Taller de Administración de Servidores Linux

CC5308

Clase 21: 28 de abril de 2011

Seguridad:
Comunicaciones de Aplicaciones

Luis León Cárdenas Graide
lcardena [at] nic . cl

Problema

- Seguridad: Comunicación
  - Confidencialidad, Integridad, Disponibilidad
- Storage: auto-comunicación tiempo diferido
  - Reaprovechamiento: técnicas... y problemas
- Confidencialidad: Comunicación clear-text
  - Sniffing (robo, suplantación)
- Integridad: Verificación
  - Tampering, Injection, Reply, Reflexión
- Disponibilidad
  - Downtime, Amplificación, DoS

Capa OSI 1: Físico

- Cable metálico: Pulsos EM
  - Confidencialidad: Radiación EF
    - Red... monitores, teclado... USB... cerebro
  - Integridad: Interferencia
    - Shielding, Twisting: STP
  - Disponibilidad: Cortes, desconexiones
- Coaxial, RJ-45
- ¿Prevenible? ¿Detectable?

Capa OSI 1: Físico

- Cable vidrio: Señal Óptica (también EM)
  - Confidencialidad: Irradia menos
  - Integridad: Impurezas, Atenuación
    - Reamplificación
  - Disponibilidad: Cortes, desconexiones
    - Cables submarinos + anclas
    - Cables puentes/postes + terremotos/accidentes
    - Cables subterráneos + $$$
- ¿Prevenible? ¿Detectable?
- ¿Enlace dedicado?

Capa OSI 1: Físico

- Radiofrecuencias
  - Confidencialidad: Broadcast/Direccional
    - Sensibilidad antena (Direccionales: Kilómetros)
    - ¿Jaula Faraday?
  - Integridad: Interferencia
    - Espectros estandarizados reservados legalmente
    - ¿Hornos Microondas?
  - Disponibilidad: Señal/Ruido ¿Quién grita más fuerte?
    - Distancia: Atenuación
    - Jamming
- ¿Prevenible? ¿Detectable?
- Definición legal países: bandas de frecuencias

Capa OSI 2: Enlace

- Point-to-point (no end-to-end) a-la TELCOs
  - ¿Espionaje? ¿Soborno? ¿Law enforcement?
- Cableado: Ethernet
  - ¿"Seguro"? ¿"Local"? Tomas de red, Sniffing, VPN
  - IEEE 802.1AE (MACsec)
- Radiofrecuencias
  - GSM, Wifi, WiMax, etc.
  - Wifi: corto alcance
    - "Cable seguro" => WEP: "Seguridad" "equivalente"
      - Premura industrial: Equivalentemente mala (RC4 lineal)
    - ~~WPA~~, WPA2... en algunos modos
- ¿Dispositivos limitados? ¿End-to-end?

Capa OSI 3: Red

- Dirección IP: sniffing, spoofing, reflexión, MITM...
  - v4: checksum para errores, no tampering
  - ¿Integridad datagrama?
    - "TTL" vs checksum
    - Eficiencia routers: paquetes/segundo
- IPsec: end-to-end
  - Firmas/cifrado: IP origen, datagrama
  - Default en IPv6: checksum de payload en capa superior
- VPN
  - Raw vs IPsec
  - "Net-to-net", no end-to-end
    - (Es end-to-end entre gateways)

Capa OSI 4: Transporte (y algo de 5: Sesión)

- TCP/UDP: Sniffing, spoofing, MITM, DoS...
- IPv6: Checksum en Transporte (TCP6/UDP6)
- SSL: Secure Socket Layer (end-to-end)
  - Anónimo: Intercambio Diffie-Helmann
  - Certificado en uno/ambos extremos (Cliente/Servidor)
- Overhead inicial: Inicio Sesión SSL
  - Tiempo: +Latencia por Paquetes handshake en 1era
- Overhead posterior (¡marginal!)
  - Red: +Ancho de banda por headers (número secuencia)
  - CPU: < +10%
- FUD: "SSL es lento/pesado, mejor no usarlo"

Capa OSI 5: Sesión

- Cookies (no sólo web)
  - Identificador sesión
  - Otros datos
- Tampering, sniffing, hijacking, etc.
- ¿Asegurar "la red"? ¡Capa inferior! Otras medidas
  - Cookie = Session ID: SSL previene sniffing
  - Cookie compleja: Cliente la puede adulterar (HMAC)
  - Igual preferir SSL: Configuración Sitios, Extensiones navegadores, subdominios
- ¿Session fixation? ¿CSRF?
  - "Nonces", Chequeo BD o HMAC, Login previo a cookie

Capa OSI 6: Presentación

- Fundamentos CC: Alfabetos, Lenguajes y Álgebra
  - Strings pertenecen a lenguajes formales en base a alfabetos (y posterior sintaxis)
    - Lenguaje Programación, "texto claro", red, protocolos
  - "Tipo" de strings: Todo se **representa** de alguna forma
    - ¿A qué lenguaje pertenece?
    - ¿Con qué caracteres se representa?
  - Strings "similares" de distintos lenguajes pueden **coincidir** en su representación, ¡pero son distintos!
  - Traducción de strings entre lenguajes
    - URI, {HT,X}ML, JS, HTTP, UTF, PHP/Perl, SQL, Shell
  - Representación opaca: quoting, metacaracteres
- Confusión => Inyección: XSS, *-injection

Capa OSI 6: Presentación

- String Código vs String Objetivo
- ¿Mashups? ¿Extensibilidad?
  - Metalenguaje y Metadatos
- Ojo: Lenguaje pre-post encoding
  - Stack de conversiones (LIFO)
- ¿Acoplamiento?
  - Mal diseño: Mala separación de capas
  - Stack: Múltiple**s** capa**s** de Presentación
  - Presentación no siempre es a usuario final (¿quién es?)
    - Usualmente no lo es, sino que hacia otros sistemas
      - Internos o externos
      - Que presentan hacia otros sistemas

Capa OSI 7: Aplicación

- Aplicaciones particulares: HTTPS,DNSSEC,IMAPS
- Firewall de aplicación: Filtros
  - Acoplamiento y Ad-hoc: SQL, HTML, Javascript, etc.
  - Tipos de datos
- Límites de recursos
  - Espacio: Memoria, disco
  - Tiempo Ejecución y %CPU: Peak vs acumulado
  - Red: Ancho de banda, bytes transmitidos, conexiones
  - Descriptores: Archivos, Procesos, etc.
- ¿Firewall de red? (Capa 3)
  - SOAP (puerto 80) e Inyecciones independientes de red

Actividad Personal

- Elija(*) su sitio web favorito
  - ¿Qué pasa al postear formularios que contengan alguno de los siguientes caracteres?
    - < ' > | ?%&# ; - \ " espacio(s) (o blancos)
    - Legítimo: Caracteres sin sentido en ciertos contextos
    - Excusa: "por su seguridad"
      - Usualmente: "Seguridad" = Snake Oil
    - Realidad: "por mi sistema mal hecho"
  - Observe efectos en representación y lógica de negocio
  - ¿Y las marcas de acentuación de su apellido? "Ñandú"
  - ¿Funcionan en contraseñas?
- wget --post-data + Bash $'\c'

Actividad Personal

- Elija su script shell favorito
  - ¿Qué pasa con parámetros "raros"?
    - `\;\$\'\"\\\(\&\|\ ` (espacio)
  - ¿Y con nombres de archivo "simpáticos"?
    - -nombre, 'nom bre', 'no mbre'
  - ¿Error del script, del shell, del invocante?
    - (Hint: del script) (Recuerde Tarea #1)
    - (¿Por qué? ¿Evitable? ¿Cómo? ¿Fácil?)
- Pruebe(*) wireshark y FireSheep
- (*) Sólo con autorización previa del dueño del sitio/cuenta afectado y sin dañar(!)
  - Pentesting controlado sólo en sistema propio