Seguridad en routers

Juan Manuel Imbachí Güengue / *juan.imbachi@correo.icesi.edu.co*
Jose Alejandro Galvis Nieto / *jose.galvis@correo.icesi.edu.co*
Wilmer Andrés Gómez Moreno / *wilmer.gomez@correo.icesi.edu.co*
Universidad Icesi, Cali-Colombia

Resumen

En este proyecto de investigación se ha decidido documentarse sobre diferentes maneras de encontrar vulnerabilidades en dispositivos router. Para esto se profundizará sobre qué es y para qué sirve el pentesting, se analizarán sus diferentes variantes y explicarán las fases que componen el mecanismo mencionado anteriormente. Después, estos conceptos se aterrizarán sobre los activos a los cuales el grupo tiene acceso, para finalmente enfocarse en un activo en especial y extraer conclusiones con respecto a dicho dispositivo. No obstante, en primera instancia se dará una contextualización sobre el tema y una evidenciación de por qué este proyecto es tan relevante en el ámbito de redes y comunicaciones.

Abstract

In this research project it has been decided to investigate about different ways of finding vulnerabilities about router devices. In order to do this, it will be explained what pentesting is and what it is for, its different variants will be analyzed and the phases that make up this mechanism. Then, these concepts will land on the assets to which the group has access, to finally focus on a particular asset and extract some conclusions. However, in first place there will be a contextualization on the subject and an explanation of why this project is so relevant in the field of networks and communications

Palabras Clave: Router, Pentesting, Vulnerabilidades..

I. INTRODUCCIÓN

Desde su creación en 1969, la internet ha facilitado la vida de los seres humanos, principalmente en lo relacionado a las comunicaciones. Actualmente, se usa como herramienta para gran parte de las actividades diarias, lo que conlleva a un constante flujo de información. Sin embargo, también se ve expuesta a ser robada por terceros con fines malintencionados. Es por lo anterior que se ha convertido en prioridad garantizar la seguridad de los datos en dicho medio de comunicación.

En este orden de ideas, el presente trabajo busca hacer énfasis en la seguridad en routers. No obstante, se hace necesario explicar primero para qué sirven dichos dispositivos.

Los router pertenecen a la capa de red del modelo OSI, y tienen como propósito determinar la ruta óptima para el envío de información desde el emisor hasta el receptor. Sin embargo, estos dispositivos poseen vulnerabilidades que comprometen seriamente la confidencialidad de la información que pasa a través de ellos.

Hipótesis: Los router poseen vulnerabilidades en seguridad que facilitan el robo de información sensible.

II. CONTEXTO

A inicios del año 2019 en los sistemas de Cisco, que son utilizados por muchas pequeñas empresas para administrar sus redes, se presenta una noticia en la que se informa de una vulnerabilidad crítica, la cual afecta el software de sus dispositivos, de modo que permite a un atacante remoto explotarla, sin necesidad de autenticarse y teniendo el control total sobre ese dispositivo[2].

A partir de la vulnerabilidad mencionada anteriormente, un atacante puede tomar ventaja de esta llevando solicitudes HTTP maliciosas a un dispositivo en especial. Un exploit exitoso podría permitir al atacante ejecutar de manera oculta, como un usuario de alto privilegio, un código arbitrario en el sistema operativo del dispositivo afectado[1].

III. OBJETIVOS

ALCANZABLES

- Describir el proceso de obtención de información a partir del uso de herramientas de pentesting como Metasploit Framework y hydra.
- Obtener información enviada a través de los router mediante el aprovechamiento de vulnerabilidades detectadas con un análisis de pentesting.

NO ALCANZABLES

- Identificar y describir las vulnerabilidades presentes en routers entregados por los isp a clientes en sus hogares.
- Implementar 8 herramientas de obtencion de informacion en distintos router y de otras marcas tales como ASUS o HUAWEI.

IV. Marco Teórico

A lo largo del tiempo se han desarrollado diferentes mecanismos para identificar vulnerabilidades en routers, en este proyecto de investigación se abordará el pentesting, también conocido como test de penetración. El pentesting consiste en ejecutar diversos ataques contra sistemas informáticos con el fin de identificar posibles fallos de seguridad. Existen diferentes tipos de pentesting:

A. Pentesting de caja blanca

Aquí se conoce absolutamente todo sobre el sistema que se va a intentar vulnerar. Es el tipo más completo, en efecto siempre se parte de un análisis que estudia toda la infraestructura. Por lo tanto también es muy útil ya que no se malgasta tiempo descubriendo desde cero la arquitectura. Como requiere tanta información, es normalmente realizado por miembros de la organización propietaria.

B. Pentesting de caja negra

Es el polo opuesto del método caja blanca, ya que aquí no se tiene absolutamente ninguna información sobre el objetivo. Se puede considerar como un ataque a ciegas. No obstante, también es muy enriquecedor ya que permite simular un ataque por parte de externos quienes desconocen completamente la arquitectura y que estén intentando vulnerar el sistema.

C. Pentesting de caja gris

Como se puede deducir por su nombre, es un mezcla entre el pentesting caja blanca y caja negra. Aquí se sabe cierta información sobre el sistema, sin embargo esta no es suficiente para explotar vulnerabilidades. Es por eso que se debe invertir tiempo en el "fingerprint" donde se busquen todos los posibles fallos del sistema. Es considerado por los expertos como el más recomendable a realizar.

V. Metodología

Para la metodología, se seguirán las fases del pentesting, ya que es el método que se va a utilizar para encontrar vulnerabilidades. Por lo tanto, las etapas que se llevarán a cabo son las siguientes:

1) Recopilación de información:

Lo primero será encontrar toda la información disponible sobre el sistema que se va a atacar. Es decir, que routers están disponibles para hacer uso de ellos, así como buscar en la web si ya se han reportado vulnerabilidades sobre esos modelos.

2) Búsqueda de vulnerabilidades:

En esta etapa se utilizan herramientas como Metasploit Framework y hydra en kali linux para explorar vulnerabilidades posibles en los modelos de routers que se tengan. También se determina si las debilidades que se pudieran haber encontrado (fase 1) son explotables para este caso.

3) Explotación de vulnerabilidades:

Después de haber explorado las posibles debilidades y fallos que tengan los routers, se procede a explotar dichos problemas con la herramienta que se decida.

4) Post explotación:

Esta fase no se ejecuta siempre. Todo depende del resultado que se obtenga en la etapa tres. Es posible que se deban realizar todavía más acciones a causa de lo que se haya observado anteriormente.

5) Elaboración de informes:

Finalmente se realizará un informe comunicando todos los resultados que se vieron en la investigación. El reporte será la parte de resultados y conclusiones de este documento.

VI. Procedimiento y Resultados

Una vez recopilada la información necesaria para la realización del proyecto (herramientas para análisis de vulnerabilidades, sistema operativo a usar, modelos de router disponibles en los laboratorios de la universidad), se procedió con la realización del mismo.

Para el análisis se hizo uso del SO Kali Linux que provee una vasta cantidad de instrumentos para ejecutar pentesting. Por tal razón, inicialmente se intentó trabajar con Hydra y Routersploit, no obstante, presentaban fallos en la instalación o uso de sus componentes, motivo por el cual fue necesario hacer un cambio en las herramientas a usar.

Posteriormente se probó con NMAP y Cisco Global Exploiter, y tras ver que no se poseían problemas de actualizaciones y permitían el uso de sus componentes, se procedió a iniciar las pruebas. Por motivos ajenos al grupo, el encargado del laboratorio únicamente facilitó el uso de un tipo de router, Cisco con modelo 4321, el cual no poseía vulnerabilidades reportadas en internet, y tras el respectivo análisis por medio de las herramientas mencionadas previamente, se comprobó dicho factor, concluyendo así la prueba a los router del laboratorio.

No obstante, dados los resultados poco interesantes obtenidos en el laboratorio, se decidió ampliar el alcance del proyecto y hacer un análisis en un router del rancho entregado por un ISP a un miembro del grupo. EL router a analizar fue un HITRON CGNV2, y mediante la herramienta NMAP se obtuvo

información sobre dos puertos abiertos, el puerto 80/tcp http y el puerto 5000/tcp, además de posibles vulnerabilidades CSRF y slowloris.

VI. Conclusiones

Finalmente, sobre el router Cisco 4321 no se detectaron vulnerabilidades , indicando el avance de empresas reconocidas como Cisco en temas de seguridad, al menos con este modelo de router. Por otro lado, las pruebas realizadas en el router HITRON CGNV2 indicó que este disponía de dos puertos abiertos, el 80 y el 5000, incluso mostraba información de un par de vulnerabilidades como CSRF y slowloris, lo cual permitió el cumplimiento del primer objetivo planteado, análisis de vulnerabilidades.

Mediante un ataque al puerto 80 se podrían solicitar credenciales, y de obtenerlas permitiría el acceso al panel administrativo del router o a información personal de los usuarios. Lo anterior otorgaría el control del router y sus funcionalidades, facilitando el robo de información sensible y siendo una amenaza latente para todo tipo de usuario.

VII. Referencias

[1]D. Gimenez, "Vulnerabilidad de routers Cisco," *Hackear*, 09-Mar-2019. [Online]. Available: https://hackear.com.ar/vulnerabilidad-de-routers-cisco/.

[2]"Una vulnerabilidad crítica de Cisco permite a un atacante controlar el sistema," *RedesZone*, 21-Jan-2019. [Online]. Available: https://www.redeszone.net/2019/01/21/vulnerabilidad-critica-cisco-controlar-sistema/.

[3]"How to scan for services and vulnerabilities with Nmap," Linux Hint. [Online]. Available: https://linuxhint.com/nmap-port-scanning-security/.

[4]Tutorialspoint.com, "Kali Linux Vulnerability Analyses Tools," www.tutorialspoint.com. [Online]. Available: https://www.tutorialspoint.com/kali_linux/kali_linux_vulnerability_analyses_tools.htm.

Links Extras:
Puertos susceptibles a vulnerabilidades:

http://dmrodriguez.50megs.com/portvulnerability.htm