

Práctica 1 - OSINT

Criptografía y Seguridad 2023-2

Anayanzi Delia Martínez Hernández
`anayanzi@ciencias.unam.mx`

Ivan Daniel Galindo Perez
`ivangalindo@ciencias.unam.mx`

Luis Fernando Yang Fong Baeza
`fernandofong@ciencias.unam.mx`

Febrero 2023

1 Introducción

El *Open-Source Intelligence* o mejor conocido como OSINT, es vital para cualquier prueba de penetración o *pentesting* puesto que consta de recopilar información del sistema que se está tratando de vulnerar, desde información de a nombre de quién están registrados los dominios, hasta el ver directamente qué puertos tiene abiertos el servidor que va a ser probado.

2 Procedimiento

Como existen muchísimas maneras de obtener información, de todo tipo, esta práctica consta de 3 secciones, información personal, información del sistema e información del servidor.

2.1 Información personal

En los archivos de la práctica se ha adjuntado una foto, con las herramientas necesarias, responde las siguientes preguntas.

1. ¿Cuál es el nombre real del archivo? Es decir, el nombre que se le dió por el sistema operativo.
2. ¿Qué marca es la cámara con la que fue tomada la foto?
3. ¿De qué color son las carpas del restaurante latino a unas calles?

2.2 Información técnica de un sistema

Utilizando las herramientas vistas en clase, explicar una manera de obtener información respecto a un sitio web público como por ejemplo, www.cinepolis.com.mx.

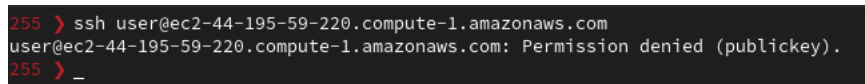
2.3 Información práctica de un sistema

Para esta práctica, se ha contratado y levantado una instancia de AWS la cual va a fungir como nuestro sistema objetivo (Al cual se le aplicarán las técnicas de OSINT), esto para trabajar en un ambiente seguro y privado. El hostname de esta instancia de EC2 es `ec2-44-195-59-220.compute-1.amazonaws.com`

Antes de empezar la práctica, se debe de verificar que la instancia está a nuestro alcance, es decir, que estamos en la misma red, esto se puede hacer de varias maneras pero el comando que se va a utilizar es:

```
ssh user@ec2-44-195-59-220.compute-1.amazonaws.com
```

La respuesta debería ser como la siguiente pantalla:



```
255 > ssh user@ec2-44-195-59-220.compute-1.amazonaws.com
user@ec2-44-195-59-220.compute-1.amazonaws.com: Permission denied (publickey).
255 > _
```

Figure 1: Salida del comando

Si por alguna razón, la salida no coincide, contactar a cualquier ayudante para resolver la situación.

2.3.1 Escaneo de puertos

Realiza un escaneo de puertos a la instancia y responde las siguientes preguntas.

1. ¿Cuántos activos tiene la instancia?
2. ¿Cuántos puertos están cerrados?
3. ¿Cuántos puertos están abiertos?
4. ¿Cuál es la versión del puerto 80?
5. ¿Qué hacen los parámetros que se le pasaron a `nmap`?

Obten una lista de palabras (mejor conocida como `wordlist`) de algún sitio o fuente confiable, con ella realiza un escaneo y encuentra la bandera oculta dentro de la aplicación HTTP en la práctica.

3 Entregables

Las respuestas se deben de entregar en un archivo de texto o PDF en el classroom. Si se desea, se puede agregar un comentario acerca de la práctica.

La fecha de entrega es el 22 de Enero de 2023 antes de las 23:59:59.