Redes WAN

Seguridad

Esteban De La Fuente Rubio
esteban@delaf.cl
LaTeX

Universidad Andrés Bello

6 may 2011

Tabla de contenidos

¿Por qué es importante?

Evitar:

- Perdida de privacidad.
- Robo de información.
- Responsabilidad legal.
- Estafas.
- Etc.

Conceptos sobre seguridad

- Amenaza: evento que puede desencadenar un incidente.
- Impacto: consecuencia de la materialización de una amenaza.
- Riesgo: posibilidad de que se produzca un impacto determinado en un activo.
- Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza.
- Ataque/incidente: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Triada CID

Se deben proteger los siguientes conceptos:

- Confidencialidad
- Integridad
- Disponibilidad

Confidencialidad

- "Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso" [ISO-17799].
- Métodos de cifrado y ocultación de la información.
- No existe ningún mecanismo de seguridad 100 % seguro.
- Lo importante es que sea lo suficientemente seguro por el tiempo que los datos lo ameriten.

Confidencialidad (2)

Métodos de cifrado:

- Simétrico.
- Asimétrico.

SSL

Se utiliza:

- Un par de claves, una pública y una privada (encriptación asimétrica).
- Un certificado de seguridad, que es una versión "firmada" de la clave pública.
  - Autofirmadas.
  - Firmadas por empresas (como Verisign).

SSL (2)

SSL handshake:

1. Servidor presenta al cliente su certificado (dentro la clave pública) y el cliente lo acepta.
2. Cliente genera un "premaster secret" y lo envia encriptado al servidor con la clave pública de este.
3. Servidor desencripta el "premaster secret".
4. Cliente y servidor generan un "master secret" a partir del "premaster secret" y luego las "session keys". Está última será la clave simétrica a utilizar durante el intercambio de datos en la sesión SSL.
5. Cliente y servidor se comunican de forma encriptada.

SSL (3)

Generar Clave Privada

openssl genrsa -des3 -out server.key 1024

Generar certificado para firmar

openssl req -new -key server.key -out server.csr

Generar certificado autofirmado

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

Integridad

- Que un mensaje (archivo) no haya sido modificado.
- Métodos de funciones hash (como md5) para determinar la integridad de un archivo.

md5sum

Crear archivo vacio y calcular hash

touch archivo && md5sum archivo

Modificar archivo y calcular hash

echo 1 > archivo && md5sum archivo

Disponibilidad

- Uptime de un servicio o equipo.
- ¿Qué uptime necesito en un servidor?

Amenazas

Las podemos dividir principalmente en 2 grupos:

- Tecnológicos.
- No tecnológicos:
  - Incendios
  - Inundaciones
  - Terremotos
  - Camiones
  - Animales
  - Etc.

Amenazas tecnológicas

- Cracker.
- Phreaker.
- Spammer.
- Phishing.
- Usuarios.

Amenazas tecnológicas (2)

Usuarios:

- Mal uso de la red.
- Consumo de ancho de banda excesivo.
- Se les debe controlar y educar.
- Para acceso a contenido utilizar proxy (como Squid).
- Para educar crear políticas de seguridad.

Squid

- Filtro de contenido.
- Web Cache.
- Permite realizar control de ancho de banda.
- Funciona en modo transparente y no transparente.

Políticas de seguridad

Se pueden definir como:

- Abiertas.
- Restrictivas.
- Cerradas.

¿cuál es la política a aplicar en la empresa? ¿es la idea? ¿de que depende?

Tipos de debilidades

- Tecnológicas: protocolo de red (tcp/ip), sistemas operativos, equipos de red.
- Configuración: cuentas no seguras, servicios mal configurados, configuraciones predeterminadas (OpenBSD).
- Política de seguridad: falta de las mismas, instalaciones que no respetan las políticas, plan de recuperación.

Tipos de amenazas

- No estructuradas.
- Estructuradas.
- Externas.
- Internas.

No estructuradas

- Personas sin experiencia.
- Utilizan herramientas de fácil acceso.
- Uso de troyanos como SubSeven.
- Bombas fork.

Ejecutar en un terminal

```
:(){ :|:& };:
```

Estructuradas

- Personas o grupos competentes técnicamente.
- Conocen vulnerabilidades del sistema.
- "Ingresan en computadoras de empresas y del gobierno para cometer fraude, destruir o alterar registros o, simplemente, para crear confusión. Por lo general, estos grupos están involucrados en los principales casos de fraude y robo denunciados en los organismos de aplicación de la ley. Utilizan tácticas de piratería informática tan complejas y sofisticadas que sólo los investigadores especialmente capacitados entienden lo que está ocurriendo." [CCNA4]

Externas

- No se tiene acceso autorizado.
- Acceso principalmente desde Internet.
- Común hoy en día también acceso desde redes WiFi.

Internas

- Provocadas por personas con acceso a la red.

Ingeniería social

- Manipulación de usuarios.
- Realizada mediante engaños.
- Phishing correspondería a esta categoría.
- Investigar quién fue/es Kevin Mitnick.

Tipos de ataques a redes

- Reconocimiento.
- Acceso.
- Denegación de servicio.
- Virus, gusanos y troyanos.

Reconocimiento

- Descubrimiento de servicios, sistemas y/o vulnerabilidades.
- Recopilación de información previa para otro tipo de ataque.
- Interés máximo es encontrar vulnerabilidades a explotar.
- Métodos:
  - Información en internet (whois).
  - Barridos ping (nmap).
  - Escaneos de puerto (nmap).
  - Analizadores de tráfico (wireshark).

Reconocimiento (2)

Escanear red

nmap -v -sP red/mask

Escanear máquina

nmap -v -A host

Acceso

- Obtención de acceso a una máquina o servicio.
- Al no ser un acceso autorizado se incurre en un delito informático.
- Accesos apuntan a obtener cuenta de usuario root del sistema.
- Métodos:
  - Obtención de contraseñas (john).
  - Explotación de confianza.
  - Redirección de puertos (caso de explotación de confianza).
  - Hombre en el medio.

Denegación de servicio

- Se evita el correcto funcionamiento de un servicio determinado.
- Métodos:
  - Saturación Sync (protocolo de enlace a 3 vías).
  - DDoS (ataque distribuido para saturar red, uso de zombies).
  - Ataque Smurf (tipo de DDos, inundación mediante ICMP).

Virus, gusanos y troyanos

- ¿Diferencia entre virus y gusanos?
- ¿Qué es un troyano?
- ¿Qué son las máquinas Zombie?

Be safe, use GNU/Linux.

Aseguramiento y mitigación

- Dispositivos.
- Parches y antivirus.
- Firewalls.
- IDS.
- Se debe asegurar, controlar, probar y mejorar.

Aseguramiento y mitigación (2)

Hacer una lista con 10 medidas que se puedan tomar.

Política de seguridad

- Autoridad y alcance.
- Usos aceptables.
- Autenticación.
- Acceso a Internet.
- Acceso al campus.
- Acceso remoto.
- Manejo de incidentes.

Política de seguridad (2)

- Solicitud cuentas.
- Adquisiciones.
- Auditorías.
- Confidencialidad.
- Contraseñas.
- Evaluación de riesgos.
- Normas para servidores.

Personas

- Se debe educar a los usuarios.

Seguridad basada en ocultación

- Se cree que por estar ciego un atacante nuestro sistema es mas seguro.
- Falsa seguridad.

¿Cuanto se esta dispuesto a gastar?

- ¿Tiene sentido proteger un auto que cuesta $350.000 con un sistema de alarma que sale $500.000?
- Por el contrario, si tengo datos muy valiosos, o mi uptime es crítico, ¿puedo no tener respaldos o sistemas de UPS?
- Debe haber un equilibrio entre el valor de lo que se quiere proteger y cuanto costará protegerlo.