**Footprinting**

Es la técnica utilizada para recopilar información sobre los sistemas informáticos y las entidades a las que pertenecen. Para obtener esta información, un hacker podría usar varias herramientas y tecnologías. Esta información es muy útil para un hacker que está tratando de descifrar un sistema completo. Esta recogida de información últimamente se conoce como OSINT.

**Tipo de información que se recolecta:**

* Nombre de dominio
* Bloques de red
* Dirección IP (especifica de un dispositivo)
* Arquitectura de un sistema
* Servicios activos
* Información DNS
* Sistema operativo utilizado
* Dispositivos de seguridad
* Trafico
* Extra-nets, puntos de conexión e información pública o privada
* Números de teléfono
* Sistema operativo de la máquina de destino
* Cortafuegos
* Mapa de red
* Configuraciones de seguridad de la máquina de destino
* Identificación de correo electrónico, contraseña
* Configuraciones de servidor URLs
* VPN

**Huella digital (fingerprint)**

A la información que se utiliza para identificarte y rastrearte en línea se le conoce como huella digital del dispositivo o navegador.

La huella digital del navegador puede reflejar:

* Comienzo de conexión
* Inicio de codificación
* Encabezado de idioma
* Lista de complementos
* Plataforma
* Preferencias de cookies (permitidas o no)
* Preferencias de No rastrear (si, no o no comunicado)
* Zona horaria
* Resolución de pantalla y su profundidad de color
* Uso del almacenamiento local
* Uso del almacenamiento

Es una técnica que consiste en recolectar información directamente de los sistemas informáticos de una persona o empresa para conocer más sobre su comportamiento y configuración.

Lista de este tipo de actividades que ponen en riesgo tu ciberseguridad y la de tu organización:

* Ransomware
* Malware
* Ataque botnet
* Estafa de inversión
* Estafa de la factura falsa
* Vishing
* Smishing
* Fraude del CEO

Hay dos tipos de fingerprinting que podemos utilizar:

El fingerprinting activo es el tipo de huella digital más popular. Consiste en enviar paquetes a una víctima y esperar la respuesta de la víctima para analizar los resultados.

El fingerprinting pasivo es un enfoque alternativo para evitar la detección mientras realiza sus actividades de reconocimiento.

En el contexto de fingerprinting, existen 4 tipos importantes:

* Fingerprint de usuario
* Fingerprint de dispositivo
* Fingerprint web
* Fingerprint de vulnerabilidad

Técnicas de fingerprinting

* Cookies: mejorar la experiencia mediante perfilación
* Canvas/Font: rastrear en línea y a lo largo del tiempo
* webRTC: identificar dispositivo mediante IP
* AUDIO CONTEXT: particularizar dispositivos por pequeñas diferencias
* Sniffing: escuchar lo que ocurre en la red
* Wireshark: obtener datos sobre el tráfico de red
* Ettercap: detectar redes y sistemas operativos
* Messus: detectar vulnerabilidades

Modificaciones y ajustes del navegador fingerprint

**Código malicioso (malware)**

Malware, acrónimo para el inglés “Malicious software” (software malicioso), es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar o comprometer un sistema.

**Tipos de malware**

* Ransomware
* Spyware
* Troyanos
* Adware
* Gusanos
* Botnet

Su clasificación dependerá del vector de ataque y su funcionalidad.

El vector de ataque es el método que utiliza el software para propagarse o infectar a los programas.

El malware puede tomar forma de un ejecutable, código o cualquier otro software.

**Objetivo:**

Entender el funcionamiento del código dañino, como detectarlo y eliminarlo.

Esto implica analizar el archivo binario sospechoso en un ambiente seguro para identificar sus características y funcionalidades y así mejorar las defensas de la organización.

La meta es determinar la capacidad del malware, su detección y contenerlo. también ayuda a determinar patrones identificables que pueden ser utilizados para eliminar y prevenir otras infecciones.

Determinar la naturaleza y propósito del malware: determinar si el malware roba información, es un bot HTTP, un bot de spam, un rootkit, un keylogger o un RAT.

para entender como el sistema se comprometió y su impacto.

Para identificar aspectos de red asociados al malware, el cual puede ser usado para detectar infecciones similares usando el monitoreo de red.

Para extraer indicadores basados en host como nombres de archivos y llaves de registro las cuales pueden ser usadas para determinar infección similar usando monitoreo basado en host.

Un malware crea una llave de registro, que se puede usar como un indicador para crear una forma o escanear la red para identificar los hosts que tienen la misma llave de registro.

**Tipos de análisis código malicioso (malware)**

* **Análisis estático de malware:** analizar un archivo sospechoso sin ejecutarlo.
* **Análisis dinámico de malware:** este es el proceso de ejecutar el binario sospechoso en un entorno aislado y monitorear su comportamiento.

**Análisis estático (malware)**

Implica:

* Extracción de información útil del archivo sospechoso.
* Decisión informada de como clasificarlo.
* Donde enfocar los siguientes esfuerzos de análisis.

**Técnicas (malware)**

Estas técnicas pueden revelar información diferente sobre el archivo. No es necesario seguir todas estas técnicas, y no es necesario seguirla en el orden presentado. La elección de las técnicas a utilizar depende de su objetivo y del contexto que rodea el archivo sospechoso.

Identificar la arquitectura objetivo del malware

Huellas digitales del malware

Escanear el binario sospechoso con motores antivirus

Extraer cadenas, funciones y metadatos asociados con el archivo

Identificar las técnicas de ofuscación utilizadas para frustrar el análisis

Clasificar y comparar las muestras de malware

**Determinar el tipo de archivo**

Determinar el tipo de archivo ayudara a identificar el sistema operativo del malware (Windows, Linux, etc.) y la arquitectura (plataformas de 32 bits o 64 bits).

La mayoría de los programas maliciosos basados en Windows son archivos ejecutables que terminan con extensiones como .exe, .dll, .sys…

<http://www.filesignatures.net/>

**Identificación del tipo de archivo con el método manual**

el método manual para determinar el tipo de archivo abriéndola en un editor hexadecimal.

El otro método conveniente para determinar el tipo de archivo es usar herramientas de identificación de archivos.

En sistemas Linux, esto se puede lograr usando la utilidad de file.

En Windows, **CFF Explorer,** parte de explorer suite (), puede usarse para determinar el tipo de archivo.

**Determinación del tipo de archivo con Python**

**Análisis antivirus**

**Extraer cadenas**

Las cadenas son secuencias de caracteres imprimibles en ASCII y Unicode incrustadas dentro de un archivo.

Extraer cadenas puede dar pistas sobre la funcionalidad del programa y los indicadores asociados con un binario sospechoso.

Por ejemplo, si un malware crea un archivo, el nombre del archivo se almacena como una cadena en el binario.

O, si un malware resuelve un nombre de dominio controlado por el atacante, el nombre de dominio.

**Técnicas de ofuscación**

**Packers**

* Programas que utilizan técnicas de comprensión para ocultar el contenido del ejecutable.
* El resultado es un nuevo ejecutable que se auto descomprime al ser ejecutado.
* Herramientas UPX.

**Cryptors**

* Similar al packet, pero utiliza encriptación en lugar de compresión.
* Se desencripta al ser ejecutado.

**Inspección de la información del encabezado de PE**

Los ejecutables de Windows deben cumplir con el PE/COFF

Los archivos ejecutables de Windows utilizan el formato de archivo PE (como .exe, .dll, .sys, .ocx y .drv) y estos archivos generalmente se denominan archivos ejecutables portátiles (PE).

**Análisis dinámico (malware)**

**Análisis de comportamiento**

Este es el proceso de ejecutar el binario sospechoso en un entorno aislado y monitorear su comportamiento.

Esta técnica de análisis es fácil de realizar y proporciona información valiosa sobre la actividad del binario durante su ejecución.

Esta técnica de análisis es útil pero no revela todas las funcionalidades del programa hostil.

**Implica:**

* Analizar una muestra ejecutándose en un entorno aislado y monitoreando sus actividades, interacción y efecto en un sistema.
* Herramientas de análisis dinámico y sus características.
* Simulación de servicios de internet
* Pasos involucrados en el análisis dinámico
* Monitorear la actividad del malware y comprender su comportamiento

**Monitoreo de sistema y la red**

Cuando se ejecuta un malware, puede interactuar con un sistema de varias maneras y realizar diferentes actividades. Monitorear la interacción de un malware con el sistema y la red ayudara a comprender la naturaleza y el propósito del malware.

Monitoreo:

**Monitoreo del sistema de archivos:** incluye el monitoreo de la actividad del sistema de archivos en tiempo real durante la ejecución del malware.

**Monitoreo del registro:** implica el monitoreo de las claves de registro accedidas / modificadas y los datos de registro que están siendo leídos / escritos por el binario malicioso.

**Monitoreo de red:** implica monitorear el tráfico en vivo hacia y desde el sistema durante la ejecución del malware.

Las actividades de monitoreo explicadas ayudaran a recopilar información de host y red relacionada con el comportamiento del malware.

**Otras herramientas**

Determinación de la interacción del sistema de monitoreo del sistema

Process/Monitor

En lugar de usar el administrador de tareas, con esta herramienta filtramos de una manera más fácil como esta interactuando el malware.

Permite concentrarse en eventos que son propios del malware, es un simple script hecho em Python que trabaja junto con process monitor, se ejecuta y genera un .txt con toda la información del malware, con eventos categorizados, archivo, registro y actividad de la red

Wireshark

Captura el tráfico generado por el malware, así como los servicios que ocupa y su comportamiento dentro de la red.

iNetSim

Se simulan servicios sin darle acceso a internet y desde ahí se puede ver toda su información, permite crear configuraciones y devuelve cualquier archivo con las extensiones que solicito el malware, funciona con protocolos http y https.

**Pasos del análisis dinámico**

1. Tenerlo en un entorno controlado, en una caja de arena o máquina virtual
2. Hacer la descarga de las herramientas y el malware
3. Comenzar a ejecutar con o sin privilegios las herramientas y el malware
4. Comenzar a ejecutar las herramientas para poder ver la interacción del malware
5. Por último, observar el comportamiento del malware y comparar los resultados con el objetivo que se tenía.

Poniendo todo junto: analizando un ejecutable de malware

**Análisis de código (malware)**

Es una técnica avanzada que se utiliza para comprender el comportamiento interno del binario.

**Análisis de memoria (malware)**

Es cuando se comienza el análisis por la memoria RAM, analizar los malwares que se han ejecutado.

**KEYLOGGERS**

Un keylogger puede ser un programa o un dispositivo de hardware que captura tolas las pulsaciones del teclado.

Puede capturar pantallas, sonidos e incluso video del usuario.

Se puede usar con fines maliciosos, pero también como control.

**Hardaware**

Pueden ser implementadas vía al firmware del:

BIOS de la computadora

Un keylogger de hardware incluye:

* Microcontrolador
* Utilizando memoria volátil

**Keylogger hardware**

Se pueden usar con teclados falsos como en el caso de cajeros automáticos, que captura pulsaciones, palabras y combinaciones de teclas que se usaran con fines maliciosos.

**Keylogger software**

Programa que se puede encontrar en un archivo .exe que al ejecutarlo comenzara a actuar, cuando está basado en el kernel intercepta las teclas que vamos pulsando, pero no puede ser descubierto fácilmente.

Las basadas en API van registrando los eventos del teclado y se aloja en las API del teclado como un medio de falsificación.

Basados en un script malicioso, se puede inyectar a una página web que estará escuchando los movimientos del teclado, puede comprometer el sitio remoto.

Otros están más asociados al sistema, como tablas de memoria.

Los que están conectados a un servidor enviando información de manera periódica a un sitio, correo electrónico para la recolección de información.

**Escaneo de servicios de red UDP**

**Escaneo de encabezado IDLE/IPID**

El escaneo de encabezado de IDLE / IPID funciona enviando una dirección de origen falsificada al destino

**Suplantación de identidad (spoofing)**

Es cuando un atacante o programa malicioso se hace pasar por otra persona o programa.

**Categorías de suplantación de identidad**

**Correo electrónico falsificado:** los correos electrónicos un virus informático se envían desde direcciones de correo electrónico diferentes con el fin de engañar al mejor destinatario.

**Spoofing de DN:** conocido como envenenamiento de cache, en este método se trata de introducir datos DNS corruptos en la terminal de usuario y por lo tanto impedirles que accedan a las paginas web que quieren visitar.

**Spoofing de datos:** el spoofing de DDoS es un subtipo de spoofing de IP que usan los hackers para llevar a cabo ataques de denegación de servicio distribuido contra ordenadores, redes y páginas web.

**Spoofing de ARP:** los hackers optan por el spoofing de ARP para interceptar los datos sensibles antes de que lleguen al ordenador objetivo.

**Escucha en la red (Sniffing)**

Se refiere al proceso de obtener información adicional y realizar un reconocimiento más detallado basado en la información recopilada en fase de fingerprinting.

En esta fase, se utilizan varios procedimientos diferentes con el objetivo de identificar hosts, puertos y servicios en la red de destino. Todo el propósito es identificar vulnerabilidades en canales de comunicación y luego crear un plan de pruebas.