Accessible TELNET Services

1. INTRODUCCIÓN

TELNET es un protocolo cliente-servidor que permite utilizar una máquina como terminal virtual de otra a través de la red, de forma que se crea un canal de comunicación. Permite el acceso remoto en modo texto a un equipo como si se utilizara una consola o una terminal física. Telnet se ubica en la capa de aplicación del modelo de referencia OSI, utiliza el puerto TCP 23 o puerto 2323 y está definido principalmente en las RFC 854 y 855.

Telnet no utiliza ningún tipo de cifrado, por lo que todo el tráfico entre equipos se intercambia en texto plano. Cualquier atacante con un analizador de red puede capturar el login y el password utilizados en una conexión; por lo tanto, no es recomendable utilizar telnet para conexiones remotas, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos: SSH o SSL-Telnet son las más comunes.

2. RIESGO

No se recomienda el uso de telnet desde el punto de vista de la seguridad debido a que existen varias vulnerabilidades descubiertas sobre telnet, entre las cuales se tiene:

- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (las contraseñas viajan en plano), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.

- Telnet carece de un esquema de autentificación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

Problemas de seguridad y SSH

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin Cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas. Por esta razón dejó de usarse, casi totalmente, y se popularizó el SSH, que puede describirse como una versión cifrada de telnet ya que puede cifrar toda la comunicación del protocolo durante el establecimiento de sesión.

Telnet no proporciona ningún cifrado por lo que expone información sensible o credenciales del sistema y utilizado de manera maliciosa permite tomar el control remoto de un ordenador y obtener información del computador atacado

3. DETECCIÓN

Los reportes enviados por el EcuCERT identifican los hosts que tienen el servicio de Telnet que se ejecuta en el puerto 23 / TCP el cual es accesible en Internet.

El comando que se utiliza para verificar si el puerto telnet está abierto es:

nmap -v -p 23 [IP]

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Nombre de la vulnerabilidad reportada
Dirección IP	Dirección IP del host
Puerto	Puerto desde donde se obtiene la respuesta
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
status_EcuCERT	Online: vulnerabilidad reportada por *Feeds* y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por *Feeds*, pero en el timestamp_EcuCERT no se detectó.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del dispositivo en cuestión
protocol	Protocolo por el que ingresó la respuesta (siempre TCP)
port	Puerto desde donde se obtiene la respuesta (23/TCP)
hostname	DNS reverso del host
tag	Siempre será telnet
asn	ASN de la red donde se encuentra el host
geo	País donde se encuentra el host
region	Estado/Provincia/Región donde se encuentra el host
city	Ciudad donde se encuentra el host
	Código del Sistema de Clasificación Industrial de América del
sic	Código del Sistema de Clasificación Industrial Estándar
banner	El logotipo del banner de respuesta del servicio telnet

4. ACCIONES RECOMENDADAS

Para evitar este tipo de vulnerabilidad se recomienda:

- Cerrar el puerto 23 y el puerto 2323.
- Utilizar aplicaciones equivalentes que utilicen cifrado para la transmisión de datos como SSH o SSL-Telnet.

5. REFERENCIAS

- https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec- html/node221.html
- https://guioos.wordpress.com/tag/servicio-telnet/
- https://www.ecured.cu/Telnet