

Trabajos Prácticos – Seguridad de la información – dc.uba.ar – 1er cuat. 2015

Importante: En la última semana de clases deben sí o sí presentar lo que tengan hecho hasta el momento. De no ser aprobado el TP en dicha instancia, deben recuperarlo a más tardar el 19 de julio de 2015, que es la fecha definitiva de entrega del TP.

Entregables Tp de Implementación

Resumen de 1 o 2 carillas que incluya actividades realizadas, herramientas utilizadas, librerías, material consultado, a entregar por mail hasta el 31/5.

Una presentación con transparencias y demo en vivo a dar la última semana de clases.

Un informe al final de cuatrimestre (fecha límite 19/7) 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 - Desarrollo de malware para android.

Se deben desarrollar por lo menos dos aplicaciones maliciosas para android. Se asume que la aplicación la instala el dueño del dispositivo, y acepta los permisos que la aplicación le solicita. Se debe poner una “fachada”, en por lo menos una de ellas, para que el usuario “desee” instalar la aplicación. Se recomienda utilizar una aplicación pre-existente como fachada, por ejemplo extraída de <https://f-droid.org/>

Alguna de las dos aplicaciones debe iniciarse sola ante algún evento (por ejemplo, reinicio del teléfono).

LOS DOS GRUPOS QUE HACEN EL TP TIENEN QUE HABLAR ENTRE SI PARA NO IMPLEMENTAR LOS MISMOS ATAQUES, SOLO UNO SE PUEDE REPETIR.

Cada una de las dos aplicaciones debe implementar por lo menos uno de los siguientes “ataques”

- obtener, con los mínimos permisos necesarios, una copia de todas las imágenes que se encuentran en la memoria SD del dispositivo, y enviarlas a un sitio web controlado por el atacante, teniendo en cuenta que sea lo más “stealth” posible.
- Comportarse como un remote access tool (rat), es decir, poder ser administrado en forma remota por el atacante, opcionalmente ofuscando la comunicación, y poder realizar algunas de las siguientes acciones (se puede buscar el código fuente androrat para tener algunos ejemplos, pero no vale copiar el código, y además no es muy legible)
 - Obtener contactos (y toda su información)
 - Obtener el registro de llamadas
 - Obtener los mensajes
 - Ubicación del GPS/RED
 - Tomar una foto con la cámara, en forma subrepticia.

- Capturar el audio con el micrófono
- Enviar mensajes de texto
- Abrir una URL en el browser
- Hacer que el teléfono vibre.
- Descargar un binario dinámicamente y ejecutarlo.
- Poder hacer un seguimiento de adonde se encuentra el dueño del dispositivo móvil, en base a la ubicación del mismo. Llevar un historial.
- Funcionar como keylogger, es decir, capturar la información que tipea el usuario en el teclado virtual de su dispositivo, y enviarlo a algún sitio web remoto, en forma periódica.
- Poder sacar fotografías en forma subrepticia, cuando se cumpla algún conjunto de condiciones (por ejemplo, una foto cada 10 minutos, en determinado horario, si se encuentra en alguna ubicación en particular).

Libro de referencia: Xuxian Jiang, Yajin Zhou, Android Malware, SPRINGER BRIEFS IN COMPUTER SCIENCE

TP 2 – Análisis de tráfico en redes wireless

Implementar un wireless IDS para detectar ataques a redes 802.11, y rogue access point. Describir el funcionamiento y ver como reacciona ante los ataques de crackeo de claves que, por ejemplo, usan deautenticación de clientes.

Investigar la temática de probe-requests como forma de identificar un dispositivo, y ver donde se utiliza habitualmente.

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 (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 para inyectar código malicioso, o para atacar sitios que usen http y https en forma mixta.

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