Trabajos Prácticos – Seguridad de la información – dc.uba.ar – 2do cuat. 2017

Importante: El 29/11 deben sí o sí presentar lo que tengan hecho hasta el momento a todos sus compañeros. De no ser aprobado el TP en dicha instancia, deben recuperarlo a más tardar el 11 de diciembre de 2017, que es la fecha definitiva de entrega del TP.

TPS DE IMPLEMENTACIÓN

Entregables TP de Implementación

Resumen de 1 o 2 carillas que incluya actividades realizadas, herramientas utilizadas, bibliotecas, material consultado, a entregar por mail hasta el 5/11.
Una presentación con transparencias y demo en vivo a dar el 29/11.
Un informe al final de cuatrimestre (fecha límite 11/12) de por lo menos 12 carillas, en letra arial 10, espaciado simple, contando lo que hicieron y las decisiones que tomaron (no incluye código fuente). Incluir como probar las aplicaciones desarrolladas.
El código fuente de las aplicaciones desarrolladas.

En el caso del TP de wireless, donde el esfuerzo de desarrollo es mucho menor, el informe debe ser más extenso y detallado.

TP 1 – Servidor de logs seguros con forward integrity

Cuando un atacante toma control total de un sistema, una de las actividades que puede hacer es modificar los registros de auditoría, para ocultar evidencia de lo ocurrido. Para evitar esto, se pueden desarrollar sistemas de registros de auditoría que tengan la propiedad de "forward integrity". Esto implica que, por más que el atacante pueda modificar los registros desde el momento que se toma el control del sistema atacado, no se pueden borrar o modificar registros previos, sin que quede evidencia. Existen distintas formas de implementar esta propiedad.
Se debe implementar un servidor de syslog centralizado (rfc 5424), utilizando estructuras (ej hash chain) que permitan detectar cambios no autorizados en los logs. Leer los siguientes artículos, y en base a eso validar con el profesor la propuesta de implementación.

Ref:
Bellare and Yee. Forward integrity for secure audit logs.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.6973&rep=rep1&type=pdf

Holt. Logcrypt: Forward Security and Public Verification for Secure Audit Logs
https://eprint.iacr.org/2005/002.pdf

TP 2 – Autoridad de timestamp y evidencia de contenido de sitio web

El Timestamp es un mecanismo que sirve para demostrar que un dato existe y no fue alterado a partir de un momento dado en el tiempo. Un Timestamp es emitido por una Autoridad de Timestamping que actúa como tercero confiable testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

Implementar una autoridad de time-stamping (TSA) siguiendo los lineamientos del RFC3161 y RFC3628. Se debe incluir un sitio web que permita interactuar con la TSA (también es recomendable implementar algún otro mecanismo de interacción), y un documento que explicite la política de uso. A partir de dicha autoridad, implementar un servicio de "dar fe de que el contenido de una página web existía y estaba publicado en un

momento dado". Para esto, se debe generar un PDF con un snapshot de la página, firmado digitalmente, que incluya un sello de tiempo emitido por la TSA, usando el formato PAdES.

Para el último punto, tomar como ejemplo la aplicación https://www.egarante.com/productos/eg-web/

TP 3 – Análisis de tráfico en redes wireless - MITM

Implementar un Rogue AP, para poder sniffear, por ejemplo, tráfico de teléfonos celulares que hagan probe requests a redes abiertas (ya sea con nombre comunes o con respuesta a los nombres de redes incluidos en los probe-requests). Implementarlo contra dispositivos de personas allegadas (con su consentimiento), y analizar el tráfico que generan los dispositivos en distintos momentos (cuando está en stand-by, cuando esta usándose alguna aplicación en particular). Detectar aplicaciones que hacen mal uso de la red (información sensible en tráfico no cifrado, reintentos muy frecuentes, alto consumo de ancho de banda) o que, por ejemplo, envían datos de los usuarios sin cifrarlos (de ser posible, probar el tráfico que se genera cuando se instala una aplicación). Usar un sniffer y un IDS de red para analizar el tráfico que pasa por el AP, para detectar cosas fuera de lo habitual y desarrollar alguna herramienta propia que detecte singularidades en el tráfico. Intentar analizar el tráfico generado por otros dispositivos con conexión inalámbrica, como por ejemplo smart-tvs.

Investigar y probar los mecanismos de MITM para inyectar código malicioso, o para atacar sitios que usen http y https en forma mixta (ya sea mediante el Rogue AP o, por ejemplo, haciendo spoofing utilizando bettercap). De ser posible, desarrollar algún plugin para bettercap.

Libro de referencia: Hacking Exposed wireless, 3rd. Edition.

TP DE INVESTIGACIÓN

Entregables TP de investigación

Resumen de 1 o 2 carillas que incluya documentación investigada por mail hasta el 5/11**. Son muy importantes las referencias académicas.**
Una presentación con transparencias e informe preliminar para el 29/11.
Un informe al final de cuatrimestre (fecha limite 11/12) de por lo menos 22 carillas, en letra arial 10, espaciado simple.

TP4 – Seguridad en IoT

Hacer un reporte sobre seguridad en la relación a los dispositivos identificados con el concepto de internet de las cosas. Tener en cuenta cuestiones de seguridad física, jtag y uart, chain supply. Investigar y probar como analizar el firmware de varios dispositivos, para buscar vulnerabilidades (como por ejemplo passwords hardcodeadas, o fallas en el código de la interface web del dispositivo). Mecanismos de upgrade seguro de Firmware. Firmware malicioso. Ataques a los mecanismos de comunicación con los dispositivos, y su administración y uso a través de internet. Ataques famosos que utilizaron dispositivos IoT. Investigar acerca de dispositivos a la venta en Argentina.

Algunas Referencias

https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

https://github.com/devttys0/binwalk