AUDITORIA A LA RED DE UNA EMPRESA

OSCAR MARIO GIL RIOS

INGENIERO DE SISTEMAS

ESPECIALISTA EN REDES E INTEGRADOR DE TECNOLOGIAS

UNA AUDITORIA DE REDES

- Es, en esencia, una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información.

PASOS PARA REALIZAR UNA AUDITORIA A LA RED

- El primer paso para iniciar una gestión responsable de la seguridad es identificar la estructura física (hardware, topología) y lógica (software, aplicaciones) del sistema (sea un equipo, red, intranet, extranet), y hacerle un **Análisis de Vulnerabilidad** para saber en qué grado de exposición nos encontramos.

PROPUESTA DEL AUDITOR

- así, hecha esta "radiografía" de la red, se procede a localizar sus falencias más críticas, para proponer una **Estrategia de Saneamiento** de los mismos; un **Plan de Contingencia** ante posibles incidentes; y un **Seguimiento Continuo** del desempeño del sistema de ahora en adelante.

Etapas a implementar en la Auditoría de Redes

- **Análisis de Vulnerabilidad**
- Éste es sin duda el punto más crítico de toda la Auditoría, ya que de él dependerá directamente el curso de acción a tomar en las siguientes etapas y el éxito de éstas. Existen herramientas como scaneadores de red que permiten detectar estas vulnerabilidades en el sistema.

ANALISIS DEL AUDITOR

- A través de los análisis y reportes arrojados por medio de las anteriores herramientas, se procede a implementar procedimientos en función de acabar con las vulnerabilidades encontradas, de modo que en compañía de directivos y personal encargado de la seguridad de la red se implementarán acciones que consideren necesarias.

Estrategia de Saneamiento

- Identificadas las "brechas" en la red, se procede a "parchearlas", bien sea actualizando el software afectado, reconfigurándolo de una mejor manera ó remplazándolo por otro que consideremos más seguro y de mejor desempeño.

Estrategia de Saneamiento

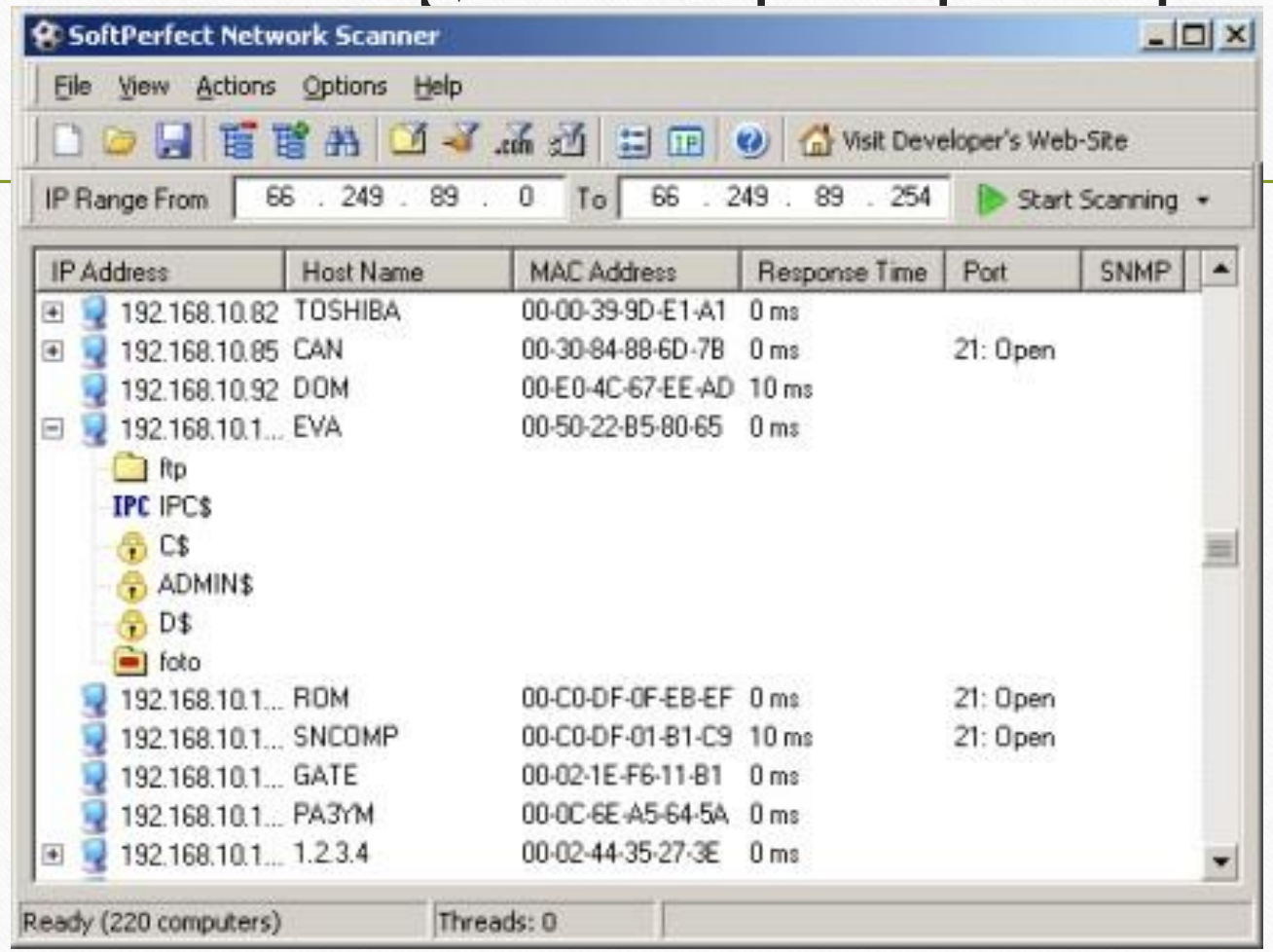
- Las bases de datos, los servidores internos de correo, las comunicaciones sin cifrar, las estaciones de trabajo... todo los puntos críticos deben reducir el riesgo. En los casos más extremos, la misma infraestructura física de la red deberá ser replanteada, reorganizando y reconfigurando sus *switches*, *routers* y *firewalls*.

Plan de Contingencia

- La red ha sido replanteada, el software ha sido reconfigurado (o rediseñado) y el riesgo ha sido reducido; aún así, constamente se están reportando nuevos fallos de seguridad y la posibilidad de intrusión siempre está latente. Un disco rígido puede fallar, una base de datos puede corromperse o una estación de trabajo puede ser infectada por un virus; para ello hay que elaborar un "Plan B", que prevea un incidente aún después de tomadas las medidas de seguridad, y que dé respuesta ante posibles eventualidades.

Seguimiento Continuo

Como señala **Bruce Schneier**, reconocido especialista de esta área, *«la seguridad no es un producto, es un proceso»*. constantemente surgen nuevos fallos de seguridad, nuevos virus, nuevas "herramientas" (scaneadores) que facilitan la intrusión en sistemas, como así también nuevas y más efectivas tecnologías para prevenir estos problemas; por todo ello, la actitud ante la seguridad de debe ser activa, procurando estar "al corriente" de lo que esté sucediendo en la materia, para ir cubriendo las nuevas brechas que vayan surgiendo y -cuando menos- para hacerle el trabajo más difícil a nuestros atacantes.


SoftPerfect Network Scanner
File View Actions Options Help
Visit Developer's Web-Site
IP Range From 66 . 249 . 89 . 0 To 66 . 249 . 89 . 254
Start Scanning
IP Address | Host Name | MAC Address | Response Time | Port | SNMP
192.168.10.82 TOSHIBA 00-00-39-9D-E1-A1 0 ms
192.168.10.85 CAN 00-30-84-88-6D-7B 0 ms 21: Open
192.168.10.92 DOM 00-E0-4C-67-EE-AD 10 ms
192.168.10.1... EVA 00-50-22-B5-80-65 0 ms
ftp
IPC$
C$
ADMIN$
D$
foto
192.168.10.1... ROM 00-C0-DF-0F-EB-EF 0 ms 21: Open
192.168.10.1... SNCOMP 00-C0-DF-01-B1-C9 10 ms 21: Open
192.168.10.1... GATE 00-02-1E-F6-11-B1 0 ms
192.168.10.1... PA3YM 00-0C-6E-A5-64-5A 0 ms
192.168.10.1... 1.2.3.4 00-02-44-35-27-3E 0 ms
Ready (220 computers)
Threads: 0