PEC1 - Parte 3

Metodología ejercicio 1

1. Enumerar dispositivos presentes en la captura
2. Averiguar su rol y descartar equipos no relevantes
3. Analizar trafico HTTP entre el resto de dispositivos
4. Ahondar en la opción mas probable
5. Expandir a partir de esta nueva información, distintos ordenadores que han estado en comunicación.
6. Averiguar, en la medida de lo posible, mediante distintos tipos de trafico, el nombre del usuario, nombre del equipo.

Metodología ejercicio 2

En general, en este ejercicio he seguido un enfoque mas general al inicio (Analizando los archivos contenidos en el `.zip`) pero mucho mas dirigido a continuación, gracias a los datos recopilados en el análisis inicial.

Los pasos que se han seguido en este ejercicio han sido:

1. Analizar los archivos adjuntos en el `.zip`
   - En este paso, he visto que se trata del Keylogger HawkEye.
   - Ademas, tenemos una hora a la que se ha detectado.
   - También, tenemos el tipo de protocolo que usa el Malware, FTP
2. Analizar el archivo `.pcap` con Wireshark de forma general, con los filtros `Basic` y `Basic+`.
   - Estos filtros no han revelado demasiada información relevante
3. Usar el filtro `kerberos` y añadir una columna para el `CNameString`
   - En este paso, se ha detectado el nombre de usuario del ordenador, ademas del nombre del ordenador.
4. Analizar el trafico `FTP` con el filtro `ftp`
   - Vemos de forma clara que el trafico `ftp` incluye tanto texto conteniendo las credenciales del usuario del equipo como capturas de pantalla
5. Filtramos de nuevo con `ftp-data` para poder obtener los archivos enviados a través de la red

Los hash de los archivos descargados están incluidos en el documento `parte2/tablas.pdf`