar de revelar sus planes.

Este escenario se basa en especulaciones. Como no es posible verificar que el rumor es cierto, y además se sabe que los dos empleados en cuestión son muy hábiles con los computadores, es necesario ser muy cuidadosos con la recolección de la evidencia. Es necesario, ante todo, buscar tráfico sospechoso. Las direcciones IP de los computadores de los sospechosos son 10.100.17.48 y 10.100.18.5, respectivamente.

La captura correspondiente a este caso se puede encontrar en el archivo covertinfo.pcap

8. Punto de vista del hacker

A través del curso, normalmente se miran las cosas desde el punto de vista del administrador de la red. Sin embargo, en esta caso se tomará el punto de vista del hacker, que trata de acceder a información sensitiva dentro de la empresa.

En este caso, usted es un empleado de la compañía que está tratando de atacar, y dispone por lo tanto de recursos limitados. La red de la compañía es una Ethernet sencilla, con pocos switches y enrutadores.

En este caso, usted decide averiguar el password de administración de uno de los enrutadores de la empresa. Usted averiguó que la dirección IP de la estación del administrador de la red es la 192.168.1.100, y la del enrutador es la 192.168.1.1

La captura de información correspondiente a este caso está en el archivo hackersview.pcap.

Las soluciones a este laboratorio deberán desarrollarse en grupos de 3 personas, y entregarse el 12-MAR-08. Se habilitará un enlace en Moodle para subir las soluciones.

El objetivo de esta sesión de laboratorio es ensayar algunas técnicas de hacking ético (particularmente, técnicas de rastreo, enumeración y detección de vulnerabilidades), en sistemas Linux y Windows

Para esta práctica de laboratorio se requiere lo siguiente:

- Un computador con Linux Ubuntu instalado

Las preguntas que aparecen en la guía deben contestarse y presentarse por escrito la próxima semana. Algunas de las preguntas podrían exigir investigación adicional.

TÉCNICAS DE RASTREO (SCANNING)

Una vez determinada la red a atacar, el primer paso es determinar qué equipos están conectados a la misma. Existen varias técnicas para hacerlo.

La primera es empleando ICMP, es decir, el comando ping. Varias herramientas permiten hacerlo:

- `fping`, que requiere tener un archivo de las direcciones IP que se desean comprobar.
- `nmap`, que puede hacer el proceso automáticamente sobre toda una subred.

Para usar `fping`:

- Abra una consola.
- Cree un archivo, e introduzca en él 10 direcciones IP de equipos que estén en la misma subred de su estación de trabajo.
- Una vez creado el archivo, ejecute fping empleando el nombre del archivo como entrada:

```
fping –f nomarchivo.txt
```

Pregunta: ¿Cuáles de los equipos que listó en su archivo están activos?

El problema con las técnicas de scan mediante ping, es que normalmente el servicio de ping está bloqueado a nivel de los firewalls. Esto fuerza a emplear técnicas como el TCP ping. **Pregunta: ¿En qué consiste esta técnica?**

La herramienta nmap emplea por omisión un ping ICMP, más una variante de la técnica de TCP ping para determinar qué equipos están activos en la red destino.

Para usar `nmap`:

- Primero ejecute `nmap`, sin parámetros, para verificar que esté instalado en la máquina.
- Si no está instalado, realice la instalación ejecutando el comando `sudo apt-get install nmap`

- En la misma consola, invoque a `nmap`:

```
nmap -sP 192.168.130.0/24
```

Pregunta: ¿Qué resultados arroja `nmap`?
Pregunta: ¿Cuál es la utilidad de la opción `-sP`?

- Consulte el manual en línea de `nmap` para averiguarlo.
- Usando Wireshark o Ethereal, determine qué paquetes envía nmap a los equipos destino.

Se puede cambiar el puerto destino que emplea nmap para hacer el ping scan. Emplee el comando:

```
nmap -sP -PS5 192.168.130.0/24
```

Pregunta: ¿Qué hace la opción `-PS` en este caso? Emplee Wireshark o Ethereal para comprobarlo.

Compare el listado que arroja el `nmap -sP` con el que arroja el `nmap -sP -PS80`. **Pregunta: ¿Hay alguna diferencia?** Explique el porqué.

TÉCNICAS DE ENUMERACIÓN (ENUMERATION)

Conocidos los equipos que están activos en la red a atacar, el siguiente paso es determinar qué puertos están abiertos en cada uno de ellos, y qué servicio corre en cada uno de los puertos abiertos. Si es posible, también se debe averiguar qué tipo de sistema operativo está corriendo la máquina, y las versiones del software de servicios que escucha en cada uno de los puertos abiertos.

Una de las formas más populares de enumeración es mediante un escaneo TCP SYN. **Pregunta: ¿En qué consiste este tipo de escaneo?** (es decir, averigüe qué información envía nmap, y qué información espera espera recibir del computador escaneado. Emplee Wireshark o Ethereal para verificar esto).

El escaneo TCP SYN se ejecuta de la siguiente manera desde `nmap`:

```
nmap -sS dir_host
```

Ejecute este comando contra cuatro de los equipos que encontró activos en la primera parte de este laboratorio. **Pregunta: ¿Qué puertos están abiertos en cada uno de ellos?**

Existen otros esquemas de enumeración. **Averigüe en qué consiste cada uno de ellos, y cómo se invocan desde `nmap`:**

- TCP FIN
- TCP XmasTree

- TCP NULL
- TCP ACK

Invoque el escaneo de puertos contra alguno de los equipos que encontró activos en la primera parte del laboratorio, empleando cada una de estas opciones, y emplee Wireshark para capturar el tráfico de la red y verificar el funcionamiento de cada una de dichas opciones.

Para averiguar la versión del sistema operativo de la máquina remota, se emplea una técnica conocida como fingerprinting de la pila TCP/IP del sistema operativo. **Pregunta: ¿En qué consiste esta técnica?**

La manera de hacerlo con `nmap` es la siguiente:

```
nmap -O dir_host
```

Otra herramienta muy útil para este propósito es p0f. **Instálela** (`sudo apt-get install p0f`), lea el manual y explique en forma concisa cómo funciona. **En particular, explique qué la hace diferente a nmap.**

Para averiguar qué servicio está corriendo en un puerto en particular, la manera más sencilla es hacer un telnet por el puerto en cuestión, y observar el banner o respuesta del servidor.

Ensaye a hacer esto contra alguna de las máquinas que encontró con puertos abiertos en la parte anterior del laboratorio. ¿Qué banner obtuvo en cada puerto?

Los banners de protocolos como TELNET, FTP, POP y SMTP son fácilmente reconocibles. Sin embargo, existen protocolos (como HTTP) donde es necesario iniciar el diálogo con el servidor para obtener más información. Por ejemplo, una manera típica de ocasionar respuesta de un servidor Web es la siguiente:

- Hacer un telnet por el puerto (típcamente, el 80).
- Una vez se logre la conexión, introducir `GET / HTTP/1.0` (en mayúsculas). Esto solicitará al servidor web enviar la página raíz.
- Tras presionar ENTER dos veces, aparecerá primero la respuesta HTTP (en la que figura el banner), y después, la página web.

Trate de averiguar las versiones del software que está corriendo en dos servidores, cuyo nombre o dirección IP será suministrado por el profesor.

Existen programas que permiten hacer todas las operaciones de escaneo y enumeración desde un entorno integrado. Una de ellas es `cheops`.

Instálela ejecutando el comando `sudo apt-get install cheops`. Para invocarla, abra una consola de texto y digite `sudo cheops`.

Deje que el computador agregue la subred a la que pertenece su equipo. Observe qué equipos aparecen. Pueden adicionarse redes, empleando el comando **Viewspace -> Add Network**.

Haga clic derecho en algún equipo que le parezca interesante, y escoja la opción **Scan**. **Interprete los resultados**.

Por último, presione el botón **More…** que aparece en la ventana de **TCP Portscan**. **Interprete los resultados.**

EMPLEO DE UN DETECTOR DE VULNERABILIDADES

El software de detección de vulnerabilidades no debería faltar entre las herramientas de cualquier administrador de red. Si se mantiene debidamente actualizado, permite analizar los equipos de la empresa y descubrir huecos potenciales de seguridad.

Uno de los más empleados, por su facilidad de uso, y por el hecho de ser gratuito, es Nessus.

Para instalarlo:

- Digite el comando `sudo apt-get install nessus nessusd`
- A continuación, cree un usuario dentro de la herramienta Nessus. Emplee para ello el comando sudo nessus-adduser. Cuando se le soliciten, suministre el nombre y la contraseña del usuario que desee agregar. El tipo de autenticación debe ser PASS, y las reglas deben ir en blanco.

Para ejecutarlo:

- En una consola de texto, digite `sudo nessusd`. El sistema avisará cuando se acaben de cargar los plugins de escaneo.
- En otra consola de texto separada, digite `nessus&`
- En la pestaña “Nessusd host”, digite el nombre de usuario y la contraseña que creó en la instalación. Presione LOGIN.
- Acepte el certificado de seguridad que Nessus le ofrece.
- En la pestaña de “Target selection”, escriba la dirección de un host que el profesor le especifique.
- En la pestaña de “Plugins”, revise las vulnerabilidades que se van a chequear.
- Presione “Start the scan”. El análisis de vulnerabilidades comenzará.

PREGUNTAS:

- Interprete los resultados. ¿Qué bondades le ve a una herramienta de este tipo?
- ¿En qué consiste un plugin peligroso?
- En algunas de las pantallas que verá, Nessus dice que no está registrado. Averigüe y describa el proceso que debe hacerse para registrar Nessus. ¿Qué beneficios supone registrar a Nessus?