Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

PING

Podemos comprobar si hay conexión con un equipo específico. También podremos medir el tiempo que tardan dos nodos en comunicarse.
Este comando también lo podemos usar dentro de un bash.

ping [opciones] [destinatario]

ping 192.168.1.131

Opciones:

-c: Con esta opción, puede especificar cuantos paquetes enviar.
-s: Esta opción le permite cambiar el tamaño por defecto de los paquetes.
-w: Especifica un tiempo en segundos en el que la ejecución del comando terminara. Sin importar cuantos paquetes el comando haya enviado o recibido.

ping –c4 –s233 192.168.1.131

Tracer / traceroute

Determina la ruta a un destino y su latencia, es decir, lo que tarda en cada salto y los saltos que tiene que dar. Primero se manda un paquete de datos con un TTL (periodo de vida). Por cada router que pasa disminuye este TTL del paquete en una unidad antes de reenviar el paquete al siguiente punto. Por eso, gracias al TTL podemos saber la cantidad de «saltos» que ha dado el paquete desde un origen hasta un destino. Sin embargo, cuando el TTL de un paquete llega al valor cero, sin alcanzar su destino final, el router devuelve al equipo de origen un mensaje ICMP de «Tiempo agotado».

Opciones;

-h: Esta opción nos permite especificar el número de saltos máximos que puede realizar el comando Tracert.

Whois

Es un protocolo de consulta y respuesta gracias al cual es posible consultar bases de datos donde se almacenan los usuarios registrados que están en un recurso de Internet

Algunos de los parámetros de uso de whois son:

-h HOST: permite establecer una conexión con el host de la base de datos de WHOIS.

-H: Suprime la visualización de renuncias legales

-p PORT: permite conectarnos al puerto de red PORT.

--verbose: detalles completos

Al usar el comando whois debemos tener en cuenta los siguientes términos:

- Registry: hace referencia a la empresa que administra la lista donde se aloja un conjunto de nombres de dominio
- Registrant: es el propietario legal del dominio
- Registrar: hace uso de un registrador para realizar el registro

theHarvester

The Harvester es una herramienta para la obtención de información en fuentes abiertas. Para ello, utiliza métodos pasivos para, de esta manera, conseguir la información que estamos buscando sin interactuar directamente con el objetivo final (dominio, persona, etc…) a través de los diferentes motores de los principales buscadores y servicios utilizados, o si lo preferimos de forma activa haciendo fuerza bruta, resoluciones inversas, etc…

theHarvester –d gmail –l 500 –b bing

whatweb

Nos da por consola la estructura de la web (mas o menos como waapalyzer)

whatweb –v blacksystem.es

wafw00f

Nos da información de los firewall o demás que tenga esa pagina

wafw00f blacksystem.es

dirb

Nos va a buscar directorios y subdirectorios dentro de una pagina web desde un diccionario por defecto (se podría cambiar)

dirb https:/aytocobeta.com

Footprinting y Fingerprinting = Recolección de información

- Footprinting: es la etapa, primera de un test de intrusión la cual se recolecta información.Su principal fuente es Internet, lo cual se puede encontrar gran cantidad de información.

- Fingerprinting: Esta etapa, consiste en recolectar información directamente del sistema de una organización, para aprender mas sobre su configuración y comportamiento. Esta etapa es aconsejable realizarla en una auditoría autorizada, ya que supuestamente cuyo “atacante” tiene permisos para realizar dicha acción.

Definición:
Es la primera y mas importante fase del Hacking Ético. El atacante o auditor de seguridad tratará de recopilar de forma metodológica toda la información que mas pueda al respecto del objetivo”. Dentro de las características del proceso de recolección de información se encuentran:

- No se realiza ningún tipo de escaneo o contacto con la maquina objetivo.
- Permite Construir un perfil del Objetivo, sin interactuar con él.
- Existen menos herramientas informáticas que en las otras fases.
- Recolección de Información Pública (Ingeniería Social, Google Hacking)

Técnicas usadas

Son muchas las técnicas utilizadas y recursos disponibles para el proceso de recolección de Información. Algunas de ellas son:

•Herramientas de red: Whois, Traceroute, Ping entre otros.

•Información del sitio Web corporativo

• Google Hacking

• Extracción de Metadatos

• Automatización con Plug-in Firefox

• Scripts públicos

• OSINT

• Ingeniería Social

Plugins Firefox y OWASP Mantra

Dentro del Firefox de Kali, le damos a las 3 rayas de arriba a la derecha y pinchamos en Add-ons and Themes,

- buscamos wappalyzer y lo añadimos a nuestro Firefox. Este plugin nos da información de la estructura de la pagina web a auditar (servidor web, lenguaje de programación, versiones, etc)

- IP Address and Domain Information: este plugin nos dará información de ip, whois, localización del servidor, ASN, etc.

- Instalamos Owasp-Mantra en nuestra Kali: desde Kali ponemos sudo apt-get update. Despues

sudo apt-get install owasp-mantra-ff.

Para ejecutarlo ponemos en la terminal owasp-mantra-ff, se abrirá y tenemos que poner arriba la dirección que queremos recolectar información (algunas no abrirán). Bajamos con el raton abajo a la derecha de la pagina y aparecerá un menú oculto le damos a la Pr (passive recon) y nos dará un monton de ventanas con info.

Ejercicio

Recolección de información

1- Haremos una recolección de información de una web. La web será www.nike.es

2- Realizaremos un ping para ver conexiones.

3- Usaremos passive recon para la recolección principal. Toda la información recolectarla en un txt guardada en la carpeta recolección. Lo importante es ver el grado de investigación de datos que conseguís.

4- Hay que conseguir como objetivo principal, el nombre de la persona que tiene patentada la marca.

5- Sacar correos electrónicos de la web que vosotros elijáis.