PRÁCTICA 6: ARRANQUE DE HERRAMIENTAS FORENSES DESDE LA RED (PXE).

PXE (Preboot eXecution Environment) es un entorno de ejecución antes del arranque para la propia tarjeta de red. Casi todas las tarjetas de red contienen un chip (memoria ROM) donde se encuentra este sistema de arranque y que permite a la tarjeta de red arrancar el sistema informático sin necesidad de cargar un SO.

Normalmente se utilizan los servidores PXE para poder instalar y/o ejecutar sistemas operativos mediante la red sin necesidad de depender de memorias USB ni de tampoco de DVDs. Además otra gran ventaja que el booteo por red nos ofrece, es la posibilidad de poder instalar sistemas operativos (Windows, Linux, etc.) cuando los equipos no disponen de lectores de CD/DVD o estén dañados.

Durante nuestra práctica laboral como peritos forense informático nos podemos enfrentar a multitud de situaciones que pondrán a prueba tanto nuestros conocimientos como las herramientas de que disponemos. Por ejemplo, puede ser interesante la posibilidad de ejecutar sistemas operativos LIVE sin depender de memorias USB dado que existen miles de herramientas (distribuciones Linux, herramientas forenses y/o entornos de rescate) y difícilmente podremos llevarlas todas en unos cuantos pendrives.

NOCIONES BÁSICAS SOBRE PXE

La especificación del Preeboot eXecution Environment (PXE) describe un entorno cliente-servidor estandarizado que inicia un conjunto de software, principalmente una imagen de un sistema operativo, obtenido de una red. En el lado del cliente solo se requiere un controlador de interfaz de red (Network Interface Controller, NIC) compatible con PXE, y un pequeño conjunto de protocolos de red, como DHCP y TFTP

Los orígenes de protocolo PXE se remontan a los primeros dıas de los protocolos BOOTP/DHCP/TFTP y, debido a su gran utilidad, a partir de 2015, forma parte del estándar Unified Extensible Firmware Interface (UEFI), por lo que lo hace el estándar de facto en la industria. En los centros de datos modernos y otros grandes sistemas en red, PXE es la opción más frecuente para el inicio, la instalación y la implementación del sistema operativo.

El entorno PXE se basa en una combinación de protocolos de Internet estándar de la industria, a saber, UDP/IP, DHCP y TFTP. Estos protocolos se seleccionaron porque se implementan fácilmente en el firmware de la NIC del cliente, lo que da como resultado ROMs PXE estandarizadas de tamaño reducido. La estandarización, el pequeño tamaño de las imágenes de firmware de PXE y su bajo uso de recursos han favorecido que el lado del cliente del estándar PXE se implemente de forma idéntica en una amplia variedad de sistemas, desde potentes computadoras cliente a máquinas de una sola placa e incluso dispositivos “System on Chip“. Como se ha mencionado anteriormente, PXE hace uso de los protocolos DHCP y TFTP cuyas funciones son:

- DHCP se usa para proporcionar los parámetros de red del cliente apropiados y específicamente la ubicación (dirección IP) del servidor TFTP, donde se encuentra disponible el Network Bootstrap Program (NBP) y otros ficheros complementarios.
- Una vez configuradas las propiedades de red, el cliente puede acceder a los ficheros de arranque del servidor TFTP, ya que conoce su dirección y el nombre del fichero de arranque. A continuación, el cliente lo transfiere a su propia memoria RAM, verifica que es un fichero de arranque válido, y finalmente lo ejecuta. Estos ficheros de arranque contienen una lista con un pequeño conjunto de

ficheros complementarios para ejecutar un SO minimalista (WindowsPE, un núcleo de Linux básico + initrd, etc). Esta instancia del sistema operativo carga sus propios controladores de red y la pila TCP/IP. En este punto, las instrucciones restantes necesarias para iniciar o instalar un sistema operativo completo no se proporcionan a través de TFTP, sino que utilizan un protocolo de transferencia robusto (como HTTP, CIFS o NFS) y ya no es gestionada por PXE, si no por el propio sistema operativo, y dependiendo del que se escoja, empleará una implementación diferente.

Objetivos principales de la práctica:

- **Instalación y configuración del entorno de arranque por red PXE en un ordenador que hará las veces de estación de trabajo forense.**

Se pide:

- Crear una máquina virtual: por ejemplo una distribución Debian con 2GB de RAM y 10 GB de disco duro que actuará como estación de trabajo forense.
- Investiga en Internet sobre los ficheros y servicios relacionados con PXE:
  - Ficheros de arranque y configuración (“pxelinux.0”, “pxelinux.cfg”, “ipxe”, etc).
  - DHCP
  - TFTP
  - DNSmasq
- Instalar en la máquina virtual los servicios necesarios para poner en funcionamiento el arranque con PXE.
- Configurar una distribución de análisis forense (CAINE o KALI) para que arranque desde la red.
- Documenta todo el proceso anterior.