SYPER 2011 - Práctica 3

Footprinting, scanning, ennumeration, OS fingerprinting

Footprinting

1.¿Qué es "Footprinting"?

2.Dada una organización, averigüe toda lo que pueda usando el DNS: servidores de correo, servidores DNS, Servidores WEB, etc.

3.Mencione, busque e instale herramientas que realicen footprinting. Describa la funcionalidad de las mismas. Compare la relevancia de la información obtenida con cada una.

4.Visite el sitio http://www.netcraft.net/ y pruebe la funcionalidad del mismo contra el dominio microsoft.com. ¿Que información valiosa de descubrimiento obtuvo?

5.Visite el sitio http://www.archive.org/web/web.php y pruebe la funcionalidad del mismo contra el sitio web de la UNLP: www.unlp.edu.ar. ¿Qué ventajas presenta esta herramienta respecto de otras herramientas de footprinting? ¿De que fecha data la página más antigua a la que puede acceder?

Scanning de puertos

6.¿Qué es "Port Scan" o "Escaneo de puertos"? ¿Cuál es su objetivo?

7.Mencione y explique brevemente las diferentes técnicas de escaneo que existen. Utilice nmap para realizar escaneos utilizando diferentes técnicas. Nota: para ver como usar nmap con las diferentes técnicas, ver http://nmap.org/book/man-port-scanning-techniques.html

8.Utilizando el LiveCD provisto por la cátedra, abra una terminal de root y realice un escaneo de puertos utilizando nmap a la IP local.

- **nmap 127.0.0.1**

Compruebe si los puertos detectados son los mismos que están corriendo en la máquina, los cuales puede consultar con el comando:

- **netstat -nlutp4**

¿Qué diferencias en cuanto a puertos y protocolos encuentra?
Determine la/s forma/s de utilizar nmap para obtener toda la información brindada por el comando **"netstat -nltup4"**

9.Abra una terminal de root en el LiveCD y utilice el comando **hping3** para escanear puerto de la siguiente manera, al mismo tiempo que utiliza en otra terminal de root el comando "**tcpdump -i lo -n**" para observar los paquetes involucrados.

- hping3 -c 3 -S -p 80 localhost
  - ¿Qué significa la respuesta?

    - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

- hping3 -c 3 -S -p 113 localhost
    - ¿Qué significa la respuesta?
    - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

- hping3 -c 3 -2 127.0.0.1 -p 631
    - ¿Qué significa la respuesta?
    - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

- hping3 -c 3 -2 127.0.0.1 -p 6
    - ¿Qué significa la respuesta?
    - Observando la salida de tcpdump, ¿Qué método de escaneo de puertos se está simulando en este caso?

10.Suponiendo que el IPID de los paquetes que envía el "host A" es predecible. ¿Desde la "host X" como se podría utilizar el comando **hping3** para realizar un idle scan del puerto 23 del "host S"?
    - Especifique los comando de **hping3** necesarios para realizar el scan

11.¿Es posible detectar un escaneo de puertos? Piense en distintas alternativas que pueden resultar viables en la detección del mismo.

Scanning de vulnerabilidades

12.¿Qué es un "Escaneo de vulnerabilidades"? ¿Cuál es su objetivo?

13.Mencione, busque e instale herramientas que realicen escaneo de vulnerabilidades (sobre la plataforma que usted elija). Describa la funcionalidad de las mismas. Compare. ¿Cuál elegiría? ¿Qué diferencias presentan este tipo de herramientas con las que realizan "Escaneo de puertos"?.

Fingerprinting

OS Fingerprinting
14.¿Qué es OS Fingerprinting? ¿Cómo funciona?

15. Nmap es una herramienta que además de permitir escanear puertos, implementa diversas tecnicas de OS Fingerprinting: http://nmap.org/book/osdetect.html. Utilice nmap para detectar la version de distintos sistemas operativos. ¿Fue correcto el resultado alcanzado por la herramienta? Intente realizar las pruebas contra distintos sistemas operativos.

Service Fingerprinting
16.¿Qué es fingerprinting de servicios? ¿Funciona igual que el OS fingerprint?

17.Haciendo fingerprinting de servidores HTTP en forma manual. Usando telnet o netcat realice las siguientes pruebas:

- HEAD
- GET / HTTP/1.0
- GET /algo_que_no_existe HTTP/1.0

Contra los siguientes sitios:

- www.google.com.ar → <**telnet www.google.com.ar 80**>
- www.microsoft.com.ar
- www.microsoft.com
- lihuen.linti.unlp.edu.ar
- www.biol.unlp.edu.ar

¿En base a la información que cada servidor dio a los distintos requerimientos. Puede identificar ¿que productos que se están usando como servidor web?¿Puede determinar la versión utilizada?

18.En base a la información brindada en http://www.net-square.com/httprint/httprint_paper.html. Como puede realizarse fingerprint de un servicio HTTP cuando el banner grabbing no es posible?

Enumeración

19.¿Qué es enumeración?

20.Busque, instale y pruebe herramientas de enumeración de: Netbios, SNMP, Cuentas de usuario, DNS, Servicios de directorio, etc.

21.¿Qué es "Google hacking"?¿Qué tipo de información nos brinda como resultado? Cite distintos tipos de ejemplos que permitan encontrar:

- Paginas de acceso a administradores de bases de datos tipo phpmyadmin
- Archivos de usuarios y passwords de acceso a servidores Frontpage
- Paginas de camaras web públicas.

Nota:
Una distribución linux que puede resultar útil para investigar y encontrar nuevas herramientas de seguridad es backtrack. http://www.backtrack-linux.org/.