CIBERSEGURIDAD EN ENTORNOS DOMÓTICOS E IoT

INDICE

1-INTRODUCCIÓN

Actualmente (2023) existe unos 50 mil millones de dispositivos IoT en todo el mundo y eso sin tener en cuenta el despliegue de las redes 5G que son capaces de soportar 1 millón de dispositivos conectados por cada km cuadrado de cobertura. El auge de los dispositivos conectados a internet y el aumento en la capacidad de las redes de transmisión ha multiplicado el uso de "cosas" conectadas a la red. Dispositivos de todo tipo facilitan la vida del ser humano y están integrados en todos los sectores de la sociedad.

Pero este progreso también ha favorecido el aumento de riesgos que comprometen la privacidad y también la seguridad del usuario. El índice de ciberataques a todo dispositivo que se encuentre conectado a la red o con un acceso inalámbrico activado crece de forma exponencial cada año.

Según el último informe del Check Point Research, (proveedor líder de soluciones de ciberseguridad para gobiernos y empresas corporativas de todo el mundo) los ciberataques en España el primer trimestre de 2023 se cifraba en unos 1248 por semana. Si segmentamos el objetivo de los ataques a nivel mundial, obtenemos los siguientes datos:

-El sector de Educación/Investigación fue el más afectado en número de incidencias, con una media de 2.507 ataques por organización a la semana.

-El sector Gubernamental/Militar fue el segundo más atacado con 1.725 ataques por semana

- Se registra un aumento significativo del sector de la Salud, en el que se alcanzó un promedio de 1.684 ataques semanales.

Por su parte en el sector del IoT se ha detectado un aumento alarmante en el número de ciberataques y los datos en el primer semestre de 2023 indican que a nivel mundial el volumen de malware experimentó un aumento del 2% a nivel mundial. Sin embargo, la cantidad de ataques de malware de IoT se incrementó un 87%. Es precisamente el malware el principal sistema de ataque a dispositivos IoT. De cara a poder implementar una protección adecuada a dichos ataques, es importante conocer cuáles son los principales tipos de ataques a los que se encuentran expuestos los dispositivos.

2- COMPONENTES IoT

Los componentes típicos de un proyecto IoT son:

1- Sensores y actuadores

Existen multitud de sensores y dispositivos IoT; sensores de humedad, temperatura, luz, enchufes inteligentes, bombillas.

2- Aplicación móvil

Los sistemas IoT acostumbran a disponer de una aplicación móvil que permite gestionar y visualizar el estado de la instalación desde aplicaciones proporcionadas por el fabricante de un dispositivo, como alarmas, bombillas o enchufes inteligentes, hasta desarrollos mucho más complejos.

3- Protocolos de comunicaciones en red

Los sistemas IoT utilizan diferentes protocolos de comunicaciones, que podemos agrupar en las siguientes tipologías:

- TCP/IP
- Radio corto alcance: NFC, RFID, Bluetooth, BLE.

  Se utilizan en aplicaciones en las que los dispositivos comunican a corta distancia; relojes inteligentes, dispositivos médicos como bombas de insulina etc.
- Radio largo alcance: LoRa, LoRaWAN, Sigfox.

  Se utilizan en aplicaciones en las que los dispositivos comunican a gran distancia;

4- Plataformas Cloud

Existen diferentes plataformas en la nube en la que desarrollar aplicaciones IoT. Los protocolos más extendidos para comunicar los dispositivos con las diferentes plataformas son MQTT y HTTP

3-DOMOTICA VERSUS IoT

La domótica puede considerarse como el conjunto **de sistemas inteligentes usados para automatizar funciones domesticas** dentro de las casas y que además pueden ser controladas desde un dispositivo interno de la casa como un Smartphone. En este apartado debemos tener en cuenta que el control puede ser realizado a un nivel interno usando por ejemplo bluetooth o desde el exterior del domicilio a través de la red internet siendo aquí donde se produce un solapamiento con el concepto de IoT.

Internet de las Cosas (IoT) prolonga Internet más allá de los ordenadores y los teléfonos inteligentes a una amplia gama de aparatos como electrodomésticos(domótica), procesos industriales y diferentes tipos de entornos como se verá más adelante. Los dispositivos están conectados a internet a través de sensores, actuadores y microprocesadores. El problema surge cuando los electrodomésticos, sensores, o calefacción están conectados a internet, ya que en este punto ya perdemos el control de nuestros datos y por ello a nivel de seguridad, IoT es menos fiable que un entorno domótico que está aislado en nuestro domicilio. Podemos por tanto afirmar que internet de las cosas es una prolongación de la domótica que si bien no es imprescindible si es

muy utilizado por usuarios de todo el mundo que quieren tener el control de sus instalaciones desde fuera del propio entorno doméstico.

Según lo indicado, tanto las instalaciones internas de casas particulares como los edificios e instalaciones de instituciones públicas y privadas presentan mayor vulnerabilidad ante un ciberataque cuando estás son conectadas a la red internet ya sea por medios físicos como cable o fibra o por ondas electromagnéticas mediante conexiones WIFI y/o radio.

4-TIPOLOGIA DE SISTEMAS IoT

Veamos ahora diferentes casos de uso de los sistemas IoT, abarcando este concepto las instalaciones domóticas tal como ya hemos visto. Los ejemplos mostrados a continuación no recogen todas las tipologías posibles sino las más frecuentemente utilizadas.

IoT Industrial

Se trata de aplicaciones IoT destinadas a un entorno industrial y se basan en el uso de nuevas tecnologías como la Inteligencia Artificial, *Machine Learning*, gestión de Big Data o Ciberseguridad. Estas tecnologías pueden servirse de sistemas IoT, empleados para controlar y optimizar los procesos productivos de fábricas dedicadas a diferentes sectores.

IoT Militar

Son aplicaciones IoT empleadas en proyectos, como es el caso de UAV´S (aviones con armamento no tripulados), misiles controlados telemáticamente etc. Algunos de estos proyectos pueden ser empleados posteriormente en aplicaciones industriales o domésticas (por ejemplo, ARPANET derivo posteriormente en INTERNET)

IoT Smart meter

Son aplicaciones IoT que permiten obtener medidas de forma remota de todo tipo, ya sean consumos energéticos (luz, agua) o de otro tipo.

IoT Smart City

Se aplica en todo aquello que tenga que ver con la gestión de recursos y servicios en una ciudad o población. Desde la gestión de residuos urbanos o la gestión de energía y agua hasta los servicios de transporte o gestión del tráfico entre otros.

IoT Smart building

Se aplican en servicios IoT destinados a la gestión y control del equipamiento usado en todo tipo de inmuebles. Desde el estado de la estructura, el consumo y la eficiencia energéticos, el funcionamiento de todos los servicios como ascensores, ventilación

hasta la gestión de la calefacción, las alarmas de incendios o fuego etc. Estas solucionesse pueden encontrar en edificios de administraciones públicas, museos, bibliotecas o instalaciones militares.

IoT Smart Home

También es conocida como Domótica, y está destinada a facilitar las tareas domésticas. Por ejemplo, detectar qué alimentos faltan en el frigorífico y solicitar la compra de estos de forma automática. También bombillas inteligentes o enchufes programables se pueden conectar a la red WiFi doméstica y por tanto ser controlados con el *Smartphone.*

IoT Wearables

Se aplica en todo tipo de dispositivos usados en personas, ya sea con ropa. aparatos médicos o teléfonos móviles. El más extendido es el *Smartphone* que es el núcleo y soporte de casi todo lo que una persona lleva conectado. Dispositivos tales como los *smartwatches* o las *smartbands* se conectan mediante *bluetooth* para obtener la información. Por su parte, las *Smart clothes* (E-*Textiles*) son prendas de ropa con tecnología incrustada con diferentes propósitos.

IoT Connected Car

Están relacionadas con todas las soluciones IoT instaladas en un vehículo y que están orientadas a facilitar la conducción y evitar accidentes. Algunos ejemplos ya en uso son el *park assist* que permite aparcar el vehículo sin tocar el volante, los detectores de sueño o el detector de velocidad máxima superada, por ejemplo.

5- CONCEPTOS BÁSICOS DE CIBERSEGURIDAD[1]

Router: Dispositivo que nos permite conectarnos a Internet en nuestro hogar. Podemos conectar nuestros dispositivos a Internet a través de un cable de red o mediante la conexión wifi.

Cortafuegos: Cuando navegamos por la Red y accedemos a una web, esta se comunica con nuestro equipo para establecer la conexión entre ambos. Las herramientas conocidas como *firewall* o cortafuegos analizan esas conexiones para impedir aquellas que puedan suponer un riesgo para nosotros.

Ingeniería social: Estrategia de engaño que utilizan los ciberdelincuentes para ganarse nuestra confianza y conseguir que compartamos nuestros datos con ellos, como contraseñas o datos de nuestra tarjeta, o que les demos acceso a nuestros

[1] Los conceptos básicos se han obtenido del blog de la página web del INCIBE https://www.incibe.es/ciudadania/blog/conceptos-basicos-de-ciberseguridad-que-debes-conocer

dispositivos.

Cifrado: Proceso que sirve para convertir un documento o un archivo en una versión ilegible para todas aquellas personas que no posean la clave para descifrarlo. Sirve para proteger la información de todas aquellas personas que no deberían acceder a ella bajo ningún concepto.

HTTP/HTTPS: Siglas de los protocolos más utilizados para la navegación por Internet. HTTPS es la versión segura y nos garantiza que la información que se transmite entre nuestro dispositivo y la página web está cifrada y protegida, especialmente en el envío de datos personales, como contraseñas o datos bancarios.

Biometría: Mecanismo para bloquear el acceso a nuestros dispositivos que, en vez de utilizar una contraseña o un patrón, utiliza algún elemento de nuestro cuerpo, como la huella dactilar o nuestro rostro.

6-SEGURIDAD EN IoT

A diferencia de pruebas de seguridad tradicionales, las pruebas de seguridad IoT requieren examinar y desmontar los dispositivos y trabajar con unos protocolos de red que no se encuentran en otros entornos, analizar aplicaciones móviles para controlar dispositivos, y examinar cómo los dispositivos se comunican con los servicios web el en el cloud.

Por otro lado, las restricciones impuestas por la propia tipología del sistema, como el uso de dispositivos pequeños, de bajo coste y bajo consumo aumentan la inseguridad de los mismos. Así, por ejemplo, en lugar de usar criptografía de clave pública, usan claves simétricas[2], ya que consumen menos recursos. Además, estas claves a menudo no son únicas y están grabadas en el firmware o el propio hardware, con lo que los atacantes pueden extraerlas.

Principales vulnerabilidades en dispositivos domóticos/IoT

1. Contraseñas fáciles o grabadas en el propio dispositivo: Mediante ataques de fuerza bruta es posible acceder a los dispositivos.

2. Servicios de red inseguros que se ejecutan en el dispositivo ponen en riesgo la integridad de los datos.

3. Interfaces inseguros Los diferentes interfaces (web, API, cloud, aplicaciones móviles) con las que comunica el dispositivo adolecen en algunos casos de procedimiento de autenticación y /o encriptado inexistente o débil.

4. Mecanismos de actualización inseguros a la hora de actualizar los dispositivos;

[2] Se usa una única clave compartida para cifrar y descifrar mensajes entre el emisor y el receptor. Una vez que ambas partes tienen acceso a esta clave, la remitente cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra con la misma clave.

firmware.

5. Uso de componentes inseguros u obsoletos El uso de estos componentes o librerías pueden comprometer el acceso al sistema.

6. Insuficiente protección de la privacidad al usar datos personales utilizados de manera inadecuada o sin permiso

7. Transferencia de datos y almacenamiento inseguro por falta de encriptado y control de acceso a datos sensibles

8. Falta de gestión del dispositivo por falta de soporte de seguridad.

9. Configuración de fabrica insegura.

10. No se adoptan medidas que puedan evitar o limitar los accesos no autorizados a los dispositivos.

7-TIPOLOGIA DE CIBERATAQUES

Ingeniería social: Los ataques de ingeniería social utilizan el engaño y la suplantación de identidad para inducir a la gente a realizar una acción que beneficie al ciberdelincuente. La ingeniería social no sólo se lleva a cabo mediante métodos digitales. Los ingenieros sociales recurrirán a cualquier táctica para construir las estructuras necesarias para engañar a la gente. Esto puede incluir el uso del teléfono o entrar en una oficina y charlar con el personal. Uno de los métodos más conocidos es el Phishing, el cual se presenta en varios formatos, como el correo electrónico, las llamadas telefónicas, las publicaciones en las redes sociales y los mensajes de texto. Aplicando la simulación, la confianza se anima a los destinatarios a divulgar información personal, como contraseñas y datos de tarjetas de crédito.

Ataques de fuerza bruta: es un intento de descifrar una contraseña o nombre de usuario, o de descubrir la clave utilizada para cifrar un mensaje, que consiste en aplicar el método de prueba y error con la esperanza de dar con la combinación correcta finalmente. En función de la longitud y complejidad de la contraseña, descifrarla puede llevar desde unos segundos hasta varios años. Algunos hackers tienen los mismos sistemas como objetivo a diario durante meses e, incluso, años.

Los diccionarios son la herramienta básica. Se pueden usar diccionarios íntegros y ampliar palabras con ayuda de caracteres especiales y números. En un ataque estándar, un hacker elige un destino y combina posibles contraseñas con el nombre de usuario seleccionado. A este tipo de ataques se les denomina ataques de diccionario.

Existe una variante que es el ataque de fuerza bruta inverso que consiste en invertir la estrategia de ataque, comenzando con una contraseña conocida (como las contraseñas filtradas disponibles en línea) y buscando millones de usuarios hasta que se encuentra

una coincidencia. También hay disponibles algunas herramientas automatizadas que pueden ayudar en los ataques de fuerza bruta, como Brutus, Medusa, Ncrack etcétera.

MitM: Man-in-the-Middle ("hombre en el medio"), es un tipo de ataque destinado a interceptar, sin autorización, la comunicación entre dos dispositivos conectados a una red. Este ataque le permite manipular el tráfico interceptado de diferentes formas, ya sea para escuchar la comunicación y obtener información sensible, como credenciales de acceso o para suplantar la identidad de alguna de las partes. Para que un ataque MitM funcione correctamente, el delincuente debe asegurarse que será el único punto de comunicación entre los dos dispositivos, es decir, el delincuente debe estar presente en la misma red.

Botnets: Se trata de una red de robots que los atacantes ponen en marcha utilizando malware para secuestrar una red de dispositivos. De esta forma, los ciberdelincuentes consiguen controlar los dispositivos desde un solo punto desde el que lanzar ciberataques. Algunos dispositivos como routers y especialmente los que forman parte del IoT suelen contar con configuraciones poco seguras, así como, con contraseñas débiles. Estas configuraciones débiles son usadas por los ciberdelincuentes para obtener acceso al dispositivo y convertirlo en parte de la *botnet*.

DDoS: o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente. El atacante sobrecarga su objetivo con tráfico de Internet no deseado para que el tráfico normal no llegue a su destino previsto. Durante un ataque DDoS, los atacantes utilizan una gran cantidad de equipos infectados, incluidos dispositivos del Internet de las cosas (IoT), además de ordenadores personales y servidores de red, para enviar una gran cantidad de tráfico a sus objetivos.

8-PROTECCIÓN ANTE CIBERATAQUES

Administración del dispositivo: Utilizar usuario y contraseña, y siempre que sea posible, habilitar un segundo factor de autenticación (por ejemplo, biometría).

No usar nombres de usuario genéricos, como root, administrador, admin etcétera ni tu propio nombre o el de familiares. Para establecer una contraseña robusta, esta debe contar al menos con ocho caracteres como mínimo e incluir mayúsculas, minúsculas, números y símbolos, teniendo siempre en cuenta que cuanto más larga sea la contraseña más difícil será desbloquearla. En caso de utilizar acceso desde app móvil, descargarla de repositorios oficiales y siempre mantenerla actualizada a la última versión disponible.

Gestión de los dispositivos: Implementar canales seguros de comunicación para cifrar la información que se envía y recibe desde el dispositivo IoT; por ejemplo, cuando se utilice el navegador web se verificará que el protocolo es “https”.

Aplicar las últimas actualizaciones y parches de seguridad tan pronto como sea posible. Los dispositivos IoT deben estar actualizados y recibir actualizaciones de software igual que un ordenador o un teléfono móvil. Es recomendable comprobar regularmente la web del fabricante del dispositivo para verificar si se está utilizando la última versión de software.

Protección de Router y ordenadores de control: El router en nuestro domicilio o centro de trabajo, es el principal punto de acceso inalámbrico para un posible atacante ya que accediendo al mismo puede acceder a cualquier dispositivo domótico u ordenador que tengamos conectado a nuestra red. Se deben usar cortafuegos que filtre las conexiones que se establecen desde y hacia el dispositivo y siempre que sea posible, se deben desactivar las funciones de administración a través de Internet.

La seguridad física del dispositivo también debe tenerse en cuenta. Por ello, se deben implementar medidas que eviten robos o modificaciones fraudulentas.

Formación y concienciación: Los usuarios que gestionan y utilizan los dispositivos IoT deben estar formados en materia de ciberseguridad para evitar situaciones que puedan poner en riesgo la seguridad de los dispositivos. Es frecuente cometer graves imprudencias por dejadez y desconocimiento lo cual derivará en un fallo de seguridad que cualquier ciberdelincuente puede aprovechar. Todos hemos sido alguna vez víctimas de intentos de estafa cibernética ya sea por mensaje corto, correo, llamada etcétera y por ello es necesario no bajar nunca la guardia y estar al día en lo concerniente a seguridad informática y nuevas amenazas.

9-FIREWALL WINDOWS

Un firewall nos permite permitir o denegar el tráfico que va y viene desde una o varias interfaces de red, podremos controlar el tráfico de forma exhaustiva, porque el firewall se encarga de comprobar la cabecera de todos los paquetes para ver si cumple con las reglas definidas en el sistema. El sistema operativo Windows 10 dispone de un firewall bastante avanzado que nos permitirá crear reglas con el objetivo de permitir o bloquear cierto tráfico, de esta forma, podremos controlar todas las conexiones entrantes y salientes en detalle.

- **Control de entrada y salida:** El firewall de Windows 10, cuenta con funciones que permiten definir reglas de entrada y salida para controlar el tráfico de entrada y salida, desde el propio equipo.

- **Filtrado de paquetes:** Este firewall se utiliza para realizar un filtrado a los paquetes. Este los puede bloquear si es necesario, siempre basándose en los

criterios que define el usuario. Tales como la dirección IP, los protocolos y los puertos.

- **Monitorización:** El firewall de Windows 10 puede realizar una monitorización de la actividad en línea, y así poder generar informes sobre los eventos de seguridad. Esto nos permite identificar y solucionar los problemas de seguridad, de una forma más efectiva.
- **Protección de red pública:** El firewall puede detectar y proteger las redes públicas de forma automática. Esto quiere decir, que puede configurarse para bloquear todos los accesos que no están autorizados a los servicios del equipo.

10- PRÁCTICAS BÁSICAS Y AVANZADAS

ESCANEO DE REDES WIFI

El propósito del desarrollo de WPA (Wi-Fi Protected Access) fue corregir los errores de seguridad que presenta WEP (Wired Equivalent Privacy es decir Privacidad equivalente a cableada). En este sentido WPA incorpora mejoras tanto en la autenticación como en la encriptación. Aunque no se han reportado a la fecha vulnerabilidades a nivel del protocolo, existen esquemas que permiten bajo ciertas condiciones romper la seguridad de una red inalámbrica con WPA/WPA2. Por ejemplo, a través de la explotación del protocolo TKIP (Temporal Key Integrity Protocol) y de una característica denominada WiFi Protected Setup que se usa para facilitar la autenticación automática de dispositivos a la red wireless. Para corregir estos temas y mejorar la seguridad surgió posteriormente la versión 2 de WPA o también llamado WPA2.

Aun así, es factible utilizar un ataque de claves de fuerza bruta, basado en diccionario, o híbrido sobre la red objetivo. Por supuesto, el éxito de la misión y el tiempo que tome ejecutar el ataque dependerá de la longitud de la clave y de si ésta está o no basada en criterios de complejidad

Práctica 1: Mapeando WLANs con el CMD

El objetivo de esta práctica es demostrar que con cualquier PC domestico o portátil podemos hacer un rastreo de redes WIFI disponibles obteniendo su SSID y tipo de cifrado para saber si existe alguna red abierta por descuido del usuario (con la primera línea de comandos) o una información más detallada que incluye canal de radio y fuerza de señal o tipo de radio (segunda línea de comandos)

1. Usaremos un ordenador con sistema operativo Windows y el comando netsh incluido con Windows.

2. Abrimos una línea de comandos con Cmd y ejecutamos uno de los siguientes comandos:

netsh wlan show networks mode=ssid

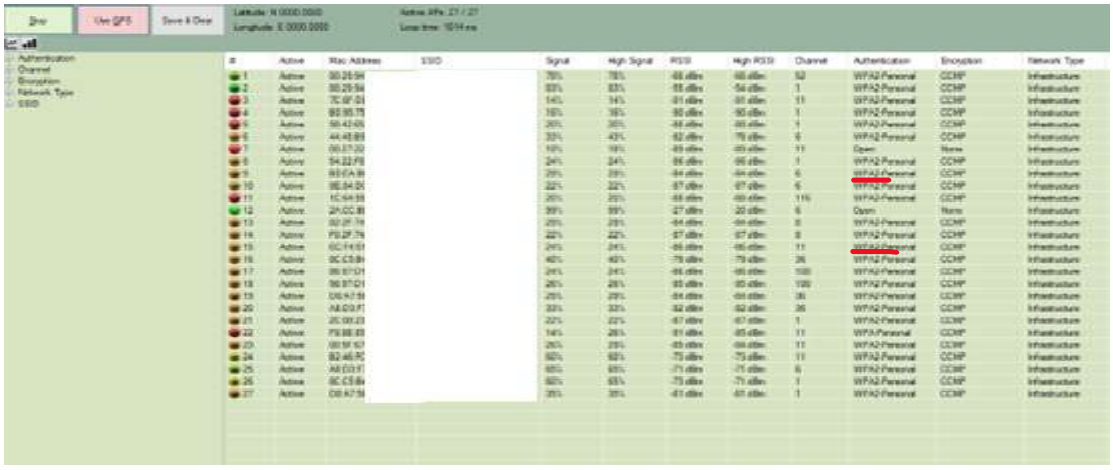
netsh wlan show networks mode=bssid

Tal como puede verse en la imagen adjunta se ha obtenido información valiosa para el control de la vulnerabilidad, incluida una red que no está protegida.

Práctica 2 : Mapeando WLANs con Vistumbler desde Windows

El objetivo de esta práctica es similar a la anterior, pero usando un programa de distribución gratuita que corre sobre Windows y que presenta una interfaz de usuario mucho más sencilla y entendible.

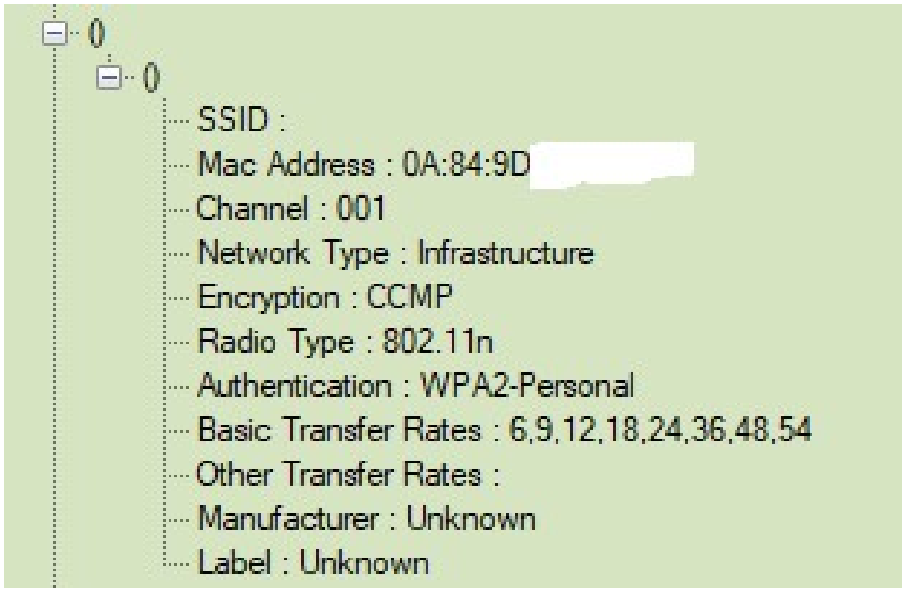
En la siguiente imagen se ha realizado un escaneo donde se han detectado dos redes abiertas y sin protección (subrayado en rojo). Se han borrado datos de SSID de todos de usuarios y parte de su MAC..



Si quisiéramos obtener más información de alguna red podemos realizar filtros en la columna izquierda y también usar el menú de herramientas del programa.

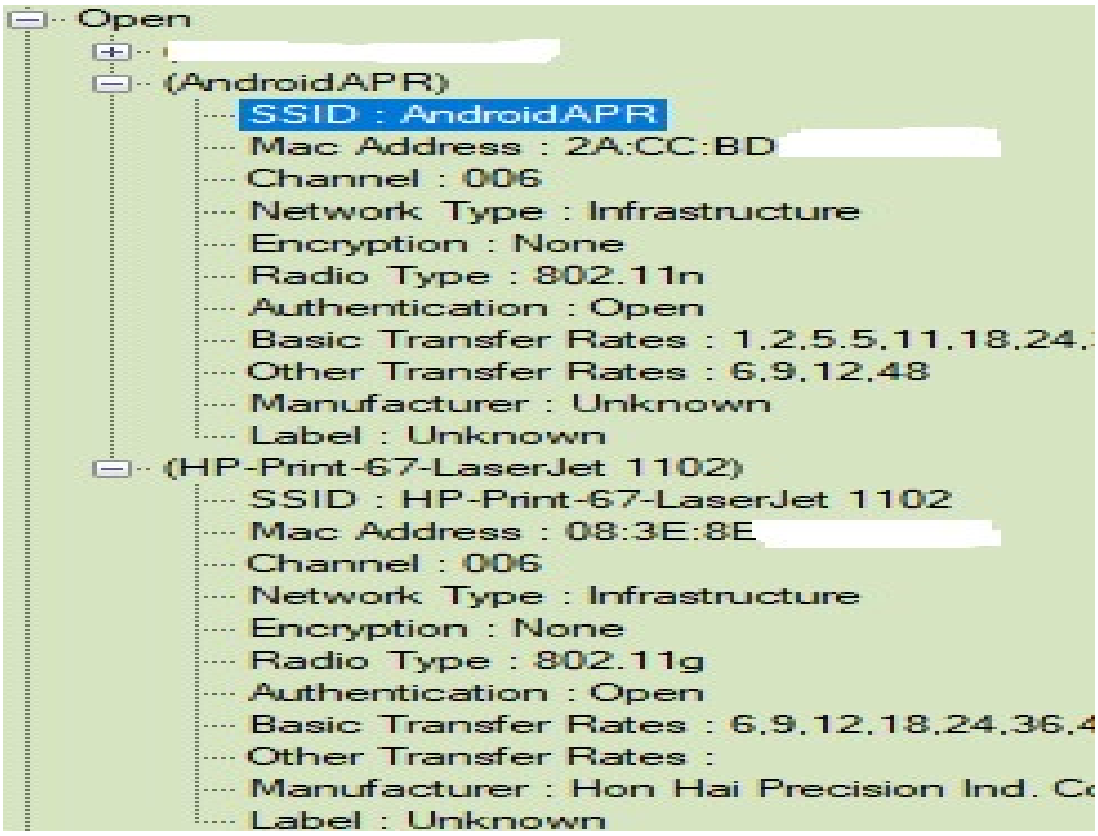
Vamos a realizar un filtro de las redes abiertas para obtener todos los datos relativos a dichas redes tal como se muestra en la siguiente imagen. En la parte izquierda he obtenido información detallada de una de las redes abiertas (realizado sobre mi propio móvil como ejemplo).

En la siguiente captura vamos a obtener información de una red que tiene oculto su SSID y a pesar de todo es detectada y de la cual se obtiene también su información básica como el número de MAC (parcialmente borrado).



En la última captura y como ejemplo del peligro que supone dejar dispositivos en red sin contraseña, se muestra el mapeo de una impresora que se encuentra conectada a una red internet sin protección. Un posible atacante podría acceder y ordenar hacer copias sin fin, por poner un ejemplo.

En el detalle puede observarse que se está aplicando el filtro “open”, es decir el de redes sin contraseña. Al tener acceso a su MAC se podría realizar un ataque de desautenticación (ataque Karma)



MORALEJA: Tras la realización de las dos primeras prácticas podemos concluir que es muy recomendable usar siempre cifrados WAP2 en nuestros dispositivos, ya sean ordenadores portátiles, tablets, móviles, routers o módulos IoT y utilizar claves robustas de al menos 8 caracteres que use una combinación de números, símbolos y letras mayúsculas y minúsculas.

La segunda recomendación es no dejar NUNCA activado por defecto el WIFI ni el Bluethoot de nuestros dispositivos (portátiles, móviles, tablets) salvo que los necesitemos, ya que son una puerta abierta a un posible ataque.

PROTECIÓN DE CONTRASEÑAS

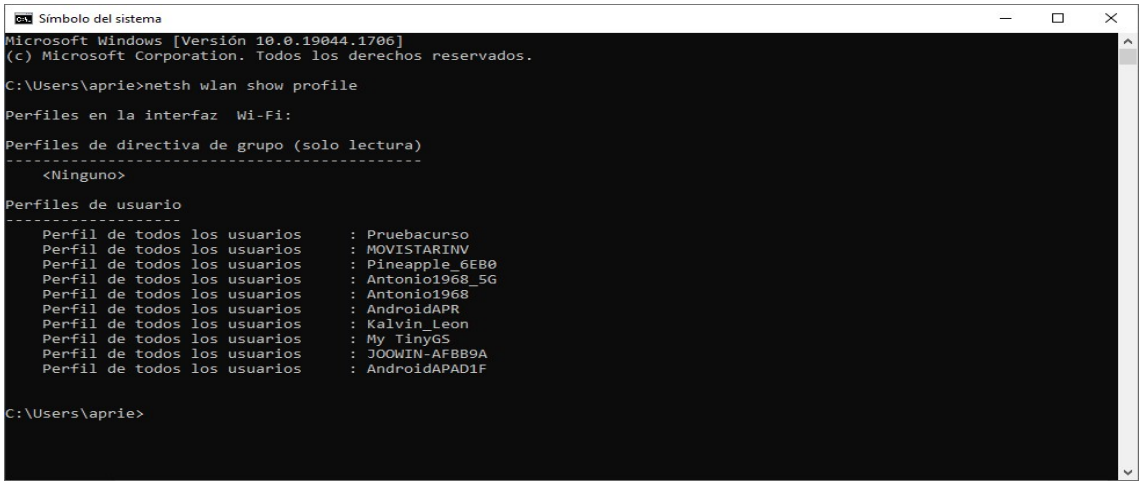
Práctica 3: Recuperando contraseñas WIFI en Windows

El objetivo de esta práctica es concienciar sobre el riesgo de usar ordenadores compartidos en el centro de trabajo o en nuestros domicilios particulares cuando nos llevamos trabajo a casa. Al ser equipos que pasan por muchas “manos” se debe prestar especial atención a la seguridad y protección de nuestras contraseñas.

En la práctica usaremos nuevamente el Cmd y el comando netsh para recuperar contraseñas que han sido usadas en el acceso a cualquiera de las redes WIFI con las que nuestro equipo se ha conectado. De esta forma lo que es un comando útil en caso de que nosotros nos olvidemos de la contraseña de

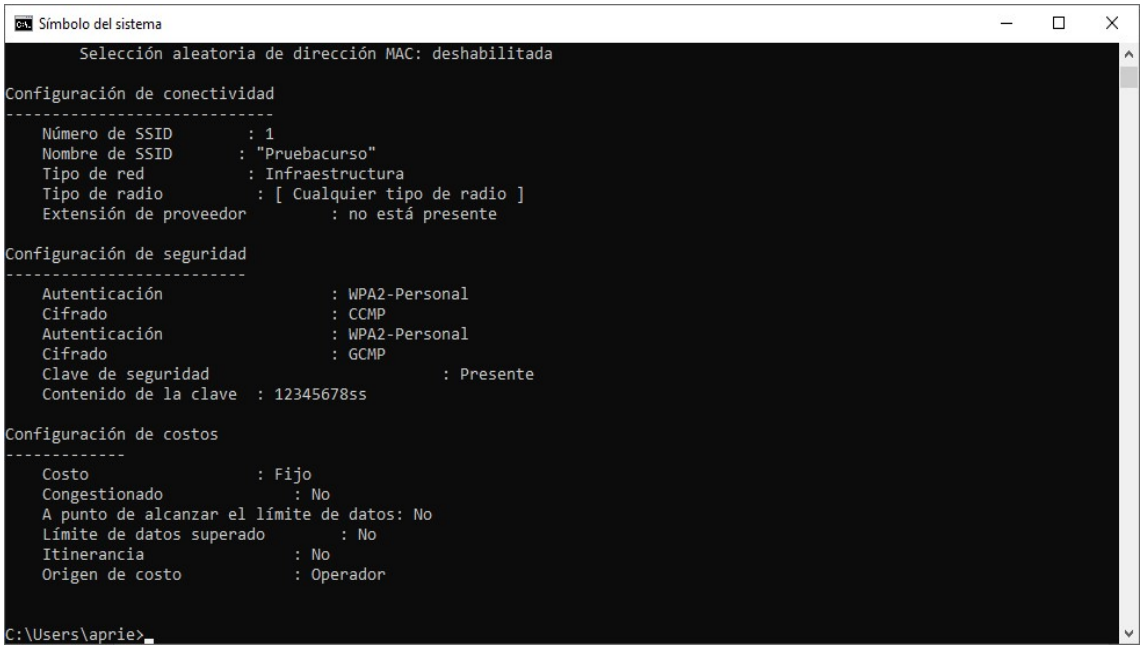
conexión, se convierte en un verdadero peligro para quien quiera usarlo con fines de hackeo.

1-Despues de abrir CMD teclear: netsh wlan show profile



2- Seleccionamos red y tecleamos: netsh wlan show profile name=”Nombre perfil” key=clear

Ejemplo: netsh wlan show profile name=”Pruebacurso” key=clear



Se puede ver claramente que el comando ha recuperado la contraseña usada en la red” Pruebacurso”. Si esta red fuese la de tu domicilio la clave quedaría totalmente expuesta.

MORALEJA: Siempre que uses dispositivos compartidos con terceros o en tu entorno laboral borra cualquier huella de contraseña y/o redes WIFI que hayas utilizado para la conexión a internet.

Como eliminar huella de conexiones WIFI en Windows 10

A continuación, se indican dos procedimientos para borrar conexiones WIFI desde entornos Windows. Para el resto de los sistemas operativos como Linux, Android o MacOS se usan procedimientos similares.

1. Hacer clic en el botón derecho en icono de la esquina inferior izquierda de la pantalla.
2. Entrar en opción de configuración y luego en opción Red e Internet
3. Después entramos en la opción WIFI y luego en administrar redes conocidas como en la imagen adjunta

4. Seleccionamos la red que queremos borrar y pulsamos en la opción “dejar de recordar”.

5. También podemos hacerlo desde el cmd con el comando nesth. Si usamos la res del ejemplo anterior el comando seria como sigue:

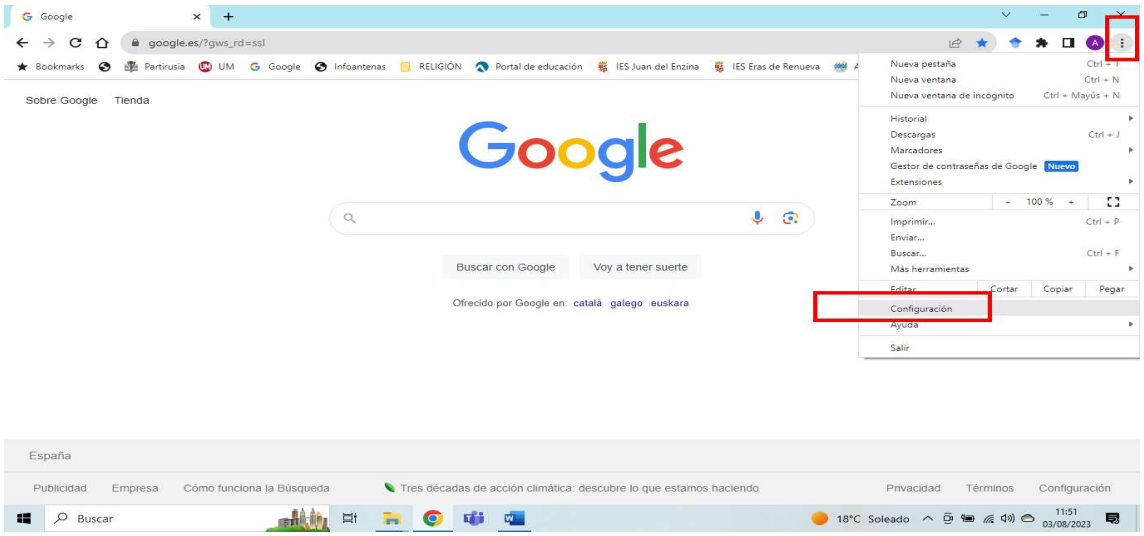
netsh wlan delete profile name="AndroidAP8033"

Práctica 4: Obteniendo contraseñas guardadas en navegador Chrome

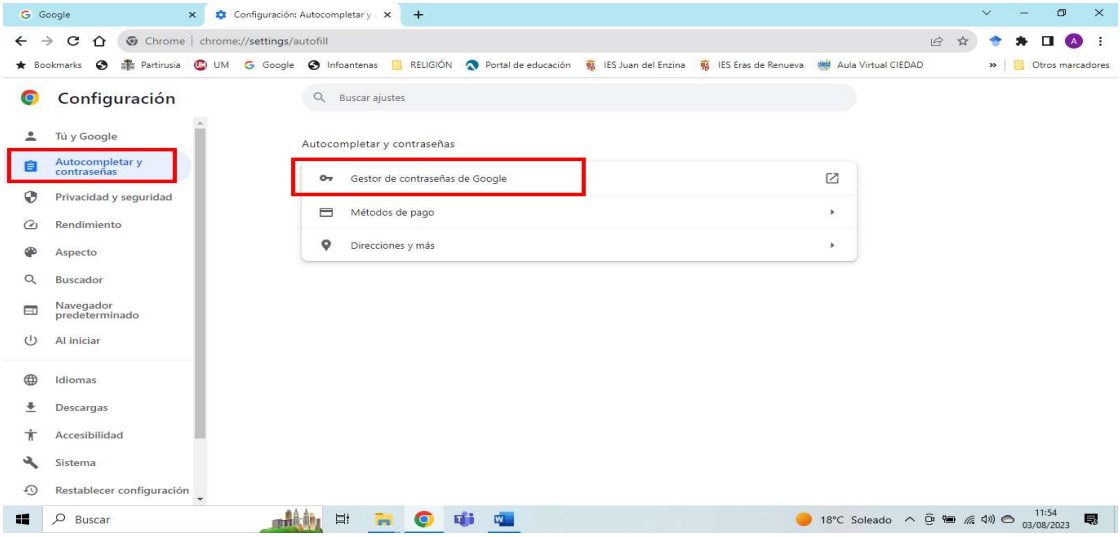
Una práctica muy común y que supone un riesgo añadido en nuestra seguridad informática, es la opción de "recordar contraseña" que nos ofrece el sistema operativo una vez nos hemos identificado con login y contraseña en un portal web por ejemplo. Si el ordenador es compartido, como en el ejemplo anterior, las claves pueden recuperarse con facilidad en caso de que no existan perfiles de usuario para el acceso mediante PIN o contraseña.

Se realizará el ejemplo sobre el navegador Chrome que es uno de los más habituales pero el resto de los navegadores tienen opciones similares.

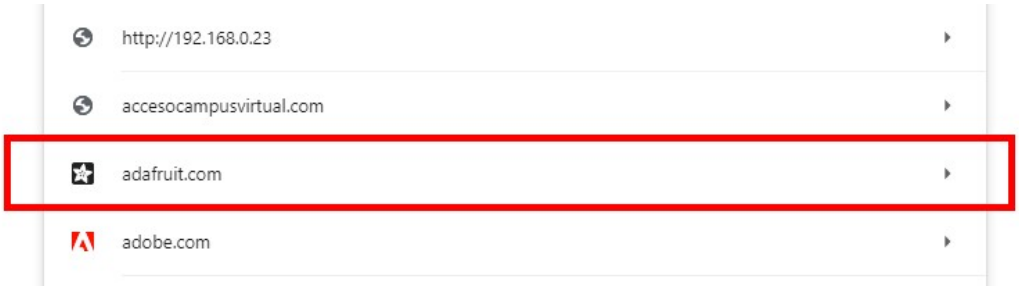
1. Accedemos a la configuración del navegador según se muestra en pantalla en los tres puntos de la esquina superior izquierda y luego entrando en configuración.



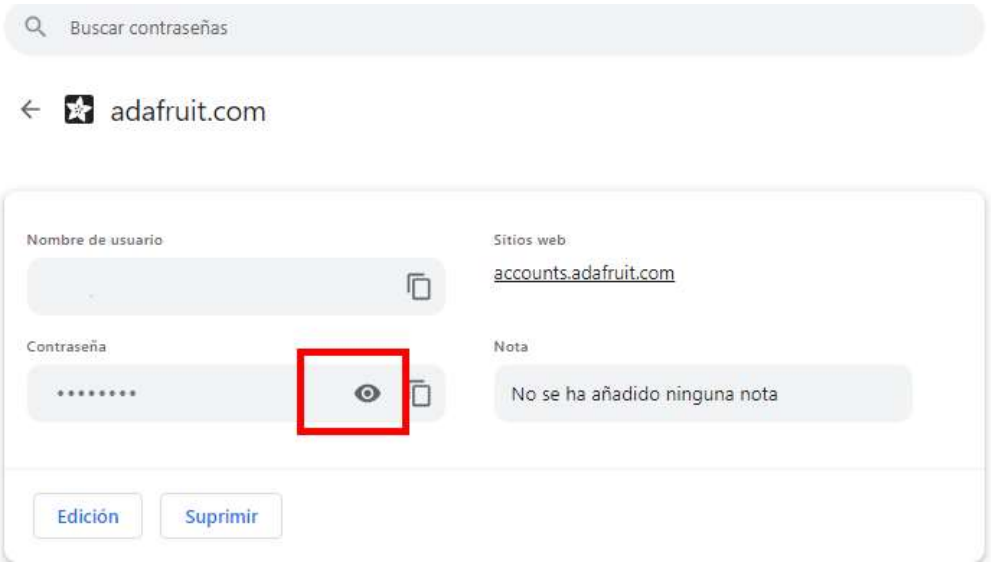
2. Después entramos en auto completar contraseñas y a la derecha en gestor de contraseñas de Google



3. Se mostrará un desplegable de todos aquellos lugares donde nos hemos conectado con clave. En mi caso he seleccionado la plataforma de control Iot mediante protocolo MQTT de Adafruit que es la que me da acceso a todo el control domótico de mi domicilio.



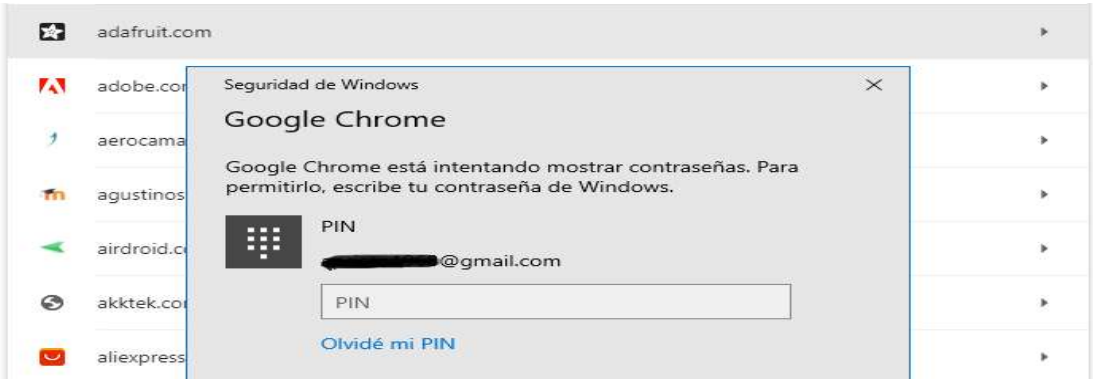
4. Al entrar veríamos nuestro nombre de usuario (en mi caso lo he borrado en la imagen por seguridad) y si pulsamos en el icono del OJO, tendríamos acceso a la contraseña de la plataforma tal como se puede ver aunque en mi caso no la muestro ya que es un ejemplo real.



MORALEJA: NUNCA utilices la opción de "recordar contraseña" en ordenadores compartidos y si es posible, tampoco en el ordenador de tú domicilio.

Además, todos los accesos al sistema operativo deben ser mediante PIN o contraseña, lo cual dificulta en gran medida el acceso a nuestras claves.

Siguiendo con el ejemplo anterior, sí yo tengo configurado un PIN para acceder a mi portátil o a mi cuenta de usuario, al intentar acceder a la misma plataforma Iot, el resultado sería que el navegador me pide dicho PIN para acceder a los datos, tal como podemos comprobar en la siguiente imagen:



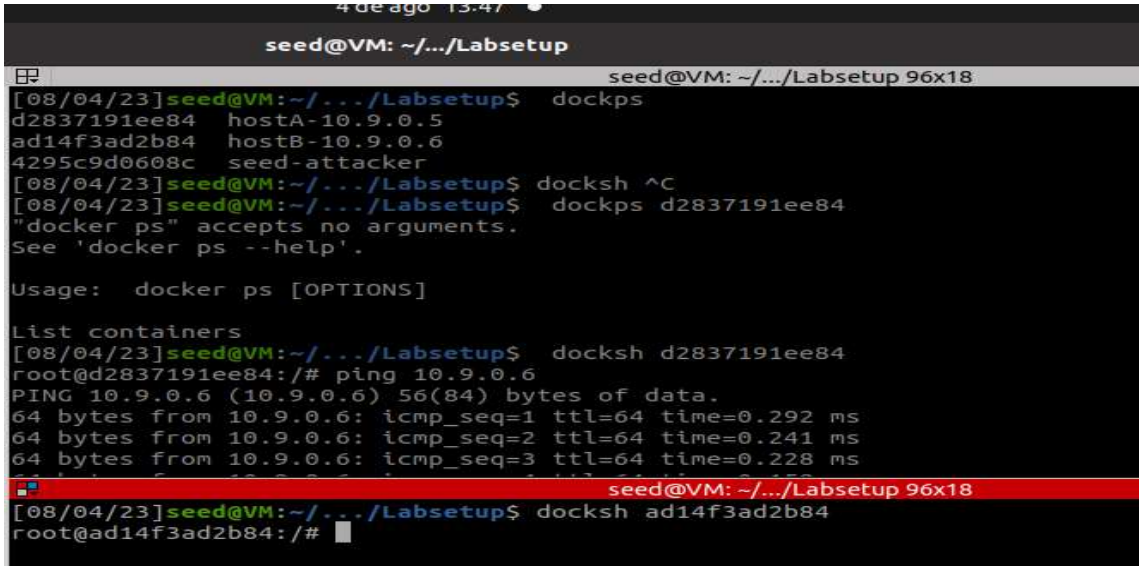
PRÁCTICAS AVANZADAS

Las prácticas avanzadas se realizarán y explicaran por el profesor durante el desarrollo del curso por lo que en este manual solo se dan unas breves pinceladas.

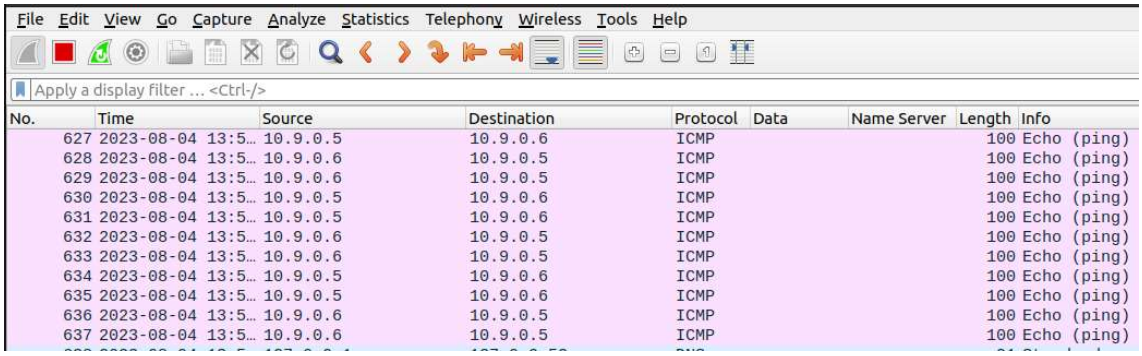
Práctica 5: MitM(Man-in-the-Middle)

El objetivo de la práctica es simular que disponemos de dos ordenadores virtuales que se comunican entre sí. Para ello usaremos una máquina virtual sobre entorno Linux. Un posible atacante ha conseguido acceder a la misma red y está “esnifando” datos de la comunicación entre usuarios.

En la imagen adjunta se puede comprobar que hemos creados dos hosts (A y B) con direcciones IP diferentes y se ha realizado un ping entre uno y otro para comprobar que tenemos comunicación. Como se aprecia, el host destino está contestando.

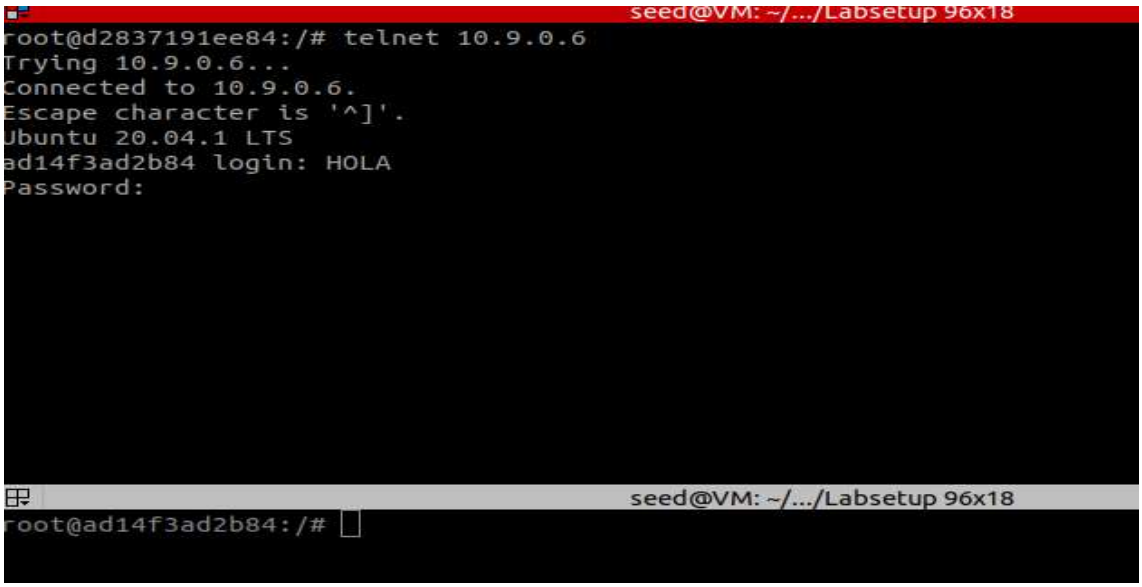


Para poder interceptar el trafico de datos entre host, usamos uno de los múltiples programas destinados a tal fin y obtenemos el intercambio de ping entre el host A y el host B tal como se puede apreciar en la imagen adjunta.

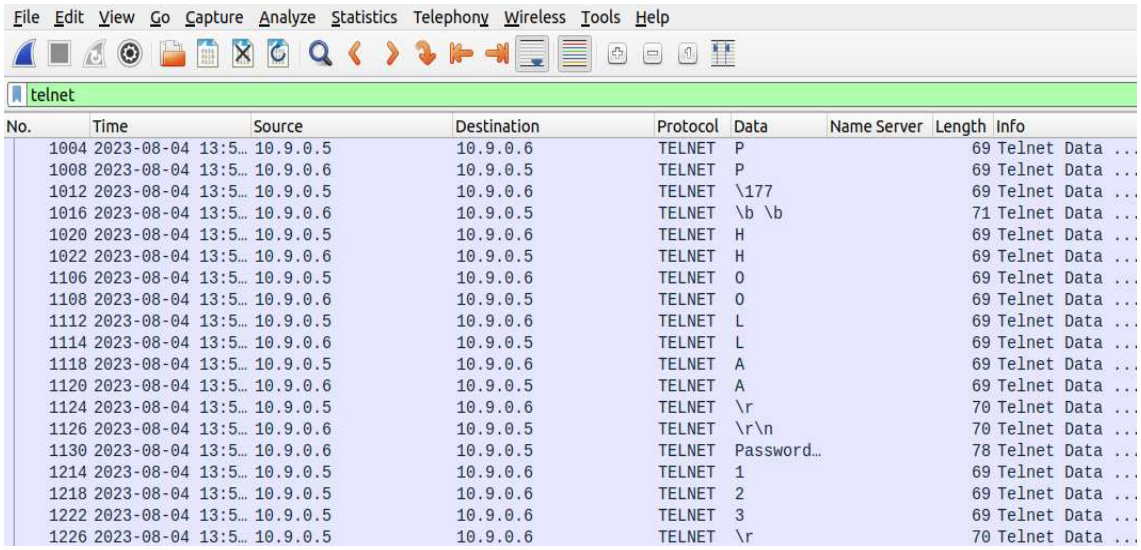


Realizamos una segunda prueba donde realizamos una conexión telnet entre el host A y el host B. Al realizar dicha conexión se nos pedirá un password y una contraseña. En la imagen siguiente puede comprobarse dicha operación entre los hosts virtuales. El

password usado no puede verse ya que el entorno Linux no muestra las contraseñas al teclearlas, pero para este ejemplo hemos usado el siguiente “1 2 3”.



Usando de nuevo el programa sniffer, obtenemos el login (HOLA) y el password (1 2 3) tal como puede apreciarse en la imagen.



MORALEJA: Además de las ya recomendadas, usar siempre protocolos de comunicaciones seguros. El protocolo de intercambio de ficheros Telnet sigue usándose hoy día a pesar de su vulnerabilidad. En su lugar usar un protocolo seguro como SSH (Secure SHell) que es un protocolo de red destinado principalmente a la conexión con máquinas a las que accedemos por la línea de comandos.

Práctica 6: Ataque de desautenticación

El objetivo de la práctica es demostrar que un ciberdelincuente con un dispositivo de bajo coste puede realizar un ataque que desconecte nuestros dispositivos de la red

legítima para luego forzar una conexión a un punto de acceso simulado con conexión a internet que pasaría por dicho dispositivo. En ese momento ya estaríamos en las manos del atacante, ya sea con nuestro móvil, portátil o dispositivo IoT con conexión a internet. EL procedimiento que usan es el siguiente:

1- Escaneo de las redes WIFI de su entorno
2- Captura de los SSID de la victima
3- Selección de la MAC de la víctima y ataque de desautenticación
4- Difusión falsa de las SSID usadas por la victima hasta lograr conexión
5- Uso de programas sniffer para obtener datos

Se muestra una pantalla de ejemplo del entorno de trabajo sin desarrollar. La práctica se realizará en directo durante la impartición del curso.