

Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros (Hacking ético)

Fase de reconocimiento (footprinting)

El footprinting ('reconocimiento') es el proceso de recogida de información en internet sobre algo muy concreto.

Más información

- <https://www.jesusninoc.com/03/16/busybox-the-swiss-army-knife-of-embedded-linux/>
 - <https://www.jesusninoc.com/03/17/crear-una-version-de-linux-con-buildroot-para-el-router-de-fibra-optica-mitrastar-gpt-2541gnac-de-movistar-mips-gnu-linux/>
 - <https://www.jesusninoc.com/03/16/listar-los-ficheros-del-directorio-raiz-en-el-router-de-fibra-optica-mitrastar-gpt-2541gnac-de-movistar-desde-powershell/>
 - <https://www.jesusninoc.com/03/13/ver-la-tabla-de-direcciones-arp-asociadas-a-un-router-de-fibra-optica-mitrastar-de-movistar-con-powershell/>
-

Fase de escaneo (fingerprinting)

Consiste en, mediante la interacción con el sistema objetivo determinar qué puertos hay abiertos y, qué versiones hay en los procesos detrás de dichos puertos. Además, sería interesante determinar también el sistema operativo del sistema a auditar.

Monitorización de tráfico

Un sistema de monitorización de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Ejemplo

- <https://www.jesusninoc.com/03/31/analisis-de-trafico-con-wireshark-arrancar-explorer-exe-en-windows-8-1/>
-

Más información

- <https://www.jesusninoc.com/05/29/introduccion-wireshark/>
 - <https://www.jesusninoc.com/05/01/analisis-de-conexiones-de-red/>
 - <https://www.jesusninoc.com/03/13/microsoft-message-analyzer/>
 - <https://www.jesusninoc.com/04/02/localizar-geograficamente-una-ip/>
-

Interceptación de comunicaciones utilizando distintas técnicas

Consiste en analizar el tráfico transmitido por la red de comunicaciones.

Más información

- <https://www.jesusninoc.com/03/15/analisis-de-conexiones-udp-con-wireshark/>
 - <https://www.jesusninoc.com/04/03/analisis-de-conexiones-tcp-con-wireshark/>
 - <https://www.jesusninoc.com/03/14/analisis-de-imagenes-con-wireshark/>
-

Manipulación e inyección de tráfico

Consiste en modificar el tráfico transmitido por la red de comunicaciones.

Más información

- <https://www.jesusninoc.com/07/20/softperfect-network-protocol-analyzer/>
- <https://www.jesusninoc.com/03/17/analisis-de-conexiones-udp-con-microsoft-message-analyzer/>
- <https://www.jesusninoc.com/03/16/analisis-de-conexiones-udp-con-softperfect-network-protocol-analyzer/>
- <https://www.jesusninoc.com/03/19/modificar-datagramas-udp-con-softperfect-network-protocol-analyzer/>
- <https://www.jesusninoc.com/04/02/modificar-la-direccion->

[ip-de-origen-en-mensajes-udp-con-softperfect-network-protocol-analyzer/](#)

- [https://www.jesusninoc.com/03/31/analisis-de-una-peticion-a-mysql-con-softperfect-network-protocol-analyzer/](#)
 - [https://www.jesusninoc.com/08/07/cat-karat-packet-builder/](#)
 - [https://www.jesusninoc.com/08/09/colasoft-packet-player/](#)
-

Herramientas de búsqueda y explotación de vulnerabilidades

Las vulnerabilidades son fallos de seguridad en aplicaciones informáticas que pueden convertir los sistemas en presa fácil de diversos tipos de software malicioso.

Ingeniería social. Phishing

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos.

Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

Más información

- <https://www.jesusninoc.com/phishing/>
-

Escalada de privilegios

La escalada de privilegios es el acto de explotar un error, un fallo de diseño o una supervisión de la configuración en un sistema operativo o una aplicación de software para obtener un acceso elevado a los recursos que normalmente están protegidos de una aplicación o un usuario.