Trabajos Prácticos – Seguridad de la información – dc.uba.ar
Primer cuatrimestre 2019

Importante: El 30/5 deben presentar por mail un resumen de 1 o 2 carillas con los avances al momento. El 3/7 deben sí o sí mostrar lo que tengan hecho hasta el momento, dando una clase de 20 minutos con transparencias al resto de sus compañeros. La fecha definitiva de entrega del TP es el 21 de julio de 2019, por correo electrónico.

TP 1 – Epignosi

Se debe desarrollar una aplicación para android llama Epignosi. Se asume que la aplicación es instalada por el dueño del dispositivo, y este acepta los permisos que la aplicación le solicita. La aplicación debe ser una aplicación educativa y de concientización, mostrando a los usuarios, con datos reales del dispositivo, qué se puede hacer con los permisos que le dieron a una aplicación (ver la ubicación del usuario aunque la aplicación no esté en primer plano, tomar información de los contactos, hacer uso indiscriminado de internet, manipular sms, tomar fotos en forma subrepticia, exfiltrar archivos, etc.). La aplicación debe ser compatible con la API de Android 7. Incluir en el informe un breve resumen de cómo ha ido cambiando el modelo de permisos de este sistema operativo.

TP 2 – Exafriste

Desarrollar una aplicación maliciosa para windows, Exafriste, que obtenga información de la sesión del usuario logueado y la exfiltre a internet (ya sea vía web, telegram, u otro mecanismo).

Se debe obtener información que pueda luego ser utilizada para hacer un ataque posterior, por ejemplo, de spear phishing, o directamente poder utilizar las credenciales robadas.

Entre la información a extraer, se debe tener en cuenta especialmente la información del perfil de los navegadores (cual/es están en uso, historial de acceso, bookmarks. De ser posible extraer credenciales sin cifrar o exfiltrar el archivo cifrado e intentar descrifrarlo offline). Tener en cuenta que varios de estos datos están en bases de datos en formato sqlite.

También se debe tener en cuenta software instalado, e información relevante del mismo (cuentas de usuario configuradas, contraseñas de software de IM, correo electrónico, etc).

Se puede programar en powershell. Se recomienda tener en cuenta la funcionalidad de herramientas de terceros existentes, como por ejemplo aquellas que figuran en https://www.nirsoft.net/ o las incluidas con caine https://www.caine-live.net/

La aplicación debe tener una estructura modular, para poder incorporar chequeos fácilmente en etapas posteriores.

De ser posible, implementar algún mecanismo propio de ofuscación de la aplicación, para dificultar su detección/análisis.

Entregables Tps de Implementación (Epignosi y Exafriste)

Un informe de por lo menos 12 carillas, en letra arial 10, espaciado simple, contando lo que hicieron (el informe no incluye el código fuente). Incluir como probar las aplicaciones desarrolladas.
Entregar el código fuente y los binarios, si corresponde.

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 propios y de personas allegadas (con su consentimiento), y analizar el tráfico que generan los dispositivos en distintos momentos (cuando está en stand-by, cuando está

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 ejecuta una aplicación por primera vez, luego de instalarla). Usar un sniffer y un IDS de red para analizar el tráfico que pasa por el AP, para detectar cosas fuera de lo habitual. Analizar el tráfico generado por otros dispositivos con conexión inalámbrica, como por ejemplo smart-tvs. Hacer un análisis exhaustivo de las consultas de DNS que realizan los dispositivos e intentar identificar qué servicios están relacionados con dichas consultas. En todos los casos, más allá de la prueba con el Rogue AP, se puede levantar un Access Point por software y configurar los dispositivos para que lo usen.

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).

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

Entregables Tp3

Un informe de por lo menos 24 carillas, en letra arial 10, espaciado simple, detallando las pruebas realizadas, y los hallazgos.