PEC1 - Parte 2

Tutorial 1 - Changing your column display

Problemas encontrados

No se han encontrado problemas durante la realización de la practica

Lecciones aprendidas

No era consciente de la posibilidad de ocultar columnas y de eliminar columnas. De forma que un usuario puede tener columnas útiles ocultas para posteriormente activarlas para revelar la información. El flujo de trabajo se vuelve mas sencillo con la posibilidad de ocultar columnas debido que el analista no tiene que filtrar tanta información innecesaria.

Tutorial 2 - Identifying hosts and users

Problemas encontrados

Durante el Tutorial, se indica que se abra el contenido del bloque nombrado: "Bootstrap Protocol (Request)" pero en esta versión de wireshark, el contenido de esa sección esta situado directamente dentro de la sección "Dynamic Host Configuration Protocol (Request)" Para solventar el problema, se ha abierto dicha sección y se ha procedido con el Tutorial.

Otro problema que me he encontrado, en la sección "Host Information from NBNS Traffic", es que no entendía exactamente que estaba observando. Entiendo ahora que el cliente 10.2.4.101 esta haciendo preguntas al router para registrarse en la red, como MARTIN-WIN-PC (Reiteradas veces, porque el router no responde (Por eso también emite el paquete a 10.2.4.255)) y posteriormente averiguar la dirección de WPAD.

Lecciones aprendidas

En general, todo el funcionamiento del protocolo NBNS, ya que no era consciente de su uso ni finalidad. Ademas, entiendo que se puede usar para establecer una correlación entre la MAC y la IP de varios dispositivos que usen Windows o MacOS de la red.

En la sección de análisis del "user-agent", he aprendido los distintos campos que pueden venir en el user-agent.

Es muy importante, como en cualquier tarea de análisis saber exactamente lo que uno busca. Ademas, las herramientas como el buscador y filtro de Wireshark facilitan mucho la tarea del filtrado debido a su potente lenguaje de filtrado.

Tutorial 3 - Display filter expressions

Problemas encontrados

No se han encontrado problemas durante la realización de la practica

Lecciones aprendidas

Saber que el protocolo SSDP se usa para descubrir dispositivos PnP y que no se usa de forma normal en el trafico de web, por tanto, no debería ser incluido en el filtrado. Por este motivo, se debe eliminar del filtrado usando la notación !(SSDP)

Seguir un flujo, aunque se usen diferentes protocolos. Viendo la captura que se nos ofrece para que analicemos, si seguimos el flujo, como indica el Tutorial, podemos observar que se solicita la dirección IP del servidor FTP C&C. Desde aquí, debemos ser capaces de intuir que va a existir una comunicación por FTP entre el servidor C&C y nuestro ordenador infectado. Si seguimos nuestra intuición, podemos llegar a averiguar que archivo se sube al servidor.

Entender que para saber buscar el trafico especifico, debemos poder intuir que tipo de malware estamos buscando, o aproximadamente que protocolos puede usar o no.

La capacidad de guardar filtros, para no tener que volverlos a escribir cada vez que se quieran usar. De esta forma, podemos construir filtros sobre los actuales, para acabar con filtros potentes, dependiendo de que es lo que queramos encontrar o comprobar.

Tutorial 4 - Exporting objects from a pcap

Problemas encontrados

No se han encontrado problemas durante la realización de la practica

Lecciones aprendidas

Saber que aunque se registra el contenido que pasa por la red, ademas, se guarda el contenido que pasa por ella. La noción de que se puede descargar el documento que ha pasado por la red en un momento determinado es muy importante. De esta forma, podemos recuperar archivos que puede que ya no existan en nuestro sistema si no llega a ser por Wireshark. Cuando un sistema esta infectado por un virus, hacer esto puede ayudarnos a detectar el tipo de virus y como funciona.

No sabia que el trafico SMTP se podía guardar en formato IMF

Guardar trafico de red en formato RAW, proporciona mucha flexibilidad.