Explotación de Vulnerabilidades en IoT (Internet de las Cosas)

Alexandra Cortes Tovar, José Ricardo Vásquez Vega, Juan Sebastián Vásquez Vega
Escuela Colombiana de Ingeniería Julio Garavito
Ingeniería de Sistemas

***Resumen*—El Internet de las Cosas (IoT) ha revolucionado la interconexión de dispositivos, permitiendo la automatización y recolección masiva de datos en diversas áreas como el hogar, el transporte y la salud. Sin embargo, con este crecimiento, también surgen importantes riesgos de seguridad. Este artículo analiza qué es el IoT, qué dispositivos forman parte de este ecosistema y cómo las vulnerabilidades en estos sistemas pueden ser explotadas, afectando la privacidad y la integridad de la información. Se discuten también algunos enfoques para mitigar estos riesgos.**

***Palabras clave*—IoT, Seguridad, Vulnerabilidades, Explotación, Ciberseguridad.**

I. INTRODUCCIÓN

El Internet de las Cosas (IoT, por sus siglas en inglés) se refiere a la interconexión de dispositivos físicos que pueden recopilar y compartir datos entre sí y con sistemas centrales. Esta tecnología ha permitido la automatización en hogares, ciudades y empresas, lo que facilita tareas diarias y mejora la eficiencia. Según un informe de Cisco IBSG, el IoT ha alcanzado una escala sin precedentes, con miles de millones de dispositivos conectados a nivel mundial *[1]*. Sin embargo, este crecimiento no está exento de desafíos, particularmente en términos de seguridad *[2].*

Por otra parte, a pesar de los numerosos beneficios del IoT. La vasta cantidad de datos generados por los dispositivos IoT crea nuevos vectores de ataque, exponiendo potencialmente información confidencial y comprometiendo la integridad de sistemas críticos *[2].* Este artículo explora los principales riesgos de seguridad asociados con el IoT y cómo los atacantes pueden explotar las vulnerabilidades en estos sistemas.

II. ¿QUÉ ES EL IOT Y QUÉ DISPOSITIVOS LO COMPONEN?

El IoT abarca una amplia gama de dispositivos, desde sensores y cámaras de seguridad hasta electrodomésticos inteligentes y dispositivos médicos. Estos dispositivos están conectados a la red, lo que permite la transmisión continua de datos para su monitoreo y análisis. El informe de Cisco destaca que el IoT incluye sistemas que van desde dispositivos personales como wearables hasta infraestructuras críticas *[1]*. La interconexión masiva de dispositivos plantea nuevos desafíos en términos de gestión y seguridad *[2]*.

Los dispositivos del IoT tienen un uso extensivo en sectores como el hogar, la salud y la industria. Por ejemplo, los wearables monitorean la actividad física y signos vitales, lo que permite un diagnóstico temprano de problemas de salud *[2]*. En el hogar, el IoT permite la automatización de tareas cotidianas, como el control de luces y termostatos *[2]*.

III. RIESGOS DE SEGURIDAD Y VULNERABILIDADES EN EL IOT

El rápido crecimiento del IoT ha expuesto numerosas vulnerabilidades que pueden ser explotadas por atacantes. Algunos de los riesgos más comunes incluyen la falta de autenticación adecuada, la exposición de datos sensibles y la insuficiente encriptación en la transmisión de información. Según Coy Sosa *[2]*, muchos dispositivos IoT presentan fallos críticos en la seguridad que permiten a los atacantes acceder a redes y obtener información personal, transformando a los dispositivos en parte de redes de bots o botnets.

Una de las vulnerabilidades más frecuentes es la insuficiente autenticación y autorización. Muchos dispositivos IoT utilizan contraseñas por defecto, lo que facilita los ataques de fuerza bruta. Además, la falta de actualizaciones de seguridad y la exposición de datos no encriptados en la nube aumentan el riesgo de ataques *[2]*. Otra amenaza crítica es la explotación de fallos en la comunicación entre dispositivos, como en el caso de las vulnerabilidades en la red SSHowDowN Proxy que permite el control remoto no autorizado de dispositivos *[2]*.

Algunos de los principales riesgos de seguridad en el IoT incluyen:

1. **Insuficiente autenticación y autorización:** Muchos dispositivos IoT utilizan contraseñas predeterminadas o débiles, lo que facilita los ataques de fuerza bruta. Según estudios de OWASP, la autenticación insuficiente es una de las principales causas de compromisos en sistemas IoT. Por ejemplo, muchos dispositivos de cámaras de seguridad no requieren configuraciones complejas para su autenticación, lo que los convierte en objetivos fáciles para los atacantes.

2. **Acceso remoto y control total del sistema**: Una de las vulnerabilidades más críticas del IoT es la posibilidad de que los atacantes obtengan acceso remoto a los dispositivos, lo que les permite tomar control completo

del sistema. Esto ha ocurrido en varios casos documentados, como el hackeo de dispositivos domésticos, donde se utilizó una red de más de 100,000 dispositivos IoT para enviar correos maliciosos *[4]*.

3. **Exposición de datos sensibles:** Los dispositivos IoT recolectan y transmiten grandes cantidades de datos, a menudo sin las protecciones adecuadas de encriptación. Esto significa que la información confidencial, como ubicaciones GPS o datos de salud, puede ser interceptada durante la transmisión *[2]*. Este tipo de exposición específicamente es preocupante cuando se trata de dispositivos médicos o dispositivos que manejan información personal como cámaras de seguridad *[1]*.

4. **Actualizaciones insuficientes:** Muchos dispositivos IoT no están diseñados para recibir actualizaciones regulares de software, lo que significa que las vulnerabilidades conocidas a menudo permanecen sin parchear durante largos períodos de tiempo *[2]*. Esto permite a los atacantes explotar fallos de seguridad conocidos en estos dispositivos, comprometiendo su integridad.

5. **Insuficiente protección contra malware:** Uno de los mayores riesgos del IoT es que los dispositivos comprometidos pueden ser utilizados para lanzar ataques a gran escala. Por ejemplo, los dispositivos IoT pueden ser reclutados en redes de botnets, inyectando software malicioso y luego se utilizan para lanzar ataques de denegación de servicio distribuidos (DDoS). Esto fue evidente en el ataque de Mirai en 2016, que comprometió miles de dispositivos IoT para lanzar un ataque DDoS masivo contra múltiples servicios en línea *[4]*.

IV. MITIGACIÓN DE VULNERABILIDADES

Para reducir los riesgos asociados con el IoT, es esencial adoptar prácticas de seguridad sólidas. Esto incluye la implementación de protocolos de autenticación fuertes, la encriptación de datos en tránsito y la actualización periódica del firmware de los dispositivos. Organizaciones como OWASP han desarrollado pautas para asegurar los dispositivos IoT, recomendando prácticas como la limitación de la recolección de datos sensibles y el uso de redes privadas virtuales (VPN) *[2]*.

Algunas de las estrategias clave incluyen:

1. **Autenticación robusta:** Una de las primeras medidas para mitigar los riesgos es asegurar que todos los dispositivos IoT utilicen contraseñas seguras y autenticación multifactor. Además, es importante que los dispositivos incluyan mecanismos que obliguen a los usuarios a cambiar las contraseñas predeterminadas al configurar el dispositivo por primera vez *[2]*.

2. **Encriptación de datos:** La encriptación de extremo a extremo es crucial para proteger los datos que se transmiten entre dispositivos IoT y los servidores en la nube. Al encriptar los datos, se asegura que la información no pueda ser interceptada o manipulada durante su transmisión *[4]*.

3. **Actualización de firmware y parches de seguridad:** Asegurarse de que los dispositivos IoT reciban actualizaciones de seguridad de manera regular es fundamental para mitigar vulnerabilidades conocidas. Los fabricantes de dispositivos deben implementar sistemas de actualización automáticos que permitan a los dispositivos instalar parches sin intervención del usuario *[2]*.

4. **Concientización del usuario**: Una parte clave de la mitigación también recae en los usuarios. Es importante concientizar a los usuarios sobre los riesgos de mantener configuraciones predeterminadas. Los usuarios deben ser instruidos para cambiar las contraseñas por defecto y utilizar medidas de seguridad adicionales como redes privadas virtuales (VPN) para proteger los dispositivos conectados *[4]*.

5. **Uso de redes segmentadas:** Otra medida importante es la segmentación de redes, que separa los dispositivos IoT de la red principal de la empresa o del hogar. Esto limita el daño que un atacante puede causar en caso de comprometer un dispositivo IoT *[2]*.

V. PROFUNDIZACIÓN CASO DE USO – EXPLOTACIÓN DE VULNERABILIDAD

El Internet de las Cosas (IoT) ha revolucionado la interconexión de dispositivos, permitiendo una recolección masiva de datos en áreas como el hogar, transporte, y salud. Sin embargo, esta conectividad plantea riesgos significativos, especialmente en dispositivos como cámaras de vigilancia, que son puntos de acceso potenciales para atacantes si no cuentan con la protección adecuada. Según el informe de Cisco IBSG, el IoT alcanzó una escala sin precedentes en 2020, superando los 50 mil millones de dispositivos conectados globalmente [1]. Esta masificación expone vulnerabilidades que pueden ser explotadas, afectando la privacidad y la integridad de los usuarios. En este trabajo, se explotará la vulnerabilidad CVE-2018-9995 en cámaras IoT, mediante el uso del script getDVR_Credentials.py en un entorno Kali Linux.

Descripción de la Vulnerabilidad

La vulnerabilidad CVE-2018-9995 afecta a ciertos modelos de DVR, permitiendo que un atacante pueda obtener credenciales de administrador sin necesidad de autenticación. Esta falla ocurre debido a la falta de validación en solicitudes HTTP específicas, las cuales pueden explotarse para acceder al dispositivo. A través de la explotación de esta vulnerabilidad,

los atacantes pueden ver en tiempo real la transmisión de las cámaras conectadas y manipular configuraciones de los DVR afectados.

Descripción del Ataque

Para explotar esta vulnerabilidad, se utiliza el script getDVR_Credentials.py en un sistema Kali Linux, el cual automatiza el proceso de envío de solicitudes HTTP maliciosas para obtener las credenciales de los dispositivos DVR afectados.

A. Explicación del Script getDVR_Credentials.py

El script getDVR_Credentials.py fue diseñado específicamente para aprovechar la vulnerabilidad CVE-2018-9995. A continuación se describe su funcionamiento:

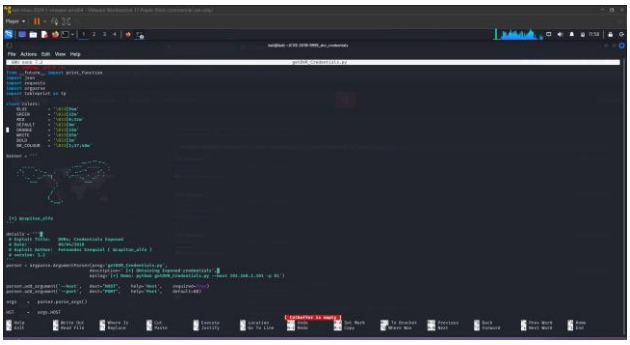

Ilustración 1. Script getDVR_Credentials.py. Fuente: Propia.

1. **Conexión al Dispositivo**: Utilizando la biblioteca requests de Python, el script envía una solicitud HTTP a la dirección IP y puerto específicos del DVR que se desea atacar. Kali Linux se utiliza como sistema operativo para ejecutar el script, dada su robustez y enfoque en ciberseguridad.
2. **Solicitud Maliciosa**: El script envía una solicitud con encabezados manipulados (headers), diseñados para explotar la vulnerabilidad del firmware en el DVR. Estos encabezados maliciosos engañan al dispositivo, haciéndole percibir la solicitud como legítima, pero en realidad están configurados para obtener las credenciales de usuario sin autenticación.
3. **Respuesta del DVR**: Debido a la falta de validación en el DVR, el dispositivo responde con las credenciales de administrador en un formato legible. Esta información incluye nombres de usuario y contraseñas, permitiendo acceso completo a la configuración del dispositivo.
4. **Automatización del Proceso**: El script permite ingresar múltiples direcciones IP y puertos en un solo comando, facilitando la automatización de la explotación. Una vez ejecutado, genera una lista completa de credenciales para cada DVR vulnerable encontrado.

B. Ejecución del Script en Kali Linux

La ejecución de getDVR_Credentials.py en un entorno Kali Linux permite explotar la vulnerabilidad CVE-2018-9995 de forma segura y controlada. A continuación, se describen los pasos específicos llevados a cabo para la ejecución de este script y la obtención de credenciales de DVR vulnerables:

1. **Clonación del Repositorio**: Para comenzar, es necesario clonar el repositorio que contiene el script en Kali Linux, un sistema operativo especializado en ciberseguridad que incluye herramientas de redes y monitoreo avanzadas. La clonación se realiza con los siguientes comandos:

   - "git clone https://github.com/ezelf/CVE-2018-9995_dvr_credentials.git"
   - "cd CVE-2018-9995_dvr_credentials"
   - "pip install -r requirements.txt"

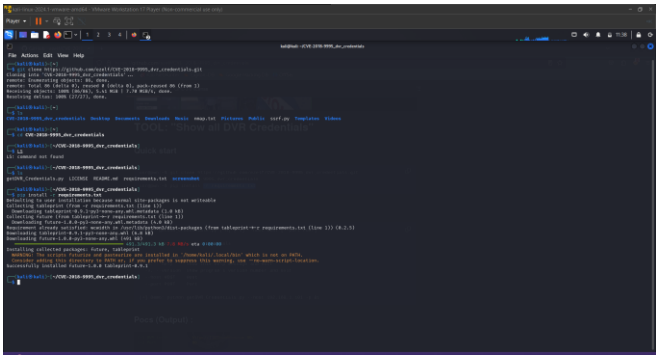

Ilustración 2. Comandos utilizados. Fuente: Propia.

Kali Linux ofrece un entorno seguro para realizar pruebas sin riesgo de comprometer otros sistemas. En este paso, se descargan los archivos necesarios y se instalan las dependencias especificadas en requirements.txt, permitiendo que el script pueda ejecutarse correctamente.

2. **Identificación de DVR Vulnerables**: Utilizando técnicas de búsqueda avanzada, como Google Dorks y Shodan, se localizan los DVR expuestos en la red:
   - **Google Dorks**: Se realiza una búsqueda con intitle:"DVR login" para encontrar páginas de inicio de sesión de DVR expuestas públicamente.

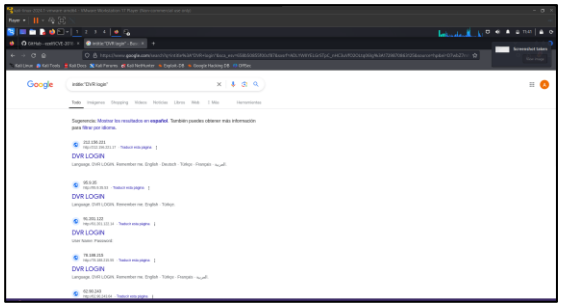

Ilustración 3. Resultados de la búsqueda. Fuente: Propia.

- **Shodan.io**: Utilizando el filtro Html:"/login.rsp", Shodan ayuda a identificar dispositivos DVR en red que son accesibles desde internet y potencialmente vulnerables.

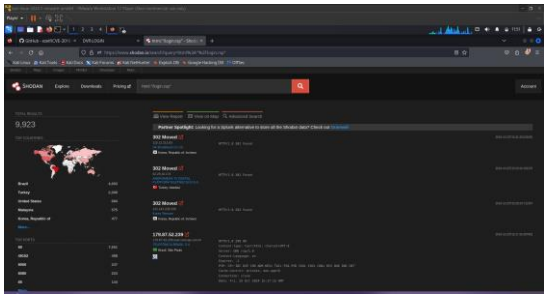

Ilustración 4. Resultados del uso del filtro en Shodan.io. Fuente: Propia.

La identificación de dispositivos vulnerables se basa en buscar IPs de DVR que responden en la red y cuya interfaz de autenticación es débil o accesible sin protección. Esta información permite al script dirigirse a los dispositivos que son susceptibles al ataque.

3. **Ejecución del Script**: Una vez que se ha recopilado una lista de IPs y puertos vulnerables, se procede a ejecutar el script para recolectar las credenciales de acceso con el siguiente comando:
“python getDVR_Credentials.py --ip <DVR_IP> --port <PORT>”

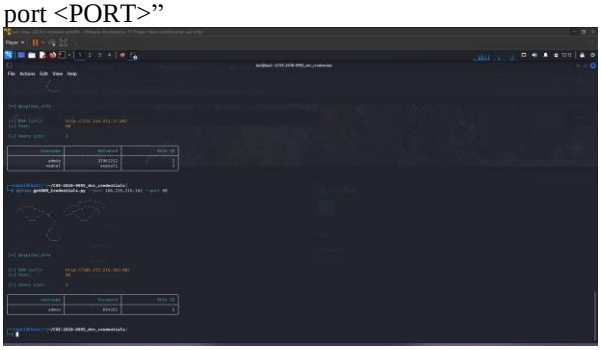

Ilustración 5. Ejecución del script. Fuente: Propia.

En este paso, el script envía una solicitud HTTP manipulada a la IP y puerto del DVR objetivo. La solicitud contiene encabezados que explotan la vulnerabilidad del dispositivo, forzándolo a devolver las credenciales sin verificar la autenticidad del remitente. Si el DVR es vulnerable, responde con el nombre de usuario y contraseña, que son guardados por el script para su posterior uso.

4. **Acceso a la Transmisión en Tiempo Real**: Con las credenciales obtenidas, se utiliza un navegador con la extensión **IE Tab** (que permite visualizar páginas en modo Internet Explorer) para simular el acceso en tiempo real a la interfaz web del DVR

- **IE Tab en Chrome**: Esta extensión permite cargar la interfaz de administración del DVR de manera que los recursos de la cámara puedan visualizarse de forma continua.

Ilustración 6. Extensión de IE Tab en Chrome. Fuente: Propia.

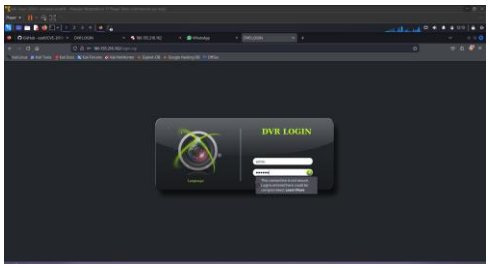

Ilustración 7. Ingreso de credenciales dados por el script. Fuente: Propia.

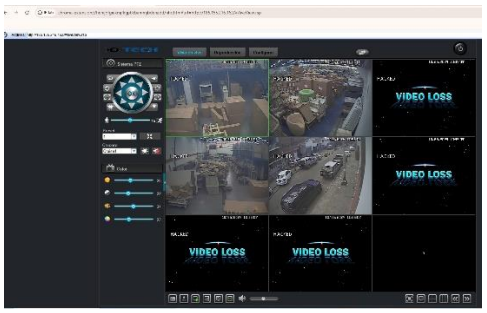

Ilustración 8. Demostración del ingreso de las cámaras. Fuente: Propia.

Usando las credenciales, es posible ingresar a la interfaz de configuración del DVR y ver las transmisiones de cámaras conectadas en tiempo real. Este paso final demuestra el riesgo significativo de privacidad y seguridad, ya que un atacante puede observar, grabar, o incluso controlar los dispositivos de videovigilancia sin que el propietario lo detecte.

Escenario de Laboratorio Controlado

Para ejecutar el ataque en un entorno seguro y ético, se creó un laboratorio controlado que accede a un sistema de vigilancia IoT con dispositivos DVR y cámaras IP. Este laboratorio permite observar los efectos de la vulnerabilidad en un ambiente controlado netamente académico.

1. **Entorno de Red Privada en Kali Linux**:

   - **Kali Linux como Sistema Operativo Base**: Kali Linux fue elegido como plataforma de ataque, debido a su versatilidad y las herramientas integradas que ofrece para pruebas de ciberseguridad, como análisis de red, escaneo de vulnerabilidades y ejecución de scripts. Kali Linux actúa como el sistema desde el cual se ejecutan todos los ataques, asegurando un entorno controlado y seguro para la experimentación.

2. **Equipos y Herramientas Utilizadas**:

   - **DVRs y Cámaras IP**: Se utilizaron DVRs que presentan la vulnerabilidad CVE-2018-9995, conectados a varias cámaras IP. Estos dispositivos representan el objetivo en la simulación del ataque y sirven para evaluar la efectividad de los controles de mitigación.
   - **Herramientas de Búsqueda (Shodan y Google Dorks)**: A través de Shodan y Google Dorks, se simula la identificación de DVRs vulnerables, imitando técnicas de reconocimiento que un atacante podría usar en un entorno real. Estas herramientas permiten localizar DVRs y cámaras expuestas con configuraciones de seguridad inadecuadas.
   - **Extensión IE Tab en Navegador Chrome**: Esta extensión permite que la interfaz de las cámaras sea visualizada en modo Internet Explorer, simulando un acceso en tiempo real al DVR para observar la transmisión de video de las cámaras, tal como un atacante lo haría con las credenciales obtenidas.

3. **Diagrama del Escenario de Red**:
   En el diagrama del escenario, se muestra la disposición de los dispositivos conectados en la red: la computadora Kali Linux desde la cual se lanza el ataque, el servidor DVR objetivo, y las cámaras IP que transmiten en tiempo real. La computadora atacante se conecta al DVR usando la IP y el puerto correspondiente. Desde allí, accede a la interfaz de administración del DVR para ver y gestionar la transmisión de las cámaras.

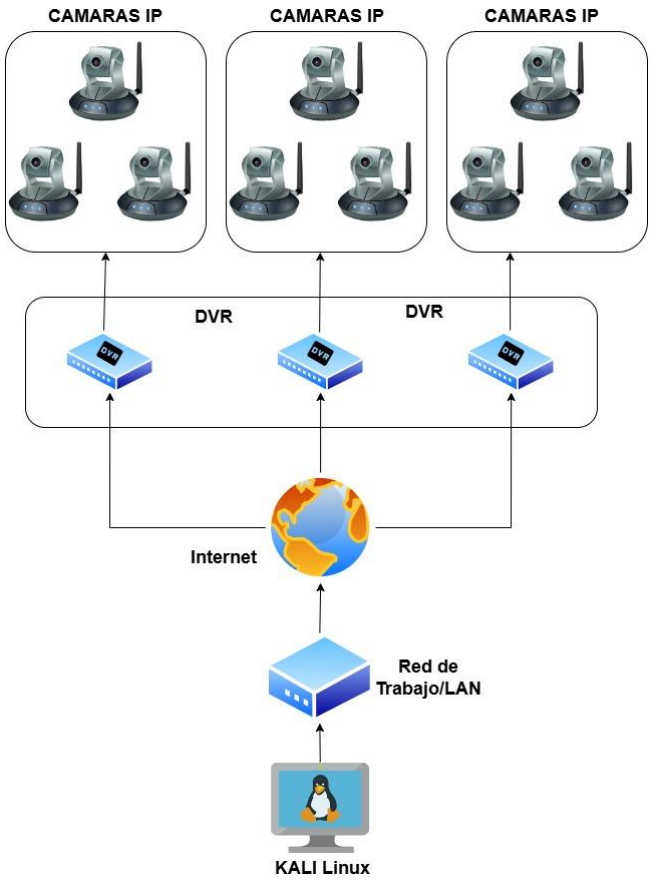

Ilustración 9. Diagrama de infraestructura de trabajo. Fuente: Propia

Este diagrama también resalta los enlaces de red utilizados y el flujo de tráfico de datos, mostrando cómo el tráfico HTTP manipulado permite al atacante capturar credenciales y, posteriormente, controlar las cámaras.

Controles y Pruebas de Mitigación

Para abordar la vulnerabilidad CVE-2018-9995 y reducir el riesgo de explotación en dispositivos DVR y cámaras IP, se proponen las siguientes soluciones de seguridad, que representan prácticas recomendadas para mejorar la protección de dispositivos vulnerables en entornos de IoT.

1. **Autenticación Robusta**
   La implementación de autenticación multifactor (MFA) añade una capa de seguridad que requiere una verificación secundaria (como un código de autenticación en el teléfono o un token) junto con la contraseña. Esto ayuda a bloquear el acceso no autorizado, incluso si un atacante ha obtenido el nombre de usuario y la contraseña.

   Al requerir MFA en los DVR, un atacante que intente ejecutar el script getDVR_Credentials.py no lograría acceder al dispositivo sin completar el paso de

autenticación adicional, mejorando significativamente la seguridad de estos dispositivos frente a accesos no autorizados.

2. **Cifrado de Datos en Tránsito**
   Se recomienda habilitar el cifrado de extremo a extremo en la comunicación entre el DVR y el cliente mediante el protocolo HTTPS. Esto protegería la transmisión de datos, asegurando que la información intercambiada esté cifrada y no pueda ser interceptada en texto claro.

   Con HTTPS habilitado, los datos, incluidas las credenciales de inicio de sesión, estarían cifrados durante su transmisión. Esto evitaría que un atacante pudiera interceptar credenciales en texto claro, reduciendo así el riesgo de exposición de información sensible.

3. **Actualización de Firmware**
   Aplicar las actualizaciones de firmware recomendadas por los fabricantes que incluyan parches de seguridad para corregir la vulnerabilidad CVE-2018-9995 es crucial para evitar que los dispositivos sean susceptibles a este tipo de ataques.

   Al actualizar los dispositivos a las últimas versiones de firmware, se puede bloquear el acceso no autorizado explotado por getDVR_Credentials.py. Esta medida es esencial para corregir la vulnerabilidad en dispositivos que aún no han sido protegidos.

4. **Monitoreo de Redes con Sistema de Detección de Intrusiones (IDS)**
   La implementación de un IDS en la red monitorea el tráfico entrante en busca de actividades sospechosas, como múltiples intentos de autenticación o solicitudes con encabezados HTTP anómalos, alertando al equipo de seguridad sobre posibles intentos de intrusión.
   Un IDS sería capaz de identificar y notificar en tiempo real la actividad maliciosa generada por intentos de ejecución del script getDVR_Credentials.py, permitiendo al equipo de seguridad reaccionar de inmediato ante cualquier intento de acceso no autorizado.

V. Conclusión

El Internet de las Cosas (IoT) ha revolucionado el mundo moderno, facilitando la conectividad de miles de millones de dispositivos y transformando sectores como el hogar, la industria, y la seguridad. No obstante, las vulnerabilidades inherentes a estos sistemas representan serias amenazas a la privacidad y la seguridad de los usuarios. La explotación de la vulnerabilidad CVE-2018-9995, demostrada mediante el uso de Kali Linux y el script getDVR_Credentials.py en un laboratorio controlado, evidencia la criticidad de estas fallas en dispositivos IoT como los DVR. La capacidad de acceder sin autenticación a estos dispositivos representa un riesgo significativo, ya que permite a un atacante observar y manipular flujos de video en tiempo real, comprometiendo la privacidad y seguridad de los usuarios.

Para aprovechar plenamente los beneficios del IoT sin comprometer la seguridad, es crucial implementar medidas de protección robustas, tales como autenticación multifactor, cifrado de datos y actualizaciones regulares de firmware. Estos controles no solo mitigan el riesgo de ataques, sino que también fortalecen la infraestructura IoT contra vulnerabilidades futuras. Los resultados de este estudio destacan la necesidad urgente de adoptar un enfoque proactivo hacia la seguridad de los dispositivos IoT, integrando prácticas como el monitoreo de redes con sistemas de detección de intrusiones (IDS), para una defensa en profundidad que garantice la protección integral.

Solo mediante un enfoque sistemático y preventivo en la gestión de la seguridad de dispositivos IoT se podrán aprovechar los beneficios de esta tecnología sin comprometer la privacidad y la seguridad de los usuarios. Este estudio subraya la importancia de mantener controles de seguridad actualizados y de fomentar la conciencia sobre los riesgos del IoT para minimizar su impacto en la sociedad.

References

[1] D. Evans, Internet of Things: How the Next Evolution of the Internet Is Changing Everything, Cisco IBSG, 2011.

[2] W. A. Coy Sosa, IoT - El Internet de las Cosas y sus riesgos en los pilares de la seguridad de la información, Universidad Piloto de Colombia, 2020.

[3] Cardenas-Quintero, D., Ropero-Silva, E., Puerto-López, K., Sanchez-Mojica, K., Castro-Casadiego, S., & Ramírez-Mateus, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. Mundo Fesc, 10(19), 162-179.

[4] Cardenas-Quintero, D., Ropero-Silva, E., Puerto-López, K., Sanchez-Mojica, K., Castro-Casadiego, S., & Ramírez-Mateus, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. Mundo Fesc, 10(19), 162-179

[5] Ezelf, CVE-2018-9995 DVR Credentials Exploit Script. [Online]. Available: https://github.com/ezelf/CVE-2018-9995_dvr_credentials

[6] R. Biderbost, "CVE-2018-9995 DVR Credentials Bypass Vulnerability - Exploit Demonstration," YouTube, 10-Jul-2018. [Online]. Available: https://www.youtube.com/watch?v=0El37ceehYs&ab_channel=RogerBiderbost