Introducción al Hacking Ético

Lic. Bruno Zappellini Emiliano De Marco Andrada
Germán Bianchini Lucas Krmpotic Maximiliano Aguila

2019

Resumen

En este laboratorio pondremos en practica todo lo visto en la primera clase del curso

Laboratorio 1

Footprinting:

1. Liste distintos medios que se le ocurran que pueden llegar a ser utilizados para averiguar información de modo pasivo.
2. Piense en alguna organización que tenga un sitio WEB en el dominio ".com.ar"
   a) Use el portal de consultas que ofrece una entidad de registro de dominios para obtener información sobre un dominio dado. El sitio de registro de dominios .ar es http://nic.ar
   b) Use el protocolo DNS para averiguar información de la organización como:
      a) IPs de los servidores de correo (identificando cuál de ellos es el primario)
      b) IPs de los servidores DNS (identificando cuál de ellos es el primario)
      c) IPs de los servidores WEB.
   c) Use consultas de WHOIS para averiguar información sobre la organización responsable sobre los bloques IP que la organización usa.
   d) Use buscadores para recolectar en forma pasiva, otro tipo de información de la organización, como ser: archivos .doc y .xls, teléfonos, direcciones de mail, nombres de las personas que trabajan en la organización, etc.
3. Visite el sitio http://www.netcraft.net/ y pruebe la funcionalidad del mismo contra el dominio www.unp.edu.ar. (Consigne aquí al menos 8

datos de la organización).

4. Visite el sitio http://www.archive.org/web/web.php y pruebe la funcionalidad del mismo.
   a) Utilícelo para consultar información cacheada sobre su organización.
   b) Observe las primeras versiones de su portal y cómo fue cambiando
   c) Observe las primeras versiones de Google (año 1998)
   d) ¿Qué ventajas presenta esta herramienta respecto de otras herramientas de footprinting?

Escaneo de puertos

a) Escaneo de puertos

El objetivo será realizar los escaneos desde la máquina virtual Kali hacia la máquina real u otra que el instructor pueda poner a disposición. Utilizaremos nmap para realizar escaneos utilizando diferentes técnicas. Nota: para ver cómo usar nmap con las diferentes técnicas, ver http://nmap.org/book/man-port-scanning-techniques.html

Nota : *Antes de empezar a realizar las pruebas determine qué puertos de la máquina real están abiertos y cuáles cerrados. Utilice el comando netstat: - Linux ejecute en la consola: netstat -nat (puertos TCP) / netstat -nau (puertos UDP) - En Windows ejecute en la CLI: netstat -na*

Para realizar un escaneo de puertos TCP use el comando:
`nmap -sV <IP_destino>`

Para realizar un escaneo de puertos UDP use el comando:

```
nmap -sU <IP_destino> -p <puerto abierto>
nmap -sU <IP_destino> -p <puerto cerrado>
```

5. Utilizando la máquina virtual provista por la cátedra, abra una terminal de root y realice un escaneo de puertos TCP 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 -nltp4`

6. En el ejercicio anterior, ¿Se detectaron como abiertos todos los puertos que estaban realmente abiertos? Utilice nmap indicando EXPLICITAMENTE que se requiere que se revisen todos los puertos TCP

Fingerprinting

7. ¿Cuál es la finalidad de realizar OS fingerprinting? ¿Cómo se lleva a cabo?

8. Utilice nmap para realizar OS fingerprinting de distintos sistemas operativos. ¿Fue correcto el resultado alcanzado por la herramienta?

Nota: Nmap es una herramienta que además de permitir escanear puertos, implementa diversas tecnicas de OS Fingerprinting: http://nmap.org/book/osdetect.html.

9. ¿Cuál es la finalidad de realizar fingerprinting de servicios? ¿banner grabbing es la forma mas sencillo de realizarlo?

Enumeración

10. ¿Qué es enumeración?
11. ¿Como haría enumeración sobre alguno de los siguientes protocolos y servicios de consulta?
    a. Redes WiFi presentes en la Facultad
    b. Dispositivos bluetooth activados
    c. Recursos presentes en una red windows (servidores / impresoras / shares)
    d. Información de DNS de algún dominio en particular (usar con responsabilidad)
12. Realizar enumeración de DNS con Kali
    Utilice DNS ENUM para hacer una enumeración del DNS del dominio unp.edu.ar, para ello:
    1. Abra la aplicación dnsenum (KALI Linux → Information Gathering → DNS Analysis → dnsenum) y ejecute el comando de la siguiente manera:

    `` `dnsenum unp.edu.ar -f file.txt` ``

Google Hacking

13. ¿Qué es "Google Hacking"? Nota: Ver el sitio http://www.hackersforcharity.org/ghdb/
14. ¿El Google Hacking es una técnica activa o pasiva?
15. Utilizar Google Hacking para dar con:

- Páginas de administración de impresoras LaserJet
  `intitle:"hp laserjet" inurl:info_configuration.htm`

- Páginas de cámaras web públicas. Busque en Google alguna de las siguientes:

```
"ViewerFrame?Mode="
camera linksys inurl:main.cgi
allintitle: "Network Camera NetworkCamera"
intitle:Axis 2400 video server
intitle:"Live NetSnap Cam-Server feed"
intitle:"Live View / - AXIS"
intitle:"LiveView / - AXIS" | inurl:view/view.shtml
intitle:liveapplet
intitle:snc-cs3 inurl:home/
intitle:"WJ-NT104 Main"
inurl:LvAppl intitle:liveapplet
inurl:indexFrame.shtml "Axis Video Server"intitle:"EvoCam" inurl:"webcam.html"
inurl:lvappl
inurl:axis-cgi/jpg
inurl:indexFrame.shtml Axis
inurl:"MultiCameraFrame?Mode=Motion"
inurl:/view.shtml
inurl:/view/index.shtml
inurl:"viewerframe?mode=motion"
```

- Archivos que contienen mensajes de error de acceso denegado (relacionados a claves/passwords) alojadas en el dominio .ar
  `intext:"access denied" "using password" site:ar`
- Direccionando las búsquedas
  - Si usted quiere buscar algo en particular, por ejemplo que este alojado en el dominio .ar o el dominio .com.ar deberá agregar a la búsqueda el TAG site:ar o site:com.ar respectivamente
  - Si se quiere buscar páginas en cuya url aparezca alguna palabra en particular como ser "info" habrá que usar en la búsqueda el TAG inurl:info
  - Si se quiere buscar algún tipo de archivo en particular, por ejemplo archivos excel, habrá que usar en la búsqueda el TAG filetype: xls
  - Con la información dada, busque Webmails en ecuador que no utilicen encripción en las comunicaciones, es decir usan el protocolo http
    Tips (combinar las siguientes):
    * webmail
    * inurl:http://
    * site:ec

- Con la información dada, busque archivos de Excel o Word que estén públicos dentro de la organización en la que ud. trabaja.