Trabajo Práctico 01

SEGURIDAD INFORMÁTICA

Modalidad: Grupal, Obligatorio, Sin Nota

如果我聽它 我會忘記它，如果我看到它我記得它，如果我這樣做我理解它

Este TP se le entrega en PDF y **NO debe ser pasado a Word** para su resolución.

Opciones:

Imprimir, contestar a mano, tomar foto, y pasar a un único PDF.
Resolver con las herramientas incluidas en Acrobat sobre el PDF dado.
Resolver en hoja aparte a mano o PC, pegar sobre el PDF en el lugar correspondiente

Se entrega en la plataforma en un único PDF

INTEGRANTES DEL GRUPO

1. Bárbara Covarrubias
2. Otto Gonzalez
3. Franco Fazzito
4. Franco Balich
5. Malena Aguillon

Fecha de entrega	Aprobado?
7/9/22	

Los TPs **no** llevan nota numérica promediable, solo aprobado o no

- *Los aprobados tendrán 4 en la paltaforma solo para identificación*
- *Los no aprobados tendrán 2 en la plataforma y se deberán rehacer hasta ser aprobados*
- *En ningún caso la nota se promediará numericamente*
- *Los TPs se rehacen la cantidad de veces necesaria hasta quedar aprobados*
- *La fecha de entrega nominal de los TPS Obligatorios es 21 dias*
- *Pasada esa fecha el grupo no podrá acceder a coloquio aunque cuente con el promedio sufuciente*

PARTE 1 – CONCEPTOS TEÓRICOS.

La Seguridad es un punto obligatorio en todo desarrollo tecnológico ya sea este un sistema de comunicaciones, un software financiero, un control de procesos industriales o simplemente la PC que usamos diariamente.

Este apunte es un compendio de buenas prácticas destinado exclusivamente a ser usado en las clases presenciales o virtuales de la asignatura **SEGURIDAD INFORMÁTICA** dictadas en la **Universidad Abierta Interamericana.**

Para este apunte procuré trabajar siguiendo la taxonomía de Bloom

Entremos en tema

La seguridad de la información en la empresa usualmente se puede dividir en dos grandes ramas y es de acuerdo con esta división que trabajaremos en la primera parte de la asignatura

1. **La correspondiente del gerenciamiento**: manejo de los planes, políticas y normas.

2. **La correspondiente a la técnica**: instalación, configuración y mantenimiento de los equipos

Esto da origen a posiciones dentro del organigrama y por tanto a distintas responsabilidades.

CISO: Chief Information Security Officer que reporta directamente al **CIO** (Chief information officer). Según el tamaño de la empresa pueden ser la misma persona en empresas pequeñas o haber más capas intermedias en grandes empresas.

La responsabilidad normalmente correspondiente al **CISO** es de supervisar y dar tareas al:

Gerente de seguridad quien maneja al personal técnico y al staff de seguridad, no requiere amplios conocimientos técnicos específicos sino de visión general de las necesidades de seguridad de la empresa.

Administrador de seguridad es el encargado del dia a dia en los temas técnicos y administrativos.

Técnico de Seguridad es el que tiene los conocimientos de hard y software para configurar, implementar y solucionar problemas de seguridad.

Entendiendo que es seguridad de la información.

Veamos una mala definición de seguridad informática

Estado de encontrarse libre de daños

La anterior es mala definición pues no solo es el estado sino todo el proceso que lleva a mejorar las condiciones de seguridad. No debe olvidarse que nunca se está en un estado de completa seguridad, sino que debe buscarse la mejor protección posible y rentable.

Todo tiene su precio y el de la seguridad de la información, aparte del evidente de los costos de equipos y personal para atenderlos son los “inconvenientes” que trae agregar procedimientos de seguridad.

Para lograr un adecuado manejo de la seguridad es necesario tomar en cuenta sus tres pilares fundamentales habitualmente conocidos como CIA, sin tener relación con la agencia de inteligencia.

- **Confidencialidad**: Solo las partes autorizadas pueden acceder a la información
- **Integridad:** Asegura que la información es correcta
- **Disponibilidad** (**A**vailability): Los datos están accesibles SOLO a los usuarios autorizados.

Seguridad de la información o seguridad informática

Hay diferencias entre ambos términos, mientras que **Seguridad de la información** tiene mas que ver con los aspectos administrativos, normativos y de políticas, **Seguridad informática** se relaciona mas con los aspectos técnicos de configuración y de protección.

Normalmente se considera que la seguridad de la información incluye a la seguridad informática.

Vulnerabilidades

Estamos en un estado de vulnerabilidad cuando estamos expuestos a ser atacados o dañados. Las vulnerabilidades pueden venir de

a) **Plataforma**. El Hardware y el Sistema Operativo pueden tener vulnerabilidades correspondientes a:

   i. **Legacy**: Los sistemas heredados, aunque no tienen amplia difusión actualmente, tienen vulnerabilidades que pueden causar inconvenientes en nuestros sistemas.
   ii. **Plataformas** On-Premises. Son aquellas que se encuentran en la localización de la empresa usualmente en el DATA CENTER, que suelen no estar correctamente configurados.

   iii. **Plataformas "Cloud"**. Se trata de infraestructura compartida por varios usuarios sobre redes remotas contratadas por un cierto tiempo. La principal característica positiva, que es el acceso desde distintos lugares, es también fuente de vulnerabilidades a causa principalmente de problemas de configuración.

b) **Configuraciones**. Muchos son los seteos de seguridad y por tanto es factible que se produzcan errores, como ser

   i. No modificar los pass por default
   ii. No cerrar los puertos / servicios no usados
   iii. Mala configuración de la cuenta root
   iv. Exceso de permisos
   v. No uso de protocolos seguros
   vi. Mecanismos de encriptación poco seguros
   vii. Errores humanos

c) **Terceras partes**. Entidades ajenas a la nuestra que requieren accesos a nustra red para el trabajo.

i. **Principio del eslabón as débil**. El ataque se puede iniciar a partir de una vulnerabilidad de una tercera parte e ir ganando acceso a nuestra red / Almacenamientos / procesos.

d) **Patches**. Es una actualización en seguridad del software empleado. Son necesarios de mantener al día, pero pueden generar nuevas vulnerabilidades.

i. En caso del firmware es dificultoso de patchear
ii. Aparte de las mayores aplicaciones de software no hay muchos patches
iii. Retrasos en la instalación a causa de la posibilidad de crear problemas con las aplicaciones ya en funcionamiento.

e) **Dia Cero** (Zero Day). Cuando no es el desarrollador sino un *threat actor* (entidad amenazante) quien detecta la vulnerabilidad nos encontramos expuestos ya que tenemos 0 dias de aviso de peligro.

Vectores de ataque.

Es el camino usado por la entidad amenazante para atacar. Los vectores mas comunes son.

a) **Email**: Por esta vía ingresa mas del 90% de los malwares
b) **Wireless**: Fácil acceso si no está adecuadamente protegida
c) **Medios removibles**: Un pendrive “accidentalmente” olvidado en la cafetería puede ingresar malwares al sistema.
d) **Acceso directo**. Cuando se accede físicamente a la maquina
e) **Medios sociales**. Un atacante puede conocer cuando un determinado empleado toma sus vacaciones y usar ese conocimiento a su favor
f) **Cadena de suministros**. Suministros que llegan a la empresa atacada conteniendo malware
g) **Cloud**. Son mecanismos mas complejos que permiten mas oportunidades de encontrar debilidades

Ataque con Ingeniería Social.

Suelen descansar en principios psicológicos.

Muchos son los ejemplos de este tipo de ataque que no requiere de conocimientos técnicos sino de la habilidad de persuadir a la victima que nos de la información buscada mediante engaños.

Dado que este libro es predominantemente técnico solo se deja un PDF con los puntos mas importantes del tipo de ataque.

Es importante hacer notar que este tipo de ataque es MUY DIFUNDIDO y causa mas problemas que otros ataques con mas elaboración técnica.

PARTE 2 – RESOLUCIÓN.

Básicos

> ***Nota**: Es muy conveniente hacer los TPs en una máquina virtual*

Se requiere conocimiento básico **del stack de protocolos TCP-IP** *en caso necesario recurrir al libro TCP IP de Douglas Comer*

Cuestionario de repaso TCP IP

Complete en los lugares que se indica, las sentencias 1 a 8 con las siguientesopciones. *En caso de dudas consulte en Internet*

Address Resolution Protocolo; ARP Cache; Cat; Domain Name System; Dynamic Host Configuration Protocol; Gateway; Host address; Ifconfig; Internet Control Message Protocol; Internet Protocol; Ipconfig; Media Access Control; Network Address; Ping; Resolv.conf; Subnet mask; Time to live; Transmission Control Protocol / Internet Protocol

1. Las Letras IP corresponden a: Internet protocol
2. La Media access control es la dirección física de su interface de red que fue asignada por la compañía que fabricó la placa.
3. Ipconfig/renew actualizará la dirección IP obtenida desde el servidor Dynamic host configuration protocol
4. Los cuatro ítems necesarios para conectar una máquina a internet son: Gatway; internet protocol; host address; Domain Name System
5. La Subnet mask se usa para separar la parte de host de la parte de red de la dirección IP
6. Resolv.conf es el archivo que contiene la dirección del servidor DNS en Linux
7. El comando Cat permite mostrar el contenido de los archivos de texto en Linux
8. Para comprobar la conectividad de una red se usa el comando ping

NOTA: *Si tiene problemas con el ejercicio anterior lea nuevamente el libro TCP IP de DouglasComer*

Cuestionario de revisión

1. Alicia tiene un trabajo en el que reporta al CISO y tiene a su cargo a un grupo de técnicos de seguridad. ¿Cual es su cargo?

   Security administrator
   Security technician
   Security officer
   Security manager

2. ¿Cual de los siguientes asegura que la informacion no fue alterada por ninguna persona no autorizada?

Confidencialidad
Integridad
Disponibilidad
Trazabilidad

3. ¿Cual de las siguientes NO es verdadera?

La seguridad es un objetivo a lograr
La seguridad incluye los pasos para protegernos del daño
La seguridad es un proceso
La seguridad se debe lograr a cualquier costo

4. ¿Como decide el vendedor cual debería ser el *seteo* por default del sistema?

Elije el mas seguro de los posibles
Elije uno cualquiera al azar
Elije el que permita el uso inmediato del producto
Elije aquel dado por los estándares de la industria

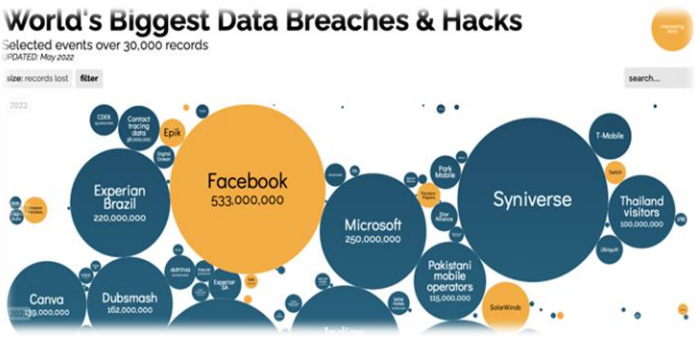
5. ¿Cual es el termino que mejor describe la conexión entre una organización y una tercera parte?

a. System integration
b. Platform support
c. Resource migration
d. Network layering

6. Exploración de información

a. Abra su navegador y busque:
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Debe ver algo similar a la imagen de la derecha



En esta imagen se pone de manifiesto las violaciones de seguridad.
Note que se puede visualizar por año y que el tamaño de la burbuja es proporcional a la gravedad del daño.

Note también que poniendo el cursor sobre las burbujas se brinda mayor información
Algunas burbujas señalizadas con otro color incluyen ¨historias de interés¨ elija una y explíquela brevemente

⇨LinkedIn fue hackeado, ha resultado ser una violación de 117 millones de contraseñas, en el 2012. Las empresas suelen proteger las contraseñas de los clientes cifrándolas. Pero LinkedIn no había agregado una capa fundamental de seguridad que haga que el texto confuso sea más difícil de decodificar.
El impacto fue que los hackers vendieron la base de datos robada de LinkedIn en un mercado negro en línea.
La compañía como solución: pidió que se cambie la contraseña y agregue algo llamado autenticación de dos factores.
Dicha autenticación requiere un mensaje de texto cada vez que se inicie sesión desde una computadora nueva.
También tomo la medida de invalidar todas las contraseñas de los clientes que no se han actualizado desde que fueron robadas.

En la parte inferior encuentra las violaciones de los datos ordenados por SENSIBILIDAD, lea la información y explique a que se hace referencia con "SENSIBILIDAD de los datos".

⇨Se considera sensible aquellos datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, etc. Los datos personales son todos aquellos datos que permiten identificar a una persona.Podemos decir que la sensibilidad es el grado de importancia del dato. Ejemplo: los datos de una tarjeta de crédito son más sensible (más importante) que un correo electrónico.

b. Vamos ahora a https://informationisbeautiful.net/visualizations/top-500-passwords-visualized/

¿Cuáles son los Password más empleados? ¿Por qué NO DEBEMOS USARLOS?

⇨ A veces queremos que nuestras contraseñas sean simples y fáciles de recordar, debido a eso hay categorías de contraseñas más comunes, estas son algunas: animales, comida, nombres, alfanumérico simple, deporte, al azar. Elegir este tipo de contraseña es un error muy grande porque es propenso a ataques. Una contraseña es tan importante como la información que protege. Por ello, si las contraseñas son lo suficientemente fuertes y seguras conseguiremos dificultar en gran medida el trabajo de aquellos que traten de realizar un ataque para obtener nuestros datos.

Una categoría de ataque muy popular es el **ramsomware**. Explique que es.

⇀ Es un ataque donde partes o archivos del sistema infectado son encriptados, esto por lo general es con el objetivo de pedir una suma de dinero prometiendo desencriptar los archivos si se paga el monto, se trata de un secuestro de información.

c. Entre a https://informationisbeautiful.net/visualizations/ransomware-attacks/

Y explique algún ataque de los allí presentados.

⇨ Canon recibe un ataque de ransomware y robo de datos de los servidores de la compañía. Después de rastrear una interrupción sospechosa en el servicio de almacenamiento de fotos y videos en la nube que causo que los usuarios perdieran archivos.
Canon encontró actividad no autorizada en su red entre el 20 de julio y el 6 de agosto, donde los datos a los que accedió el atacante incluían datos sensibles de los empleados.
Luego se utilizo un método de extorsión donde roban datos antes decifrarlos y amenazan con filtrar los archivos a menos que la víctima pague el rescate.

7. Para este punto DEBE estar trabajando con Windows , en caso de utilizar MAC o LINUX haga este punto con las máquinas de la facultad.

   a. Determine que Windows esta Ud corriendo Windows 10

   Entre en página del scanner de windows en

https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide

   b. Baje la versión de escaner correspondiente a su sistema (32 o 64 bits) y lance el programa MSERT
   c. Acepte y seleccione QUICK scan. Luego de unos momentos le dirá si hay software dañino en su PC
   d. En caso de problemas de click en VIEW para ver detalles y corra nuevamente pero ahora en FULL scan
   e. Cierre todas las ventanas

Comente los resultados.

Luego de realizar el escaneo rápido, la aplicación comprobó que en mi computadora no hay ningún tipo de virus, spyware y algún otro tipo de software inseguro que necesite ser detectado y eliminado

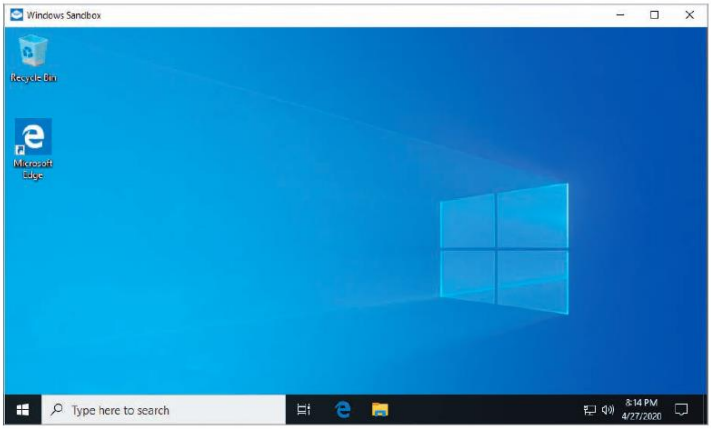
8. En seguridad informatica es común hablar de utilizar como un mecnismo de protección un ***sandbox***, explique que es:

En seguridad informática se entiende como sandbox a una maquina virtual que se encuentra aislada del sistema operativo principal de la computadora, permitiendo que en ella se pueda ejecutar software inseguro sin afectar a la computadora.

NOTA: *Para realizar este punto, trabajaremos con **Windows Sandbox** incluido en W10 professional, Enterprise y educational (No Home), en caso de no tener algunas de estas versiones, mas adelante instalaremos VirtualBox*.

a. Verificar que tenemos activada la virtualización.

   i. Boton derecho en *taskbar* y seleccionar *Task manager*
   ii. Clic en *Performance* tab
   iii. En virtualizacion debe decir ENABLE, de no ser asi debe reiniciar, entrar al BIOS y encender la virtualización.
   iv. En alguna versiones antiguas de BIOS deberá desactivar *Hyper-threading*.
   v. En el buscador escriba Windows Features, Clic en Windows sandbox para activar.
   vi. Click Start, buscar Windows Snadbox, dar clic y se abrirà una pantalla similar a la mostrada.
   vii. Instale el buscador CHROME y vea que funcione adecuadamente



   viii. Cierre Windows Sandbox, abralo nuevamente y explique que ve

Podemos observar que al ser una máquina virtual completamente nueva y aislada no contamos con google Chrome por lo que tenemos que instalarlo desde 0 donde se muestra la pantalla de bienvenida de Chrome, seguido de eso y una vez configurado ya podemos utilizarlo.
Luego al momento de salir de la máquina virtual una vez instalado observamos que esta misma máquina virtual una vez cerrada se perderá todo su contenido y se perderá de forma permanente por lo que en el siguiente inicio deberemos configurar nuevamente el Chrome.

9. Ahora es un buen momento para crear una maquina virtual si es que aun no la tiene en su notebook. Durante la cursada usaremos **VirtualBox** corriendo **Windows** y **KaliLinux**. Estas VM no seran usadas ahora sino en próximos TPs NO OBLIGATORIOS, eso significa que si no puede instalarlas en su máquina por ser la de uso laboral, eso no influira en la aprobación de su cursada.

10. Elija 2 videos de youtube relacionados con la seguridad informática

    a. Indique sus direcciones
    b. Véalos, compare sus cualidades (claridad expositiva, profundidad, exactitud).
    c. Explique brevemnete que aprendió en ellos

A) FASTCASH 2.0 | EL MAYOR HACKEO A CAJEROS AUTOMÁTICOS DE LA HISTORIA
https://youtu.be/cjgnYIWFbd4
LA CIBERGUERRA: El caso de Stuxnet
https://youtu.be/FaeP6xoZOXc

B) Ambos videos dan una explicación muy clara para principiantes en ciberseguridad sobre dos casos de ataques informáticos, pero se diferencian en que, durante la explicación del primero video, en este se trata de agregar humor entre explicaciones, mientras que el segundo solo al inicio, lo cual hacen para llamar la atención de espectador.
Pero por otro lado el primero explica cómo fue la técnica de hackeo en detalle, mientras que el segundo solo por encima.
Además, el segundo video dice las fuentes de algunos datos y conceptos básicos de ciberseguridad mientras que el primero no.

C) De ellos aprendimos la grabe que puede ser un ataque cibernético, en el primero con Fashcash como un grupo de ciberdelincuentes ataco una serie de bancos alrededor del mundo e intento robar 2 mil millones de dólares por un ataque coordinado. Mientras que en el segundo video se menciono la ciberguerra que se esta viviendo en la actualidad entre diferentes países y menciona el malware Stuxnet el cual fue utilizado para atacar un modelo muy específico de PLC y se esparcía por USBs, pero fue muy complicado detectar que hacia y a que modelo especifico atacaba, solo luego de mucha investigación se comprobó que el virus estaba diseñado para atacar los PLC, computadoras que controlaban las centrifugadoras de uranio de Irán que se usaban en secreto para la creación de armamento nuclear en el país y haciendo que estas centrifugadoras se rompieran por culpa del virus, causando miles de centrifugadoras dañadas.

11. Busque en Internet informacion sobre *phishing simulators,* explíque que son, pruebe el funcionamiento de alguno de ellos y de su opinion crítica.

Se utiliza para analizar la factibilidad de que los usuarios de su organzación caigan en trampas de ingeniería social.

Una simulación replica el comportamiento de un ciberataque real, en los siguientes aspectos:
- Duración de la campaña, usualmente un par de horas
- Medio utilizado para entregar el ataque, generalmente vía email
- Presencia de técnicas de ingeniería social en las cabeceras y cuerpo del mensaje
- Uso de enlaces o archivos adjuntos
- Uso de sitios web falsos, réplica de otros reales
- Medición de las acciones del usuario, es decir, si abre el correo, si hace clic en un enlace, etc.

Cabe destacar que una simulación no captura información sensible y es inocua para el usuario final o la organización.
Los ataques reales de Phishing finalizan cuando el ciberdelincuente logra capturar, por ejemplo, las credenciales del usuario. En cambio, una simulación, puede mostrar un mensaje educativo luego de que el usuario realiza una acción riesgosa, como enviar información privada en un formulario.
La función principal de la simulación de Phishing es comportarse como un Phishing real.

Por ejemplo, que las campañas duren un mes, que engañen a la mayor cantidad de usuarios posibles, o que los correos de simulación no sean detectados por tecnologías de seguridad.
Esta expectativa no es coherente con la realidad. Si deseamos simular una trampa de Phishing, ésta debe comportarse como un Phishing real.

12. Herramientas sencillas.

NsLookup.

Permite la búsqueda en **servidores DNS**
En Windows ingrese al *Command Prompt* y realice una búsqueda en nslookupp www.uai.edu.ar ¿qué le devuelve el comando? Explique brevemente lo que observa

nslookup www.uai.edu.ar
Server: gpon.net
Address: fe80::1

Non-authoritative answer:
Name: www.uai.edu.ar
Address: 200.32.31.7

El comando devuelve el servidor DNS que utiliza la herramienta para hacer las consultas, luego en Address la dirección del servidor usado. Abajo en el segundo grupo aparece "Non-authoritative answer" que significa que la respuesta DNS es desde un servidor que tiene en caché una copia de las consultas realizadas.

Por ultimo en Name aparece el nombre del dominio que fue buscado y luego la dirección que corresponde a ese dominio.

tracert

Nuevamente desde el promt ingrese: tracert www.uai.edu.ar que nos da el recorrido desde nuestra máquina hasta la ingresada como destino. Explique lo que se observa.

Nos aparece la dirección real del dominio elegido en este caso 200.32.31.7,
luego va diciendo uno a uno todos los nodos y routers por los que va pasando el mensaje enviado, las direcciones IP y la latencia en cada uno de estos hasta llegar al destino.

Por último nos indica si la traza pudo ser completada en un máximo de 30 saltos o menos que contempla la ejecución del tracert.

Puede ocurrir que en algunas líneas obtenga asteriscos. ¿Por qué?

Cuando se ejecuta el tracert se le solicita a cada nodo por el que pasa el paquete el tiempo de respuesta de cada uno cuando pasa por ahí el paquete. Cuando se obtienen asteriscos junto con el mensaje "Tiempo de espera agotado", significa que los nodos tienen limitado el tracert en los equipos por medio de ICMP Rate Limiting para prevenir que los routers queden afectados por ataques DDoS.

Otra razón es por que el nodo no ha devuelto un paquete dentro del tiempo esperado, es decir que no ha habido respuesta desde ese nodo al enviar el paquete.

Pruebe en vez de hacer las pruebas con **ICMP** como hace tracert, usar **TCP** .

TraceTCP - https://github.com/SimulatedSimian/tracetcp/releases

¿Observa alguna diferencia?

Se observa que con TraceTCP las direcciones IP aparecen antes que los dominios a diferencia de tracert donde aparecen los dominios de los nodos primero y posteriormente las direcciones IP.

Pero los nodos que dan Tiempo de espera agotado en Tracert siguen siendo los mismos que dan tiempo de espera agotado en TraceTCP.

Way Back Machine

Supongamos ahora que queremos usar el soft relacionado con esteganografía **Infostego** (www.antiy.net). ¿Lo encuentra? Al momento de escribir este TP ya se había eliminado. ¿Como recuperarlo? **Way back Machine** nos permite recordar que TODO LO QUE ENTRA A LA RED NO SE VA NUNCA.

- ⇨ Busque www.archive.org e ingrese a www.antiy.net. En el cuadrom superior de **waybackmachine** ¿Existe aquí **infostego**? ¿Se puede bajar? Experimente y explique lo observado.

⇨ Sí, efectivamente desde archive.org se puede retroceder en la linea temporal de la pagina y se puede descargar Antiy Infostego 3.0 de la página del 14 de agosto de 2006.

Es como si se tomasen snapshots completos de la página a lo largo de su historia.

A diferencia de la página actual de Antiy que unicamente permite la descarga de AVL Pro y Virus Submit Tools.

Shodanhq

Se trata aquí de uno de los más potentes scanner, de ser posible regístrese para obtener el mejor rendimiento. Explique muy brevemente lo que se ofrece. https://www.shodan.io

Es un buscador, ofrecen busquedas de sistemas de control, bases de datos, servidores. Parece muy utilizado para buscar dispositivos conectados, como camaras de seguridad y busquedas compartidas recientes.

Se pueden usar filtros como de país, ciudad o puertos para encontrar dispositivos, tambien se puede filtrar por sistema operativo, organizaciónes y otros. Al encontrar información sobre un dispositivo se puede conocer la dirección MAC, el nombre del host, la IP interna, el protocolo del puerto, la versión y fecha del firmware.

Entre a la página de NVD https://nvd.nist.gov/vuln

Luego de “pasear” por la página explique

¿De qué se trata?

Es el sitio del Instituto Nacional de Estándares y Tecnología del gobierno de los Estados Unidos, contiene una base de datos a nivel nacional de las vulnerabilidades con estadísticas, listados, entre otros.

¿Cuantas vulnerabilidades se detectaron en el mes pasado?

Recibidas 2343, Analizadas 2378, Modificadas 1553 y re analizadas por la base de datos 594.

Describa brevemente que son las métricas CVSS v3 y CVSS v2.

El CVSS es un sistema que provee una manera de capturar las principales características de las vulnerabilidades y produce un puntaje numérico reflejando la severidad de las mismas. Se encuentra custodiado pro el Foro de Respuesta de Incidentes y Equipos de Seguridad (FIRST) por sus siglas en inglés y es un estándar abierto que puede ser usado libremente.

Son tres grupos de métricas usadas para calcular el puntaje, el primer grupo llamado BASE busca representar cualidades relacionadas con la vulnerabilidad, el segundo TEMPORAL, indica las características que cambian con el tiempo y las métricas de ENTORNO consideran características únicas para el contexto del usuario que hace la evaluación.

La diferencias entre la v2 y la v3 son varias, entre ellas están que la ultima agrega una métrica de alcance que establece un componente específico que es el vulnerable y otros componentes que puedan resultar afectados a los que se les llama componente impactado. También que se sustituye el vector de acceso de la v2 que es el medio para acceder a la vulnerabilidad por el "vector de ataque" que considera escenarios para explotar la vulnerabilidad.

Y para terminar, de una breve pero conceptual información de los siguientes ataques muy importantes en su momento.

Evento	Información
WannaCry	Fue un ataque a nivel mundial en 2017 que utilizó el criptogusano WannaCry, el objetivo eran computadoras con sistema operativo Windows ecriptando los datos y pidiendo un pago en Bitcoins. Se propagó explotando una vulnerabilidad de EternalBlue, un exploit desarrollado por la NSA para sistemas operativos Windows antiguos.
SolarWind	Fue un ataque que afectó directamente a la empresa SolarWinds que comprometió a su herramienta Orion, herramienta que funciona como una plataforma de administración y monitorización de la infraestructura diseñada para simplificar la administración de TI en diversos entornos. El 13 de diciembre de 2020 se dio a conocer el ataque a la vulnerabilidad sobre esta herramienta que es usada por empresas que integran la lista de Fortune 500 y organizaciones gubernamentales de los Estados Unidos.
Ataques Hoteles Marriott	Fue una filtración de los datos de 500 millones de clientes del grupo de hoteles Marriott International por parte de un hacker el viernes 30 de noviembre del 2018. Los datos afectados eran los registros de detalles de las reservas efectuadas hasta el 10 de septiembre de 2018 y Marriott desconoce si los atacantes tuvieron acceso a los medios de pago usados.
Ataque a Datos de LinkedIn	Fue una filtración de datos que sufrió LinkedIn en junio del 2021 en donde se filtraron los datos de 700 millones de usuarios, los cuales fueron puestos a la venta. Según el sitio RestorePrivacy el hacker realizo el ataque debido a un mal uso de la API oficial de LinkedIn para descargar los datos, algo que había pasado en el abril del mismo año.