“ATAQUES Y EVALUACIÓN DE VULNERABILIDADES (Parte II)”

Trabajo Preparatorio N°2

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se tratara temas acerca ´ de ataques y evaluación de vulnerabilidades dentro de un entorno que se puede controlar y realizar un análisis de la confianza que tenemos como seres humanos para dar información muy fácil sobre si mismo y esto ayude a realizar cualquier ataque.**

***Index Terms*—Análisis, Ataque, Confianza, Entorno, Ser Humano.**

I. Introducción

En el área de las seguridades se tiene dos tipos de ataques como se indico posteriormente ahora se realizara un análisis de las vulnerabilidades que se tiene con los ataques que se pueden realizar siguiendo paso a paso dicha acción utilizando técnicas como:

- Fingerprinting: Ayuda a recolectar información de manera directa y sirve como una herramienta de rastreo a un usuario.
- Footprinting: Permite obtener información de manera legal.

De igual manera se realizara una prueba de concepto de ataque de ingeniería social, dejando ver las vulnerabilidades que se tiene como seres humanos al dar de manera muy fácil información importante de uno mismo dejado ver que como seres humanos somos somos la parte o el elemento mas débil en la estructura de protección en al seguridad de cualquier tipo de red

II. Objetivos

- Explotar las vulnerabilidades de un equipo dentro de un entorno controlado.
- Hacer una prueba de concepto de un ataque sencillo de ingeniería social.
- Analizar técnicamente los resultados de las distintas fases de estos ataques.

III. Cuestionario

A. Revisar el marco teórico para la realización de la práctica.

B. Explique en que consiste Fingerprinting y Footprinting. (máximo una carilla).

Ambos términos hacen referencia a técnicas para recoger información de un objetivo dentro de una red.

Fingerprinting

Consiste en la recolección de información de forma directa desde el sistema informático de un individuo u organización que navega en la red, es así como se busca llegar a conocer el comportamiento y configuración de los mismos. Sirve como una herramienta para rastrear a un usuario mientras navega por el Internet [1]. Algunos sitios web utilizan las huellas digitales del navegador para la detección de posibles fraudes; mientras que algunos comerciantes utilizan esta técnica para conseguir datos acerca de diferentes usuarios con el fin de poder generar ingresos por publicidad [1].

En el caso que se desee recoger información del sistema se utilizan ciertas herramientas como:

- nmap
- nbtscan
- Módulos auxiliares con Metasploit

Dicha información puede ser estado de los puertos, vulnerabilidades que existen, versiones de software, sistema operativo, etc mediante el uso de las siguientes técnicas:

- Phishing: Basada en probabilidad, envía información confiable de forma masiva con el fin de solicitar información, generalmente esto se realiza mediante correos electrónicos.
- Ingeniería social: Mediante el uso de habilidades sociales y técnicas psicológicas se obtiene información ya sea mediante técnicas pasivas como la observación o técnicas activas que puede ser buscar en la basura,
- Sniffing: Captura el tráfico presente en la red, puede ser realizado mediante aplicaciones como: Wireshark o Ettercap.

- Scanning: Busca conseguir información mediante el uso de puertos libres o vulnerabilidades [2].

Footprinting

Consiste en adquirir información de una manera legal que se base a la información publica presente en la red, medios de comunicación, redes sociales, sitios web de trabajo, Google, entre otros. Existen dos tipos de footpring los cuales son [3]:

- Activo: Realizar una huella al ponerse en contacto directo con la máquina de destino.
- Pasivo: Consiste en recopilar información de un sistema ubicado a una distancia remota del atacante [4].

Permite reunir las configuraciones de seguridad básicas de una máquina objetivo junto con la ruta de red y el flujo de datos, es decir, mediante este método se puede conocer [3]:

- Sistema operativo de la máquina de destino.
- Cortafuegos
- Dirección IP
- Mapa de red
- Configuraciones de seguridad de la máquina de destino
- Identificación de correo electrónico, contraseña
- Configuraciones de servidor
- URLs
- VPN [4]

C. Consulte para que sirve que usos se le puede dar a nmap (máximo una carilla).

nmap es un porgrama de código abierto que tiene muchas funciones, entre las principales se encuentra el rastreo de puertos, pero también como software de detección de SO. Es usado para evaluar la seguridad de diferentes sistemas informáticos, descubrir servicios o servidores en una red; así, nmap envía paquetes definidos a otros equipos y analiza sus respuestas [2].

Posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones [5]

Sus principales características son:

- Descubrir servidores.
- Identificar puertos abiertos.
- Determinar que servicios se encuentran en ejecución.
- Determinar el sistema operativo y versión del dispositivo.
- Conocer características del hardware de red de la máquina.

Su uso es principalmente en el campo de seguridad informática y también para hacking debido a que su detección es muy complicada dado a que fue creado para evadir los sistemas de detección de intrusos (IDS) y no interferir con las operaciones de la red y de sus dispositivos [5].

Puede funcionar en sistemas operativos basados en Unix (GNU/Linux, Solaris, BSD y Mac OS X), y también en otros Sistemas Operativos como Microsoft Windows y AmigaOS.

D. Explicar la diferencia entre un payload de tipo bind y reverse. (máximo una carilla).

El payload de tipo bind o con conexión directa posee una variable RHOST la cual es la dirección de la maquina a la que quiere acceder, por lo que nosotros nos conectamos a la víctima pero posee una ventaja que es que no nos da nuestra propia dirección pero la mayor ventaja que nos brinda esta conexión es que garantiza el anonimato. [7]. La conexión se realiza con los siguientes pasos:

Se ejecuta el código en la maquina remota

- Se ejecuta el código en la maquina remota
- Se deja en un puerto una shell
- La variable RHOST del payload debe ser la dirección IP de la víctima. [7].

Mientras que el Reverse es lo contrario ya que esta utiliza un fichero (puede ser .py .exe o cualquier extensión)conjuntamente con la dirección IP de la persona que esta atacando o de un servidor que escoja las dirección que quiera el atacante.

En el caso de esta conexión si el payload no se encuentra correctamente cifrado (como el PHP de meterpreter) el administrador de dominio puede conocer nuestra dirección ip y si existe un fallo en el servidor de control este puede explotarlo y tumbar nuestro sistema. [6].

REFERENCES

[1] "¿Que es footprinting y fingerprinting?" https://www.ticarte.com/contenido/que-es-footprinting-y-fingerprinting (accedido jun. 15, 2021).

[2] Y. González, "Fingerprinting: ¿Qué es y para qué se usa?", Grupo Atico34, jun. 17, 2020. https://protecciondatos-lopd.com/empresas/fingerprinting-que-es/ (accedido jun. 15, 2021).

[3] "Footprinting y Fingerprinting", Ciberseguridad. https://ciberseguridad.com/amenzas/footprinting-fingerprinting/ (accedido jun. 15, 2021).

[4] "Técnicas Footprinting y Fingerprinting para recoger información", Solvetic. https://www.solvetic.com/tutoriales/article/2740-tecnicas-footprinting-y-fingerprinting-para-recoger-informacion/ (accedido jun. 15, 2021).

[5] "Nmap: the Network Mapper - Free Security Scanner". https://nmap.org/ (accedido jun. 15, 2021).

[6] "Payload Reverse o Bind ¿Cuál elegir?". https://cyberh992017.wordpress.com/2017/04/26/payload-reverse-o-bind-cual-elegir/. (accedido jun.15,2021).

[7] "Explotación de Aplicaciones y Sistemas". https://isidrojara.com/projects/uclm/EASIsidroJara.pdf. (accedido jun.15,2021).