

# Seguridad e Integridad de Sistemas

## ▼ Primer Parcial

▼ 08-08-2022

Docente: Arturo Ocampo Silva

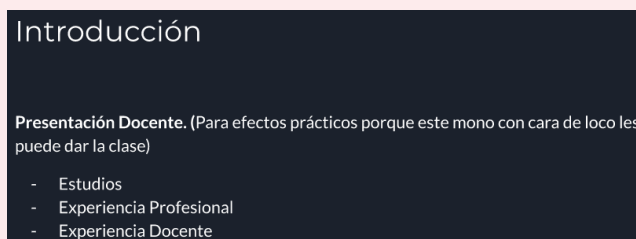
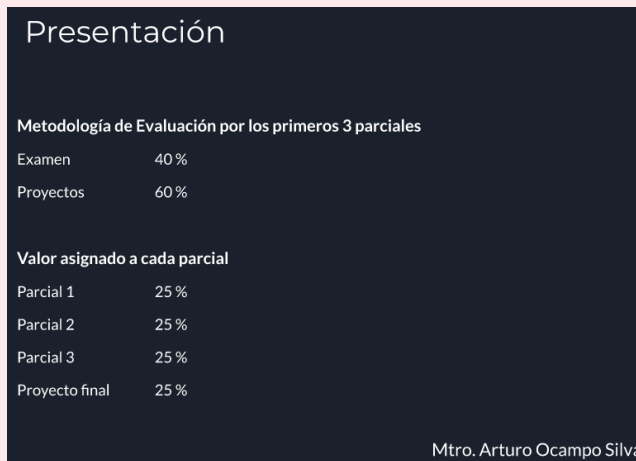
Evaluación:

- Exámenes: 40%
- Proyectos: 60%

Generalmente aplica para los primeros 3 parciales

4 parciales con 25% cada uno

Es enemigo de leer diapositivas así que cuidado con eso al exponer D:



# Introducción

## Presentación Docente.

- Forma de trabajo
  - Evaluación de Proyectos (Hasta 72 horas previas)
    - Portada 2 %
    - Índice 5 %
    - Introducción (Variable nunca menor a 5 %)
    - Objetivo ( 5%)
    - Desarrollo (Variable nunca menor a 50 %)
    - Conclusión (Variable nunca menor a 10 %)
    - Bibliografía 3 %
- Examen
- Entrega de Calificaciones
- Problemas por documentos que mágicamente se clonan

# Introducción

## Presentación Docente.

- Formato de clase
  - Presentación (Ya verán que tienen sus bemoles)
  - Preguntas
  - Colaboraciones
  - Observaciones
  - El italiano
  - Aula virtual
  - Pase de lista

# Validando

|                                |                                                                            |
|--------------------------------|----------------------------------------------------------------------------|
| MDM (Mobile Device Management) | Sniffer                                                                    |
| Cuadrante Mágico de Gartner    | Virtualbox                                                                 |
| ISO                            | Pentesting                                                                 |
| Vlands                         | <ul style="list-style-type: none"><li>- Badstore</li><li>- OWASP</li></ul> |
| Túneles                        | Esteganografía                                                             |
| Proxy                          | Llaves públicas y privadas                                                 |
| Host Bastión-firewalls         | Fingerprint, footprint                                                     |
| LOGS                           | Nmap - Haciendo ruido                                                      |
| Seguridad Biométrica           | Cañon de IONES                                                             |
|                                | USBdeview                                                                  |

Introducción: Qué pretenden, de qué van a hablar, de qué se va a tratar, cómo van a sacar provecho del proyecto

Desarrollo: El grueso del proyecto

Conclusión: se logro el objetivo, qué problemas se tuvieron



## Bibliografía importante

Respecto a proyectos, no está bien copiar y pegar de Wikipedia.

En el examen, son teórico-prácticos. No hay que memorizar, hay que entender. Se pueden sacar apuntes o tener libros pero prohibido comunicarse entre alumnos.

Consejo: En examen no se copia ni pega de las diapositivas.

Las fechas de entrega de calificaciones las cumple el profesor a rajatabla. Siempre antes de subir a sistema, las da personalmente.

Sólo el jefe de grupo tiene comunicación con el profesor

De proyectos clonados, el profesor distribuye la calificación

Mejor calidad que cantidad (mejor no presentar trabajos con muchísimas páginas, pero que sí tenga calidad)

## Formato de clase

Están en Aula Virtual las diapositivas

Asistencia: A los 15 para acabar la clase

Si hay COVID, el justificante sólo se trata con comprobante de COVID

▼ 09-08-2022

# Introducción

Debemos entender que el activo más importante de toda organización es la información. Y si ya se que sone bien hojaldra.. Pero para cualquier organización bien estructurada hasta el dueño es prescindible.. 20 segundos para dedicar cantos gregorianos al profe... No más porque le da tirría y nos mira feo..

Por lo que retomando. **Seguridad Física.**

Mucho antes de que cualquier otro tipo de seguridad fuera creada, la seguridad física ya existía como podemos apreciar a continuación.

- Los egipcios usaban candados hace más de 2,000 años
- Si la información era importante, era grabada en piedra, o en tiempos posteriores escrita en papel
- Si la información iba a ser transmitida o movida de una localidad a otra, esto usualmente se hacía con guardias

Lo anterior debido a que como ya entendimos la información es poder por ende siempre será un botín sumamente interesante para el enemigo.

## Introducción

El activo más importante para toda organización es la información.

Mucho antes de que cualquier otro tipo de seguridad ya existía como:

- Los egipcios usaban candados

Entonces desde la antigüedad podemos enumerar un número importante de medidas de seguridad, específicamente para la información tanto almacenada como en tránsito nos encontramos.

- Guardias
- Paredes
- Perros
- Y una buena cantidad de etc. La imaginación humana siempre ha sido increíble.

Y como hemos podido analizar todo la seguridad física que estudiamos responde a la legítima preocupación de los propietarios de la información de proteger su activo máspreciado del enemigo.

Desde la antigüedad siempre había seguridad como:

- Guardias
- Paredes
- Perros

“Una empresa tiene que cuidarse de alguien que esté en el interior” como los espías o personas que se vendían

Imaginemos lo que podía pasar si por ejemplo los planes de Guerra de una invasión eran descubiertos. En definitiva el enemigo se encontraría en franca posición privilegiada.

Es por eso que con el paso del tiempo se procedió a buscar métodos para proteger la información que fueran más allá de las simples medidas físicas, desarrollándose las primeras técnicas de **cifrado**, que nos proporcionaban una **confidencialidad** a prueba incluso de la traición de quienes transportaban la información.

Entre los primeros ejemplos de cifrado encontramos que los Espartanos (Si esos de la película de los 300) usaban una forma de cifrado conocida como Escítala



Mtro. Arturo Ocampo Silva

Algunas metodologías de seguridad son el cifrado.

Por su parte los hebreos usaban una forma básica de sistema criptográfico conocido como ATBASH el cual trabajaba cada letra usada con otra letra con la misma distancia del final del alfabeto ejm: A = Z, B = Y, etc

Durante la edad media se desarrollaron Cifradores de sustitución más elaborados. Esto tan pronto como los individuos comenzaban a romper los esquemas simples de cifrado.

- En el siglo IX, Abu al-Kindi publica lo que se considera el primer documento sobre cómo romper sistemas criptográficos, "Un Manuscrito para Descifrar Mensajes Criptográficos"

Trata sobre análisis de frecuencia para romper códigos criptográficos

Después surgió el ATBASH (abecedario volteado) y el código César (recorrer 5 posiciones del abecedario)

Abu al-Kindi publicó el primer documento de cómo romper sistemas criptográficos "Un manuscrito para descifrar mensajes criptográficos"

IPMB BMVNOPT

HLM VCXVFVMGVH ZOFNMLH

HOLA ALUMNOS

SON EXCELENTES ESTUDIANTES

Próximamente habrá una tarea y será programar o hacer una fórmula para descifrar el cifrado César teniendo el cifrado que se busca

- Sólo hasta después de la segunda parte del siglo XX, la ciencia del cifrado y criptografía se mueven más rápido, esto debido al gobierno de USA que crea con este fin la National Security Agency (NSA)

- Nota: Muchos de las invenciones y sistemas criptográficos nunca fueron patentados, porque se consideraban muy importantes para ser liberados, ya que los enemigos obtendrán información sobre ellos

Sólo hasta la WWII se vuelve muy importante hacer cifrado y criptografía.

Muchas invenciones y sistemas criptográficos nunca fueron patentados porque se consideraban muy importantes para ser liberados y los enemigos obtendrían información sobre eso.

El cifrado clásico = secretismo

La tecnología tiene un problema grave. Nuestros creadores de tecnología siempre se les olvida que hay personas malas

Hay muchas tecnologías como las llamadas telefónicas que tenían muchas problemáticas de seguridad por lo anteriormente mencionado

Mientras que el cifrado ofrece otro nivel de seguridad necesario, la historia muestra que esto no es suficiente.

- Tenemos sistemas, como la telefonía, que son vulnerables. Al mismo tiempo se comienza el trabajo para interceptar las emisiones electrónicas de otros sistemas. Resultado de esto es el desarrollo del programa TEMPEST que a su vez provoca las primeras iniciativas para desarrollar equipos que fueran menos vulnerables al robo de señales

Nota: TEMPEST no es acrónimo de nada, pero una buena interpretación es "Tiny Electro Magnetic Particles Emitting Secret Things"

"Pequeñas partículas electromagnéticas que emiten cosas secretas"

TEMPEST en sí no significa nada, es un proyecto, pero la gente conspiranoica creyó que TEMPEST era una interpretación muy illuminati.

El problema con la seguridad en las señales se repite a sí mismo desde que el primer teléfono sin alambres fue liberado. Como dato histórico los primeros teléfonos inalámbricos no contenían nada de seguridad si sus vecinos tenían la misma frecuencia o se contaba con un "scanner", la conversación era fácilmente interceptada y malas noticias. Los primeros teléfonos celulares también eran fácilmente interceptables.

Afortunadamente ha habido avances en la seguridad de las señales, tales como la tecnología de spread spectrum (Espectro Extendido) desarrollada nuevamente por los militares. Esta tecnología de modulación se implementa mediante dos métodos diferentes:

- Direct-sequence spread spectrum (DSSS -Espectro ensanchado por secuencia directa). Para efectos prácticos en este se agrega un patrón de bits redundantes que refuercen la señal y que en caso de que la misma sea interceptada para quien escucha no sea más que ruido. Quien recibe previamente recibirá la secuencia de desensamblado lo que le permitirá entender el mensaje (Realizará el proceso inverso al ensanchado)

El espectro ensanchado replica la información y la empalma para "crear ruido" pero puede descifrarse quien sepa cómo replicó y cuánto retraso le dio para empalmarla

- Frequency-hopping spread spectrum (FHSS-espectro ensanchado con salto de frecuencia). En este previamente establecen emisor y receptor una tabla de frecuencias de emisión, durante la comunicación constantemente variarán entre estas frecuencias en intervalos de tiempo denominados dwell time (ejem. cada 400 ms) de manera que si algún atacante intenta interceptar la comunicación, sólo podrá tener una fracción de la comunicación. Esta técnica también utiliza la zona de los 2.4GHz, la cual se organiza en 79 canales con un ancho de banda de 1MHz cada uno.

Estos sistemas de transmisión proveen seguridad y por consecuencia lógica mejoran la confiabilidad

FHSS se trata de saltar entre frecuencias de radio para no ser interceptados

Recomendados: Álvaro Chirou y Chema Alonso

Chema Alonso dice que la peor forma de garantizar la seguridad de una empresa es decirle a todos que es impenetrable porque te pones en la lista de los hackers para atacar

Seguridad no es cerrarte completamente, es también recuperarte lo más pronto posible.

Ahora la seguridad ha tomado un papel importante en las comunicaciones pero como todo tiene un pero y el humano es el único ser en este planeta que comete 2 veces el mismo error hay vamos de nuevo, con el advenimiento de la Internet y el crecimiento del e-commerce ha incrementado la necesidad de seguridad, ya que el internet nuevamente no se diseñó como un entorno seguro "Diablos" y aparte de eso ¿ ahora cual es el problema ?

- Los usuarios hogareños no usan más conexiones de marcado lentas (dial-in), ahora usan DSL o cable o Fibra Óptica.
- No sólo se ha incrementado el ancho de banda, sino que muchos de los sistemas se encuentran siempre encendidos, lo que significa que el atacante puede beneficiarse del ancho de banda disponible por los usuarios para lanzar su ataque.
- La necesidad de seguridad en la red puede ser subrayada por el alto índice de ataques exitosos tales como Nimda, Code Red (colapsaba servidores mediante hilos abiertos), SQL Slammer (Provocaba denegación de servicios), a nivel servidores, pero a nivel casero tenemos a W32.KOOBFACE, BACKDOOR.BANECHANT a nivel gobiernos BACKDOOR.DARKMOON, BACKDOOR.WEEVIL y el rey de los malditos TROJAN.CRYPTOLOCKER de este último tipo es el "i wanna cry" (
  - I wanna cry inicio en el 2017 y a la fecha se sabe continúa activo, afecto aproximadamente 230,000 equipos alrededor del mundo paralizando los sistemas informáticos de 150 países provocando pérdidas estimadas en 4,000 millones de dolares (fuente: <https://www.kaspersky.es/resource-center/threats/ransomware-wannacry>)
  - Nimda por sí sólo, se cree que infectó a más de 1.2 millones de computadoras. Una vez que Nimda infecta un equipo escanea el disco duro cada 10 días en busca en direcciones de correo, que usaba para copiarse en otros equipos
- "Exploits" de este tipo subrayan la necesidad de una mejor seguridad en la red

El módem hace proceso de telefonía. El router no. Éste trabaja con una topología de estrella y anillo interno conectado las 24 horas al día. Es por esto que el delincuente no va a tener tanto fallo.

Infinitum nos asigna una IP pública con ventajas y desventajas. Como ventajas pueden publicarse servicios al exterior o acceder por túneles SSH, pero como desventajas es que si no se es consciente de la situación, delincuentes tienen el ojo puesto en uno

TotalPlay maneja el NATeo, que maneja una IP pública hacia el router pero no da la IP de los usuarios hacia el interior del router, por lo que el atacante vería el router pero nunca los dispositivos del interior

Primero hay un ataque para determinar dónde está una IP. Puede ubicarse una IP

Con una IP NATeada es más segura pero menos eficiente.

Jamás hay que tener un Windows como Escritorio Remoto pues es uno de los protocolos más vulnerables que hay.

### ¿ Cómo han respondido las Organizaciones ?

- Implantando mejor seguridad en la red
- Incluyendo sistemas de prevención o detección de intrusos (IDS -Intrusion Detection System o IPS - Intrusion Prevention System), antivirus así como productos de filtrado de correo electrónico

Sin embargo estos productos no previenen el crimen, simplemente mueven al criminal a otros sitios no protegidos.

# Resumen

- Amenazas
- Vulnerabilidades
- Esquemas de defensa
- El enemigo y sus motivos.
- Esquemas básicos de defensa

## ▼ 10-08-2022

Revisión del WannaCry con Nissan que afectó el firmware de un robot de la planta

IDS: Sistema de detección de intrusiones

IPS: Sistema de prevención de intrusiones

Un firewall es igual a un IPS

Pregunta de examen: Diferencias entre IPS e IDS

No pueden invertir más en seguridad que lo que están cuidando. Aplica en seguridad física como digital (pregunta de examen)

Hacker no es lo mismo que delincuente

Un delincuente busca fines económicos como el robo de información mientras que el hacker lo hace bajo una metodología y documentando todo lo realizado

Hay mucha extorsión en aeropuertos por:

- La gente viaja por negocio
- Porque la gente al viajar al menos pasan 2 horas de tener en modo avión y la gente puede extorsionar con que la persona está secuestrada

Algunos motivos del delincuente son extorsión, obtener dinero, obtener la identidad, venganza.

¿Qué necesito para una CURP? Fecha de nacimiento, Nombre y lugar. Con esto es sencillo obtener datos personales para un delincuente

El peor problema en legislación es usar el término ciber, porque la ley está muy verde en términos informáticos. Por ejemplo el robo de aparatos físicos está bien definido pero el "ciber-robo" no está bien definido, tampoco está bien definido el "ciber-fraude"

Para el delincuente informático, phishing para la posesión de parejas tóxicas es un negocio para todos ellos

En mucho tráfico de redes, un delincuente puede poner un router con un desvío de DNS a un DNS envenenado al cual caen todos porque no es común que la gente cambie manualmente los DNS, sino que lo haga solo el DHCP con base en un metasploit todo porque los usuarios se conectaban a una red pública

Hay videos de Chema Alonso sobre lo anterior

Cuando un delincuente más quiere sacar, más se pone en riesgo

Esquemas básicos de defensa: no conectarse a redes públicas, de hacerlo, no tener el DNS de manera automática, olvidar redes

# Introducción a la seguridad

## Problemas de seguridad en las aplicaciones

- El punto inicial a considerar es que en la mayoría de los problemas de seguridad que son detectados en los servicios web, estos no fueron provocados por fallas en los sistemas de protección de los servidores web, en su lugar los problemas se generan por malas prácticas por parte de los programadores y algunos administradores.

Los principales problemas de seguridad en las aplicaciones son:

- Problemas de diseño.
- Problemas de implementación.
- Problemas de operación.

Por lo anterior, debemos de prestar mucha atención desde el comienzo del **Ciclo de Vida de Desarrollo Seguro de Aplicaciones (SSDLC)**.

\* Una vez liberada nuestra aplicación, esto es, en la fase de producción, debemos gestionar la seguridad de la misma y estar al siempre pendiente.

Muchos de los programas, el problema que tienen es que los errores de desarrollo causan que los delincuentes se aprovechen de estos.

Las aplicaciones web de entrada son inseguras porque son fácilmente vulnerables ya que el usuario puede meter información. Lo que pasa es que al crear el internet nunca se pensó en seguridad

Las aplicaciones en una intranet no son tan inseguras, pero lo que pasa es que no están al alcance de cualquier persona, sólo al interior de la empresa.

Aunque den flojera las normativas ISO están hechas para brindarnos seguridad.

## Objetivos de seguridad para los sistemas de información y comunicaciones TIC

Una aplicación debe de cumplir con los siguientes **objetivos de seguridad**:

- ❖ **Identificar** a las personas que acceden a la información manejada por un sistema o a los recursos del mismo.
- ❖ **Autenticar** a las personas que acceden a la información manejada por un sistema o a los recursos del mismo.
- ❖ Controlar el acceso a la **información** manejada por un sistema o a los recursos del mismo.
- ❖ Proporcionar **confidencialidad** a la información manejada por un sistema.
- ❖ Proporcionar **integridad** a la información manejada por un sistema o a los recursos del mismo.
- ❖ Mantener la **disponibilidad** de la información manejada por un sistema o de los recursos del mismo.
- ❖ **No repudio**! Proporcionar la prueba de que una determinada transmisión o recepción ha sido realizada, no pudiendo su receptor/transmisor negar que se haya producido.
- ❖ **Trazabilidad**. Proporcionar los controles que determinen que en todo momento se podrá determinar quién hizo qué y en qué momento

¿Cuál es la diferencia entre codificar y cifrar?

Hablando de cifrar finalmente se puede descifrar.



Al hablar de codificar es como hablar, pues el español es un código, así como el inglés, alemán o ruso. El código es darle un significado completamente diferente a las cosas. Es complejo porque no hay una forma completamente de decodificar

Película: Códigos de Guerra

México tiene de las mejores legislaciones del mundo dado que los bancos están bien restringidos para hacer sus procesos. Países como Argentina tienen problemas de clonación de tarjetas

#### ▼ 11-08-2022

El phishing lo usan los delincuentes para aprovecharse de la buena acción de ayudar de la gente

Luego como desarrolladores metemos malas mañas, por ejemplo cuando nos traen contra tiempo y trabajamos con información y generalmente no reforzamos la seguridad

¿Por qué el desarrollador y el DBA deberían ser diferentes? Porque el desarrollador tendría mucha información de estructura y datos almacenados en la base de datos

Gráfica de examen:

Entre más cómoda sea una aplicación bancaria, más insegura es. Entre más segura, más incómoda de usar

La documentación viene de ISO 27002

Otro objetivo de seguridad debe ser la integridad porque la información que se hagan en peticiones debe ser transparente (usaremos md5)

Investigar criptografía MD5

¿De qué se trata la disponibilidad como objetivo de seguridad? Tener disponible la información únicamente en el periodo en el que debe estar disponible, no más, no menos. Y también que sea sólo esa persona

Algunos errores son por mal desarrollo (como las backdoors)

El no repudio, como objetivo de seguridad es para asegurar que transacciones o cuestiones para que pueda comprobarse que se hicieron las transacciones

Es bueno distribuir el correo electrónico para distintos servicios

La trazabilidad, como objetivo de seguridad es hacer el trazado de la información que es por dónde pasó. Por dónde fue la información y hacer un seguimiento de la información. Pues con no repudio y con trazabilidad finalmente puede confirmarse si la persona es o no es quien quiere autenticarse

#### ▼ 12-08-2022

Todo lo anterior nos lleva al triángulo de seguridad de la información



# Triangulo de Seguridad de la Información



El primer error de diseño es, por ejemplo, al validar un login se especifica mucho si se equivocó en usuario o contraseña y no. Una medida de seguridad es no saber en un login si el usuario está mal o la contraseña en específico (está mal decirle “usuario erróneo” o decirle “contraseña errónea” específicamente. Mejor sólo decir “usuario o contraseña erróneo” para ambos casos)

Los jefes son enemigos de bloquear por 30 minutos después de hacer un login de 3 intentos

Como medida de seguridad el estándar ISO 27002 establece que podemos ver si ya están tratando de acceder a una cuenta varias veces, pues es cambiar la cuenta al usuario que quiere ser vulnerado

## Problemas de Seguridad

Los principales problemas de seguridad en las aplicaciones son

- ▶ Vulnerabilidades de seguridad en el diseño.
- ▶ Vulnerabilidades de seguridad en el código.
- ▶ Problemas funcionales de seguridad como autorización, control de accesos, etc.
- ▶ Vulnerabilidades de seguridad debidas a fallos de configuración.
- ▶ Problemas de seguridad debidos a la gestión de la seguridad una vez desplegada la aplicación.

Una buena política que manejan las grandes empresas es tener repositorios de código privados. Muchos tienen regla de código para no sacar código en internet pues sacarlo de internet hay que leer línea por línea el obtenido por internet

¿Qué pasa con la configuración de seguridad? Va muy ligada a la actualización de los sistemas. Por ejemplo usar sistemas obsoletos es malo. Windows 8 permite tronar la contraseña del usuario fácilmente.

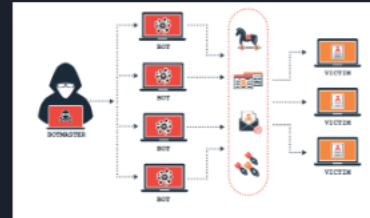
▼ 16-08-2022

## Vulnerabilidades

UNIVER  
DE 2

Vulnerabilidades de distinta naturaleza pueden dar lugar a que se materialicen amenazas que constituyan ataques a la aplicación como:

- Robo de contraseñas
- Ingeniería social.
- Errores y puertas traseras.
- Fallas de autenticación.
- Fallos de protocolo.
- Fuga de información.
- Ataques exponenciales Virus y gusanos.
- Ataques de denegación de servicio. (Dos -Denial of Service)
- Ataques de denegación de servicio distribuido o (DDoS Distributed Denial of Service)
- Botnets
- Ataques activos



Próximamente habrá una tarea (algo así como bastop) que es una máquina virtual para montar una página web super mal montada y después con OVVASP para probar después con la máquina virtual anterior

Luego se trabajará con TryHackMe

Hay que tener cuidado al trabajar con datos sensibles (como raza, religión, etc...)

## Riesgos aplicaciones en móviles.

UNIVER  
DE 2

Actualmente tanto nosotros como las empresas dependemos de manera muy importante de los teléfonos celulares por lo que es importante ser conscientes de los principales riesgos de seguridad que se generan por su uso.. Es decir por las aplicaciones en los móviles son:

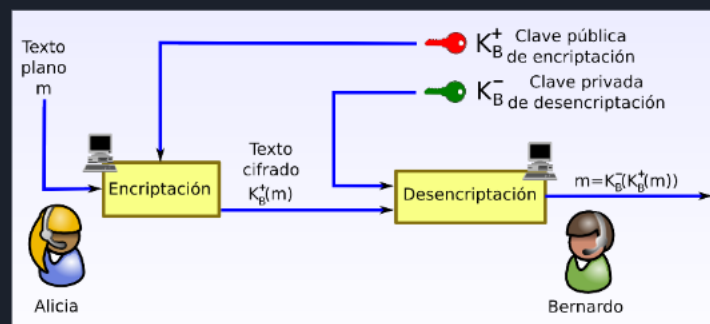
- Almacenamiento inseguro de datos.
  - Todo desarrollador es el responsable de proteger los datos de las personas, empresas o instituciones que utilicen sus aplicaciones.
  - Es muy recomendable que los datos no sean almacenados durante períodos de tiempo muy largos, al mismo tiempo procurar que sean anónimos, a fin de proteger tanto al usuario como al desarrollador.

## Riesgos aplicaciones en móviles.

- Controles frágiles en el servidor.
  - Siempre será necesario que validemos los datos de entrada que vaya a procesar nuestra aplicación, sea móvil o no.
  - Debemos darnos tanto tiempo como presupuesto para probar y validar la seguridad de nuestras aplicaciones, un error común es que por tener prisa de sacarla al mercado dejamos a un lado los riesgos para el usuario.
  - Conocer los riesgos de vulnerabilidad del lenguaje de programación que usamos para el desarrollo de nuestra aplicación.

- Fuga de datos involuntaria.
  - Se genera principalmente cuando una aplicación maliciosa coloca los datos sensibles o confidenciales en una ubicación de fácil acceso dentro del dispositivo móvil.
- Algunas medidas de seguridad para contrarrestar de raíz estas situaciones son:
  - Utilizar procedimientos almacenados ya que generalmente son seguros contra la inyección de SQL.
  - Validar todas las entradas, tipo, sintaxis, antes de que se muestren o almacenen los datos. (Inyección de código).
  - Rechazar la entrada no válida en lugar de intentar comprobar datos potencialmente hostiles.
  - Tener especial cuidado al conectarse a la base de datos u otros sistemas de soporte.

- Encriptación rota.
  - Lo ideal es utilizar algoritmos de cifrado para evitar cualquier violación a la seguridad, aunque la realidad es que es muy costoso y principalmente requiere tiempos largos de desarrollo, prueba y liberación. Es por ese motivo que normalmente los pequeños desarrolladores no lo utilizan (presupuesto y tiempos ajustados para la comercialización o liberación de la aplicación.)



- Códigos fuente desconocidos.
  - Muchos desarrolladores, por cuestiones de tiempo o falta de dominio del lenguaje de programación, optan por utilizar códigos fuente ya realizados por otras personas, o simplemente los copian de la web.
  - Algunos delincuentes proporcionan "amablemente" dicho código, en espera de que un incauto lo utilice, para posteriormente sacar el mayor provecho.
  - Siempre se debe verificar la procedencia de la fuente de nuestro código... si no están seguros de ella, ¡no la utilicen!. Algunas empresas tienen a disposición de sus desarrolladores repositorios de procedimientos, fortaleciendo de esta manera la seguridad de la organización.
  - Parte de las funciones del líder de desarrollo debe ser la vigilancia constante y oportuna de este tipo de situaciones. La metodología Agile por eso promueve juntas de monitoreo constantes.

## Introducción a Ethical Hacking

UNIVERSIDAD DE AG

Ya identificamos los posibles riesgos en las aplicaciones, identificamos al enemigo y sus motivos (Pues tu dices profe loco.. Ya que), aún nos falta analizar las vulnerabilidades de redes. Pero antes de irnos de largo. ¿Quién podrá salvarnos ? Acaso ¿ El chapulín colorado ?.

Ni malle. Para eso tenemos de nuestro lado a profesionales de la seguridad denominados Ethical Hackers. Que respetan principalmente las cuestiones éticas, morales y principalmente legales.

## Ethical Hacking en Monitoreo

UNIVERSIDAD DE AG

Se les conoce también como auditorías de seguridad e implica la evaluación constante y a conciencia no solo de la infraestructura técnica de seguridad es importante evaluar las políticas, los procedimientos para prevenir los ataques. las habilidades de los miembros del equipo y principalmente los procedimientos para recuperarnos en caso de que se presenten los incidentes. Y también es válido recurrir al esquema denominado Bug Bounty mediante plataformas como HackerOne o BugCrowd, entre otras.

Honestamente la forma más fácil de ser víctima de la delincuencia es pensar. "Estoy lo suficientemente cubierto para no ser víctima de ningún acto delictual."

Ejemplo al 3 de Febrero de 2022 de Bug Bounty. Google ofrece hasta 1.5 millones de dolares a quien encuentre vulnerabilidades en sus teléfonos pixel

<https://bughunters.google.com/about/rules/6171833274204160>

Pero más allá de esto google ha centralizado su plataforma de bug hunters. Por lo que en su página podrán encontrar todos los retos abiertos e incluso una academia para volverte un bug hunter exitoso.

<https://bughunters.google.com/learn>

# Ethical Hacking en Monitoreo

Github ha realizado lo propio.

<https://bounty.github.com/>

Apple

<https://developer.apple.com/security-bounty/>

Microsoft

<https://www.microsoft.com/en-us/msrc/bounty>

Facebook

<https://www.facebook.com/whitehat>

Se les conoce también como auditorías de seguridad e implica la evaluación constante y a conciencia no solo de la infraestructura técnica de seguridad es importante evaluar las políticas, los procedimientos para prevenir los ataques. las habilidades de los miembros del equipo y principalmente los procedimientos para recuperarnos en caso de que se presenten los incidentes.

Honestamente la forma más fácil de ser víctima de la delincuencia es pensar. “Estoy lo suficientemente cubierto para no ser víctima de ningún acto delincuencia.”

▼ 17-08-2022

## Esquemas de defensa

En una red

Un Host Bastion mantiene la seguridad hacia el interior de la empresa

DMZ: Zona demilitarizada. Equipos de cómputo para que las personas puedan verlas. Tienen la IP pública. Equipos al interior de la red tendrán una IP privada.

Un Host Bastion mantiene equipos detrás del firewall y protege todo lo que va a estar al interior.

La DMZ queda hasta cierto punto desprotegida

Un IDS es un sistema detector de intrusos. El IDS permite identificar errores al configurar cosas como el firewall. También puede identificar un ataque desde el interior. Es muy importante el IDS

Cuando se tienen equipos en distintas redes, no se puede proteger todo con un firewall. Nos encontramos con que hay equipos fuera del edificio corporativo. Para trabajar en este esquema, hay que usar un sistema MDM

Ahora se usan más redes virtuales y toda la cuestión de virtualización.

Al volverse uno más vulnerable se usa la MDM y BYOD. ¿Qué implica la tecnología MDM? Que si te roban el celular, no pasa nada, porque el teléfono sólo es un punto de acceso, no contiene la información

BYOD es una metodología que trae a los usuarios un dispositivo de gusto personal

MDM es la tecnología y BYOD es la metodología

▼ 18-08-2022

El Ethical Hacking en monitoreo

Para hacer una cuestión de hackeo hay que hacerlo donde está permitiendo o donde haya un contrato. El hacerlo de manera correcta trae beneficios como el BugCounty

Por ejemplo Google publicó el 3 de febrero del 2022 una oferta de 1.5 millones de dólares a quien encuentre vulnerabilidades en sus teléfonos píxel.

Existe una página bughunters.google.com

GitHub, Apple, Microsoft y Facebook también tienen sus páginas

Ejemplos de Google

Ejemplos de GitHub

Ejemplos de Facebook

Más adelante se verá el footprinting y el fingerprinting

Registrarse a una organización Dragon Jar (dan conferencias y se puede aprender muchísimo)

La forma más fácil de ser víctima de delincuencia es pensar que estoy seguro de la delincuencia y peor publicarlo

## Unidad 2: Seguridad en las redes de comunicación

Preparando nuestros equipos

Instalar el fping con `dnf install fping` o `apt install fping`

Instalar nmap OJO si instalamos la versión 7.92-core22 `sudo snap install nmap`

Como instala snap no queda casada con el controlador de red por lo que hay que agregarla con `snap connect nmap:network-control`

Tip: Academia ESET es una academia gratuita con cursos de paga y gratis

### ▼ 19-08-2022

Para proteger algo hay que conocerlo, para esto debe usarse fping

Llevamos sólo la configuración de Virtual Box

Instalar la badstore y se tarda unos 10 minutos. Hay que esperar un buen rato y esperar por todo el proceso

Registrar las vulnerabilidades y reparar las vulnerabilidades (incluyendo inyección) se saca 100 en el primer parcial

Linux tiene una ventaja sobre Windows ya que en terminal da detalle de cualquier error

Será necesario más adelante la instrucción fping ya que a seguridad se puede hacer una revisión general de la red y podemos ver todos los equipos con los que estamos trabajando

El Warchar es un sniffer

### ▼ 22-08-2022

## Seguridad de las comunicaciones

Vamos a trabajar con WARCHAR

¿De dónde viene el candadito del navegador? Significa que en esa página el viaje y comunicación está cifrado

¿Qué es un DNS?

La importancia de trabajar los DNS manuales es muy demostrable en la vida diaria

Hay varias autoridades certificadoras:

- ACE (Agencia de Certificación Electrónica). Busca proporcionar protocolos de seguridad bastante eficientes (maneja la seguridad de VISA y MasterCard)
- FESTE (Fundación para el Estudio en la Seguridad y Telecomunicaciones). Trabaja en el área de comercio

- SISCER (Sistema de certificaciones). Se encarga de cajas de ahorro. Pertenece a intercomputer y trabaja con varios bancos
- PS (Publishing Service). Empresa española y sólo trabaja a nivel europeo y maneja niveles de seguridad interesantes
- Verisign. Controla 2 de los 13 servidores raíz que operan los servidores de dominio
- Digicert. Sirve como intermediario de Verisign

Estos certificados no se ven normalmente, generalmente se vería la empresa intermediaria.

Siempre hay que revisar los certificados por seguridad

Bajar el WARCHAR para el viernes

Las tarjetas bancarias tienen 3 métodos de seguridad: el número de tarjeta, la fecha de vencimiento y los tres números de atrás

En el examen necesitaremos hacer una validación de una página (campo de asunto, detalles y general)

#### ▼ 23-08-2022

Root Servers: Servidores que traducen del DNS a la IP

Estos servidores sólo son 13

Con un router aplicando DNS privados, primero revisa los privados y después sale a los servidores y redes públicas

Verisign controla 2 de los servidores

“anyCast” y el procesamiento distribuido son distintos.

Al solicitar una dirección DNS, se buscan los servidores y cualquier servidor podrá contestar y contestará el que esté más libre o el más cercano.

La diferencia con procesamiento distribuido ahí sí, todas las máquinas tienen partes distintas de la ejecución y busca qué equipo busca el usuario y a esa manda el procesamiento

Otro servidor lo mantiene el Instituto para la formación científica en Marina del Rey, California

Otro servidor más está alojado por Cogent Communications

Otro lo tiene el departamento de defensa de Estados Unidos, otro el Laboratorio de Investigación de la Armada de EEUU

Otro lo tiene Autonomica

#### ▼ 24-08-2022

### Incautaciones de dominio del sitio web en 2010

Se ha visto el 29 de noviembre de 2010 se vio la incautación de WikiLeaks.

Se han evitado cosas para que EEUU tenga el control de la red aunque EEUU sigue insistiendo

La Deep Web se define básicamente como información sin indexar

El 29 de noviembre del 2010 comienza a darse la ley antiterrorismo en las redes por lo que se exige que todos los proxys registren el flujo de las IPs

ICANN

LACNIC

La implementación IPv6 tiene mejor documentación en español porque latam es puntera en esta tecnología

### Comunicaciones y canales seguros

El uso de BYOD con la metodología MDM se complica y hay tres opciones para utilizar tres tipos de canales

Intranet y red local son distintos. Una intranet proporciona servicios. Una red local no tiene nada, sólo equipos conectados a una red común.

Seguridad: Las VPN tienen una IP destino y la IP del host. El número de VPN es el número de saltos que puede dar el paquete antes de desaparecer en la red.

▼ 25-08-2022

No fui a clase :(

▼ 26-08-2022

Poner en modo promiscuo la tarjeta de red virtualizada

Puentear todas las redes de las máquinas virtuales

Hay que poner marcado cable conectado a todas las máquinas virtuales

```
fping -s -g -r1 172.16.96.0/22
```

El -s sirve para dar un resumen al final

El -g agrupa los resultados

El -r serán las repeticiones que harán

Si se va a usar en casa, la máscara en lugar de ser 22 será 24

La badstore se usa 1024 de memoria, un procesador y el kernel se usa un Ubuntu con el más bajo aceptable

Se carga un navegador

Se accede a la dirección ip de la badstore

Al entrar a WireShark hay que leer la tarjeta de red correspondiente

▼ 29-08-2022

# Seguridad en Redes de Computadora.

Mtro. Arturo Ocampo Silva



## Unidad II

### Comunicaciones y Canales Seguros.

Al hablar de un canal “seguro” hablamos específicamente de la protección que debemos brindar a la comunicación entre el cliente y el servidor, para esto necesitamos hablar de autenticación y principalmente de encriptación.

Este tema toma relevancia especial cuando hablamos de BYOD ya que el personal puede conectarse desde cualquier lugar a nuestra información. Por lo que requerimos garantizar que solo se conecte quien está autorizado y que la información no sea fácilmente interceptada.

Canal Seguro. Para aumentar la seguridad del canal podemos utilizar 3 estrategias.

- Uso de Túneles.
- Uso de VPN.
- Uso de Proxy.

## Comunicaciones y Canales Seguros.

### VPN (Virtual Private Network)

Para la comprensión de este tema tienen que recordar sus clases de redes, donde se estipula claramente lo que es una red privada (Intranet, red local, etc), debido a que la VPN funciona como una extensión de esa red local, pero como su nombre lo dice mediante una red virtual que circula a través de una red pública.

Para esto el flujo de información de nuestro o hacia nuestro equipo del exterior circulara de nuestro equipo al carrier y del carrier directamente al servidor VPN, el cual será el encargado de gestionar nuestras comunicaciones, por lo que para el resto del mundo la dirección ip pública visible NO será la de nuestro router, será la del servidor VPN.

¿ Pero y la seguridad ?

Para esto las VPN utilizan el cifrado y principalmente la tunelización por lo que ninguno de los equipos intermedios pueden identificar la información que están transmitiendo.

## Seguridad.

La tunelización básicamente es el meter cada paquete con sus respectivos protocolos, IP origen, ip destino, versión de protocolo, TTL del paquete y datos en otro paquete con características independientes del que contiene y cuyo encabezado contiene como destino la IP del servidor VPN. Ahora aunque no es obligatorio la realidad es que todas las VPN además de la tunelización realizan un proceso de encriptación mediante el uso de protocolos de seguridad como IPSEC u OpenVPN (entre otros) .

Además trabaja a nivel de Sistema Operativo, por lo que permite proteger todo el tráfico del usuario, no solo el de una aplicación específica.

## Comunicaciones y Canales Seguros. Proxy

Este es un servidor intermedio al que nos conectaremos para poder enmascarar nuestra dirección IP , pero a diferencia de una VPN trabaja sobre una aplicación en específico y realmente no encripta la conexión del usuario, por lo que nos sirve más como una medida para filtrar los paquetes que ingresan a nuestra organización. restringiendo el tráfico de manera adecuada . Existen esencialmente 3 tipos de proxies.

- **Proxy transparente.**

Intercepta la comunicación en la capa de red sin que se de cuenta el usuario, permite filtrar contenido y aplicar restricciones

- **Proxy abierto.**

Se encuentra a disposición de todo el público y permiten principalmente evadir restricciones de ubicación y obtener anonimato.. (Neta no los recomiendo.)

- **Proxy Cache.**

Guarda el contenido de las páginas visitadas de manera que cuando el mismo usuario o alguien más dentro de la intranet desee visitar la misma página esta se cargue de manera más rapida.

### Sub-Tipos de Proxies transparentes.

- **Proxy inverso.**

Se integra como un WEB service (Entras a una página web dentro de la intranet) y reenvía las solicitudes que recibe a uno o más servidores de origen. No es necesario configurar los clientes para utilizarlos.

- **Proxy NAT.**

Su función exclusiva es la de permitir ocultar la IP de los equipos que se encuentra detrás de él mediante la función de nateo.

### Entre los proxies abiertos nos encontramos 2 subtipos.

- Proxies HTTP ó WEB: Son la forma más sencilla de un proxy, se instalan en el navegador y con estos se redirige el tráfico del usuario para mantener oculta su IP.
- Proxies Socks: Estos también trabajan desde un navegador pero a diferencia del anterior permite filtrar las aplicaciones, por lo que controla el uso de DNS y más importante el flujo de las aplicaciones web que pasan por él. Incluso puede filtrar cuando se usa el protocolo UDP.

## Protocolos y mensajes seguros

UNIVERSIDAD DE ALCALÁ

Los protocolos son la serie de reglas e instrucciones que se deben cumplir a ambos lados para poder establecer comunicación. (más técnico define el formato de los datos que son enviados entre los distintos componentes de una red informática.)

Cada vez es más necesario el utilizar protocolos de red que garanticen la seguridad e integridad de los datos en tránsito independientemente del medio de red utilizado, esto debido a que cada vez se maneja mas información confidencial y delicada, como pueden ser números de tarjeta de crédito, datos personales, etc.

Los protocolos de seguridad más allá de solo permitir la comunicación como puede ser TCP/IP, http o ftp deben garantizar el cifrado de los datos, manejar un "control de la estructura y secuencia de datos" (lógica) así como autenticación.

Algunos de los protocolos de seguridad más reconocidos son: SCP, SFTP, SMTPS, IMAPS, SSH y HTTPS

## Aplicaciones y Servicios Seguros

UNIVERSIDAD DE ALCALÁ

En cuanto a las aplicaciones tenemos que establecer que las aplicaciones son seguras debemos considerar más que solo el que cubren nuestro requerimientos, debemos asegurar que contaremos con el soporte para la implementación, para el funcionamiento, que la empresa se mantendrá en el mercado, que el proveedor cuenta con la experiencia y aval de otras empresas y que es reconocido en su rubro. Para esto la mejor herramienta de apoyo es el cuadrante mágico de Gartner. Ahora una aplicación si no se implementa sobre servicios seguros, difícilmente podrá mantenerse aceptablemente segura. Para esto deberemos considerar servicios seguros como son DNS seguros ( quad9, cisco (opendns), fortigate, norton, etc).

Los servicios son un conjunto funciones que apoyaran en el uso de la red basándose en los protocolos. Ejemplo de estos son DNS, DHCP entre otros.

# Arquitectura Segura en Internet

## SSL / TLS

Son protocolos criptográficos que proporcionan autenticación y cifrado de la información entre servidores, máquinas y aplicaciones que operan sobre una red (ejemplo un cliente conectándose a un servidor web). SSL (Secure Sockets Layer) es el predecesor del TLS (Transport Layer Security). SSL fue originalmente desarrollado por Netscape, su última versión fue SSLv3 en 1999, TLS fue introducido en 1999 como una nueva versión del SSL 3.0.

OJO. Actualmente cuando se compra un certificado se sigue utilizando el concepto SSL aunque la realidad es que estás comprando un certificado TLS y el nombre correcto es ssl/tls.

SSL ya no existe, la nueva versión es TLS

SSL proporciona autenticación, integridad y confidencialidad de la información entre los extremos de una comunicación a través de mecanismos criptográficos

Habitualmente sólo el servidor es autenticado, y mediante esta autenticación se establece un canal confidencial, mientras que el cliente se mantiene sin autenticar. Aunque para aplicaciones de alta seguridad se puede utilizar la autenticación mutua de ambas partes, mediante la utilización de los certificados x.509.

Hay que aclarar que cuando SSL proporciona autenticaciones mutuas suele ser en ambientes pequeños o muy controlados, porque a gran escala se requeriría del funcionamiento de una PKI (Public Key Infrastructure) en ambientes tan amplios como Internet.

- Aunque menos común, también se pueden usar algoritmos criptográficos anónimos, permitiendo que el servidor no sea autenticado, estos algoritmos suelen estar deshabilitados y en muchas implementaciones del protocolo no están incluidos.

Ofrece autenticación, integridad y confidencialidad.

- Autenticación para comprobar que toda la documentación de la empresa que quiere el certificado es la que dice ser.
- La integridad permite validar el certificado con la página y a su vez va a validar el certificado con la base de datos del emisor del certificado.
- Confidencialidad para manejar los datos cifrados.

El x.509 es una evolución del x.500 donde se establece un formato para trabajar los certificados SSL. Hay dos tipos de certificaciones SSL (que en realidad son TLS)

En ambientes controlados se puede dar la certificación mutua.

Antes de entrar en detalle establezcamos. Para qué sirven:

Originalmente para

- Transacciones electrónicas (Ecommerce )
- Comunicación segura entre servidores.
- Seguridad entre bases de datos y aplicaciones
- Acceso a cuentas de usuarios del Active directory
- Acceso a correo electrónico Outlook, exchange, etc.
- Confirmar identidad como usuario.
- Navegación WEB - https.

Para Active Directory vamos a ver Kerberos

Probablemente el Active Directory no jaló en proyectos anteriores por una fecha y hora.

Principales fases de SSL:

- Autenticación del servidor: Se lleva a cabo al inicio del protocolo por medio del envío de la clave pública del servidor, en el certificado X.509 que se envía al establecer la conexión, junto con su firma digital
- El certificado del servidor debe ser validado por los usuarios.
- Generalmente los sitios web que utilizan SSL tienen sus certificados firmados por autoridades certificadoras válidas. Ojo con él generalmente.
- Confidencialidad e integridad de los datos: Una vez que el usuario ha recibido la clave pública del servidor la usará para enviar de forma segura el material criptográfico necesario para poder generar la clave de sesión.

Arquitectura SSL

- La autenticación del usuario: Consiste en una firma digital generada por el usuario haciendo uso de la clave privada y del envío de su clave pública por medio de un certificado X.509 (si se requiere autenticación mutua) es opcional, y requiere que el servidor web pueda validar este certificado
  - Se utiliza principalmente en la banca electrónica.

### Tipo de Certificado:

- SSL de Validación de Dominio (DV). Es el nivel más bajo de validación, Permite validar únicamente un dominio sin subdominios verificando tan solo que quien solicita el certificado controla el dominio que protege.
- SSL de Validación de Organización (OV). Estos certificados no solo validan el dominio sino que garantizan que la organización existe. Para esto la entidad certificadora solicitará.
  - Documento que compruebe la existencia legal de la compañía.
  - Licencia comercial emitida por el gobierno.
  - Comprobante bancario.
  - Facturas telefónicas y de servicios públicos que comprueben el domicilio de la institución.
  - Verificación de la propiedad del dominio.

- SSL de Validación Individual (IV). Verifica la identidad de la persona que solicita el certificado.
- SSL de Validación Extendida (Extended Validation (EV)). Es muy similar a OV, verifica la identidad de una organización. Sin embargo, EV representa un estándar de confianza más alto que OV y requiere verificaciones de validación más rigurosas para cumplir con el estándar de CA / Browser Forum's Extend. Generalmente solo los maneja DIGICERT.
  - La existencia jurídica de tu compañía.
  - Que el nombre legal registrado en el certificado coincida con el nombre en los registros oficiales del gobierno.
  - El domicilio de la empresa.
  - Que tu empresa tenga un número registrado y comprobable.
  - Un representante legal
  - Identificaciones del representante legal.

### Sub-tipos de Certificado:

SSL de múltiples dominios (UCC). Permite proteger todos los subdominios de una organización.

SSL Wildcard: Permite proteger todos los dominios almacenados en un solo servidor

Una firma digital no es lo mismo a una firma certificada en cuanto a documentos.

La firma digital consiste en escanear su firma y eso equivale a su firma digital ¿pero esta firma es válida? Ya que como no existe evidencia, un buen abogado tumba este tipo de firmas rápidamente.

Con una firma certificada se trata de un conjunto de números a la que le pediste a una entidad certificadora y se valida gracias a que se puede rastrear a la persona

Una firma electrónica del SAT es una firma certificada

Normalmente no se ha sacado un certificado cuando se hace código de programación y debería de sacarse este tipo de certificados

#### ▼ 30-08-2022

Repaso de SSL y TLS

Parte de los problemas de seguridad bancarios viene del TLS porque actualmente trabajamos con el TLS 3. Parte del problema al que se enfrenta al ver la gráfica de comodidad vs seguridad, generan los problemas con el celular.



Por ejemplo Bancomer se quejaba porque no se podía conectarse con dispositivos antiguos aunque no pasaba lo mismo ni con Banorte ni con Santander. A los que más les han pegado son Banorte y Santander (aunque a Bancomer también le han pegado)

## Arquitectura Segura en Internet

### IPV6 vs IPV4

#### Introducción.

- Internet en las últimas décadas enfrentó un crecimiento desmedido por lo que en el 2011 se agotaron las direcciones IPv4. ( $2^{32}$  dispositivos. = 4.300 millones)
- La aparición de IoT cada vez nos vuelve más dependientes del internet .
- La función de IPv6 es reemplazar a IPv4.( IPv6 =  $2^{128}$  direcciones disponibles = 340 sextillones de dispositivos).
- En lo relacionado a los protocolos de transporte y aplicación IPV6 es una extensión de IPV4 por lo que en su mayoría no requieren cambios para operar. (Algunas excepciones son FTP o NTP)
- IPv6 especifica un nuevo formato de paquetes diseñado para optimizar el procesamiento del encabezado de paquetes en procesadores a 64 bits

Diferencias entre IP públicas y privadas. Una es la que va del router al exterior y otra es al interior del router

IoT: Internet of things

IoTM: Internet de las cosas médicas

Todo esto lleva al desarrollo de la IPv6

- Las cabeceras de los paquete IPV4 e IPv6 son significativamente distintas por lo que de manera directa los dos protocolos no son interoperables, anteriormente esa falta de interoperabilidad **era** el mayor inconveniente para la transición de IPv4 a IPv6. Actualmente (desde el 2020) los dispositivos manejan la interoperación de manera transparente al usuario.

Aquí vamos a empalmar con nuevos conceptos que deja obsoletos algunos conceptos de redes como el IPv4

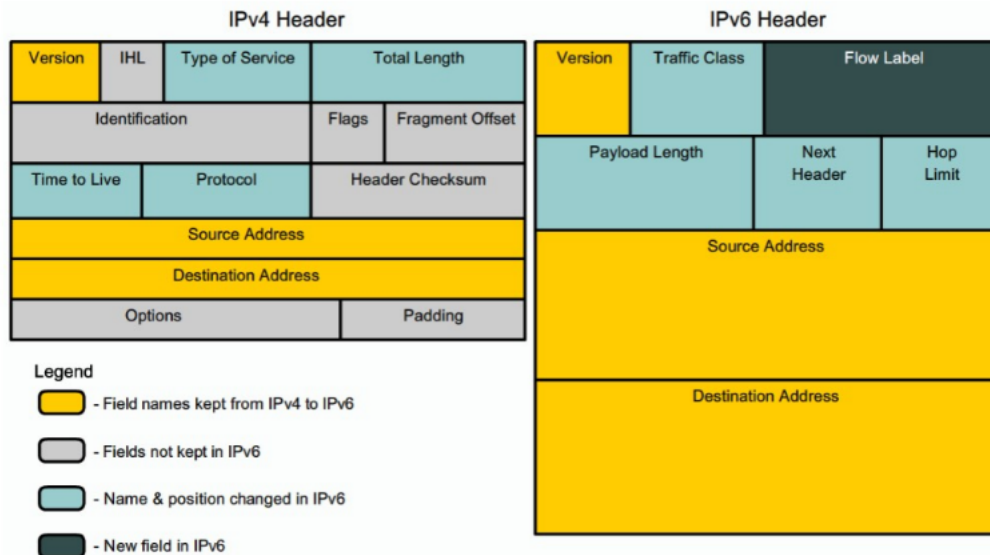
El IPv6 busca que todos los equipos trabajen con IP pública

Hay autores que siguen diciendo que IPv6 es inseguro (aunque al analizarlo, la realidad es que es falso)

Las velocidades no suben pero sí las capacidades de transportación de datos por lo que las redes no funcionan más rápido sino más eficiente.

Otro detalle es la cuestión de las cabeceras porque las cabeceras se reducen y la capacidad de transportación aumenta

México tiene un nivel muy alto sobre IPv6



Para una bibliografía sobre seguridad de IPv6 lo mejor es tomar solamente a Cisco

#### Diferencias más significativas.

| IPv4                                      | IPv6                                                                      |
|-------------------------------------------|---------------------------------------------------------------------------|
| Cabecera 20 Bytes                         | Cabecera 40 Bytes Bloques de 64 bits ideal para estos procesadores        |
| Type of Service (QOS Calidad de Servicio) | Traffic Class (QOS Calidad de Servicio)                                   |
| /                                         | Flow Label                                                                |
| Total Length                              | Payload Length                                                            |
| Protocol                                  | Next Header (encabezado capa de transporte indica si lleva tcp/UDP/ Quic) |

| IPv4                   | IPv6                 |
|------------------------|----------------------|
| Time to Live           | Hop Limit            |
| Direcciones de 32 bits | Direcciones 128 bits |

El protocolo Quic permite un flujo de datos más rápido pero más inseguro

IPv6 trabaja todo con el protocolo IPC lo cual le dan sus características

Investigar para qué sirve IPC



### Características nuevas.

- **Autoconfiguración de host con Neighbor Discovery Protocol (NDP)**
  - Los nodos IPv6 pueden configurarse a sí mismos cuando son conectados a una red IPv6 esto lo hace usando mensajes de descubrimiento de routers de ICMPv6
  - Si la autoconfiguración no es la adecuada para una aplicación se pueden usar protocolos a nivel de aplicación como Dynamic Host Configuration Protocol para IPv6 (DHCPv6) o recurrir a la vieja confiable de configurar los nodos de manera manual con una IP estática
- **Multicast.** Mejora la capacidad de envío de un paquete único a múltiples destinos ya que las comunicaciones multicast se incluyen como parte de la especificación base de IPV6.(RFC3307).

En IPv6 desaparece el DHCP e IPv6 no usa broadcast

El DHCP en IPv6 es una función opcional pero es peligroso por usar el NDP.

IPv6 para asignar direccionamiento sí valida la MAC Address del dispositivo y analiza cada dispositivo para que la MAC Address sea parte de su dirección

¿Por qué es necesario poder clonar la MAC Address? Realmente se había pensado para hacerse de forma benéfica Te permite "hasta cierto punto" identificar de dónde viene la comunicación

Probablemente el viernes hacemos el sniffeo, clonamos la Mac Address y comprobamos lo que hicimos

El protocolo UDP se usa en menor escala pero se usa mucho al hacer búsquedas de DNS

IPv6 ya no maneja los DNS con UDP, sino con TCP lo cual da más seguridad

Lo malo es que interceptar el DNS puede permitir hacer phishing y ahora con IPv6 ya no podrán interceptarse los IPv6

#### ▼ 31-08-2022

- **Procesamiento simplificado en los routers**
  - Desaparece Checksum, que si bien es una excelente medida de seguridad es redundante con funciones de protocolos superiores (Como IPSec ).
  - Se reduce la fragmentación, lo que reduce de manera significativa el procesamiento que deben llevar a cabo los routers.
- **Seguridad a Nivel de Red.**
  - (Internet Protocol Security (IPSec) que es el protocolo que permite dotar de confidencialidad, integridad y autenticación deja de ser opcional.
  - IPSec se auxilia de 2 protocolos para garantizar la integridad, autenticación y confidencialidad, atributos que hereda a s IPv6 (Authentication Header(AH) y Encapsulating Security Payload (ESP).
  - IPSec también provee un mecanismo para el intercambio de las claves denominado IKE Internet Key Exchange.

- Soporte mejorado para las extensiones y opciones. Se codifican las opciones de la cabecera IP permiten límites menos rigurosos en la longitud de opciones y mayor flexibilidad para introducir nuevas opciones en el futuro.
- Payload Length. A diferencia de IPv4 donde la longitud de los encabezados de los paquetes es variable y en base a un algoritmo se determina dónde empieza y termina un paquete (limitado a 20 bytes) en IPv6 los paquetes siempre tienen 40 bytes de encabezado
- Uso de jumbogramas. (Jumbopayload) Los paquetes pueden ser de hasta 4gb. OJO esta es una opción configurable no aplica para todos los paquetes y se depende completamente de la capacidad de los routers para la comunicación ya que en IPv6 NO se pueden fragmentar paquetes en los routers. Por lo que se usa un Path MTU Discovery que usando una técnica similar a la de IPv4 envía mensajes a través de la ruta para determinar cuál es la MTU mínima general. (Si cambia la ruta se pierde el datagrama)

No todos los paquetes IPv6 traen por default enviar jumbogramas

- Quality of Service (QoS). Recordemos que QoS indica la capacidad de la red para sostener un comportamiento adecuado del tránsito que circula en ella, asegurando la entrega de información pero priorizando las de desempeño crítico (aplicaciones en tiempo real) . IPv6 mejora esta implementación consiguiendo mayor rendimiento y aprovechando mejor el ancho de banda existente.
- IP Móvil. Al hablar de una IP única mundial, Esta IP puede acompañar a nuestro equipo a cualquier lugar del mundo.

Había switches bien cacas que no eficientaban el envío de paquetes y ahora los modernos sí tienen QoS

La lista ARP tiene dos columnas, en una tiene las MAC Address y en otra las IPs. El comando en Linux es sólo "arp"

EL QoS es requerimiento de IPv6

El NDP (Neighbor Discovery Protocol)

Su principal objetivo es resolver las direcciones IPv6 en direcciones MAC válidas que son las direcciones de hardware propias de cada dispositivos.

La lista ARP es sustituida por neighbor cache

Asigna el gateway de manera automática apoyándose en Router Advertiser Protocol

Realiza un proceso de DAD (Duplicate Address Detection para garantizar que ningún otro dispositivo la utiliza en la red).

DAD NO es un protocolo, es un proceso

NDP está integrado a los protocolos IPv6

El DHCP para pedir una dirección la máquina hace un broadcast (le tira a todas las máquinas a ver quién contesta solicitando el direccionamiento) y el DHCP le contesta dándole la información de direccionamiento, dándole el ARP

En IPv4 todo se hace por broadcast

Supóngase una IP 148.211.6.144/22

Donde el 22 es la máscara o el prefijo.

El último número corresponde al host del equipo que está conectándose

Con base en los vecinos, logra identificar el prefijo

Aquí se usará tanto un unicast como multicast

¿Cuándo conviene hacer un direccionamiento manual? Cuando se está en una intranet, porque en el exterior se puede duplicar alguna IP y generará problemas

El NDP usa:

Neighbor Solicitation (NS): Este mensaje le pregunta a un host con una dirección IPv6 en particular la de destino.

Neighbor Advertisement (NA): Este mensaje lista la dirección IPv6 y MAC del remitente

En una IPv6 que haya dos puntos :: significa que en la IPv6 existen puros ceros :0000: de la forma anterior y sólo puede usarse una vez.

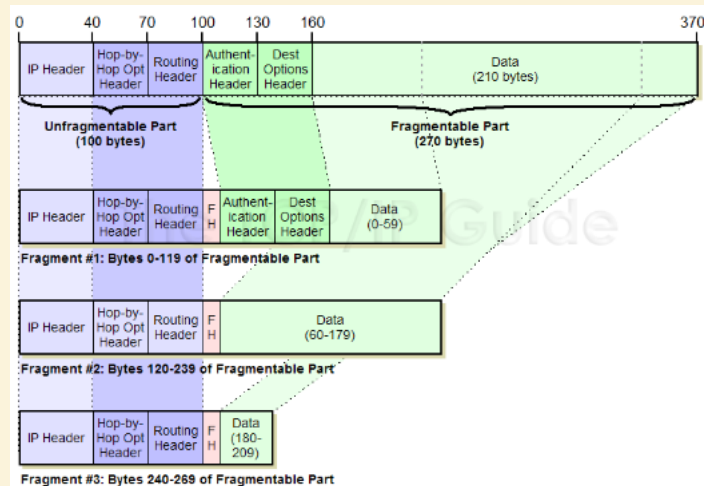
¿Por qué de repente aparece IPv6 e IPv4? Porque ahora se pueden mezclar las comunicaciones entre IPv6 e IPv4 ya que, por ejemplo, la UAA trabaja con TotalPlay empresarial que trabaja sólo con IPv4

## Usando SLAAC con Mensajes NDP RS y RA

SLAAC es el sustituto de DHCP, pues DHCP se usa en IPv4, ¿cómo lo hace?

1. Aprende el prefijo IPv6 usando el enlace desde cualquier router usando los vecinos, ahorrándose el DHCP
2. Construye una dirección desde el prefijo y el ID usando las reglas EUI-64
3. Y antes de usar la dirección primero se usa DAD para estar seguro que ningún otro host está usando la misma dirección

- La fragmentación de paquetes solo se puede realizar por el dispositivo que envía el datagrama.



- Para la detección de vecinos IPv6 usa en lugar de NDP el protocolo SEND que provee un método criptográfico independiente de IPSec.
- Permite vincular una clave de firma pública, generando una dirección generada criptográficamente que sirve al usuario como "Prueba de propiedad"
- Al no requerir NAT la seguridad del cifrado va de extremo a extremo.
- MTU (Unidad de transmisión Máxima) En IPv4 para routers y enlaces el MTU es de 56 byte, para IPv6 el tamaño del datagrama es de al menos 128 byte

### ▼ 01-09-2022

En IPv4 puede fragmentar los paquetes cualquier dispositivo. EN IPv6 no

El problema con esa fragmentación es que es una vulnerabilidad ya que pueden fragmentar, leer de dónde viene y a dónde va. En IPv6 no, pues sólo el emisor lo fragmenta

# Seguridad en Redes Inalámbricas

Mtro. Arturo Ocampo Silva

Para entrar en contexto es necesario entender que las primeras redes inalámbricas se crearon como un complemento a las redes LAN cableadas, esto derivado del surgimiento de las pc portátiles, lo que volvía necesario dotar a los usuarios de mayor movilidad utilizando para esto un acceso inalámbrico de corto alcance.

Conforme estas redes fueron evolucionando y ganando adeptos se volvió necesario crear una tecnología inalámbrica que asegurará la compatibilidad independientemente del fabricante, con el objetivo de lograr esa meta el 15 de Septiembre de 1999 un grupo de empresas Nokia, Lucent, 3Com, Aironet (Ahora propiedad de Cisco), Harris Semiconductor (Intersil) y Symbiol Technologies (motorola) se unieron para crear la wireless ethernet compatibility alliance (WECA - Desde Octubre del 2002 Wi-Fi Alliance), presentando en ese momento el Wi-Fi el cual está soportado en el estándar IEEE 802.11 High Rate (HR) y declarando al mundo que quien portara el logo de Wi-Fi, estaría garantizando su compatibilidad con cualquier otro dispositivo que portara el logo independientemente del fabricante.

Protocolos de red está el WPA o WPA2 y WEP (una metodología a considerar es la WPS)

Con la WEP puede vulnerarse una red doméstica con un cracker web en probablemente 5 minutos (según el profe)

La WiFi Alliance fue una asociación entre distintas empresas (Nokia, Lucent, 3Com, Aironet) para conectar los equipos de estas distintas marcas con redes y hacer todas las máquinas compatibles.

WiFi no es la antena. Lo que se tiene es una tarjeta de red que es compatible con el protocolo WiFi

Un poco de Historia.. Hedy Lamarr actriz de cine e inventora en 1942 patentó su "sistema de comunicación secreta" que da origen al primer estándar Wifi.

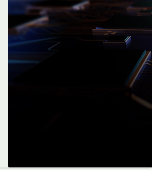
El estándar WiFi (IEEE 802.11) opera en la capa física de TCP/IP y es análogo al protocolo IEEE 802.3 (ethernet) para redes locales cableadas. Ya que fue diseñado de manera que exista una compatibilidad total entre ambos protocolos.

Desde que se creó el estándar IEEE 802.11 no ha parado de evolucionar, mejorando aspectos como el rango, la velocidad de transferencia de información, la seguridad, etc. Derivando en nuevos estándares IEEE como IEEE 802.11b, IEEE 802.11g, IEEE 802.11i, IEEE 802.11n, etc.

Recomendación:

IEEE - The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.  
IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

 <https://www.ieee.org/>



La WEP no es que sea malo en seguridad, pues maneja un cifrado Rivest Cipher 4, pero el problema radica es que trabajaba a 8 bits y no había la tecnología de hoy. También trabaja con un proceso de clave simétrica (la seguridad asimétrica es más segura)

En cuestiones de seguridad WiFi incorpora como medida de seguridad inicialmente WEP (Wired Equivalent Privacy) con la idea de proporcionar niveles de seguridad comparables a la de una red tradicional cableada, para esto utiliza los siguiente:

- Algoritmo de cifrado Rivest Cipher 4 (RC4) con **clave estática compartida por todos los usuarios de la red** de 64 y 128 bits.
  - Incluyen un vector de inicialización (IV) de 24 bits para dotar de **confidencialidad** a las comunicaciones.
- Hace uso de un código de redundancia cíclica **CRC-32** para **lograr la integridad** de las comunicaciones.
- Proporciona un mecanismo de **autenticación** que comprueba la **posesión de la misma clave compartida** utilizada para el cifrado.

¿Qué pasa cuando se selecciona el modo automático en el modo de compatibilidad? Elige cualquiera y los que quieren vulnerar, eliminan los modos WPA y WPA2 para que conecte WEP (es decir, la más vulnerable)

Al comprar módems hay que buscar mejor que el modo sea WPA3 ya que ya existe

A partir de 2001 se empezaron a detectar múltiples vulnerabilidades en WEP debido a los siguientes errores en su diseño:

- Una única clave estática que comparten todos los usuarios.
- El vector de inicialización es de 24 bits lo que provoca colisiones en puntos de acceso muy concurridos.
- Uso de un control de integridad lineal. CRC-32 (cksum)
- Cifrado RC4 como medida única de control manejando llaves estáticas.

CRC32 no es en sí malo, lo malo es que se usan muy pocos bits, pero el control de integridad CRC32 sigue usándose pero con más bits

Las debilidades del protocolo WEP como corresponde han sido ampliamente documentadas. lo que ha derivado en el desarrollo de varias herramientas de dominio público, como Aircrack, WEPCrack o Aircrack que fácilmente obtienen la clave compartida utilizada en este tipo de redes.

**OJO.** WEP es totalmente inseguro por lo que no está recomendado a excepción de que se al a única opción disponible.

Algunas herramientas: Aircrack, WEPCrack o Aircrack

WEP no tiene que estar disponible en ninguna web

Los routers antiguos dicen que si desactivan el modo de compatibilidad, no podrías conectar equipos antiguos (habrían problemas con equipos como Windows XP) o sea que por compatibilidad no habría problema

Debido a la inseguridad de WEP IEEE desarrolló un nuevo estándar el IEEE802.11i el cual fue publicado en 2004, este permite mejorar considerablemente la seguridad de las comunicaciones inalámbricas mediante la definición de dos modos de seguridad diferenciados como WPA y WPA2.

WPA busca ser compatible con el hardware existente y permitir a las redes que operaban en WEP migrar a un estándar más seguro. Para lograr la cuestión de la seguridad incorpora:

- Un mecanismo de gestión de claves dinámicas **Temporal Key Integrity Protocol (TKIP)** al cifrado RC4.
- Uso de claves dinámicas (Cambian aproximadamente cada 10,000 paquetes enviados) que además varían para cada usuario (Combinan la clave con la dirección MAC del dispositivo)

El uso de claves dinámicas es lo que empieza a proporcionar seguridad real y eso debe configurarse adecuadamente en los routers

#### ▼ 02-09-2022

No entré a clase :(

#### ▼ 05-09-2022

Ya hay fechas para exámenes

La duración es de 1 hora, hay que traer la compu o algo para conectarse a internet. Poder cargar WireShark (en el examen se cargaría un archivo como si se hubiera hecho un sniffeo)

#### WPA

- Incorpora el algoritmo de integridad conocido como Michael para generar un Message Integrity Check (MIC)
- Soporta autenticación basada en clave compartida (WPA-Personal) y también con claves diferentes para cada usuario (WPA-Enterprise) - basado en el estándar 802.1X que utiliza un server Remote Authentication Dial In Use Service para la autenticación.

#### WPA2

- Implica una ruptura con el HW que mantenga tecnología previa a su creación (Junio de 2004 se volvió obligatoria hasta el 2006)
- Basa su modelo de seguridad en el algoritmo criptográfico Advance Encryption Standard (AES), para lo que usa el modo Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) que provee confidencialidad, integridad y autenticación a los paquetes



- Usa claves dinámicas que cambian aproximadamente cada 10,000 paquetes y varían para cada usuario (Se combina con la dirección MAC del dispositivo de usuario).
- Soporta tanto la autenticación basada en clave compartida (WPA2-Personal) como la basada en claves diferentes para cada usuario (WPA2-Enterprise) que se basa en el estándar 802.1X que utiliza un servidor Remote Authentication Dial In User Service para la autenticación.

#### WPA2 - Recomendaciones.

- De ser posible se recomienda el uso de WPA2 en su versión enterprise para el despliegue de la red inalámbrica. En caso de no ser posible se debe garantizar que las contraseñas WPA2-Personal serán seguras.
- Se desaconseja el uso de WPA a menos que los dispositivos utilizados no sean compatibles con WPA2.

#### WPA2 - Vulnerabilidades

Key Reinstallation AttaCK, o KRACK (Descubierto por la Universidad de Leuven (Bélgica), es el nombre con que se conoce a la técnica que permite romper la seguridad de las redes WPA2 y conectarse a ellas. Para esto es necesario estar en rango de alcance y es importante saber que aun cuando se logra la vulneración no se lograra descifrar la comunicación https.

Las opciones de seguridad son por ningún motivo activar el protocolo de acceso WPS mantener una revisión constante de nuestra red, aplicar las actualizaciones a los dispositivos, migrar a WPA3 que está en el mercado desde el 2018 y que promete evitar los ataques mediante el uso de diccionarios

WPA Enterprise es muy usado (incluso se usa en la uni) pero el problema del Enterprise es que se tiene el router y aparte se tiene un servidor, generalmente radius, que tiene un listado de usuarios y contraseñas, por lo que al conectarse mediante WPA para validar si tienes permiso de entrar y a dónde tienes permitido entrar. Para Enterprise debes tener un servidor aparte

También hay que anular el modo automático para que no agarre WPA por automático y agarre WPA2

#### WPA3.

Actualmente existen las siguientes configuraciones.

- **WPA3-Personal:** Nosotros ponemos una contraseña única y con esta clave se conectarán todos los dispositivos inalámbricos. Es lo que se conoce como PSK (Pre-Shared Key), o contraseña precompartida. En este modo de configuración el router usará únicamente WPA3-Personal, los dispositivos no compatibles con WPA3 no podrán conectarse.
- **WPA3-Enterprise:** Tenemos un servidor RADIUS para la autenticación de los diferentes usuarios con usuario/contraseña y con un certificado digital.
- **WPA2/WPA3-Personal:** Es una opción de transición, permite al router aceptar conexiones con seguridad WPA2-Personal (con clave precompartida) y con WPA3-Personal simultáneamente.



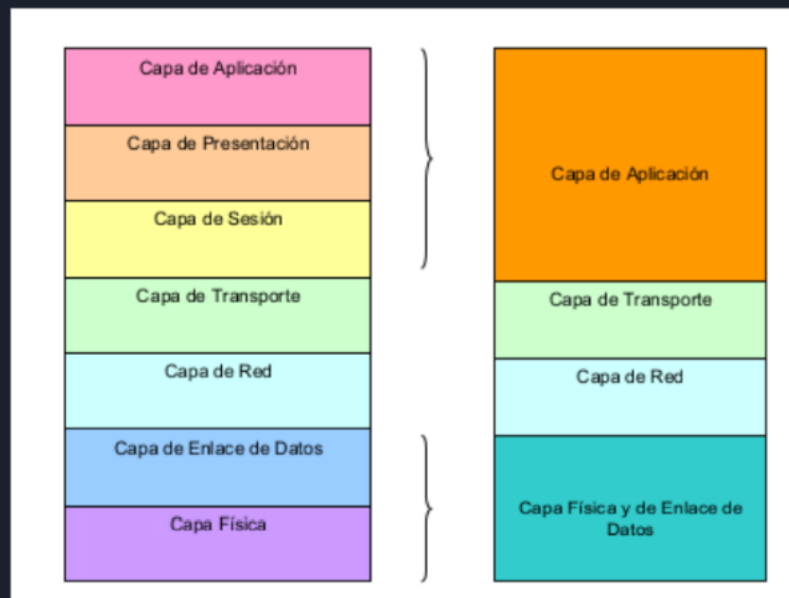
## WPA3.

### Características:

- Protección más sólida mediante un handshake más seguro
- Simplifica la configuración de seguridad en algunos dispositivos permitiendo conectarse aun sin pantalla de inicio (acceso sin contraseña) pero protegiendo mediante un cifrado de datos de manera individual cada conexión.
- Mejorar privacidad de los usuarios (Por lo descrito en el punto anterior)
- Utiliza un cifrado de 192 bits contra los 128 bits que actualmente usa WPA2

Con WPA3 ya no es compatible con equipos viejitos

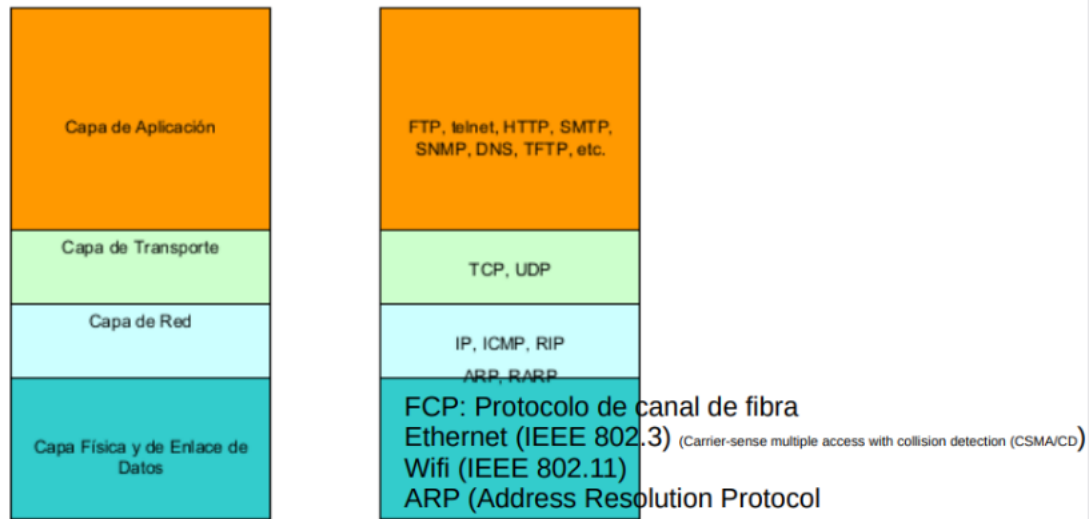
## TCP, UDP y Capas Superiores



Se ve el protocolo TCP y UDP para ver las vulnerabilidades

El modelo OSI surge como protocolo académico para que otros protocolos trabajen sobre esa misma estructura

### Ubicación de protocolos comunes



**UDP User datagram protocol:** Es un protocolo de internet que trabaja en la capa de transporte. Una aplicación puede enviar información muy rápidamente, ya que no es necesario establecer una conexión con el receptor ni esperar una respuesta. Sin embargo, no hay garantía de que los paquetes vayan a llegar completos y respetando el orden en el que fueron enviados. Además, este protocolo no ofrece ninguna protección frente a la alteración o acceso por parte de terceros. (recordemos que en IPV6 esto cambia ya que es obligatoria la verificación).

**Importante:** en IPV4 NO POSEE CONFIRMACIÓN DE ENTREGA O RECEPCIÓN

**TCP (Protocolo de Control de Transmisión) :** A diferencia de UDP permite que las aplicaciones puedan comunicarse con garantías independientemente de las capas inferiores del modelo TCP/IP. da soporte a múltiples protocolos de la capa de aplicación, como HTTP (web), HTTPS (web segura), POP3 (correo entrante) y SMTP (correo saliente) así como sus versiones seguras utilizando TLS, FTP, FTPES y SFTP para transferir archivos desde un origen a un destino, e incluso el protocolo SSH.

TCP se auxilia de ICMP

► Capa 1: De acceso al medio.



TCP/IP

Nivel de Aplicación

HTTP, FTP, POP3, TELNET, SSH, ...

Nivel de Transporte

Conexión extremo-a-extremo y fiabilidad de los datos  
TCP, UDP

Nivel de Red

ICMP, IP, ARP, RARP, ...

Nivel de Enlace de Datos

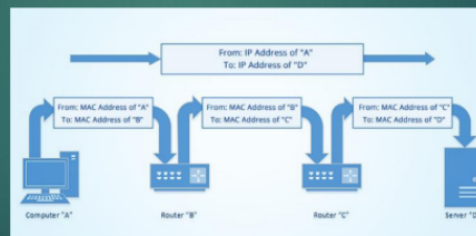
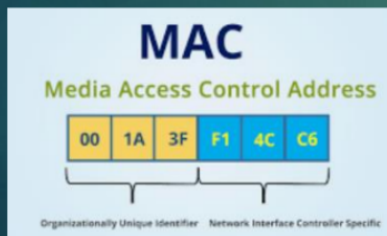
Direccionamiento físico (MAC y LLC)

Nivel Físico

Señal y transmisión binaria

► Capa 1b ( Recordemos que en TCP/IP no existe como tal):

- LLC (Logical Link Control)
- MAC ( Media Acces Control )



TCP/IP

Nivel de Aplicación

HTTP, FTP, POP3, TELNET, SSH, ...

Nivel de Transporte

Conexión extremo-a-extremo y fiabilidad de los datos  
TCP, UDP

Nivel de Red

ICMP, IP, ARP, RARP, ...

Nivel de Enlace de Datos

Direccionamiento físico (MAC y LLC)

Nivel Físico

Señal y transmisión binaria

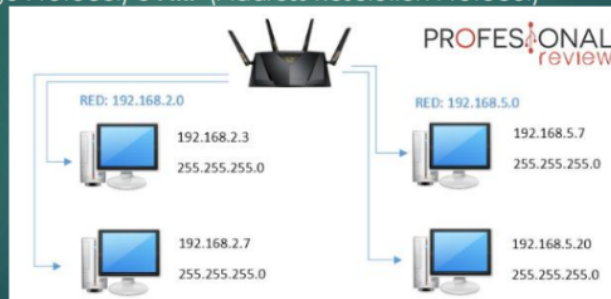
La capa 1b no existe, sólo es con fines explicativos

La lista ARP sólo funcionará a nivel de intranet

Con el comando "traceroute" puede identificarse todos los saltos que da de nuestro equipo a la IP señalada

El proceso de NATeo implica que los equipos del interior tienen una IP privada y los equipos del exterior no tienen contacto con el equipo propio

► Capa 2. Red. Se encarga de la estructura del paquete y de cómo se envían además de la **identificación del host mediante una dirección** y el direccionamiento de estos datagramas dando saltos entre enrutadores hasta llegar al destino. Aquí es donde trabaja el **protocolo IP**, así como otros protocolos como **IGMP** (Internet Group Management Protocol), **ICMP** (Internet Control Message Protocol) o **ARP** (Address Resolution Protocol)



TCP/IP

Nivel de Aplicación

HTTP, FTP, POP3, TELNET, SSH, ...

Nivel de Transporte

Conexión extremo-a-extremo y fiabilidad de los datos  
TCP, UDP

Nivel de Red

ICMP, IP, ARP, RARP, ...

Nivel de Enlace de Datos

Direccionamiento físico (MAC y LLC)

Nivel Físico

Señal y transmisión binaria

Fuente <https://www.profesionalreview.com/2020/03/21/protocolo-tcp-ip/>

Aquí se genera el direccionamiento IP

▼ 06-09-2022

iiiACABA DE COMENZAR LAS CONFERENCIAS DE DRAGON JAR!!!

<https://www.dragonjar.org/>

<https://www.dragonjarcon.org/>

ESET Latinoamérica

<https://www.academiaeset.com/>



▼ 07-09-2022

Retomamos clases

Capa 1: Acceso al medio o llamada capa física

Aquí se encuentra el LLC y lo que tiene que ver con MAC

Luego vimos la capa 2 donde vimos la parte donde se incorpora la dirección IP. Se incorporan protocolos como el ICMP. Hay protocolos enfocados a la conexión (TCP) y otros no enfocados a la conexión (UDP)

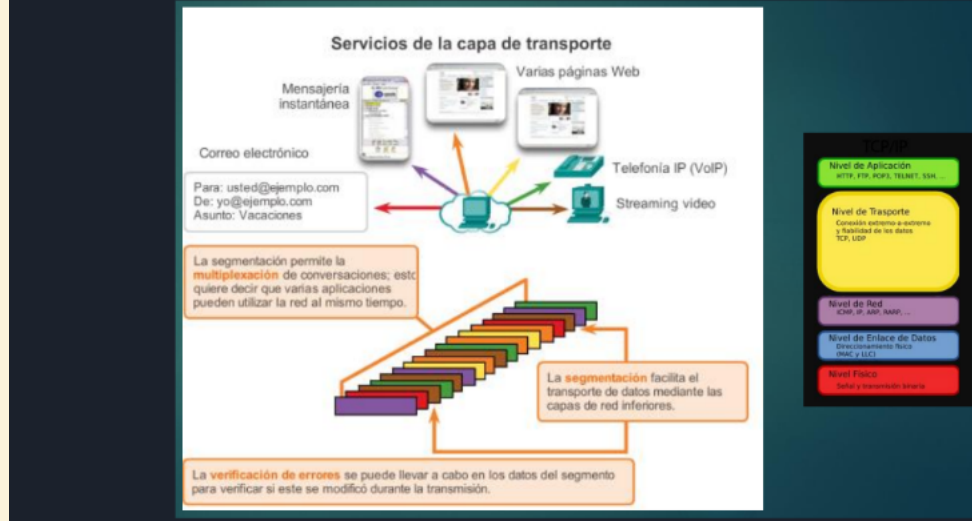
Capa 3. Transporte: Es responsable de establecer una sesión de comunicación temporal entre dos aplicaciones y de transmitir datos entre ellas. TCP/IP utiliza dos protocolos para lograrlo: Protocolo de control de transmisión (TCP), Protocolo de datagramas de usuario (UDP).

Es en esta capa donde se da la Multiplexación de conversaciones que mediante la segmentación de datos permite que se entrelacen (multiplexen) varias comunicaciones diferentes de varios usuarios distintos en la misma red en forma simultánea, proporciona los medios para enviar y recibir datos durante la ejecución de varias aplicaciones y agrega un encabezado a cada segmento para identificarlo.



Aquí ya interactúa TCP/IP. Aquí podría usarse también UDP. Aquí se da la multiplexación al trabajar con el modelo OSI.

### Capa 3. Transporte:



Aquí se ve la segmentación y como los fragmenta, aprovecha mejor el canal. Al ver en sistemas, antes el procesador ocupaba el 100% y después se manejaba la multiplexación para dividir procesos o paquetes en fragmentos más pequeños para que un procesote o paquetote no comiera toda la PC o la red en ese.

Hacía parecer que los procesos se están haciendo simultáneamente

### Capa 3. Transporte:

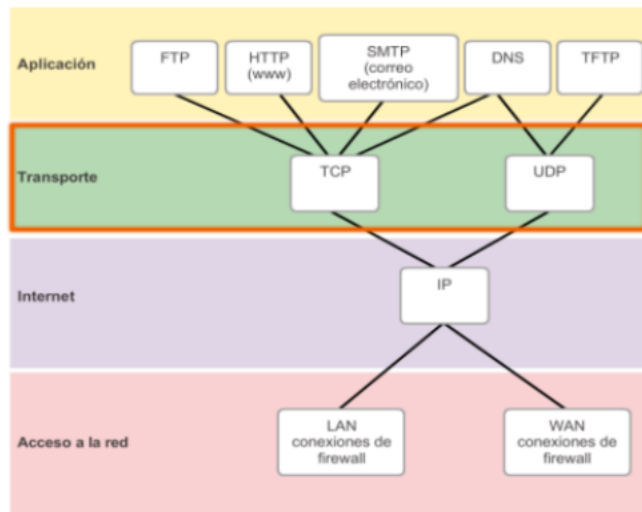
- ❖ Protocolo de control de transmisión (TCP): Proporciona una entrega confiable que asegura que todos los datos lleguen al destino. Utiliza el acuse de recibo (ACK) y otros procesos para asegurar la entrega. Mayores demandas sobre la red: mayor sobrecarga.
- ❖ Protocolo de datagramas de usuario (UDP) Proporciona sólo las funciones básicas para la entrega; no proporciona confiabilidad. Menor sobrecarga.

¿Qué pasa con ACK? Cuando dos equipos se quieren conectar, hacen una negociación con ACK y Three Way Handshake. La primera compu manda una secuencia y la segunda computadora envía esta secuencia para corroborar que la recibió correctamente mientras también manda su propia secuencia. Así la primera computadora manda nuevamente esta nueva secuencia mandando una secuencia más

Los protocolos no enfocados a lo conexión tienen un problema grave: Porque por ejemplo al transmitir streaming no puedes saber si el router de envío está caído porque, a diferencia de TCP (orientados a conexión) no hay otra computadora con confirme que no hay conexión

### Capa 3. Transporte:

### TCP o UDP

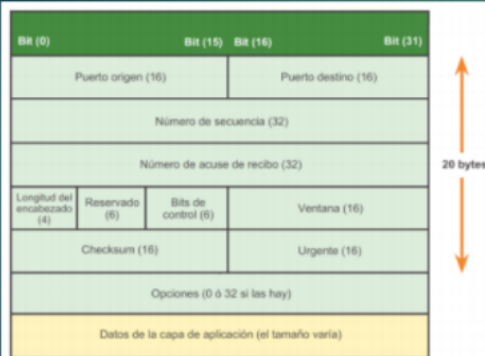


Hay 3 tipos de puertos: Puertos físicos, puertos lógicos y ???

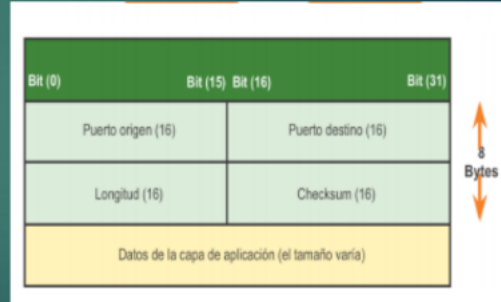
IP es protocolo no enfocado a la conexión. Tiene que apoyarse en TCP porque no tiene forma de validar si los datos llegan

Capa 3. Transporte: TCP y UDP utilizan el número de puerto para distinguir entre aplicaciones

#### RFC 793 TCP



#### RFC 768 UDP



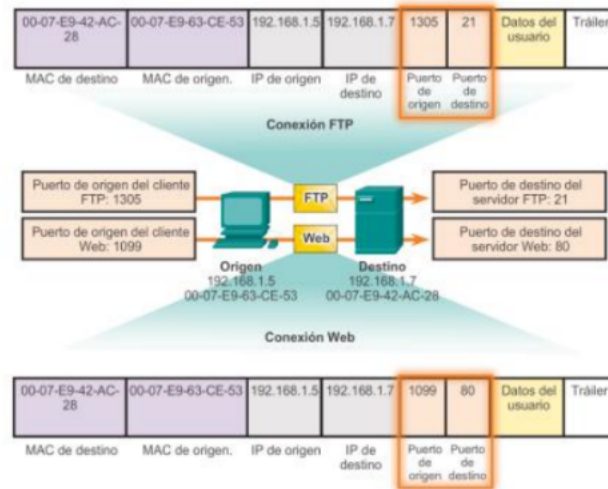
Checksum: Sha256, md5, etc..

Importante qué es RFC para redes

En RFC se documenta el uso de protocolos por lo que los delincuentes informáticos estudian mucho los RFCs de los protocolos a los que quieren vulnerar

### Capa 3. Transporte:

## Direccinamiento de puertos TCP y UDP



Analizando a nivel de seguridad:

El puerto origen no tiene realmente importancia

Hay un listado completo de los puertos para qué se usan:

<https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/>

Consejo: Darnos de alta en Cisco Academy

### Capa 3. Transporte:

## Procesos de servidores TCP



A continuación podremos analizar mejor el Three Way Handshake



Capa 3. Transporte: Recordemos que las conexiones las realiza TCP mediante el protocolo de enlace 3-way handshake. Esto lo podemos observar con wireshark.

**Paso 1: el cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.**

Protocolo TCP de enlace de tres vías (SYN)

| No. | Time      | Source          | Destination     |
|-----|-----------|-----------------|-----------------|
| 10  | 16.303490 | 10.1.1.1        | 192.168.254.254 |
| 11  | 16.304896 | 192.168.254.254 | 10.1.1.1        |
| 12  | 16.304925 | 10.1.1.1        | 192.168.254.254 |
| 13  | 16.305153 | 10.1.1.1        | 192.168.254.254 |
| 14  | 16.307875 | 192.168.254.254 | 10.1.1.1        |

Frame 10: 62 bytes on wire (496 bits), 62 bytes captured on interface 0  
 Ethernet II, Src: VMware\_b6:62:88 (00:50:56:b6:62:88)  
 Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1)  
 Transmission Control Protocol, Src Port: kiosk (1061)  
 Destination Port: http (80)

Un analizador de protocolos muestra la solicitud del cliente inicial para la sesión en la trama 10

En el segmento TCP de esta trama se muestra lo siguiente:

- El indicador SYN está establecido para validar un número de secuencia inicial.
- El número de secuencia seleccionado aleatoriamente es válido (el valor relativo es 0).
- El puerto de origen aleatorio es 1061.

**Paso 2: el servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.**

Protocolo TCP de enlace de tres vías (SYN, ACK)

| No. | Time      | Source          | Destination     |
|-----|-----------|-----------------|-----------------|
| 10  | 16.303490 | 10.1.1.1        | 192.168.254.254 |
| 11  | 16.304896 | 192.168.254.254 | 10.1.1.1        |
| 12  | 16.304925 | 10.1.1.1        | 192.168.254.254 |
| 13  | 16.305153 | 10.1.1.1        | 192.168.254.254 |
| 14  | 16.307875 | 192.168.254.254 | 10.1.1.1        |

Frame 11: 62 bytes on wire (496 bits), 62 bytes captured on interface 0  
 Ethernet II, Src: Cisco\_63:74:a0 (00:0f:24:63:74:a0)  
 Internet Protocol Version 4, Src: 192.168.254.254 (192.168.254.254)  
 Transmission Control Protocol, Src Port: http (80)

Un analizador de protocolos muestra la respuesta del servidor en la trama 11

- El indicador ACK está establecido para indicar un número válido de acuse de recibo.
- Respuesta de número de acuse de recibo al número de secuencia inicial como valor relativo de 1.
- El indicador SYN está establecido para indicar el número de secuencia inicial de la sesión de servidor a cliente.
- El número de puerto de destino 1061 corresponde al puerto de origen del cliente.
- El número de puerto de origen 80 (HTTP) indica el servicio del servidor Web (httpd).

Capa 3. Transporte: Recordemos que las conexiones las realiza TCP mediante el protocolo de enlace 3-way handshake. Esto lo podemos observar con wireshark.

**Paso 3: el cliente de origen reconoce la sesión de comunicación de servidor a cliente.**

Protocolo TCP de enlace de tres vías (ACK)

| No. | Time      | Source          | Destination     |
|-----|-----------|-----------------|-----------------|
| 10  | 16.303490 | 10.1.1.1        | 192.168.254.254 |
| 11  | 16.304896 | 192.168.254.254 | 10.1.1.1        |
| 12  | 16.304925 | 10.1.1.1        | 192.168.254.254 |
| 13  | 16.305153 | 10.1.1.1        | 192.168.254.254 |
| 14  | 16.307875 | 192.168.254.254 | 10.1.1.1        |

Frame 12: 54 bytes on wire (432 bits), 54 bytes captured on interface 0  
 Ethernet II, Src: VMware\_b6:62:88 (00:50:56:b6:62:88)  
 Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1)  
 Transmission Control Protocol, Src Port: kiosk (1061)

Un analizador de protocolos muestra la respuesta del cliente para la sesión en la trama 12

En el segmento TCP de esta trama se muestra lo siguiente:

- El indicador ACK está establecido para indicar un número válido de acuse de recibo.
- Respuesta de número de acuse de recibo al número de secuencia inicial como valor relativo de 1.
- El número de puerto de origen 1061 corresponde a
- El número de puerto de destino 80 (HTTP) indica el servicio del servidor Web (httpd).

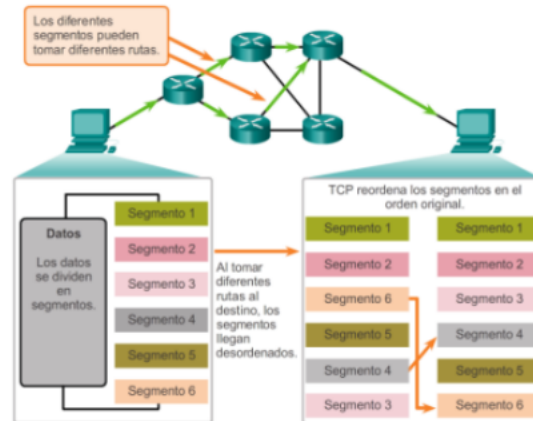
Nos damos cuenta que nos quieren vulnerar cuando empezamos a perder muchas conexiones, porque el Three Way Handshake no está dándose correctamente

### Capa 3. Transporte:

## Confiabilidad de TCP: entrega ordenada

Se utilizan números de secuencia para volver a armar los segmentos en el orden original.

Los segmentos TCP se vuelven a ordenar en el destino



Al mandar paquetes segmentados, cuando llegan al equipo, tienen que rearmarse en el orden correcto

La forma de vulnerar no es el medio, es el equipo

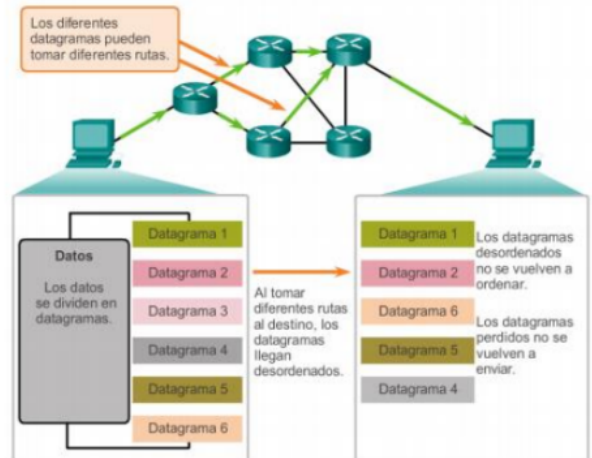
### Capa 3. Transporte:

Esto es posible debido a que la redundancia natural de la voz permite que la comunicación se entienda aun con distorsiones, pero las señales de datos no son tolerantes a fallos, cualquier error por mínimo que sea causara problemas en la comunicación. Es decir la transmisión de datos debe ser más confiable.

## Comunicación UDP

## Rearmado de datagramas

UDP: sin conexión y poco confiable



**Capa 4. Aplicación:** En esta capa se determina la aplicación para cada paquete dependiendo del puerto elegido.



El modelo OSI es la base con la que debe establecerse la conexión. TCP lo estiliza pero es la misma base.

**Capa 4. Aplicación: ( Capa de presentación y capa de sesión )**

La capa de presentación tiene tres funciones principales:

- La codificación y conversión de datos de la capa de aplicación
- La compresión de los datos
- La encriptación de los datos para su transmisión y posterior descifrado al llegar al destino.

**Capa de Sesión:** Sus funciones crean y mantienen diálogos entre las aplicaciones de origen y destino, a la vez que administra el intercambio de información para iniciar diálogos, para mantenerlos activos y para reiniciar sesiones

En esta capa también actúa ACK (ACK actúa principalmente en la capa anterior, pero también actúa aquí)

**Capa 4. Aplicación / Protocolos:**

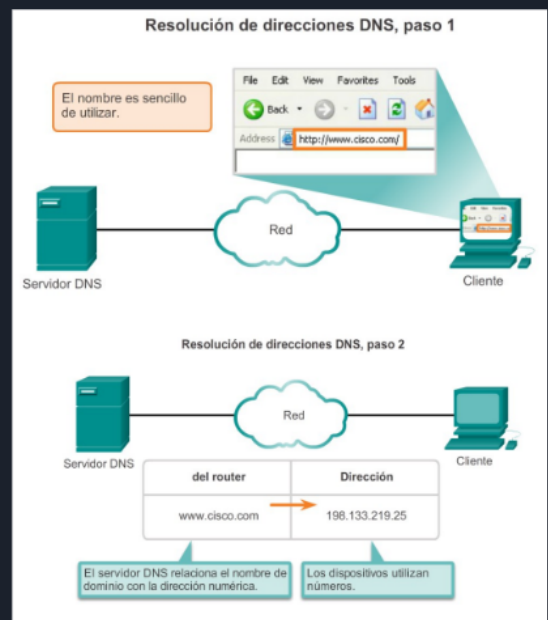
- Protocolo de servicio de nombres de dominios (DNS): se utiliza para resolver nombres de Internet en direcciones IP.
- Telnet: protocolo de emulación de terminal que se utiliza para proporcionar acceso remoto a servidores y dispositivos de red.
- Protocolo bootstrap (BOOTP): un precursor al protocolo DHCP. Protocolo de red que se utiliza para obtener información de dirección IP durante el arranque.
- Protocolo de configuración dinámica de host (DHCP): se utiliza para asignar una dirección IP, una máscara de subred, un gateway predeterminado y un servidor DNS a un host.
- Protocolo de transferencia de hipertexto (HTTP): se utiliza para transferir archivos que conforman las páginas Web de la World Wide Web

#### Capa 4. Aplicación / Protocolos:

- Protocolo de transferencia de archivos (FTP): se utiliza para la transferencia interactiva de archivos entre sistemas.
- Protocolo trivial de transferencia de archivos (TFTP): se utiliza para la transferencia activa de archivos sin autenticación del usuario.
- Protocolo simple de transferencia de correo (SMTP): se utiliza para la transferencia de mensajes y archivos adjuntos de correo electrónico.
- Protocolo de oficina de correos (POP): lo utilizan los clientes de correo electrónico para recuperar el correo electrónico de un servidor remoto.
- Protocolo de acceso a mensajes de Internet (IMAP): otro protocolo para la recuperación de correo electrónico.

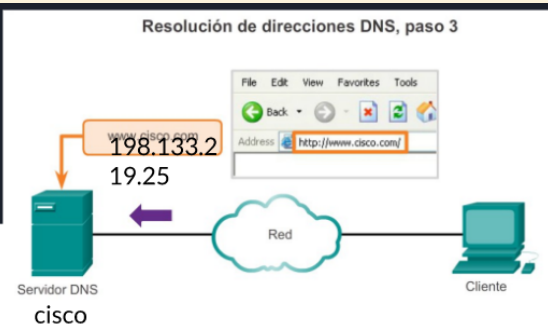
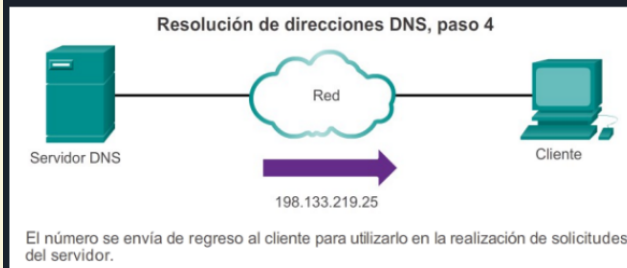
#### Capa 4. Aplicación / Protocolos / DNS

Este protocolo DNS resuelve una URL (nombre en lenguaje humano) a la dirección del dispositivo de red numérico (IP)



#### Capa 4. Aplicación / Protocolos / DNS

El protocolo DNS resuelve la URL para la dirección del dispositivo de red numérico.



El DNS Caché puede permitirle al delincuente o auditor informático decirle dónde había estado el usuario. Esto estaba en Windows 8 y previos

#### Capa 4. Aplicación / Protocolos /Formato del mensaje DNS:

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres.

- Contienen el nombre, la dirección y el tipo de registro. •
- Los tipos de registro son los siguientes: •
  - A: una dirección de dispositivo final •
  - NS: un servidor de nombre autoritativo
  - CNAME: el nombre canónico para un alias; se utiliza cuando varios servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS.
  - MX: registro de intercambio de correos; asigna un nombre de dominio a una lista de servidores de intercambio de correo.
- Si no puede resolver el nombre con sus registros almacenados, se comunica con otros servidores.

#### Capa 4. Aplicación / Protocolos /Formato del mensaje DNS:

- El servidor almacena de forma temporal la dirección numérica que coincide con el nombre en la memoria caché.
- El comando `ipconfig /displaydns` de Windows muestra todos los DNS almacenados en la memoria caché.
  - OJO. Con esta instrucción podemos averiguar en donde estuvo paseando un usuario aunque haya usado el modo incógnito (Igual no se apuren esta chiva cada 24 horas se limpia o si lo quieren a mano use `flushdns`)

#### Capa 4. Aplicación / Protocolos / Jerarquía DNS:

Los siguientes son algunos ejemplos de dominios de nivel superior:

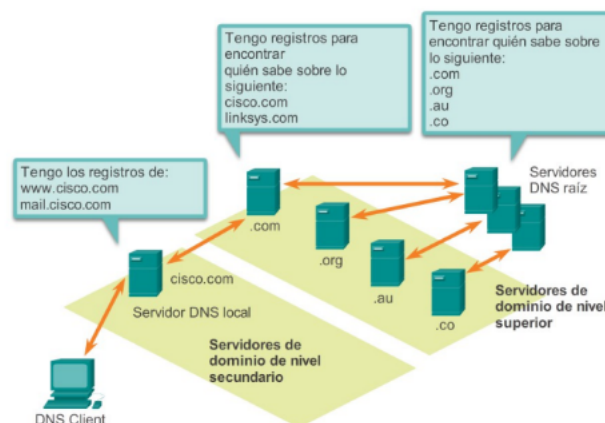
**.au:** Australia

**.co:** Colombia

**.com:** empresa o industria

**.jp:** Japón

**.org:** organización sin fines de lucro



Una jerarquía de servidores DNS contiene los registros de recursos que relacionan los nombres con las direcciones.

▼ 08-09-2022

Un servidor Radius es el que hace la doble autenticación para evitar que copiar MAC Addresses no pueda ser verificable



Cuando se tiene un router de la casa, depende de la compañía si su IP es pública o privada. Las IPs que tiene son una privada y otra pública

El cuadrante mágico de Gartner:

## BYOD (Bring Your Own Device) Cuadrante Mágico de Gartner

- Los aspirantes (Challengers). Según la web de Gartner: “tienen una buena ejecución del negocio actualmente y son capaces de dominar un gran segmento de mercado, pero aún no demuestran un real entendimiento de la dirección en que va el mercado”.
- Los líderes (Leaders). Desarrollan bien su negocio de acuerdo a una adecuada visión actual del mercado y están bien posicionados para el futuro.
- Los jugadores de nichos específicos (Niche Players). Se enfocan con éxito en un segmento de mercado específico, pero muchos de ellos no adquieren en su desempeño una visión global y no se caracterizan por hacer grandes innovaciones o por superar a sus competidores.
- Los visionarios (Visionaires). Entienden hacia dónde van los mercados e incluso pueden tener una idea para cambiar las reglas y paradigmas, pero aún no son capaces de llevar a cabo estas ideas por completo o con éxito

Normalmente los líderes compran a los aspirantes y a los visionarios.

Los jugadores de nicho pueden desaparecer si el mercado cambia debido a su altísima especialización

## Kerberos

La mitología dice que es un perro de tres cabezas que protege la entrada al inframundo

Protocolo cliente-servidor que proporciona seguridad a las transacciones en redes.

Ofrece autenticación de usuario, seguridad y privacidad

Kerberos sólo es protocolo de autenticación, NO de autorización

Kerberos confía en el usuario (ese es su problema)

El Active Directory está basado totalmente en Kerberos

Kerberos impide que las claves sean enviadas a través de la red con el consiguiente riesgo de su divulgación

Maneja una criptografía de claves simétricas

Al hablar Kerberos se considera de una intranet. Se habla de la metodología tradicional de Host Bastion donde nuestros equipos están en nuestra red. De irse al exterior necesitaríamos una VPN

Es difícil de implementar en un red que ya está operando porque

1. Las contraseñas las maneja en otro lado al default de Linux (/etc/passwd)
2. Presupone que cada usuario es de confianza y que está utilizando una máquina no fiable en una red no fiable. La seguridad no está casada ni con la MAC Address ni con la IP, sólo con un usuario y contraseña y la seguridad es simétrica, o sea que F

FTP no está Kerberizada, puede hacerse pero no es fácil

Telnet, FTP y SSH pueden ser kerberizados a partir de Kerberos v5 mientras maneje compatibilidad entre los SO

No es el ideal porque implementar SSH junto a Kerberos, pero sólo ralentiza la red (SSH de por sí hace que los túneles SSH no sean sniffables)

Kerberos depende totalmente del reloj porque si una máquina no está sincronizada con el reloj, valió KK. Sería necesario que todas las máquinas hagan referencia a un servidor NTPD (un servidor de tiempo)

Kerberos debe tener un DNS de manera correcta. Kerberos debe manejarse como DNS

- AS: Servidor de autenticación: Emite tickets para un servicio kerberizado
- TGT: Ticket Granting Ticket: Otorga la primera fase de autenticación y tiene duración limitada y debe ser mayor a la de TGS
- Cliente: Cualquier usuario, host o aplicación puede obtener un ticket de kerberos
- Credenciales: Son los tickets
- Hash encriptado: Hash de un sentido usado para autenticar usuarios
- GSS-API
- Hash
- Llaves simétricas
- KDC
- TGS: Servicio encargado de generar tickets
- Keytab: Fichero peligroso porque tiene una lista descriptada de servidores y sus claves
- Kinit
- Servicio
- Ticket
- Contraseña no encriptada

#### ▼ Recursos

Caso de Análisis problema de seguridad causado por certificados Microsoft:

<https://support.microsoft.com/es-es/topic/-este-certificado-tiene-una-firma-digital-no-válida-mensaje-de-error-después-de-instalar-el-paquete-de-continuación-de-seguridad-de-windows-nt-4-0-1b2b62d6-9d44-1257-be64-9da2f5e7b287>

#### ▼ 09-09-2022

En OWASP pueden observarse las alertas en su carpeta de alertas

#### ▼ 12-09-2022

Antes de Kerberos viene en el examen

Continuación de la sesión anterior

### Terminología de Kerberos

- AS
- TGT
- Cliente
- Credenciales
- Hash Encriptado

### Mensajes de Kerberos

Inicialmente



Hay que tener en cuenta qué es el krbtgt. Es un servicio que está a la espera de peticiones para Kerberos

1. KRB\_AS\_REQ: Utiliza por el usuario para solicitar el TGT al KDC con paquetes conformados por:
  - a. Un timestamp cifrado con la clave del cliente, para autenticar el usuario y prevenir ataques de replay
  - b. El nombre de usuario que se está autenticando
  - c. El SPN del servicio asociado a la cuenta krbtgt
  - d. Un nonce generado por el usuario
2. KRB\_AS\_REP: Respuesta del KDC para enviar el TGT al usuario. Antes de esto verifica la identidad del usuario descifrando el timestamp de la siguiente manera:
  - a. Nombre de usuario. El TGT que incluye: Nombre de usuario, clave de sesión, fecha de expiración del TGT PAC con privilegios del usuario, firmado por el KDC. Una serie de datos cifrados con la clave del usuario, que incluyen clave de sesión, fecha de expiración del TGT, Nonce del cliente, para evitar ataques de replay
  - b. Nota: El TGT dura por defecto 10 horas de validez sus llaves. A mano puede reducirse el tiempo de validez por llave
  - c. Nota: Kerberos es útil para generar las llaves y que tus credenciales no estén volando por toda la red al querer acceder a los distintos servicios, sino crear esta llave extra que no da el acceso limitado y a tiempo reducido
3. KRB\_TGS\_REQ: Ahora con un TGT, se puede pedir al servidor KDC un ticket TGS mediante un mensaje KRB\_TGS\_REQ como se indica a continuación:
  - a. Datos cifrados con la clave de sesión (nombre de usuario, timestamp, TGT, SPN del servicio solicitado, Nonce generado por el usuario). El SPN es un identificador único
4. KRB\_TGS\_REP: Una vez que el servidor KDC reciba la petición de un TGS responde
  - a. Nombre de usuario y TGS, que contiene la clave de sesión del servicio, nombre de usuario, fecha de expiración del TGS PAC con los privilegios del usuario firmado por el KDC, datos cifrados con la clave de sesión como la clave de sesión de servicio y la fecha de expiración del TGS, así como el Nonce del cliente para evitar ataques de Replay
5. KRB\_AP\_REQ: Si la negociación de seguridad previa fue correcta se le otorga al usuario el derecho de uso de la aplicación pero ahora para aprovechar ese permiso de uso deberá comunicarse con el servidor AP y si todos los datos son correctos, podrá acceder al servicio. Ojo, sólo en caso de requerir autenticación mutua se procederá a enviar el mensaje KRB\_AP\_REP al usuario
6. KRB\_AP\_REP: Si se establece el indicador de autenticación mutua, entonces regresa información al servidor a modo de respuesta.
7. KRB\_ERROR: Sólo se da si se genera un error en la comunicación
8. KRB\_VERIFY\_PAC\_REQUEST: Se hace a nivel de sistema operativo copiando los valores de la firma del certificado de atributo del privilegio (PAC)

Kerberos utiliza el puerto UDP/88 y también el TCP/88

Tomar un KDC debe hacerse desde el interior de una red, porque está en una intranet

#### ▼ 13-09-2022

### Resumen de Kerberos

Es importante Kerberizar los servicios de Telnet, ftp, sftp, smtp, etc

Es importante sincronizar la hora

Se recomienda actualizar Kerberos

También se recomienda configurar una red cliente/servidor compatible con Network Time Protocol (NTP)

### Atques a Kerberos

- Overpass the Hash / Hash the key (PTK)

Se usa para conseguir suplantar al mismo frente al KDC y acceder a los servicios del dominio disponibles para dicho usuario. Los hashes de usuario se pueden extraer de los ficheros SAM de las estaciones de trabajo, del fichero NTDS.DIT o de la memoria del proceso sass (usando Mimikatz) donde también es posible obtener las contraseñas en texto claro

- Pass the ticket (PTT)

Se consigue un ticket de usuario para lograr acceso a los recursos a los que el usuario tenga permisos. Es fácil con claves sencillas o sin encriptación. También se debe a que un administrador le deje 10 horas a la duración del ticket y eso no se cambia manualmente

- Golden ticket

Consigue un TGT con una clave krbtgt

- Silver ticket

Similar al anterior pero la clave del servicio al que se quiere acceder se toma el TGS

- Kerberoasting

Usa los TGS para crackear las contraseñas de los usuarios offline

- ASREPRoast

Busca crackeo offline de las credenciales. Cuando un usuario está configurado con el atributo DONT\_REQ\_PREAUTH no necesita preautenticación, con lo que es posible construir un mensaje KRB\_AS\_REQ sin conocer las credenciales del mismo

Un tip muy importante es que un KDC (ni ningún servidor importante) no tenga acceso a internet. Debe hacerse un puente al KDC

## Amenazas y Vulnerabilidades

### Hacking Tools & Media | Hak5 Official Site

Hak5 - industry leading hacker tools & award winning hacking shows for red teams, pentesters, cyber security students and IT professionals. Creators of the WiFi Pineapple, USB Rubber Ducky & more. Home to an inclusive information security community. Established in 2005.

 <https://hak5.org/>



La primera de todas es aquella situada entre el ordenador y la silla, llamada capa 8, que es el usuario.

Es más fácil engañarle a él que a una máquina. De aquí consiste la Ingeniería Social

La ingeniería social es convencer a la persona para que le digan a uno lo que quiere saber

La técnica más usada de hacer ingeniería social es el phishing

Consiste en enviar un correo a la víctima haciéndonos pasar por otra entidad para suplantarnos por la entidad

Términos importantes:

- Footprinting: Búsqueda de información pública de un objetivo
- Fingerprinting: Obtener la información interactuando directamente con los sistemas a atacar

El nmap ya es fingerprinting

Primera clave de la ingeniería social: Todos queremos ayudar, el primer movimiento es siempre de confianza hacia el otro. No nos gusta decir no y a todos nos gusta que nos alaben

En la búsqueda de vulnerabilidades: Obteniendo información sobre la empresa preguntando haciéndonos pasar por periodistas o nuevos empleados

En el ataque: Consiguiendo que alguien ejecute un archivo infectado haciéndose pasar por alguien con confianza

▼ 14-09-2022

Consideraciones para el examen:

- Acomodar pasillos para el profe

El footprinting no se considera delito, pues se agarra información pública

El fingerprinting ya, dependiendo del país, puede considerarse delito

nombredepagina.com/robots (la uri /robots probablemente la tenga la badstore)

WebHTTrack

dnsdumpster.com

Encuentra información importante de una organización

#### ▼ Repaso

urlencoded-form

ACK: ENCargado del control de envío de paquetes. Como efecto residual, determina el inicio y final de la conexión

PAC: Privilegios de usuario

Jumborgramas para ipv6. Datagramas para ipv4

Diferencias entre codificar, cifrar

ISO 271012

Firma digital y firma cifrada

HoneyPot: Equipo señuelo sin seguridad para que ataquen a ese equipo. Nos permite aprender de dónde nos están atacando

Proxy enmascara una IP, no encripta la conexión

MDM: Programa que administra lo que haces en tu dispositivo móvil

#### ▼ 15-09-2022

Primer parcial

## ▼ Segundo Parcial

#### ▼ 19-09-2022

No hubo clase. El profe le hizo el examen a Fer

#### ▼ 20-09-2022

Revisión de examen

#### ▼ 21-09-2022

### Amenazas y vulnerabilidades

httrack es una herramienta así como webhttrack para descargar un frontend completo

Los gobiernos de latam son muy vulnerables porque los gobiernos no dejan a los desarrolladores hacer bien su trabajo

Al usar el httrack pueden usarse comandos como

cat \*.html | grep contraseña

Otro paso puede ser preguntar por los buscadores

dnsdumpster trae muchas estadísticas por dns

Con whois puede darse una dirección para ver los datos del personal de informática

Con un dork de bing podemos ver todo de una ip

De un día para otro pueden dejar de funcionar los dorks

Algunos interesantes son

- site
- “ ”
- OR o |
- AND
- -
- \*
- define
- cache
- filetype

Ejemplo:

site: .gob.mx “login”

▼ 22-09-2022

No entré a clase :(

▼ 23-09-2022

HAY QUE REGRESARNOS A LO DE DORK DE BING



▼ 26-09-2022

No hubo clase

▼ 27-09-2022

## Amenazas y vulnerabilidades

Basadas en dorks

No son las únicas vulnerabilidades que existen. Podemos seguir trabajando con el footprinting

Hay que proteger áreas privadas con autenticación de usuario, cifrar información confidencial.

Para evitar el escaneo del servidor usaríamos el IDS

Para footprinting:

Con linux puede usarse el whois <URL>

Página cual es mi ip

Otro método muy común es buscando errores a peticiones HTTP

Otra es buscar que una persona de una organización nos mande un correo electrónico y analizar los encabezados del que envió el correo para analizar servidores SMTP y otra cosa

Otras cosas es usar los metadatos de los archivos

exiftool en linux funciona para mostrar todos los metadatos de la información

Algunas variaciones del comando son:

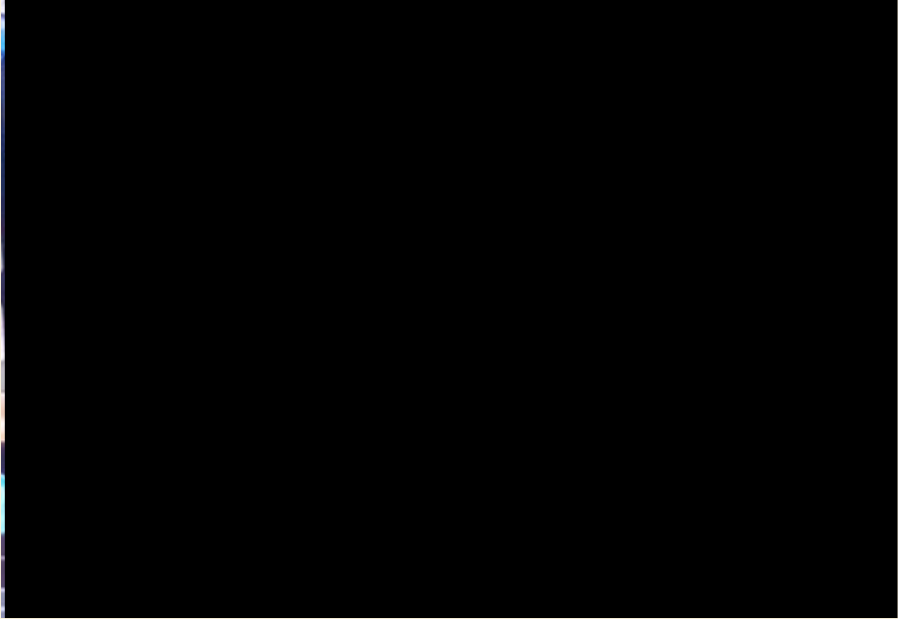
```
exiftool <archivo>  
exiftool -all <archivo>
```

### ▼ 28-09-2022

The Harvester

haveibeenpwned





Dnsdumpster o the harvester para la tarea

▼ 29-09-2022

Medidas de seguridad

- Cuidar la información pública de internet
- Tener muy bien configurados los servidores web y DNS de la compañía y actualizados
- Tener separados los correos de la entidad de los personales
- Limpiar documentos públicos de los metadatos

Ya salimos del footprinting, es decir lo legal

Un buen punto de inicio puede escanearse los puertos buscando puertos abiertos de servidores de la entidad e intentando identificar qué hay detrás de los puertos. Para esto puede usarse nmap

A cada puerto se le asigna un número comprendido entre 0 y 65535

Del 0 al 1023 son estandarizados

Del 1024 al 49151 son para servicios registrados

Los últimos son de los sistemas operativos a los programas cliente de manera dinámica

Los primeros dos tipos los regula la IANA

El tercer tipo de puertos son dinámicos y van cambiando

Hay distintos tipos de escaneo:

- TCP SYN
- TCP connect
- TCP FIN
- UDP

La técnica de escaneo de puertos trae dos problemas

1. Hace mucho ruido
2. Si se hace todo de golpe, puede levantar sospechas por parte del administrador de seguridad

Lo mejor es hacer escaneos poco a poco

Hay mecanismos para bloquear escaneos:

1. Un firewall se come todos los paquetes y se protege un equipo
2. Un IDS porque puede sniffearse todo lo que pasa en una red

#### ▼ 30-09-2022

Segmentar 192.168.10.0/24 en 4 redes

Primero se convierte a binario

Se usarán 2 bits por lo que en lugar de 24 se usará 26: 192.168.10.0/26

Ahora nos conectaremos con el router

#### ▼ 03-10-2022

No hubo clases por el congreso de ICI

#### ▼ 04-10-2022

No hubo clases por el congreso de ICI

#### ▼ 05-10-2022

No hubo clases por el congreso de ICI

#### ▼ 06-10-2022

No fui :(

#### ▼ 07-10-2022

No fui :(

#### ▼ 10-10-2022

Empezaremos teóricamente con el Hacking Ético

Hay que determinar qué información queremos cuidar

#### ▼ 11-10-2022

Introducción a ethical hacking

#### ▼ 12-10-2022

Recordar que puede ser pregunta de examen que un contrato tiene que estipular si el correo es una herramienta de trabajo para poder revisarlo, de lo contrario se consideraría correspondencia y revisarlo es un delito

Importancia de un contrato y aspectos legales de una empresa

Source forge projects jnetmap

Info spyware foro

#### ▼ 13-10-2022

Al trabajar con redes, si se empalma cable, se utiliza una terminal que es una cajita donde se agarra y se ponen los cables con una pinza ponchadora y luego un RJ45 pero con eso se pierde más o menos el 20% del cableado original

Pocas personas usan cableados termorretráctiles con aleaciones de oro para perder menos que permite que se pierda como un 10%

## Crackeo

Técnica para entender y alterar el funcionamiento de un programa sin contar con su código fuente y con un objetivo específico basándose en compilación inversa



La clasificación de medidas de protección:

- Duración limitada
- Restricciones numéricas
- Número de registro

Otro tip: Usar software crackeado en máquinas virtuales (como ver Cuevana)

Técnicas de protección de software:

- Cifrado (Armadillo)
- Registro interactivo
- Registro y comparación de parámetros
- Fichero clave
- Programas limitados
- Protección por hardware (WatchDogs)
- Comprobación de presencia de disco

Métodos de crackeo

- Programas de depuración (OllyDbg, softice)
- Desensambladores

Herramientas:

- Frogsice
- Procdump
- Armadillo Killer
- Extras
  - Editor hexadecimal UltraEditor
  - Readpe (pev.sourceforge.io)
  - Para .net (ilspy.net)

Hay un montón de descompresores en la presentación

La técnica de crackeo más sencilla es bajo protección numérica (para este podemos buscar bien en el registro de Windows o en ficheros)

La otra es el número de registro que también se almacena en el registro de Windows

Se puede optimizar Windows con una herramienta llamada sysccleaner (o un nombre similar)

#### ▼ 14-10-2022

Práctica de uso del cañón de iones

#### ▼ 17-10-2022

Esteganografía

Estegoanálisis

Diferencia entre esteganografía y criptografía

Esteganografía es esconder

Tipos de esteganografía:

- Pura

- Con clave secreta
- De texto

OpenPuff (Windows)

Steghide (Linux)

Outguess (Linux)

SpamMimic (Online)

Segmentación 256: no existe

Metodología:

- Esteganografía de Bacon
- LSB
- Inyección

Para inyección:

```
cat > texto-seguro.txt
ls
more texto-seguro.txt
cat UAA.png texto-seguro.txt > UAA-secure.png
ls
more UAA-secure.png
hexeditor -C UAA-secure.png
```

#### ▼ 18-10-2022

No hice apuntes D:

#### ▼ 19-10-2022

No hice apuntes D:

#### ▼ 20-10-2022

No hice apuntes D:

#### ▼ 21-10-2022

No fui a clase :(

#### ▼ 24-10-2022

No hice apuntes D:

#### ▼ 25-10-2022

Para el examen:

Son 10 preguntas

Tener acceso al correo institucional

Enviar

Instalar Steghide

Sha256Sum

Comandos:

hexeditor

hexdump

sha256sum

tail

steghide —embed -cf

steghide —extract -sf

## ▼ Itinerario de estudio para el examen

[7:00 - 7:30] Las bases de Linux (comandos, configuraciones, etc.)

[7:30 - 7:45] Teoría de inicios del parcial

[7:45 - 8:00] Teoría de Footprinting

[8:00 - 10:00] Comparando distintos casos de las tareas de footprinting

[10:00 - 10:30] Esteganografía en imágenes

[10:30 - 11:00] Esteganografía en textos

### ▼ 26-10-2022

Continuación de virus

### ▼ 27-10-2022

Aplicación del segundo parcial

### ▼ Las diapositivas del parcial

#### ▼ Material de clase unidad 3

# Amenazas y vulnerabilidades

Mtro. Arturo Ocampo Silva

## Amenazas y Vulnerabilidades

Temas

- Introducción
- Ingeniería Social
- Footprinting
- Fingerprinting
- Análisis de la Información

La primera de todas ellas y la más importante es aquella situada entre el ordenador y la silla, también llamada capa 8. El usuario

- Pues es más fácil engañarle a él que a una máquina
- Partiendo de este principio se verá en qué consiste la Ingeniería Social
- Ingeniería Social es la técnica de engaño a las personas para que revelen información sensible
- O incluso para que lleguen a comprometer el sistema ellos mismos
- Ya sea adrede (por ejemplo algún empleado descontento) o por desconocimiento

La técnica más usada a la hora de hacer ingeniería social, el phishing

- Consiste en enviar un correo a la víctima haciéndonos pasar por otra entidad para que introduzca los datos de la entidad a la que queremos suplantar.

• Términos importantes:

- Footprinting: Consiste en la búsqueda de información pública de un objetivo.
- Fingerprinting: Consiste en obtener la información interactuando directamente con los sistemas a atacar.
- Footprinting es mucho más silenciosa que la segunda, incluso llegando a ser totalmente inadvertida para la víctima

En seguridad informática siempre el eslabón más débil es el usuario, ya que un alto porcentaje de la gente que utiliza ordenadores o dispositivos conectados a Internet tiene escasos o nulos conocimientos de informática y desconoce el peligro de la información de Internet, por ello, los atacantes son capaces de utilizarlo en su beneficio.

Es mucho más fácil engañar a una persona que intentar romper un algoritmo de cifrado o encontrar un hueco en el protocolo TLS. Algunos tipos de engaño clásicos consisten en pedir al usuario que: Utilice un USB infectado, abra un correo ó nos facilite su contraseña haciéndonos pasar por un administrador del sistema.

Las claves de la Ingeniería Social son: Todos queremos ayudar, el primer movimiento es siempre de confianza hacia el otro, no nos gusta decir «No» y a todos nos gusta que nos alaben.

Recordemos que la ingeniería social surge del aumento de la seguridad de los sistemas informáticos en la actualidad y puede ser usada en cualquier fase de un ataque.

En la búsqueda de vulnerabilidades: Obteniendo información sobre la empresa preguntando a un empleado convenciéndole de que somos un periodista o un empleado nuevo de la empresa.

En el ataque: Consiguiendo que alguien ejecute un archivo infectado haciéndose pasar por alguien en quien tenga confianza.

#### Ejemplos de ingeniería social:

Mandar un correo a una persona haciéndonos pasar por un familiar suyo que quiere hacerle una transferencia, y le pedimos el número de tarjeta de crédito o varios datos personales. Si la persona carece de conocimientos de Seguridad, probablemente revele dicha información al atacante.

Mediante correo electrónico suplantación identidad de alguna gran entidad o empresa (Apple, Google...), servicio del estado (correos, hacienda, la policía...), banco o página web... de la cual se desee obtener información. La página fraudulenta podrá así recopilar las credenciales de las víctimas.

#### Ejemplos de ingeniería social:

Incitar a abrir documentos o archivos infectados, haciéndolos pasar por documentos importantes, por información comprometedor de la persona, publicidad engañosa, etc.. Recordemos «En toda empresa siempre hay un despistado que hace clic en todo. Vacaciones gratis, clic; fotos de famosos, clic».

A veces con preguntar al administrador de seguridad de la empresa en que trabajas la IP del servidor FTP y te la dirá.

En ocasiones será necesario enviar spam masivo a los empleados de la empresa esperando que alguno haga clic en un enlace.

Sentarse al lado de la víctima esperando que introduzca su contraseña en el móvil para verla por encima del hombro.

| Esquema más detallado:           |                                                                                                                     |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Pasivas</b>                   | Observación                                                                                                         |
| <b>No presenciales</b>           | Correo electrónico<br>Teléfono<br>Correo ordinario y fax                                                            |
| <b>Presenciales no agresivas</b> | Hablar con la gente<br>Vigilancia<br>Seguimiento<br>Acreditaciones falsas<br>Desinformación                         |
| <b>Presenciales agresivas</b>    | Suplantación de identidad<br>Chantaje o extorsión<br>Despersonalización (alcohol, drogas...)<br>Presión psicológica |

- Algunas medidas para reducir estas técnicas son:
  - La concienciación de las personas de los temas relacionados con la seguridad.
  - Nunca compartir la contraseña (pues nadie debería pedírsela).
  - No contar información de la empresa a gente externa a ella...
  - Tener un servidor de correo electrónico interno que pueda filtrar el spam. (Nel ya no ahora solo tener bien configurado el antispam o un antivirus chicles)
  - No mezclar correo personal con correo de trabajo.
  - Tener poca o al menos bien organizada la descentralización en la empresa, es decir, tener bien definidos los segmentos a través de los cuales va a ser transmitida la información hasta llegar al ejecutivo.

Más

ejemplos de ingeniería social:

- Dejar «olvidado» un USB en el suelo o en una mesa cercano al de la persona que queremos atacar.

Probablemente, una persona sin conocimientos de informática lo introducirá en su ordenador para ver qué contiene, a partir de ahí si está configurado el modo de auto ejecutables se podrán realizar acciones en segundo plano como el Rubber Ducky USB, que actúa como un teclado externo y es capaz de ejecutar scripts como si el atacante tuviera el ordenador delante. O como algún archivo infectado que la víctima ejecute

¡ Las personas son muy curiosas !

Veamos un poco en: <https://hak5.org/>

Más ejemplos de ingeniería social:

- Dejar «olvidado» un USB en el suelo o en una mesa cercano al de la persona que queramos atacar.

Probablemente, una persona sin conocimientos de informática lo introducirá en su ordenador para ver qué contiene, a partir de ahí si está configurado el modo de auto ejecutables se podrán realizar acciones en segundo plano como el Rubber Ducky USB, que actúa como un teclado externo y es capaz de ejecutar scripts como si el atacante tuviera el ordenador delante. O como algún archivo infectado que la víctima ejecute

¡ Las personas son muy curiosas !

Veamos un poco en: <https://hak5.org/>

Gracias al alumno que nunca fue mi alumno..... El sabe quien rehackings es.....

Más ejemplos de ingeniería social:

Ingeniería social persona a persona, ya sea por teléfono, por chats o en persona.

En la actualidad, en internet podemos encontrar todo tipo de información referente a cualquier persona si sabemos buscar. Gracias a toda esta información un atacante puede ser capaz de asumir un rol para poder engañar a otra persona.

Redes como LinkedIn pueden darnos información del entorno de trabajo de una persona.

Facebook puede darnos información de las costumbres, aficiones, familiares...

Footprinting:

Esta búsqueda de información no se considera delito, ya que es información pública y la entidad no debería detectarlo. Se buscará cualquier dato que pueda ser de utilidad para poder lanzar posteriormente un ataque.

- Existe un mecanismo que utilizan algunas páginas web para que los buscadores como Bing o Google no indexen ciertas páginas de un sitio web en sus bases de datos, es el llamado robots.txt, el cual se encuentra en la URL: [www.nombrepagina.com/robots](http://www.nombrepagina.com/robots)

Si visitamos esa dirección web podremos encontrar también una gran fuente de información, ya que se suele utilizar para poner las direcciones de páginas de administración del sitio o zonas restringidas de la entidad.

OJO ESTA ÚLTIMA YA ES OBSOLETA Y SOLO SERÁ ÚTIL SI EL DESARROLLADOR ES O NOVATO O UN PELMAZO



Footprinting:

Otra forma de FootPrinting consiste en: Descargar el código fuente del sitio web entero con herramientas como httrack en Windows o webhttrack para Linux o Mac OS X.

Esta herramienta dispone tanto de modo de uso gráfico como en consola, con ella podremos descargarnos todo el sitio web de una entidad:

- El código HTML, las imágenes, documentos y archivos que tenga e incluso las páginas a las que enlace.
- Ojo las herramientas se deben usar con precaución, pues permite la descarga simultánea de muchos objetos (imágenes, documentos, páginas...) y puede llegar a saturar la red si se realizan muchas conexiones al mismo tiempo.

- Una vez las descarguemos podremos realizar búsquedas en el código fuente de comentarios en los que el programador de la página maneje información sensible,

Como nombres de usuario y contraseñas por defecto, enlaces como los ya mencionados anteriormente o cuentas de correos y nombres reales. Ejem: El formato de un comentario HTML es: `<!-- comentario del código -->`

- Estas búsquedas se pueden realizar mediante consola de comandos con órdenes como:

- `cat *.html | grep contraseña`
- `cat *.html | grep -A 3 "<!--"`

El siguiente paso será preguntar a los buscadores

(Google, Bing...) por el dominio del que queremos obtener información, es muy probable que sus crawlers o arañas (bots que navegan por internet de forma autónoma para indexar páginas en la base de datos) indexen ciertas páginas que no deberían ó que nos muestran información que haya en alguna página que sea muy difícil encontrar manualmente. A la hora de preguntar a los buscadores se utilizan una serie de palabras clave para especificar más la búsqueda. Dependiendo de cada buscador pueden ser diferentes, y en este caso se explicarán para los dos más importantes, Google y Bing.

Otra forma de encontrar información importante de la organización es mediante el uso de [dnsdumpster.com](https://dnsdumpster.com/)

<https://dnsdumpster.com/>

Antes de entrar de lleno en el footprint veamos lo que podemos hacer.. Extra. Extra.. Calientita al 14 de Septiembre 10:24

ya tenemos los servidores. Ahora veamos qué empresa lo tiene. whois

pero queremos más.. Ahora con un dork de bing aprendamos TODO sobre esa IP — ip: numerodelaIP

Y listo datos, datos, datos y más datos

Algunos ejemplos de dorks, para Google: (Actualizado al 21 de Septiembre de 2022)

- site: Solo muestra resultados del dominio web indicado, Si se especifica alguna palabra más, solo la buscará en ese dominio.
- " " Obliga a que se realice una búsqueda donde aparece de manera exacta el término dentro de las comillas.
- OR o | Busca que aparezca uno u otro término.
- AND Solo muestra el resultado si contiene las 2 opciones.
- - Excluye el resultado
- \* Funciona como comodín
- define: Diccionario online
- cache: Muestra la versión en cache de una pagina.
- filetype: Regresa un determinado tipo de archivo.

Algunos ejemplos de dorks, para Google:(Actualizado al 21 de Septiembre de 2022)

- related: Muestra los sitios relacionados a un dominio.
- intitle: Muestra páginas con un contenido específico en el título
- allintext: Solo se muestran las paginas que en su texto tengan de manera especifica el texto que se esta indicando.
- stocks: Muestra información bursátil sobre una empresa.
- in Te permite realizar conversiones
- map: Te permite ver la ubicación en google maps de un sitio.
- inurl: Lo buscado debe estar dentro de la URL

Algunos ejemplos de dorks, para Google: (Actualizado al 21 de Septiembre de 2022)

- enlace: Busca una página o punto de enlace definido por nosotros.
- intext: Permite buscar dentro del contenido de los archivos.
- libro: Te permite localizar libros específicos.
- inanchor: Permite buscar por una palabra o frase ancla.

Algunas combinaciones exitosas.

intitle:"index of" inurl:ftp Te permite identificar ftps abiertos

inurl:/proc/self/cwd Podemos identificar web servers vulnerables. Increíblemente peligroso

allintext:username filetype:log Este nos permite buscar el log de errores de sql por lo que podemos obtener mucha información de la base de datos.

Algunos ejemplos de dorks, para Google: (Actualizado al 21 de Septiembre de 2022)

typefile:env Recuerden que en los .env suelen estar las variables y configuraciones generales. Estos archivos deberían estar en el backend pero nunca faltan los atolondrados. Aquí podemos encontrar direcciones IP, nombre de usuarios y passwords sin encriptar.

intitle:index.of id\_rsa -id\_rsa.pub Detecta si están expuestas las llaves privadas del ssh.

filetype:log username putty Nos permite detectar si un sistema con windows tiene acceso por ssh mediante putty. identificando además el usuario utilizado.

Algunos ejemplos de dorks, para Google: (Actualizado al 21 de Septiembre de 2022)

typefile:env Recuerden que en los .env suelen estar las variables y configuraciones generales. Estos archivos deberían estar en el backend pero nunca faltan los atolondrados. Aquí podemos encontrar direcciones IP, nombre de usuarios y passwords sin encriptar.

intitle:index.of id\_rsa -id\_rsa.pub Detecta si están expuestas las llaves privadas del ssh.

filetype:log username putty Nos permite detectar si un sistema con windows tiene acceso por ssh mediante putty. identificando además el usuario utilizado.

filetype:xls inurl:"email.xls" Este chiste se cuenta solo.

link: Te permite visualizar todos los sitios que tienen enlace a tu página o a alguna página web.

Algunos ejemplos de dorks, para Google: (Actualizado al 21 de Septiembre de 2022)

site:.edu filetype:xls inurl:"email.xls" Variante del anterior.

filetype: sql "MYSQL dump" (pass|password|passwd|pwd) site: xxxxxxx

inurl:index.php?id=

yadentrodelapáginaencontradaconelanterior/index.php?id=' or '1'=='1'-- (inyección)

inurl:index.php?id= site:unapagina

site:edu filetype:pdf allintitle:restricted

Evitar ser víctima de los dorks y evitar que los motores de búsqueda indexen su información confidencial.

Proteja las áreas privadas con una autenticación de usuario y contraseña y también mediante el uso de restricciones basadas en IP.

Cifre su información confidencial (usuario, contraseñas, tarjetas de crédito, correos electrónicos, direcciones, direcciones IP, números de teléfono, etc.).

Ejecuta escaneos de vulnerabilidad regulares contra su sitio, estos generalmente ya usan consultas populares de Google Dorks y pueden ser bastante efectivos para detectar los más comunes.

Ejecuta consultas de dorks periódicas en tu propio sitio web para ver si puede encontrar información importante antes de que lo hagan los malos. Puede encontrar una gran lista de idiotas populares en la base de datos Exploit DB Dorks.

Si encuentra contenido confidencial expuesto, solicite su eliminación mediante Google Search Console.

Otras medidas para evitar el escaneo de nuestro servidor, es la instalación de firewalls así como de IDS

OJO. Es importante saber que existen diversos dorks para diversos buscadores, por lo que será importante probar el dork que nos interese en los diversos navegadores.

El siguiente paso es utilizar los sitios web de búsqueda de información de un dominio. Estos nos permitirán obtener información valiosa del dominio objetivo como su dirección IP, su registro de dominio (mediante consultas Whois), su localización en mapas, los subdominios, sus trazas, sus servidores de DNS...

<https://www.cual-es-mi-ip.net/geolocalizar-ip-mapa>

OJO. Hay que ser conscientes de que esto solo será útil cuando el servidor pertenece a la organización. Y lo más importante tiene IP- Publica.

Otro método para obtener información de los servidores

web y los sistemas operativos que utilizan es a través de peticiones HTTP, que, aunque cada vez ocurra menos, muchos webmaster se olvidan de personalizar los errores 404 Not Found (que se obtiene cuando se intenta consultar una página de un dominio que no existe) los cuales muestran información sensible del servidor. Para el análisis del tipo de los servidores web o sistemas operativos se puede utilizar el correo electrónico, analizando las cabeceras de los mensajes. Se tiene que conseguir que la persona o entidad nos envíe un email.

El siguiente paso es el análisis de los metadatos Datos que se almacenan junto con los documentos para poder ayudar a su identificación, suelen tener gran cantidad de información más de la que deberían, ya que en documentos de texto pueden

contener:

- El nombre del usuario que lo escribió
- La fecha de creación
- Fecha de la última modificación
- La aplicación con la que se ha creado, el sistema operativo...
- Pero también se encuentran en más tipos de ficheros como imágenes (pudiendo tener localización GPS o el tipo de cámara que la realizó), pdf, documentos de Excel...

El siguiente paso es el análisis de los metadatos datos que se almacenan junto a los archivos. Algunas formas sencillas de revisar los metadatos es mediante.

- pdftinfo
- identify -verbose
- exiftool

Para borrar los metadatos utilizaremos la última herramienta.

exiftool -all:all= nombreadarchivo

▪ El siguiente paso es encontrar todos los correos de la entidad para una ingeniería social, phishing o para ver las dimensiones de la organización, démonos cuenta que las grandes entidades poseen servidores de correo propio y son fáciles de encontrar por su dominio (@uah.es, @ucm.es...)

▪ Se pueden utilizar dos herramientas que se encuentran en la distribución Kali Linux, en concreto hablamos de Maltego y de The Harvester.

Tras haber obtenido los correos de las personas de la organización, tanto los del dominio como los privados, se puede aprovechar un servicio web llamado

<https://haveibeenpwned.com/>

## Medidas de seguridad / recomendaciones.

Para minimizar el efecto de estos procesos de footprinting por parte de las organizaciones y/o personas:

- Cuidar la información pública que hay en Internet, configurar lo que se quiere que sea público y privado
- Tener bien configurados y actualizados los servidores web y DNS de la compañía
- Tener separados los correos de la entidad de los personales
- Limpiar los documentos públicos de metadatos

Para lograr este fin el mejor punto de inicio suele ser el escaneo de puertos, buscando los puertos abiertos en los servidores de la entidad e intentando identificar que hay detrás de esos puertos. Para esto haremos uso de herramientas que te permitan analizar el objetivo como nmap.

Nmap se basa en el envío de paquetes de diferentes tipos a los puertos de un servidor esperando una respuesta de éste, dependiendo del tipo de paquete que se envíe será un tipo de escaneo diferente, algunos son más sigilosos, otros son más efectivos, otros no son solo para analizar puertos, sino también para saber si hay algún tipo de firewall, o incluso para analizar la seguridad de los certificados que proporciona un servidor web.

Pero primero es importante recordar cuál es la importancia de los puertos. A cada puerto se le asigna un número comprendido entre el 0 y el 65535. Estos se dividen en tres áreas:

- Los puertos que van desde el número 0 al 1023 reciben la denominación de **puertos estandarizados** y la Internet Assigned Numbers Authority (IANA) asigna protocolos fijos y otros recursos a la mayoría de ellos. De esta manera, por ejemplo, se ha reservado el puerto 80 para las conexiones HTTP y, por lo tanto, este se convierte en el puerto decisivo para las solicitudes realizadas a través del servidor web.
- Los números de puerto (**Puertos Registrados**) que van desde el 1024 hasta el 49151 (También los asigna la IANA) están destinados normalmente a servicios registrados, aunque se asignan también a clientes, en especial por parte de Linux. Dentro de este grupo estarían todos los servicios y aplicaciones que podemos instalar en un equipo. Aquí estarían comprendidos los juegos, aplicaciones de mensajería, voz sobre IP (VoIP),...

Por ejemplo: Plex-multimedia (32400), SIP-inicio sesion voz ip (5060), VNC-video (5900,5800), Zerotier-vpn (1802), Battlefield-game (9988),...

- Los puertos comprendidos entre los números 49152 y 65535 son los que otorgan los sistemas operativos a los programas cliente de manera dinámica. **Puertos efimeros o dinámicos**



| <b>Sistema Operativo</b>                                                                                      | <b>Puertos efímeros</b> |
|---------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Windows XP y anteriores</b>                                                                                | <b>1025 - 5000</b>      |
| <b>Linux hasta 2.4</b><br><b>FreeBSD hasta 4.6</b>                                                            | <b>1024 - 5000</b>      |
| <b>Solaris</b><br><b>Linux 2.4 o superior</b>                                                                 | <b>32768 - 65535</b>    |
| <b>Cumplen con IANA</b>                                                                                       |                         |
| <b>Windows Vista y posteriores</b><br><b>MacOS (Darwin)</b><br><b>FreeBSD 4.6 o superior</b><br><b>NetBSD</b> | <b>49152 - 65535</b>    |

¿ Ahora cómo es que funcionan los programas para el escaneo de puertos ?

Sencillo recordemos cómo se conectan los equipos por tcp.

- Al realizar el proceso de negociación en tres pasos (3-way handshake), el cliente envía un paquete SYN (synchronize = "sincronizar") al puerto de destino correspondiente.
- Si consigue llegar hasta una aplicación, recibe un paquete SYN/ACK combinado (synchronize acknowledge = "confirmar sincronización") que confirma el establecimiento de la conexión.
- El cliente responde en el tercer y último paso con un paquete ACK (acknowledge = "confirmar"), por lo que se establece la conexión y puede comenzar el intercambio de datos.

Si se establece el contacto con un puerto cerrado, el cliente recibe en el segundo paso un paquete con el flag RST (reset = "restablecer") como respuesta, por lo que se interrumpe la negociación.

Puesto que el intercambio de datos con las diversas aplicaciones resultaría por un lado muy costoso y por otro muy complejo, el escáner de puertos sólo está limitado a un sencillo intento de conexión.

#### Tipos de Escaneo

- **TCP SYN:** Se envían paquetes SYN a cada uno de los puertos con el port scanner, tras lo que se espera una respuesta por parte del host de destino. Si este responde con un paquete SYN/ACK, esto indica que el puerto correspondiente está abierto, si la respuesta es RST el puerto está cerrado. Si no hay respuesta se están filtrando los paquetes.
- **TCP connect:** Se intenta establecer una conexión como lo realizaría por ejemplo un navegador web, la conexión la controla el sistema operativo
- **TCP FIN, Xmas y Null:** Se utilizan Null y FIN, pero se lanzan como urgentes para acelerar la respuesta y buscar que se enciendan todos los puertos
- **UDP:** Se envían encabezados UDP vacíos y sin datos a todos los puertos de destino. Si un servicio responde con un paquete UDP, queda confirmado que el puerto que le pertenece está abierto. Si el router envía al port scanner el mensaje de error "Port unreachable" (Type 3, Code 3), este sabrá que el puerto está cerrado. Otros tipos de mensajes de error informan de que un filtro de paquetes bloquea el puerto. El gran problema que se deriva de escanear puertos con UDP es que requiere mucho tiempo, ya que en numerosos sistemas, la tarea de emitir los correspondientes mensajes de error puede tardar mucho tiempo por motivos de seguridad y los puertos abiertos solo responden de forma muy irregular. El núcleo de Linux limita el número de mensajes a, por ejemplo, uno por segundo, lo que significa que se pueden escanear 65.535 puertos en unas 18 horas.



Hay dos principales problemas con la técnica del escaneo de puertos:

1. Hace mucho ruido: Ya que esta técnica consiste en ir enviando paquetes a todos los puertos de los servidores
2. Si se hace todo de golpe puede levantar sospechas por parte del administrador de seguridad (si hay)

Lo mejor es siempre hacer los escaneos poco a poco

Hay mecanismos para bloquear estos escaneos y sistemas para alertar de ellos:

- Los firewall, cortafuegos o IPS pueden ser dispositivos hardware o programas software que mitigan estos escaneos de puertos, filtrando los paquetes de IP's externas o filtrando el tipo de paquetes (sobre todo los de tipo ICMP o ping).
- Los IDS o Intrusion Detection System, son sistemas de alarma que se colocan dentro de una red (normalmente suelen ser ordenadores analizando el tráfico) y que alertan de comportamientos anómalos en el sistema

La herramienta NMAP entre sus características cuenta con el manejo de scripts de diferentes tipos.

- Autenticación
- Fuerza bruta
- Configuraciones por defecto
- Descubrimiento
- Denegación de servicio
- Exploiting
- Ataques externos e intrusión
- Malware
- Detección de versiones y vulnerabilidades

Para conocer los scripts de nmap a detalle se sugiere visitar.

<https://nmap.org/book/nse.html>

Para obtener el manual completo de uso.

<https://nmap.org/man/es/index.html>

Otra de las cosas que permite realizar nmap es la de intentar ocultar el tráfico que genera en sus procesos, esto lo hace mediante la opción -D. Entre más opciones incluyamos más difícil será identificar el atacante.

Una opción interesante al uso de nmap, pero trabajando con un entorno gráfico es Zenmap pero con todas las instrucciones de nmap. Nmap se basa en el envío de paquetes de diferentes tipos a los puertos de un servidor esperando una respuesta de éste, dependiendo del tipo de paquete que se envíe será un tipo de escaneo diferente, algunos son más sigilosos, otros son más efectivos, otros no son solo para analizar puertos, sino también para saber si hay algún tipo de firewall, o incluso para analizar la seguridad de los certificados que proporciona un servidor web.

```
Host is up (0.082s latency).
All 1000 scanned ports on [redacted] net (f[redacted]) are in
red states.
Not shown: 1000 filtered tcp ports (no-response)
Nmap done: 2 IP addresses (1 host up) scanned in 85.25 seconds
```

Hay un firewall

Arturo Ocampo Silva

#### Básicos de NMAP.

- nmap -sS : Es el sondeo SYN es rápido hace poco ruido es funcional para levantamientos básicos.
- nmap -sT : Sondeo TCP, usa la misma llamada de alto nivel que la mayoría de las aplicaciones de red, como navegadores o clientes P2P. Utiliza la API de conectores de Berkeley
- nmap -sX : Mejor conocido como Christmas tree. Establece las banderas FIN, PSH y URG,
- nmap -sU : Sondeo mediante UDP recuerden el problema con linux
- nmap -O : Permite intentar identificar el sistema operativo de la contraparte
- nmap -sV -O : Permite identificar S.O. y versión.
- nmap -sF : Realiza un escaneo FIN

#### Básicos de NMAP.

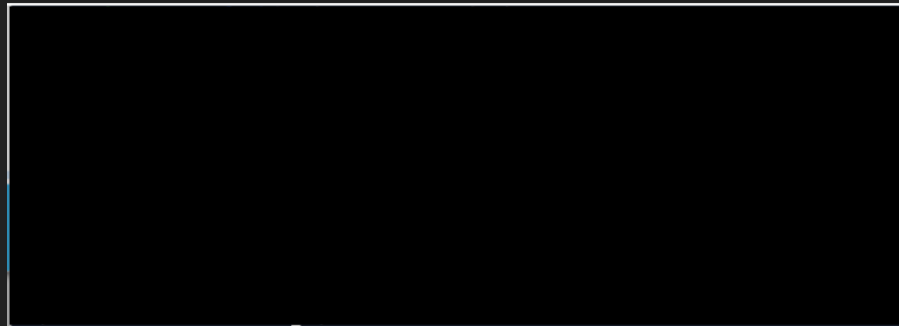
- nmap -p puerto ip: Escanear un puerto en concreto
- nmap -p desde-hasta ip : Escanear un rango de puertos
- nmap -F ip: Escanear los puertos más utilizados (modo rápido)
- nmap -top-ports cantidad ip: Escanear un número dado de los puertos más importantes
- nmap -p- ip: Escanear los 65535 puertos (todos)

Ejemplo de uso de nmap utilizando scripts para revisar los banners y escondiendonos mediante la técnica de confusión.



Un script muy útil puede ser el de identificación de banner

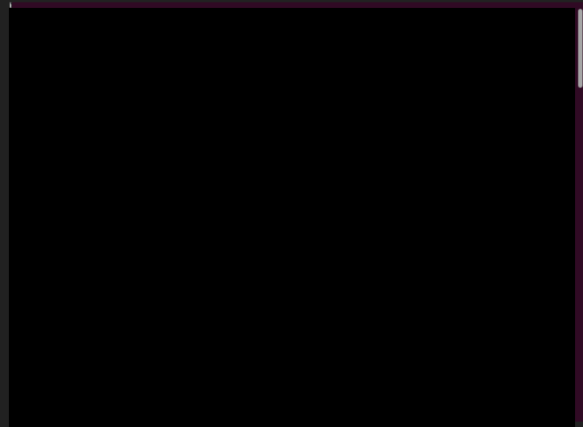
▪ Nmap se conecta a un puerto TCP abierto e imprime todo lo que recibe del servidor durante 5 segundos.



Los Scripts nos pueden ayudar a analizar la seguridad que ofrecen los certificados de un sitio web:

- Tipo de protocolo que soportan
- Que algoritmos de cifrado usan
- Podemos realizar algunas pruebas de inyección de SQL y fuerza bruta, detectar vulnerabilidades, etc.

A lado un ejemplo del uso de un script de inyección sql.



Con el siguiente script para autenticaciones (auth), que comprobará si existen usuarios con contraseñas vacías o la existencia de usuarios y contraseñas por defecto. La siguiente captura de pantalla gráfica el ejemplo:

```
aocampo@aocampo:~/Descargas$ sudo nmap -f -ss -sV --script
```

Ejemplo de uso de nmap -A para conocer el sistema operativo y -T4 para acelerar la velocidad del proceso.

Mtro. Arturo Ocampo Silva

Para identificar si nuestro correo pudiera estar comprometido.

<https://haveibeenpwned.com/>

¿Qué es el Ethical Hacking ?

(hacking ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

### ¿ En qué consiste ?

En la simulación de posibles escenarios reproduciendo ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, entendiendo que "Para atrapar a un intruso, primero debes pensar como intruso"

- Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, es aquí donde entran los servicios del Ethical Hacking , que es una disciplina de la seguridad informática que usa una gran variedad de métodos para realizar pruebas, estos métodos incluyen tácticas de ingeniería social, uso de herramientas de hacking , uso de Metasploits que explotan vulnerabilidades conocidas, en fin son válidas todas las tácticas que conlleven a vulnerar la seguridad y entrar a las áreas críticas de las organizaciones.

### ¿Por qué pagar un Ethical Hacking?

- Para detectar el nivel de seguridad interno y externo de los sistemas de información de la organización, determinando el grado de acceso que tendría un atacante.
- Para detectar las vulnerabilidades que pudieran ser vistas y explotadas por individuos no autorizados y ajenos a la información como: crackers, hackers, ladrones, ex- empleados, empleados actuales disgustados, competidores, etc. Las pruebas de penetración, están totalmente relacionadas con el tipo de información que cada organización maneja, por tanto según la información que se desee proteger, se determina la estructura y las herramientas de seguridad pero nunca a la inversa.

### ¿Por qué pagar un Ethical Hacking?

- Evaluar vulnerabilidades mediante la identificación de debilidades provocadas por mala configuración de las aplicaciones.
- Analizar y categorizar debilidades explotables, en base al impacto potencial y el riesgo.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar en medida de lo posible las vulnerabilidades reduciendo el riesgo de ocurrencia de un evento desfavorable.

### Análisis de Vulnerabilidades vs Pruebas de Penetración.

- Las pruebas de penetración se enfocan en comprobar y clasificar vulnerabilidades.
- Un análisis de vulnerabilidades se enfoca en el impacto que las vulnerabilidades tienen sobre la organización.

### Fases de las pruebas de penetración.

- Recopilación de información
- Descripción de la red ( Pueden usar herramientas como jnetmap)
- Exploración de los sistemas
- Extracción de información
- Acceso no autorizado a información sensible o crítica
- Auditoría de las aplicaciones web
- Elaboración de informes
- Informe final

### Tipos de Pruebas de Ethical Hacking.

- Con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- Sin objetivo: Se examina la totalidad de los componentes de los sistemas informáticos de la organización. Estas pruebas suelen ser las más laboriosas.
- Penetración a ciegas: Sólo se emplea la información pública disponible sobre la organización.
- Penetración informada: Se utiliza información privada, otorgada por la organización sobre sus sistemas informáticos. Se trata de simular ataques realizados por personal interno de la organización que tiene determinado acceso a información privilegiada.

### Tipos de Pruebas de Ethical Hacking.

- Externas: Se realizan desde lugares externos a las instalaciones de la organización. El objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Internas: Son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

### Modalidades de pruebas de Ethical Hacking.

Las pruebas descritas anteriormente se pueden ubicar en dos modalidades dependiendo si el desarrollo es del conocimiento del personal informático o no.

**Red Teaming :** Es una prueba encubierta, por lo que sólo un selecto grupo de ejecutivos sabe de ella. En esta modalidad son válidas las técnicas de "Ingeniería Social" para obtener información que permita realizar ataques. Es más real y evita que se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.

### Modalidades de pruebas de Ethical Hacking.

**Blue Teaming :** El personal de informática conoce de las pruebas. Esta modalidad se aplica cuando las medidas tomadas por el personal de seguridad de las organizaciones ante un evento considerado como incidente repercuten en la continuidad de las operaciones críticas de la organización, por ello es conveniente alertar al personal para evitar situaciones de pánico y fallas en la continuidad del negocio.

### Entregables en un Ethical Hacking.

- Documento que contiene a grandes rasgos una lista detallada de las vulnerabilidades encontradas y verificables.
- Lista de recomendaciones para que sean aplicadas por los responsables de seguridad en la organización.

– Informe técnico

– Informe ejecutivo

(Estos 2 últimos informes permiten a los empleados técnicos y administrativos entender y apreciar los riesgos potenciales sobre el negocio.)

### Beneficios de un Ethical Hacking.

- Buena imagen y reputación corporativa
- Obtención de un panorama sobre las vulnerabilidades halladas en los sistemas de información, que es de gran ayuda al momento de aplicar medidas correctivas.
- Descubrimiento de configuraciones inadecuadas en las aplicaciones instaladas en los sistemas (equipos de cómputo, switches, routers, firewalls) que pudieran desencadenar problemas de seguridad en la organización.
- Identificación de sistemas vulnerables por falta de actualizaciones.
- Disminución de tiempo y esfuerzo requerido para afrontar situaciones adversas en la organización.



#### Aspectos legales del Ethical Hacking.

- Deben tenerse presentes tanto por las organizaciones que prestan el servicio como por quienes lo contratan.
- Se debe abarcar la confidencialidad, que especifica que la información que los "Pen tester" encuentren no se puede usar más allá de los fines previstos por las pruebas.
- Se deben indicar claramente en el contrato los objetivos específicos de las pruebas de penetración para evitar futuros malos entendidos.
- La organización que contrata el servicio, debe garantizar que la información que se provee al "Pen Tester" es fidedigna para obtener resultados congruentes y certeros.

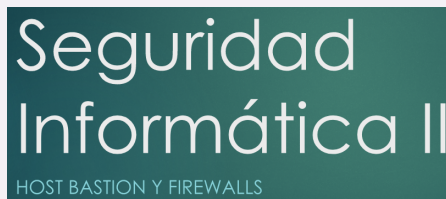
#### Consideraciones extras del Ethical Hacking.

- Dada la naturaleza de las pruebas de penetración deben entender tanto proveedor como consumidor que es limitada la posibilidad de probar toda la gama de técnicas y mecanismos que los crackers o hackers pudieran emplear para vulnerar un sistema informático y en ocasiones se llegan a obtener "falsos positivos", es decir resultados que indiquen una vulnerabilidad que realmente no es explotable.

### Algunos links útiles.

<https://sourceforge.net/projects/jnetmap/>

#### ▼ Host Bastion



Recordemos. Antiguamente se denominaba bastiones a las paredes que permitían proteger o fortificar las ciudades o los castillos. Estas murallas además de ser una barrera estática contenían en su interior espacios acondicionados para el resguardo de los hombres dedicados a la seguridad y sus respectivas armas.

Si bien en la actualidad hemos visto que este paradigma de asegurar todo al interior de nuestra organización ya no representa una verdad absoluta y que en gran medida tenemos que partir del precedente de que nuestra información se encuentra fuera de nuestro host bastion físico. Pero esto no implica que el mismo desaparezca, simplemente que ahora migramos a un entorno de host bastion virtual, donde la información que tenemos que proteger muy seguramente se encuentra almacenada en la nube. Pero la premisa sigue siendo la misma. NO QUEREMOS que cualquier persona tenga acceso a nuestra información.

## Nodos Bastion

Empecemos por definirlo. Este es nuestro punto de presencia en una red más grande comúnmente internet, digamos que es algo así como la recepción de una oficina. Donde todo el público puede llegar hasta donde se ubica la o el recepcionista. Pero finalmente solo aquellos que sean autorizados podrán ingresar. (Solo ingresarán quienes cumplan con las políticas de ingreso). Pero seamos conscientes la idea es que finalmente absolutamente todos se presentaran en ese punto, para ser bateados o aceptados pero llegarán a este punto. Por esto este equipo debe contar con las siguientes características especiales.

- Todas absolutamente todas las cuentas de este equipo deben ser frecuentemente auditadas.
- No deben existir cuentas con reciprocidad al interior de la organización.
- No se deben utilizar contraseñas que se usen al interior de la organización

## Nodos Bastion / Baluarte

- Las cuentas de administración o root debes estar inhabilitadas y bloqueadas.
- Se debe incluir cifrado para el acceso al servidor.

### Funciones de los Nodos Bastión

- Correo electrónico
- Sftp
- Servidor de VPN
- Punto de acceso a un túnel ssh
- Gateway
- DNS
- Honeypot

## Nodos Bastion / Baluarte

### Tipos de Host Bastion de manera general

- ▶ Single-homed bastión host: Tiene una única interfaz de red, Suele utilizarse para dar soporte a alguna aplicación o bien a la pagina web de la organización. Este depende completamente del router externo (Que hará la función de nateo) para la recepción de datos tanto del interior como del exterior. El host en este caso también puede estar configurado como firewall para evaluar los datos según las directrices de seguridad.
- ▶ Dual-homed bastión host: Usa dos interfaces de red. En este caso generalmente su función es trabajar como Gateway y firewall (Un buen ejemplo es fortinet). Este por obvias razones también realizara las funciones de nateo y al ser el que divide las 2 redes, nada podrá pasar por el sin ser filtrado.
- ▶ Multihomed bastión host: Este es utilizado cuando la política de seguridad requiere que todo tráfico entrante y salida sea enviado a través de un servidor proxy, tomando en cuenta que al utilizar un bastión host como interno este debe recibir todo el tráfico de un bastión host externo. Agregando con esto un nivel mayor de seguridad.



## Nodos Bastion / Baluarte

Proxy.

Antes de continuar debemos entender de manera clara las funciones de un proxy.

- **Control de acceso:** Permite controlar el acceso a Internet a través de restricciones de usuario o de direcciones IP.
- **Filtrado de contenido:** Al quedar entre los equipos y otra red mas grande como el permite controlar el acceso a sitios específicos.
- **Caché:** También pueden realizar la función de caché mejorando el desempeño de la red interna. Esto debido a que después de acceder a una página, almacena el contenido de la misma en su sistema. Después de eso otras solicitudes a esa misma página no requieren de ir a Internet.

## Nodos Bastion / Baluarte

Proxy.

- **Cabras de Sacrificio (sacrificial goat):** En este tipo de proxys se realizaran las pruebas de nuevos servicios, configuraciones o programas. Esta maquina no deberá tener acceso a ninguna parte de la red interna, no deberá contar con cuentas de usuario replicadas en otras instancias, ni deberá tener instalados programas que puedan comprometer a la organización. Recuerden que lo mas importante de este equipo es que debe ser totalmente desechable, por lo que deben asignar usuario y contraseña a todos los usuarios que la utilicen y debe de tener fecha de caducidad para evitar que estos usuarios se sientan demasiado cómodos con ella.

## Nodos Bastion / Baluarte PROXY



Imagen usada con fines académicos propiedad de ESET y [Daniel Cunha Barbosa](#)

# Nodos Bastion / Baluarte

Proxy Inverso.

Estos nos permiten filtrar y administrar el flujo de solicitudes a servidores que albergan páginas web. Sus principales funciones son:

- **Equilibrio de carga:** Debido a su estructura puede conectarse a varios servidores de destino, dirigiendo las solicitudes a cada uno de ellos sin sobrecargar ninguna. Como característica de seguridad, las solicitudes de Internet conocen solo la dirección IP del proxy y no las de los servidores y páginas de la organización.
- **Caché:** El proxy inverso almacena elementos de las páginas de la organización, buscando actualizaciones de contenido de vez en cuando, logrando con esto que los servidores internos reciban menos solicitudes de red, optimizando con esto su funcionamiento.

## Nodos Bastion/ Baluarte PROXY Inverso



Imagen usada con fines académicos propiedad de ESET y [Daniel Cunha Barbosa](#)

## Proxy del lado del MAL.

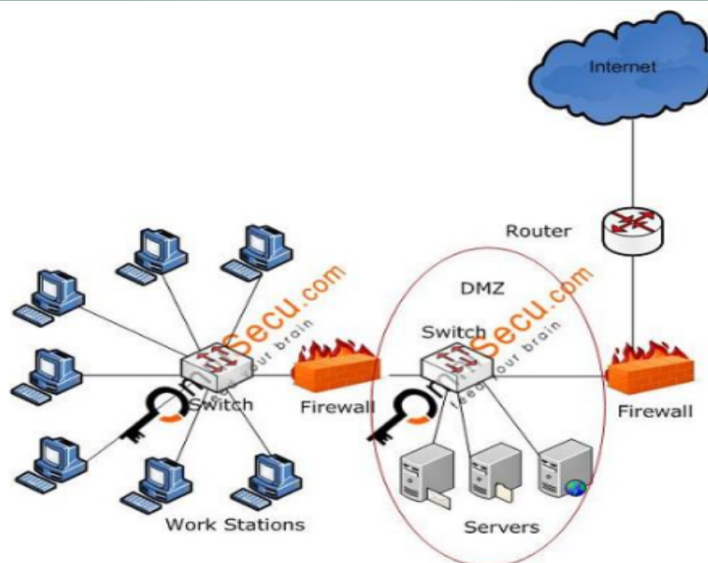
Por el poco control que existe sobre estas herramientas, (Ejemplo red TOR) cuando un atacante pretende burlar las políticas de seguridad basadas en bloqueos por zona, encuentra en estos una herramienta sumamente eficiente.

# DMZ

- DMZ. Es el área entre un router de acceso a Internet y el host bastión (que como hemos aprendido es el equipo preparado para soportar los ataques). También es conocida como zona perimetral y su función es agregar una capa adicional de seguridad a la red interna de una organización buscando que un atacante externo solo tenga acceso a los dispositivos de red y servidores contenidos en la DMZ. Al crear una DMZ (zona desmilitarizada), un usuario externo debe realizar al menos un salto en la DMZ (zona desmilitarizada) antes de poder acceder a información confidencial dentro de la red de confianza. En esta zona normalmente se colocan los servidores web, servidores FTP, DNS, servidores de correo electrónico, Honeypots.

## DMZ / front-end

<https://www.omniseccu.com/>





Ahora que entendimos como funciona un host bastion y una DMZ es necesario entrar de lleno en lo que es un Firewall.

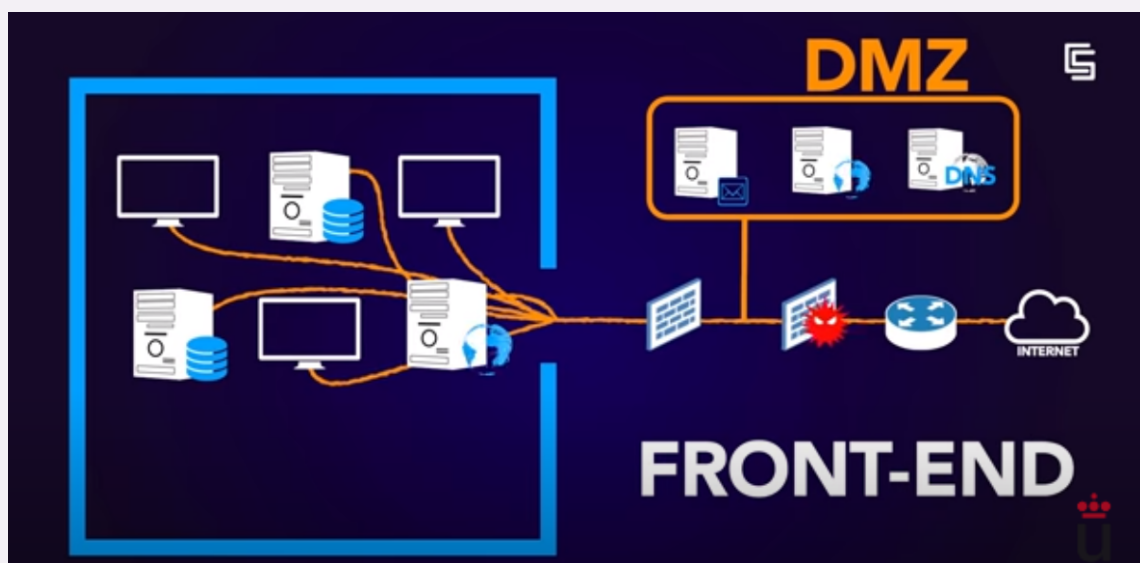
- Este equipo es el encargado de controlar la ACL (Access Control List) y lo hace en base a los encabezados de paquete. De los cuales obtiene puerto, IP, protocolo, etc.
- Existen principalmente 4 tipos de firewalls
  - Filtro de paquetes: Inspecciona las cabeceras de los paquetes para determinar si pasan o no. (Basado
  - Dinámicos (SPI Stateful Packet Inspection): Estos realizan el análisis en base al contexto de la conexión a nivel de transporte logrando determinar incluso si un paquete pertenece a una sesión abierta.
  - DPI (Deep Packet Inspection): Realizan una inspección de todos los datos a nivel de aplicación, lo que les permite identificar malware, spam, etc.
  - Proxy (Dual Home): Porque puede ver tanto las redes externas como internas, genera filtrado a nivel de pagina y de aplicación en ambos sentidos. (Su principal problema es el cuello de botella)

La arquitectura de configuración de los firewalls cuando existe una DMZ puede ser:

- Three-Legs: Se utiliza únicamente un firewall el cual usa 3 tarjetas de red, una para la red interna, otra para el internet y otra los servidores conectados en la DMZ.
- Front-End: Se utilizan 2 firewalls cada uno con 2 tarjetas de red, El primero tendrá salida al internet y a la DMZ, el segundo igual con 2 tarjetas de red, tendrá acceso a la intranet y a la DMZ.

Sin la existencia de una DMZ nos encontraremos con la arquitectura mas básica.

- Simple Dual- Homed: Se utiliza un firewall con 2 tarjetas de red (Generalmente un proxy) Una de las tarjetas ve al internet y otra a la intranet. (no es el mas recomendado por razones obvias, pero si el mas utilizado)

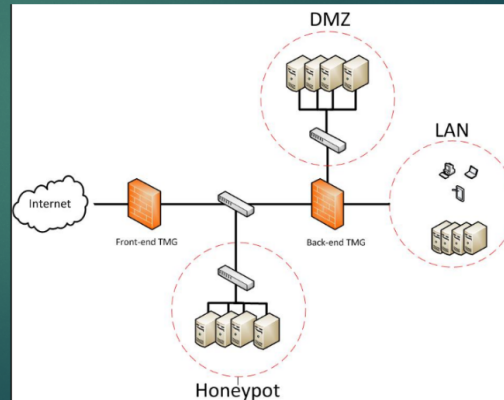




## Opciones

De las opciones mostradas se pueden explorar diversas variantes de configuración. Por ejemplo la siguiente donde se incluye un honeypot conformado por una estructura espejo a la estructura real y mezcla topologías.

Imagen usada con fines académicos  
propiedad de  
<https://esihere.wordpress.com/tag/three-legged-firewall/>



## Su importancia en los entornos actuales.

- Pudiéramos caer en el error de considerar que actualmente no requerimos de firewalls o incluso con el uso de los DOCKERS caer en el descuido de armar una estructura basada totalmente en esta tecnología. O creer que por recurrir a servidores virtuales esto ha quedado desactualizado, pero permítanme afirmar que nada más lejos de la realidad.

## Opciones gratuitas.

Smoothwall: Opción gratuita de código abierto desde el 2000. como característica maneja su propia distribución de Linux. <https://www.smoothwall.org/>

Los objetivos del proyecto se pueden resumir en:

- \* Ser lo suficientemente simple para que lo instalen usuarios domésticos sin conocimientos de Linux
- Admitir una amplia variedad de tarjetas de red, módems y otro hardware
- Trabajar con muchos métodos de conexión diferentes e ISP de todo el mundo.
- Administrar y configurar el software mediante un navegador web.
- Ejecutar de forma eficiente en hardware más antiguo y económico.
- Desarrollar una comunidad de usuarios de apoyo.
- Utilizar el patrocinio de Smoothwall Limited para promover estos objetivos.
- El proyecto de código abierto Smoothwall está financiado y respaldado por Smoothwall Limited. Todo el código del programa y otros trabajos son propiedad intelectual de sus respectivos autores, a menos que el autor los asigne y indique lo contrario. El Proyecto, en esencia, pertenece a la comunidad que contribuye a él.

Nota: la ultima versión data de 2014

## Opciones gratuitas.

Smoothwall: Opción gratuita de código abierto desde el 2000. como característica maneja su propia distribución de Linux. <https://www.smoothwall.org/>

Los objetivos del proyecto se pueden resumir en:

\* Ser lo suficientemente simple para que lo instalen usuarios domésticos sin conocimientos de Linux

- Admitir una amplia variedad de tarjetas de red, módems y otro hardware
- Trabajar con muchos métodos de conexión diferentes e ISP de todo el mundo.
- Administrar y configurar el software mediante un navegador web.
- Ejecutar de forma eficiente en hardware más antiguo y económico.
- Desarrollar una comunidad de usuarios de apoyo.
- Utilizar el patrocinio de Smoothwall Limited para promover estos objetivos.
- El proyecto de código abierto Smoothwall está financiado y respaldado por Smoothwall Limited. Todo el código del programa y otros trabajos son propiedad intelectual de sus respectivos autores, a menos que el autor los asigne y indique lo contrario. El Proyecto, en esencia, pertenece a la comunidad que contribuye a él.

Nota: la última versión data de 2014

## Opciones gratuitas.

### ► pfSense

Su última versión es la 2.4.5-p1 y es una distribución gratuita y personalizada de código abierto de Small FreeBSD adaptada para ser usada como firewall, gateway y router. Es un proyecto popular con más de 1 millón de descargas desde su inicio y se ha demostrado en innumerables instalaciones que van desde pequeñas redes domésticas que protegen una PC y una Xbox a grandes corporaciones, universidades y otras organizaciones que protegen miles de dispositivos de red. (Maneja VPN, IPV6, portales cautivos, etc).

Existe una versión de pago como caja física denominada netgate.

<https://www.pfsense.org/>

<https://www.netgate.com/>

<https://www.netgate.com/solutions/pfsense/#applications>



# Opciones gratuitas

OpenSense:

<https://opnsense.org/>

Es un Firewall y router de código abierto basado en FreeBSD las características que incorpora son:

- Traffic Shaper
- Autenticación con dos factores para iniciar sesión en la administración del sistema.
- Portal cautivo para el inicio de sesión de los usuarios, ideal para redes Wi-Fi
- Proxy caché transparente con soporte para lista negra
- VPN: incorpora tanto los modos site to site como road warrior, compatible con IPsec y OpenVPN. También incorpora compatibilidad con PPTP aunque no es recomendable su uso.
- Tiene la opción de HA (High Availability) y hardware failover, para que en caso de caída de un firewall automáticamente entre el siguiente
- Incorpora un IDS (**Sistemas de Detección de Intrusos**) y un IPS (**Sistemas de Prevención de Intrusos**).
- Servidor DNS, DNS Forwarder, DHCP server, DHCP relay, Dynamic DNS etc.
- Permite ver gráficos del tráfico en tiempo real, exportar los datos a un servidor remoto, guardar la configuración cifrada y subirla a Google Drive e incluso podremos instalar plugins para aumentar el número de opciones disponibles.
- Soporta el estándar 802.1Q VLAN para segmentar la red adecuadamente

# Opciones gratuitas

ClearOS:

<http://www.clearfoundation.com/>

<https://www.clearos.com/>

Es una distribución de Linux basado en CentOS. Está enfocado en operar como router gateway (puerta de enlace), servidor proxy, dns y firewall... Otros servicios son:

- Escaneo de virus y spam a través de la pasarela de paso para tráfico http así como imap, pop y smtp (parecido al plugin [copfilter](#) de ipcop).
- Filtrado de contenidos/protocolos a través de proxy de una manera realmente fácil y rápida.
- Firewall sencillo con detección de intrusiones.
- Servidor LDAP (substituye Active Directory) con autenticación de SAMBA como PDT (muy fácilmente configurable).
- Sistema de impresión (CUPS) y recursos compartidos (sistema de ficheros e impresoras) a través de SAMBA.
- Servidor FTP (ProFTPD), WEB (apache 2 con módulo de php) y MySQL con administración a través del proyecto phpMyAdmin.
- Servidor de correo electrónico (postfix) con soporte de captura de correo de otras cuentas (maildrop), SMTP, POP y WebMail.
- Sistema de backup de configuración del servidor (tanto local como remotamente en el servidor del proyecto).
- Informes de logs sobre cada uno de los servicios.

Si se registran tendrán vpn con ip dinámica y un espacio de almacenamiento para backups. Se administra desde https en el puerto 81.

Cuenta con soluciones en caja denominadas ClearBOX

## Opciones gratuitas

Untangle.

<https://www.untangle.com/get-untangle/>

Esta solución esta basada en Debian que nos ofrece la función de firewall y VPN ofreciendo los siguientes servicios.

- Web Filter, para evitar ingresar a sitios no deseados.
- Virus Blocker, que impide el ingreso de virus a nuestra red.
- Reports, para saber quién se encuentra en línea.
- Spam Blocker, para impedir el spam dentro de la red.
- OpenVPN, que permite accesos remotos seguros dentro de la red.
- Adblocker, esta aplicación impide la publicidad invasiva.
- Protocol Control, para evitar el uso de la red para juegos en línea.
- Phish Blocker, que impide el robo de identidad.
- Intrusión Prevention, para detectar y proteger del ataque de hackers.
- QoS, prioriza el tráfico dentro de la red.
- Firewall, para proteger la red de intrusos.
- Spyware Blocker, que impide el acceso de este tipo de malware a nuestra red.

## Opciones gratuitas

### VyOS

Solución basada en Red Hat permite realizar funciones de Neteo, Enrutamiento (destaca de manera impresionante), VPN, Firewall, DHCP, TFTP. Sus principales servicios son:

- Soporte de Wireguard
- Servidor PPPoE
- Repetidor mDNS y relé de difusión
- Soporte para la operación VRRP IPv6 y unicast VRRP
- NPTv6
- Opción QinQ ethertype compatible con los estándares

# IDS /sistema de detección de intrusos / operación.



# IDS /sistema de detección de intrusos / operación /fuente de información.

## NIDS.

Son los más populares en la detección de intrusos debido a su potencial. Utilizan el tráfico de red (paquetes TCP/IP) como fuente de información, revisando los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella. De dichos paquetes, verifican la validez de algunos parámetros y el comportamiento de los protocolos de la familia TCP/IP empleados. Este tipo de IDS tiene la ventaja de no afectar el rendimiento de las computadoras que protege debido a que utiliza como fuente el tráfico de red. No obstante, tiene una gran limitación en las actuales redes conmutadas ya que su ubicación es un elemento clave para su buen funcionamiento. Además, entre sus desventajas se encuentra su incapacidad para detectar intrusiones en paquetes cifrados, puesto que estos pueden ser únicamente descifrados en los nodos extremos de la comunicación y no en un elemento intermedio.



## IDS /sistema de detección de intrusos / operación /fuente de información.

### **HIDS.**

Protegen únicamente a la máquina en la que son instalados. Utilizan como fuente de información los datos generados por la computadora en la que operan, especialmente a nivel de sistema operativo: archivos de auditoría del sistema, archivos logs o cualquier archivo que el usuario desee proteger. Los HIDS tienen como ventaja su capacidad para detectar situaciones como los intentos fallidos de acceso o modificaciones en archivos considerados críticos. Las desventajas principales de este tipo de IDS se encuentran en el consumo de recursos del propio equipo que desea proteger y el hecho de que él mismo está expuesto a ser víctima de algún ataque

## IDS /sistema de detección de intrusos / operación /fuente de información.

### **HIDS/ Subgrupos**

- ▶ Sistemas Verificadores de Integridad (SIV): típicamente monitorizan los sistemas de archivos en busca de modificaciones relevantes.
- ▶ Analizadores de Archivos Log (LFM): comprueban los archivos logs en busca de patrones sugerentes.
- ▶ Sistemas Víctima (honeypots): sistemas que aparentan servidores o computadoras vulnerables y que se ofrecen como señuelo para desviar la actividad de los intrusos.

## IDS /sistema de detección de intrusos / operación /estrategia de análisis.

Se refiere a la técnica que utiliza el IDS, una vez recuperada la información, para identificar si se produjo o no una intrusión. Estas estrategias dividen a los IDS en dos grandes grupos:

- **IDS de detección del mal uso o uso indebido** cuentan con el conocimiento a priori de las secuencias y actividades que conforman un ataque almacenado en una base de datos. Por tanto, para detectar intrusiones dentro de la información recopilada de la fuente, se hace una comparación de la misma con los patrones de ataques almacenados y, en caso de encontrar similitud, se genera una alarma. Con este método se logra detectar intentos de explotación de vulnerabilidades típicas, de los cuales ya existe información. Esta estrategia es la más utilizada en los IDS comerciales.

## IDS /sistema de detección de intrusos / operación /estrategia de análisis.

Ventaja principal de los IDS de detección de mal uso o uso indebido.

- Al buscar sobre patrones preestablecidos generan muy pocos falsos positivos.

Desventajas:

- Incapacidad para detectar nuevos ataques
- Necesidad de mantener constantemente actualizada su base de patrones.



## IDS /sistema de detección de intrusos / operación /estrategia de análisis.

**IDS de detección de anomalías.** Los IDS basados en detección de uso indebido parten del conocimiento de lo normal y toda actividad que se aleje de este comportamiento es considerada una intrusión. Este tipo de detección evita el proceso de actualización de una base de datos de patrones de intrusión y brinda la posibilidad de detectar ataques nuevos de los cuales no se tenga información alguna. No obstante, este tipo de IDS tiene algunas desventajas que han provocado el rechazo por parte de los administradores de redes. Por ejemplo, son generadores de un gran número de falsos positivos ya que el comportamiento normal de los usuarios es extremadamente difícil de modelar, por lo variable que puede llegar a ser y, por tanto, un comportamiento inusual no tiene necesariamente por qué ser ilícito. Otra debilidad importante de este tipo de sistema es que necesita un largo período de entrenamiento, previo a su uso, para detectar los comportamientos normales de los usuarios y sistemas dentro de la red

## IDS /sistema de detección de intrusos / operación /tipo de respuesta.

Pueden ser: pasivas o activas.

- Pasivas se refieren a emisiones de informes, sonidos o el registro de las acciones ocurridas.
- Activas son las que desencadenan alguna acción en particular como: la ejecución de programas, el cierre de una cuenta o la reconfiguración del cortafuego.

Por regla general los IDS pueden soportar ambos tipos de respuesta,, ya que es recomendable reaccionar de manera pasiva ante determinadas anomalías de poca envergadura y activamente ante ataques que puedan poner seriamente en peligro la seguridad de los sistemas.

# IDS /sistema de detección de intrusos / operación /frecuencia de uso.

La frecuencia de uso clasifica a los IDS en dinámicos y estáticos.

- Dinámicos son capaces de analizar la actividad en tiempo real. Esto permite que se pueda responder adecuadamente ante un ataque cuando está ocurriendo y evitar sus efectos. Este tipo de herramientas introducen costos operativos significativos.
- Estáticos trabajan fuera de línea a intervalos específicos de tiempo. No ofrecen seguridad entre intervalos de ejecución y en casos de ataques exitosos sólo pueden ser utilizados para análisis forense

## IPTables.

Es un sistema de firewall vinculado de manera directa al kernel de linux, o bien un script que nos permite operar la seguridad del kernel, por este motivo no se puede arrancar o detener al gusto, lo que se puede hacer es activar o desactivar reglas en específico. Se puede implementar para proteger un equipo particular o bien un conjunto

de equipos.

Estructuralmente trabaja en orden por lo que todas las reglas las lee de arriba hacia abajo (Igual que la lectura estándar humana).

## IPTables.

Conceptos básicos:

NAT (Network Address Translation): En términos llanos y concretos es el permitir la comunicación entre redes públicas y privadas. Esto se logra mediante el manejo de tablas de reenvío manejadas por el router.

iptables -L: Permite verificar el contenido de iptables. (para número línea agregar --line-numbers)

NOTA: Para trabajar con iptables es necesario trabajar con privilegios de administrador.



Existen 2 formas de implementar un firewall, permisiva y restrictiva. En la permisiva partimos de que todo se permite y conforme vamos encontrando vulnerabilidades se va cerrando (NO RECOMENDADO) en el restrictivo (Más Difícil de operar) todo se prohíbe y solo se abre lo que van requiriendo los usuarios.

Iptables maneja tres tipos de reglas

- Mangle: Destinadas a modificar paquetes. Se recomienda su utilización sólo por parte de usuarios muy avanzados.
- NAT: Maneja las reglas de Prerouting y Postrouting
- Filter: Manejan el filtrado directo de los paquetes tanto de entrada al equipo como de salida o bien de paso.
- NAT: (Tablas raw, nat, mangle)

Prerouting: Tráfico entrante justo antes de ingresar en la pila del kernel. Si colocan las reglas en esta cadena las mismas se procesan antes de tomar cualquier decisión referente a donde enviar el paquete.

Postrouting: Tráfico saliente originado en el sistema local o reenviado.. Trabaja justo después de las reglas de ruteo y antes de mandar el paquete a la red.

Ejem:

```
iptables -A PREROUTING -t nat -p tcp -dport 20 -j
```

```
REDIRECT - -to-port 22
```

NOTA: Para ver las reglas de pre y postrouting usar `iptables -t nat -L -n`

Filter maneja 3 rubros para el manejo de sus reglas.

Input, output y forward en ese orden.

Nota Importante: Si el tráfico se recibe y procesa hacia la misma máquina se usa Input u Output, si se recibe y procesa hacia otra máquina o la red se utiliza forward.

NOTA Importante. Para la revisión de las reglas debes usar sniffers. De manera personal yo disfruto usando wireshark. Para la identificación de lo que deseamos filtrar es necesario recordar que todos los puertos como hemos repetido en muchas ocasiones no son otra cosa que programas corriendo en su mayoría bajo el esquema tcp estudiado de manera previa. Por lo que a continuación les dejo una tabla de los puertos más comunes.

| Puerto / Protocolo | Descripción                                        | Puerto / Protocolo | Descripción                      |
|--------------------|----------------------------------------------------|--------------------|----------------------------------|
| 13 / tcp           | Protocolo daytime / Fecha y hora actuales          | 445 / tcp          | Active Directory y gusano Sasser |
| 20 / tcp           | File Transfer Protocol (FTP) -datos                | 465 / tcp          | SMTP sobre SSL, (Email)          |
| 21 / tcp           | File Transfer Protocol (FTP) -control              | 515 / tcp          | Impresión en windows             |
| 22 / tcp           | ssh, scp, sftp                                     | 631 / tcp          | CUPS Impresión en Unix, Linux.   |
| 23 / tcp           | Telnet                                             | 993 / tcp          | IMAP4 sobre SSL (E-mail)         |
| 25 / tcp           | SMTP (protocolo simple de transferencia de correo) | 995 / tcp          | POP3 sobre SSL (E-mail)          |
| 37 / tcp           | Time Protocol. Sincroniza hora y fecha             | 1433 / tcp         | SQL - Server                     |
| 53 / udp           | DNS Domani Name System                             | 1434 / tcp         | SQL - Monitor                    |
| 67 / udp           | DHCP Dynamic Host Configuration Protocol           | 1863 / tcp         | MSN Messenger                    |
| 68 / udp           | DHCP Dynamic Host Configuration Protocol           | 3074 / tcp - udp   | Xbox Live                        |
| 80 / tcp           | HTTP Protocolo de transferencia de hipertexto      | 8080 / tcp         | HTTP                             |
| 88 / tcp           | Kerberos                                           |                    |                                  |
| 110 / tcp          | POP3 Post Office Protocol (E-mail)                 |                    |                                  |
| 137 / tcp          | NetBIOS Servicio de Nombres                        |                    |                                  |
| 138 / tcp          | NetBIOS Servicio de Datagramas                     |                    |                                  |
| 139 / tcp          | NetBIOS Servicio de Sesiones                       |                    |                                  |
| 143 / tcp          | IMAP 4 Internet Message Access Protocol (E-Mail)   |                    |                                  |

Consideraciones básicas: Con -A seleccionamos la cadena a la que deseamos agregar la regla (Input,output, forward u otra cadena personalizada) por lo que será el inicio de la mayoría de nuestras instrucciones excepto cuando se trate de insertar -I o de borrar -D.

Quedando la estructura básica para insertar de la siguiente manera: (Nota si en lugar de un protocolo se filtrara una dirección o rango se cambiará el -p por -d)

El -j indica a donde brinca, puede ser una regla o una cadena.

`iptables -I nombredcadena #posiciondondequeda -p protocoloafectado -f funcionespecificadelprotocolo -j aceptódrop`

## Ejemplos:

```
iptables -I INPUT 1 -d 192.168.0.0/24 -j ACCEPT
```

```
iptables -A OUTPUT -p tcp - -dport ssh -j DROP
```

```
iptables -D INPUT 2
```

## ▼ Tercer Parcial

### ▼ 28-10-2022

No hubo clase porque el profe le hizo el examen a Fer

### ▼ 31-10-2022

No hubo clase

### ▼ 01-11-2022

Informática forense

#### ▼ 03-11-2022

Informática forense

#### ▼ 04-11-2022

Descargamos USBDeview

Procedimientos para recuperar archivos borrados

Usamos técnicas de PhotoRec (Photo Recovery)

Usamos Photorec en Linux (otra alternativa es Recuva)

```
sudo apt install testdisk
```

#### ▼ 07-11-2022

Continuación del análisis forense

Características de la evidencia digital:

- Volátil (por trabajar con la RAM)
- Duplicable (pueden hacerse copias fácilmente pero no debe alterarse la información principal)  
Si conectamos una USB alteran los logs y puede considerarse que se alteró la información principal
- Borrable
- Reemplazable
- Alterable

Se considera como evidencia digital:

- El último acceso a un fichero o aplicación (unidad de tiempo)  
No se debe abrir un archivo ni modificarlo (por tanto, tampoco moverlo)
- Un log (en fichero)
- Una cookie en un disco duro
- El tiempo que lleva encendido el equipo
- Los procesos en ejecución
- Archivos temporales
- Restos de instalación
- Discos duros, memorias, etc.

Como tampoco debe conectarse una USB porque cambian los logs, deben usarse clonadores de discos duros

Normalmente es mejor rechazar cookies porque incluso si hay cookies generadas ilegalmente (son administradas a nivel internacional)

#### ▼ 08-11-2022

Informática forense (diapositivas)

#### ▼ 09-11-2022

Informática forense (diapositivas)

#### ▼ 10-11-2022

No hubo clase :(

#### ▼ 11-11-2022

No hubo clase :(

▼ 14-11-2022

Ya están las evaluaciones del segundo parcial

97 en el examen

95 en Footprinting



▼ 15-11-2022

Vimos calificaciones del segundo parcial y el proyecto

▼ 16-11-2022

Informática forense

▼ 17-11-2022

No fui a clase :(

▼ 18-11-2022

Práctica con programas para volcar RAM

▼ 22-11-2022

Vimos Autopsy

▼ Guía de estudio

# Análisis Forense

Consiste en reaccionar de manera adecuada, identificando además del tipo de ataque, como se fue desarrollando, tratando de identificar cada una de las partes que formaron parte del mismo.

Un buen análisis forense consta de varias partes

- Identificación del entorno
- Aseguramiento del área
- Toma de evidencias.
- Intervención del equipo



¿Por qué es importante conocer el tema ?:

Actualmente los delitos en que los delincuentes utilizan tecnología para cometer crímenes y para eludir a las autoridades van a la alza. Por ende es necesario especializarse en estas nuevas áreas para perseguir, evidenciar y enjuiciar a este nuevo tipo de criminales. O en su defecto para poder detectar, estudiar y evitar que se siga realizando la comisión del delito.

#### Glosario Forense.

**Perito:** Es el profesional dotado de conocimientos especializados y reconocidos mediante estudios superiores o entidades certificadoras que recolecta, custodia y suministra la información u opinión fundada ante los tribunales de justicia sobre los puntos relacionados con la materia de su dictamen.

**Delito Informático:** Conducta antijurídica, culpable. Dolosa o punible en que se tienen los equipos informáticos como instrumento o fin.

La máxima del perito forense es:

Se debe preservar la integridad de la información desde su recolección hasta su presentación.

Basados en la característica de que todos los dispositivos que son sujetos de un análisis forense tienen en común que tienen memoria. (Desde el punto de vista informática).

La característica más importante de una imagen forense es que se debe realizar bit a bit desde el primer hasta el último sector, garantizando que se trata de un clon. Para esto es recomendado apoyarse de los dispositivos de la empresa:

<https://www.cellebrite.com>

#### Terminología:

- Delitos Informáticos
- Informática Forense
- Pericia
- Lugar del hecho
- Indicio
- Evidencia
- Prueba
- Cadena de Custodia
- Evidencia Digital

Las 4 fases del cómputo forense son:

- Identificación
- Preservación
- Análisis
- Presentación

Características de la evidencia digital.

- Volátil
- Duplicable
- Borrable
- Remplazable
- Alterable

¿Qué debemos considerar como evidencia digital?

- El último acceso a un fichero o aplicación (Unidad de tiempo)
- Un log (en fichero)
- Una cookie en un disco duro
- El tiempo que lleva encendido el equipo
- Los procesos en ejecución
- Archivos temporales
- Restos de instalación
- Discos duros, memorias, etc.

Reglas de la evidencia digital

- Admisible
- Auténtica
- Completa
- Creíble

#### Cumplimiento de la cadena de custodia.

- Identificación y Señalización
- Fijaciones: Fotométrica y Planimetría
- Colección y Marcado
- Rotulación y Embalaje (Lacrado y Sellado)
- Traslado o transporte
- Almacenamiento
- Entrega y Verificación.

#### Algunas consideraciones al pasar un incidente

- Se debe sacar a toda persona del área
- Se debe delimitar el área
- Debemos determinar el personal disponible, preferentemente alguien de RH y un oficial que servirá como guardia de desagravio
- Los implicados se deberán separar con vigilancia y aislados.
- Se debe proyectar el tiempo ya que una vez que se abandona el área

- Se debe proyectar el tiempo ya que una vez que se abandona el área NO se puede volver a ingresar.
- En casos oficiales el orden de los peritos los da el ministerio público
- Se deben establecer colores para determinar qué perito está trabajando en cada área.
- Es altamente recomendado contar con pilas de respaldo
- La evidencia se debe agrupar

#### Algunas consideraciones al pasar un incidente

- Se debe buscar en la basura
- En caso de un teléfono fijo se debe descolgar y verificar que cuenta con línea.
- En el caso de delitos informáticos el área a delimitar puede implicar toda la red..
- En caso de existir lesionados se debe priorizar la vida de las personas.

- La investigación siempre debe realizarse en espiral hacia afuera.
- Se deben tomar las medidas necesarias para evitar sufrir lesiones por químicos, gases, etc..
- Nunca se debe cambiar el nombre a las fotos.
- No se debe hablar con nadie.

#### Algunas consideraciones al pasar un incidente

- Aterrícen los conceptos para que los entienda el juez.
- En equipos de cómputo al documentar con número de serie se debe especificar donde se tomó el número y a que pieza corresponde ese número.
- Si no se toma la evidencia por un perito certificado la evidencia se pierde.
- Los peritos deben contar con carta de protesta del cargo.
- Siempre se deben usar guates de latex.
- Nota: El número de evidencias normalmente es diferente al número de indicios en campo.
- Los peritos de la contraparte deberán pedir la evidencia al ministerio público nunca a nosotros.

Las imágenes tomadas por nosotros también deben llevar un registro.

|            |  |                     |  |
|------------|--|---------------------|--|
| Nombre     |  | ubicación:          |  |
| Extensión: |  | secuencia:          |  |
| Tamaño:    |  | fotógrafo:          |  |
| Sha 256:   |  | serie de la cámara: |  |

#### Algunas consideraciones al pasar un incidente

- Al concluir el caso todas las copias deben ser entregadas al interesado.
- La evidencia debe llevar.
  - Nombre del perito
  - Sello
  - Asunto
  - Cedula profesional
- La evidencia Federal queda en el ministerio público, la particular en las empresas.

## Clasificación de Discos Duros:

### Por su tecnología interna:

HDD (Hard Disk Drive)

SDD (Solid state drive)

HDD y SDD (Híbridos)

### Por localización:

Externos e Internos

### Tipo de Interfaz:

IDE ó ATA: Tienen un conector de 40 pines y un pin de 4 para energía. (actualmente en desuso)

SATA: Utilizan conectores más delgados y de mayor velocidad.

USB: Se usa normalmente con discos externos

PCIe: Se conectan mediante una interfaz PCI,

Al realizar análisis es importante conocer

- La velocidad del disco duro.
- Sus Características
- Su tiempo de vida aproximado

Herramientas para clonar Discos Duros: Ghost, acronis, clonezilla, Macrium Reflect Free, gparted

Volcado de memoria: Es la técnica mediante la cual obtenemos el contenido de la memoria RAM.

¿ Qué podemos obtener de esta memoria ?

1. Todo lo que se encuentra en nuestros OS en algún momento interactúa con RAM, por lo que podremos identificar malware en su estado vivo (incluyendo rootkits).
2. Contraseñas, llaves de cifrado (si el contenedor está montado, también se pueden obtener las llaves de cifrado de una imagen de memoria por ejemplo con Passware), caches, clipboards.
3. Archivos abiertos.
4. Configuraciones de hardware y software (recuerden que algunos archivos de Windows Registry son volátiles).
5. Información de red (sockets, IP's, URL's)

Volcado de memoria:

6. Procesos.

7. Obtención de evidencia a pesar de la utilización de técnicas anti forenses

(inprivate browsing, chats cifrados, etc.)

8. Actividad de internet.

9. Obtención remota de la memoria.

10 Obtener una copia de la MFT desde la memoria. (Manager File Transfer)

11 Obtención de una copia de la memoria RAM de un sistema post mortem desde el archivo hiberfile.sys

#### Herramientas

Estas deberán ser seleccionadas dependiendo del sistema operativo con el cual se trabajara.

| Sistema Operativo | Herramienta de adquisición                                       |
|-------------------|------------------------------------------------------------------|
| Microsoft Windows | Winpmem, DumpIt, win32dd/win64dd, Memoryze, FastDump, RamCapture |
| Mac OS            | Osxpmem, Memoryze                                                |
| GNU/Linux         | Linpmem, LiME                                                    |

Es importante considerar que necesitamos tener tanta capacidad de almacenamiento como memoria ram tenga el equipo, por lo que es importante recordar que cada vez tienen más memoria los equipos de computo.

Cuando nos enfrentamos a un caso de volcado de memoria surgen varias dudas. ¿Lo hacemos en local o en remoto? ¿Desconectamos el equipo de la red? Pues bien, el equipo debe estar lo más intacto posible, si queremos capturar la memoria tal cual está no debemos de desconectar de la red el equipo.

Entre realizar la captura local o remota, pues lo cierto es que depende de cada circunstancia. En equipos Microsoft Windows y entornos corporativos es muy sencillo utilizar herramientas como PSEXEC para realizar la adquisición remota, pero no siempre es el caso.



Clasificación por organización en el disco duro.

Se organizan por tipo de arreglo (Raids) por particiones y por tipo de sistema de manejo de archivos.

En windows los más comunes son FAT y NTFS.

FAT:

- Tamaño limitado de archivos hasta 4 Gb
- Tamaño máximo de volumen

Fat 12, 32 Mb – 4096 Archivos por volumen

Fat 16, 4 Gb - 65536 Archivos por volumen

Fat 32, 2 Tb – 4,177,920 Archivos por volumen

Organización del disco duro.

NTFS:

Tamaño máximo de archivos: 16 exabytes

Archivos por Volumen: 4,294,697,295

La \$Mft (Master File Table) es el corazón de NTFS, es el archivo más importante en un sistema de archivos NTFS. Ya que es el encargado de realizar un seguimiento de todos los archivos en el volumen, su ubicación lógica en carpetas, su ubicación física en el disco, y los metadatos de los archivos, incluyendo: Fecha de Creación, de modificación, fecha de acceso, así como la última fecha de acceso al archivo, todo esto como información estándar, adicional a esto tenemos tanto el tamaño y peso del archivo como los permisos de acceso de seguridad.

Organización del disco duro.

NTFS:

\$MFT, contiene toda mucha información acerca de todo el sistema de archivos. Por poner un ejemplo, correos electrónicos, también son archivos, de modo que también se pueden buscar ahí. En condiciones normales de uso la \$MFT puede expandirse pero nunca contraerse.

Cuando se elimina un archivo del disco duro, su entrada \$MFT se marca como lista para ser reutilizada. Esta entrada seguirá existiendo hasta que se sobrescribe con una nueva entrada generada por un archivo nuevo en el disco duro.

Cuando un nuevo archivo es creado en el disco duro, se sobrescribe la siguiente entrada \$MFT disponible, si no hay entradas disponibles para ser sobrescritas a continuación, la MFT comenzará a expandirse.

## Organización del disco duro.

### Ejemplo 1:

Si hay 200 entradas de la MFT y un archivo, el archivo X, se borra y luego 1.000 archivos más están creados inmediatamente después de la entrada MFT para el archivo X se sobrescribe. Aunque los contenidos del archivo pueden existir en el disco duro, la entrada MFT que incluye el nombre, metadatos, etc., se sobrescribe

### Ejemplo 2:

Hay 3000 entradas en la \$MFT. 100 se suprimen y 2 nuevos archivos se añaden inmediatamente a la unidad. Por lo tanto, 98 de las 100 entradas deben ser recuperables. Aunque si los datos de los ficheros son recuperables o no, dependerá de si han sido sobrescritos o no.

## Herramientas

- Para clonar Discos Duros sin apagar el equipo se recomienda utilizar HD Clone Basic, un software que se encuentra en el mercado por 19,90 Euros.
- Para clonar discos duros ya extraídos se puede utilizar un Dock para Disco Duro 2.5 3.5 Sata Ide Multilector Memorias Backup por \$550 mnx
- Volcado de memoria: Consiste en enviar a un archivo todo el contenido de la memoria en un momento determinado, para esto usaremos la herramienta osforensics, en su versión de prueba. El costo de la herramienta es de \$995 usd

Una vez volcada la memoria será necesario utilizar volatility o regripper para poder estudiar el contenido de la memoria.

Se recomienda ampliamente la herramienta denominada Sleuth\_kit

## Causa de fallas en Disco Duros

Cuando los discos duros son dispositivos mecánicos están sujetos al desgaste. Alrededor del 60% de los fallos del discos duros con este tipo de mecanismo se produce por un fallo mecánico predecible, mientras que el 40% de las fallas ocurren por el mal uso. Un fallo en el disco duro podría ocurrir debido a cualquiera de las razones:

- Falla Electrónica
- La BIOS no puede detectar el disco duro.
- Unidad de disco duro no puede es capaz de girar.
- Error de inicio súbito.

#### Causas:

El CPU no es capaz de generar la fuente de alimentación requerida para que el disco duro funcione normalmente, el voltaje enviado puede ser muy alto o muy bajo. Este error también se puede producir al utilizar una fuente de energía poco confiable que proporciona alimentación ininterrumpida.

#### Solución:

Asegúrate que el hardware del sistema está recibiendo la fuente de alimentación requerida. Mediante el uso de un regulador de voltaje o un UPS se puede evitar que los cambios de energía afecten al equipo.

#### Causas:

##### Falla mecánica o interna:

- El disco emite ruidos o rechina al arrancar el equipo o al acceder información.
- Archivos o carpetas desaparecen o se encuentran corruptos.
- Se bloquea o congela por completo el sistema.
- Se demora demasiado en encender el equipo.
- Toma mucho tiempo abrir o guardar archivos.

#### Causas:

Este error sucede cuando existen sectores defectuosos en el disco duro. El motor de giro deja de funcionar, la placa de circuitos está dañada o la cabeza de lectura/escritura no se mueve correctamente rayando los platos del disco al tratar de acceder o guardar información. Fallas mecánicas pueden producirse cuando el equipo se cae al suelo, se golpea o se mueve mientras está encendido o procesando información. El ataque de virus puede borrar los datos del disco duro, alterar el funcionamiento del disco duro o hacer que el sistema de archivos se corrompa.

#### Soluciones:

Trabajar adecuadamente con el equipo evitando caídas o golpes accidentales. Actualizar el sistema regular o semanal, correr un programa antivirus frecuentemente, sustituir el disco duro después de más de 5 años de uso.

#### Fallas del Firmware (Software del fabricante):

El disco duro es indetectable o no reconoce en absoluto el Sistema.

El sistema no puede arrancar o se bloquea durante el proceso de arranque.

#### Causas:

Este problema podría ocurrir sobre con un disco duro nuevo o luego de haber sido utilizado unos días. Puede existir la probabilidad de que el disco venga con fallas de fabricación.

▼ 23-11-2022

Realización del tercer parcial

▼ 24-11-2022

Continuación de Autopsy

▼ 25-11-2022

Continuación de Autopsy

## ▼ Proyecto Final

### Pasos para realizar el proyecto final

#### Actividades

| Aa Name                                                                                                                                                                              | ⌵ Equipos involucrados                                         | ☑ Hecho |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|---------|
| <u>Instalar PuTTY</u>                                                                                                                                                                | Windows Usuario                                                | ☑       |
| <u>Instalar servidor Apache y servidor SSH</u>                                                                                                                                       | Linux Usuario                                                  | ☑       |
| <u>Investigar IP Tables y configurar el servidor como IPS</u>                                                                                                                        | Linux Server 1 (IP Tables)                                     | ☐       |
| <u>Investigar Snort y configurar el servidor como IDS</u>                                                                                                                            | Linux Server 2 (Snort)                                         | ☐       |
| <u>Investigar cómo realizar que puedan compartir archivos los equipos usuario (necesario usar Samba)</u>                                                                             | Linux Usuario<br>Windows Usuario                               | ☐       |
| <u>Que el equipo Windows Usuario sea capaz de ver la página de Apache del Linux Usuario</u>                                                                                          | Linux Usuario<br>Windows Usuario                               | ☐       |
| <u>Monitorear la comunicación de la intranet con el Linux Snort (detectar pings, SSHs o escritorio compartido)</u>                                                                   | Linux Server 2 (Snort)<br>Linux Usuario<br>Windows Usuario     | ☐       |
| <u>Asegurar la intranet con el Linux IP Tables (abriendo paso al internet pero cerrando ciertas páginas) (también impedir acceso SSH o escritorio remoto a equipos desde la web)</u> | Linux Server 1 (IP Tables)<br>Linux Usuario<br>Windows Usuario | ☐       |
| <u>Atacar con nmap a los usuarios Linux y Windows</u>                                                                                                                                | Linux Ataque (NMap)<br>Linux Usuario<br>Windows Usuario        | ☐       |
| <u>Averiguar los puertos abiertos de los usuarios Linux y Windows y sus sistemas operativos</u>                                                                                      | Linux Ataque (NMap)<br>Linux Usuario<br>Windows Usuario        | ☐       |