UT 1. Ejercicios

1. Se pueden identificar las amenazas, además de cómo se explicó en clase, según los tipos de atacantes o según cómo actúan estos ataques. Completa siguientes tablas, con las definiciones de los tipos de atacantes y los ataques. Puedes añadir alguna más.

Atacante	**DEFINICIÓN**
Hacker	Es una persona capaz de detectar y explotar las vulnerabilidades de un sistema informático, normalmente, son expertos y profesionales en el mundo de la informática
Cracker	Usuario avanzado que utiliza sus conocimientos para acceder a sistemas de forma ilegal, descifrando claves y contraseñas de programas, desde robo de datos hasta simple pirateo de programas, son considerados como vándalos virtuales.
Phreaker	Es una persona que se orienta al hackeo de sistemas telefónicos, puede ser telefonía fija o de móviles, uno de sus retos es conocer la gran mayoría de sistemas telefónicos
Sniffer	Aquel que se dedica a la monitorización del tráfico en Internet en tiempo real. Utilizan programas para espiar y seguir la actividad en Internet de la víctima. Puede haber desde programas especializados hasta propio Hardware utilizado para tal.
Lammer	En Internet los “Lamers” son aquellos usuarios que presumen de tener conocimientos o habilidades sobre la informática, pero no tienen ni conocimientos ni habilidades, como mucho, conocen algunos programas básicos.
Newbie	Usuario novato en el mundo de la informática o ciber informática, conocidos coloquialmente como “noobs”.
Ciberterrorista	Persona o grupo de personas que utilizan sus conocimientos para causar terror a personas o gobiernos con fines económicos, religiosos o políticos.
Carder	Usuario que utiliza sus conocimientos para robar información de la tarjeta bancaria de la víctima. Pueden utilizar programas informáticos desde Internet e incluso la línea telefónica.

Ataque	DEFINICIÓN
Spoofing	Es la suplantación de identidad con el objetivo de hacerse pasar por otra persona en Internet y robar información privada o acceder a páginas con una identidad falsa.
Sniffing	Es una técnica utilizada para ver todo lo que ocurre en una red con el fin de acceder y obtener la información de la red.
Malware	Es software peligroso, desde un programa informático hasta un código malicioso, normalmente, con el fin de dañar o deshabilitar los ordenadores o los sistemas informáticos de una instalación.
Keylogger	Puede ser desde un software hasta un hardware dedicado a registrar todas las pulsaciones de un teclado para posteriormente guardarlo en un archivo, utilizado para mostrar al dueño del software las pulsaciones de la víctima. Muy usado para robar contraseñas.
Ingenieria Social	Es una técnica utilizada para obtener a través de la manipulación de los usuarios, información ya sea de acceso o permisos en sistemas informáticos que pueden afectar a terceros. Normalmente se utiliza teléfono o Internet para engañar.
Phising	Es una técnica muy común para obtener información de usuarios “newbies”. Con uso de programas se envía mensajes con propaganda o sitios web falsos, en la que estos usuarios “newbies” dejan su información.

2. El **INCIBE Instituto Nacional de Ciberseguridad** es un organismo dependiente del Ministerio de Economía a través de la Secretaría de Estado para el Avance Digital. Es la entidad de referencia en el desarrollo de la ciberseguridad y la confianza digital de ciudadanos y empresa.

Buscar información sobre avisos de seguridad relativos a:

a. Phising

Incibe nos informa sobre varios ataques phishing; suplantaciones a Abanca, Correos, Ruralvía, etc.

b. Ingenieria Social

Se utilizan programas para enviar información falsa de sitios webs que parecen oficiales pero son fraudulentos.

Recopilar la siguiente información de los avisos:

- **Fecha Publicación;**

Abanca – 15/09/2020
Correos – 14/09/2020
Ruralvía – 04/09/2020

- **Recursos Afectados:**

Abanca – Cualquier empleado, autónomo o empresa cliente de Abanca
Correos – Cualquier empleado, autónomo o empresa que reciba un correo suplantando una identidad.
Ruralvía - Cualquier empleado, autónomo o empresa que sea cliente de Ruralvía

- **Breve Descripción:**

Abanca – Envío de correos fraudulentos (phishing)
Correos - Envío de correos fraudulentos (phishing)
Ruralvía - Envío de correos fraudulentos (phishing)

- **Solución:**

Abanca – Ignorar el correo que intenta hacer un fraude.
Correos – Ignorar el correo que intenta hacer un fraude.
Ruralvía - Ignorar el correo que intenta hacer un fraude.

3. **Microsoft tiene una web sobre seguridad Microsoft Security Response Center, cuya misión es investigar todos las vulnerabilidades de seguridad en productos y servicios Microsoft.**

   Accede a la web de MSRC y localiza la sección donde se publican boletines en los que se informa de vulnerabilidades de Microsoft.

https://www.microsoft.com/en-us/msrc?rtc=1

https://msrc.microsoft.com/update-guide/vulnerability

https://portal.msrc.microsoft.com/en-us/security-guidance

   a. **Buscar un boletín reciente y analizar una vulnerabilidad *Crítica*, una *Importante* y una *Baja*, analizando los siguientes puntos:**

A continuación añado tablas con información sobre los boletines.

Vulnerabilidad baja	
Nombre de la vulnerabilidad:	MITRE CBE-2020-1012
Fecha de publicación	09/08/2020
Descripción de la vulnerabilidad	Existe una vulnerabilidad en los privilegios del archivo Winidit.dll y como maneja el uso de la memoria, desde este archivo se pueden ejecutar códigos con permisos superiores.
Impacto en el aula	Podría convencer a un alumno para desacargar un archivo externo que podría ocasionar problemas en el equipo
Medidas para solucionar la vulnerabilidad	Una actualización corrige este problema

Vulnerabilidad Importante	
Nombre de la vulnerabilidad:	MITRE CBE-2020-1180
Fecha de publicación	08/09/2020
Descripción de la vulnerabilidad	Vulnerabilidad remota de un código basado en el motor de scripting ChakraCore.El atacante puede obtener permisos superiores aprovechando esta vulnerabilidad
Impacto en el aula	El usuario que ha utilizado la vulnerabilidad puede acceder a otro equipo con permisos superiores y toma el control del equipo
Medidas para solucionar la vulnerabilidad	Una actualización corrige este problema

Vulnerabilidad Crítica	
Nombre de la vulnerabilidad:	MITRE CBE-2020-1452
Fecha de publicación	09/09/2020
Descripción de la vulnerabilidad	Existe una vulnerabilidad en la ejecución de un código en Microsoft SharePoint. El atacante podría acceder a las cuentas de los servidores SharePoint
Impacto en el aula	Podría conseguir información de de los alumnos que utilicen este programa
Medidas para solucionar la vulnerabilidad	Una actualización corrige este problema

b. **Buscar una vulnerabilidad *Importante* para Microsoft Excel 2016 (64-bit edition) que se haya producido en el año 2017. Indicando los mismos puntos del apartado anterior.**

Vulnerabilidad Importante	
Nombre de la vulnerabilidad:	Archivo malware
Fecha de publicación	27/02/2017
Descripción de la vulnerabilidad	El atacante puede ejecutar un código para abrir un archivo modificado.
Impacto en el aula	Podría acceder y modificar a los archivos de los alumnos
Medidas para solucionar la vulnerabilidad	Una actualización corrige este problema

c. **Amplia información acerca de las vulnerabilidades: definición, tipos, como prevenirlas, software que pueda detectarlas, etc. Puedes utilizar como fuente de información la página de INCIBE (Instituto Nacional de Ciberseguridad)**

A través de este blog se puede conseguir información actualizada.
https://www.incibe.es/protege-tu-empresa/blog/filtro/vulnerabilidades

4. **Localiza la información sobre boletines de seguridad de alguna de las distribuciones de Linux (Ubuntu, Debian, Centos …)**

Linux –> https://www.debian.org/security/

Debian –> https://ubuntu.com/security/notices

Centos –> https://lists.centos.org/pipermail/centos-announce/

5. **Existen múltiples webs donde puedes comprobar la seguridad de tus contraseñas. Inventa una contraseña de máxima seguridad.**

Una computadora, tardaría trillones de años en descubrir esta contraseña:

dia62Dnfis*isdji289&dsio

6. Asocia los mecanismos con los objetivos de la seguridad informática.

Mecanismos	Objetivos o principios de S.I
Autentificación	No repudio
Autorización	Confidencialidad
Auditoria	Disponibilidad
Encriptación	Confidencialidad e integridad
Copias de Seguridad	Disponibilidad
Imágenes de respaldo	Disponibilidad
Antivirus	Integridad y disponibilidad
Cortafuegos	Integridad
Servidores proxy	Integridad
Firma electrónica y certificados	No repudio y confidencialidad
LOPD	Confidencialidad

7. Supón que en el ordenador portátil con cámara Web integrada que tienes en tu habitación, no tiene cortafuegos activos, no hay instalado un antivirus y lo tienes siempre conectado a Internet. Un desconocido toma el control de tu portátil y te das cuenta porque te encuentras la cámara Web encendida y tú no la has conectado.

Analiza activos, vulnerabilidades y riegos, y detalla cuáles podrían ser los daños producidos y el impacto de los mismos.

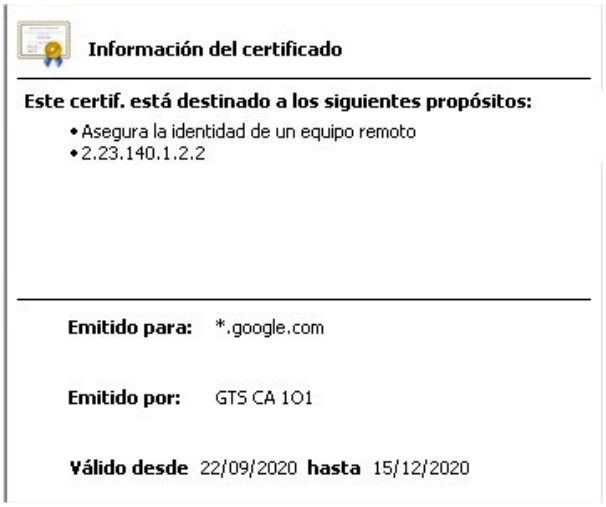
Activos:
Puede ser desde el portátil hasta los programas y datos del equipo.
Vulnerabilidades:
Estar conectado a Internet, sin ningún tipo de seguridad, antivirus, cortafuegos, etc.
Daños:
El atacante podría realizar robar, borrar con tus archivos personales.
Impacto:
Las consecuencias pueden ser altas si tienes datos bancarios.
Riesgos:
Son altos, ya que al ser tan vulnerable se pueden realizar muchos males.

8. Imagina ahora que la persona que ha tomado el control de tu ordenador no hace nada en tu ordenador y tú no te das cuenta de esta situación. Un día te dejas conectado tu DNI electrónico en el lector del ordenador.
Analiza los posibles riesgos y el impacto de los mismos.

El atacante podría utilizar el DNI electrónico de la víctima para realizar operaciones, ya sean contratos bancarios, distintos datos privados importantes.
El impacto puede ser bastante alto, ya que al conocer tus daños personales puede realizar todo tipo de problemas.

9. **Comprobar el certificado digital que utiliza Gmail a la hora de autentificar a los usuarios mediante el nombre y contraseña del mismo.**

El certificado es el siguiente:



En la zona reservada para las direcciones, podemos observar que el protocolo utilizado es HTTPS en lugar de HTTP. ¿Podrías indicar las diferencias entre estos dos protocolos?

La diferencia entre ambos protocolos es la **S** http –> http**s**.
Esto quiere decir que es seguro, utiliza **protocolos encriptados** que otorga seguridad en contra los atacantes.

Si hacemos clic sobre el candado, que se muestra en la parte derecha de la URL, se puede verificar que la conexión estará cifrada usando un certificado digital de Google.
Indica que es un certificado digital o firma electrónica y las ventajas que ofrece.

Es un fichero informático que asocia datos a una persona física, aunque, también es utilizado por organismos y personas jurídicas.

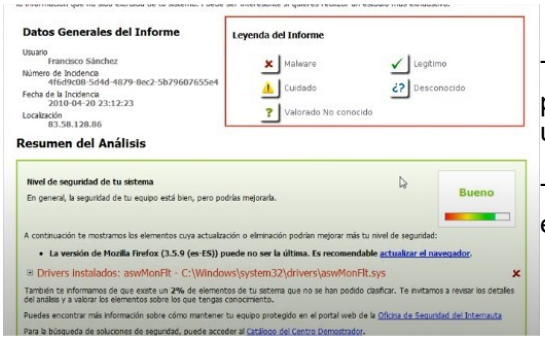
10. **Instalar secunia o connan en una MV y hacer un manual de funcionamiento del programa.**

Descargar conan o secunia herramientas gratuitas de análisis del S.O.
Tener en cuenta centro de actividades de Windows para el propio sistema

Conan

Esta herramienta lleva a cabo un análisis profundo de los elementos de riesgo en el ordenador.

Seleccionando **analizar** hace el escaneo y nos muestra aquellos programas o configuraciones que podrían tener vulnerabilidades



Tras terminar de analizar, nos carga en el navegador predeterminado
una página web con los posibles elementos vulnerables.

Tras una valoración de todo el equipo, nos muestra un estado “bueno”.

11. Mantén actualizado tu sistema operativo y aplicaciones, sobre todo los navegadores web, ya que las vulnerabilidades y amenazas cambian constantemente a través de la red. Comprueba el estado , analizando tus aplicaciones realizando un análisis desde la web con un inspector online:

Que aplicaciones tienen posibles vulnerabilidades al no estar actualizadas?

Las aplicaciones que, normalmente, suelen tener muchas vulnerabilidades al no actualizarse son:

Más peligrosos:
Navegadores de Internet.
Sistemas Operativos.

Menos peligrosos:
Aplicaciones ofimática.
Programas que usen redes.