UNIVERSIDAD PARAGUAYO ALEMANA

Ingeniería en Tecnologías de la Información Empresarial TIE

Seguridad en TICs

Prof.: Chrystian Ruiz Diaz

DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico**.

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.

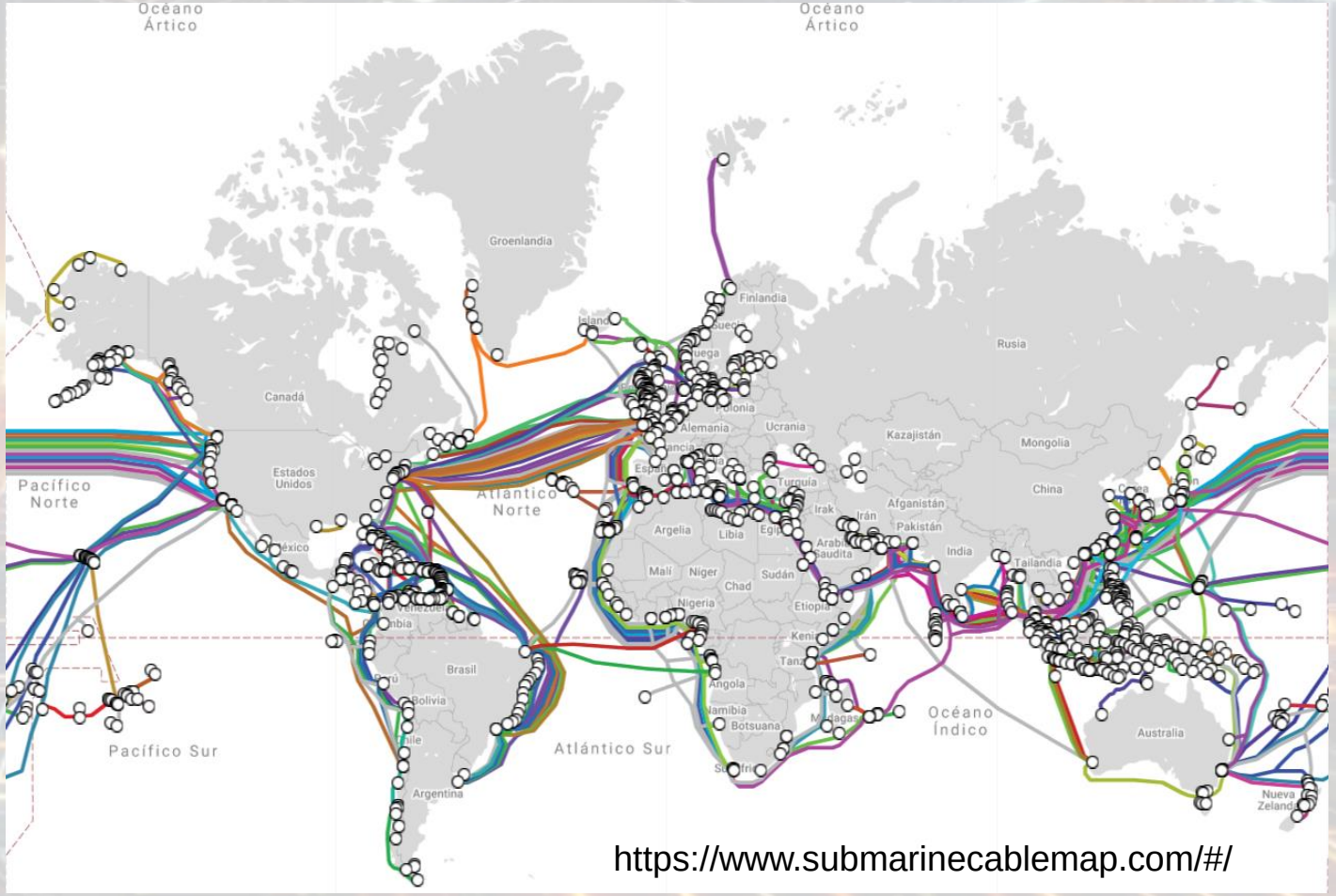
Fundamentos de Seguridad en Redes

Contenido

1. **Vulnerabilidades de los servicios de red**
   - Físico
   - Enlace de Datos
   - Red
   - Transporte
   - Sesión, presentación y aplicación
   - Ataque DoS en redes
2. **Monitorización**
   - NOC - **Network Operations Center**
   - SOC - **Security Operations Center**
     - SIEM - *Security Information and Event Management*
   - Herramientas de Monitorización
   - Técnicas de Protección
3. **Protección de Redes Inalámbricas**
   - Mecanismos de Seguridad

Vulnerabilidades de los servicios de red

Internet Análisis académico el Modelo **OSI** - *Open Systems Interconnection*



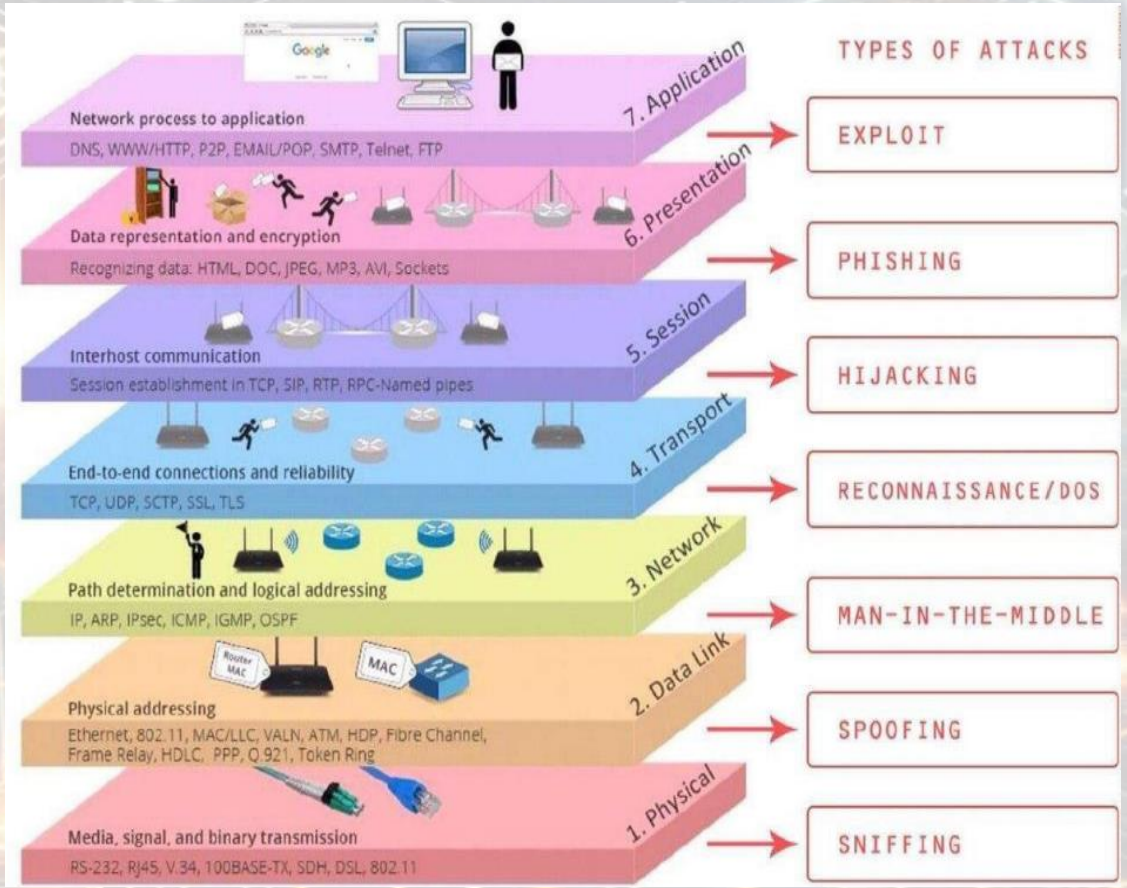
https://www.submarinecablemap.com/#/

Vulnerabilidades de los servicios de red

Cada nivel del modelo OSI presenta vulnerabilidades que pueden ser explotadas por un atacante

Nivel físico: vulnerabilidades de este nivel están relacionadas con el **acceso físico no autorizado** a los dispositivos de red :

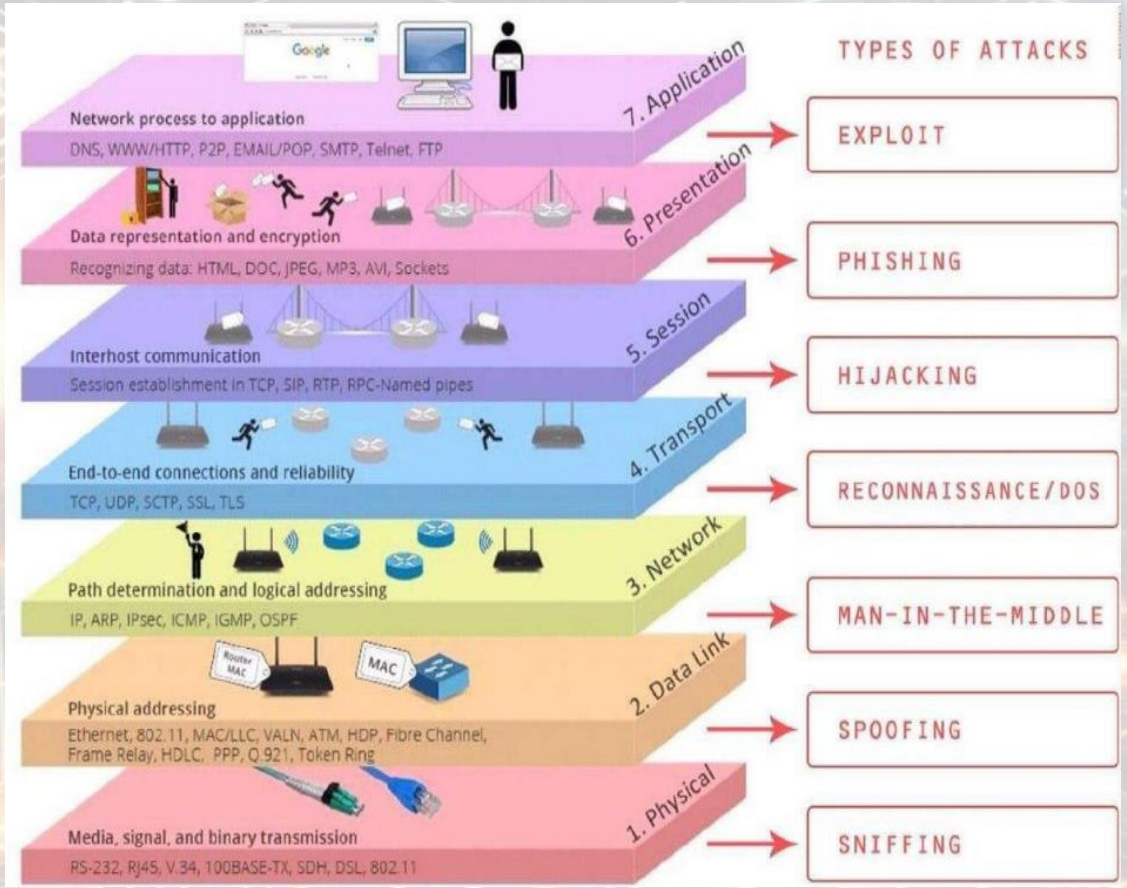
- Corte o desconexión de un cable de red o interferencias electromagnéticas ocasionadas por algún dispositivo que impidan el funcionamiento normal de la red



Vulnerabilidades de los servicios de red

Nivel de enlace de datos: vulnerabilidades asociadas al medio sobre el que se realiza la conexión, como el **control de acceso** y la **confidencialidad**

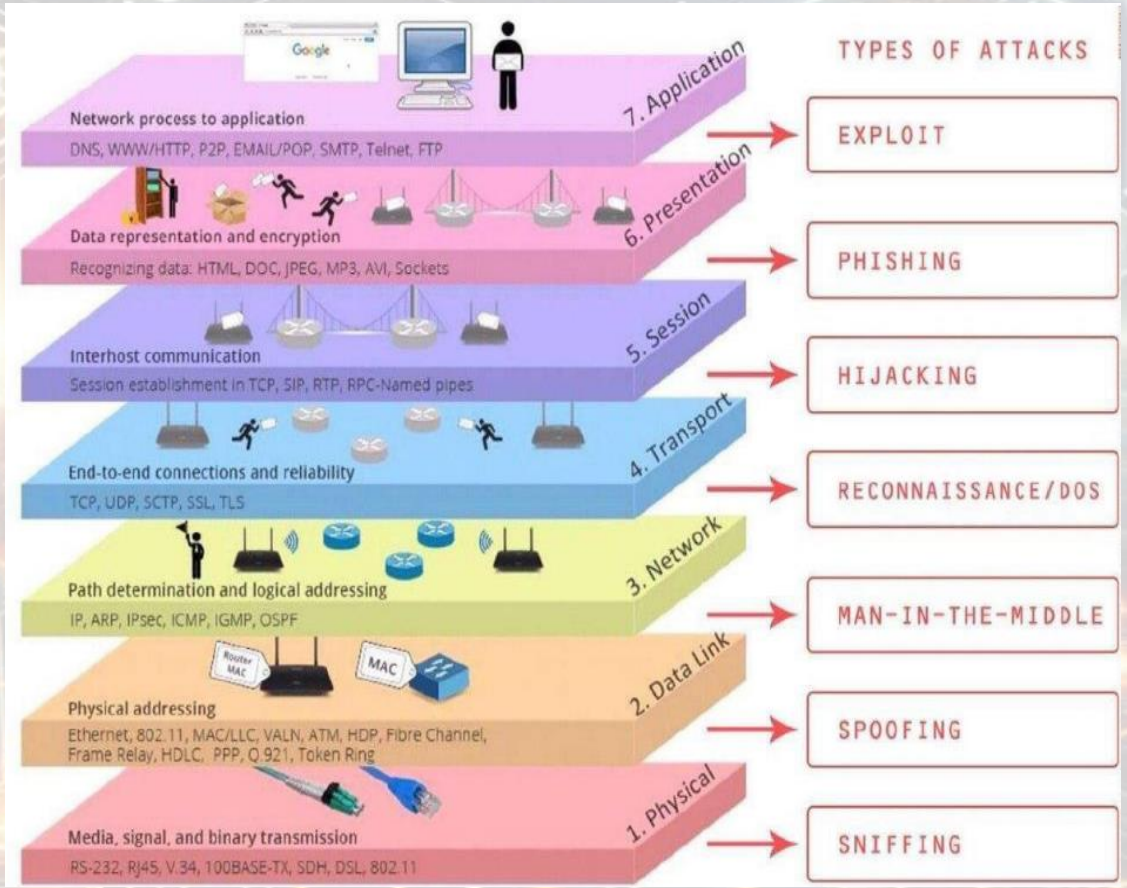
- Escuchas de red
- Falsificación de direcciones MAC- *Medium Access Control*
- Envenenamiento ARP- *Address Resolution Protocol*



Vulnerabilidades de los servicios de red

Nivel de red: vulnerabilidades asociadas a la **integridad** y **confidencialidad** de la información

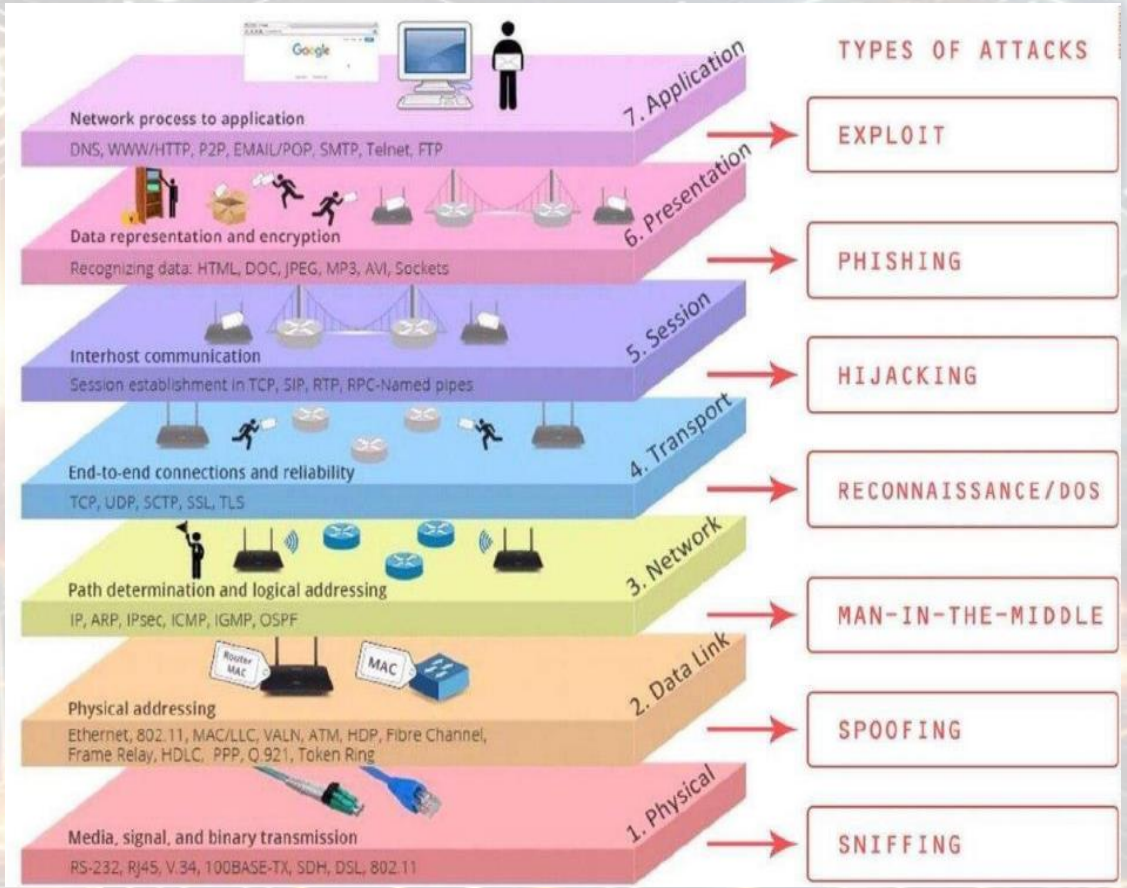
- Suplantación de mensajes (IP *spoofing)*
- Denegación de servicio (*Denial of Service* - DoS)
  - Inundación IP (IP flooding).
  - Broadcast
- Smurfing: es una técnica de DoS muy utilizada que consiste en enviar una gran cantidad de paquetes ICMP (ping) a la dirección de broadcast, falsificando la dirección de origen por la de la víctima, que recibirá la respuesta de todas las estaciones de la red
- DDoS (Distributed Denial of Service ➔ botnetDDoS (Distributed Denial of Service)



Vulnerabilidades de los servicios de red

Nivel de transporte: TCP&UDP las vulnerabilidades de este nivel se asocian a la **autenticación**, **integridad** y **confidencialidad** de la información

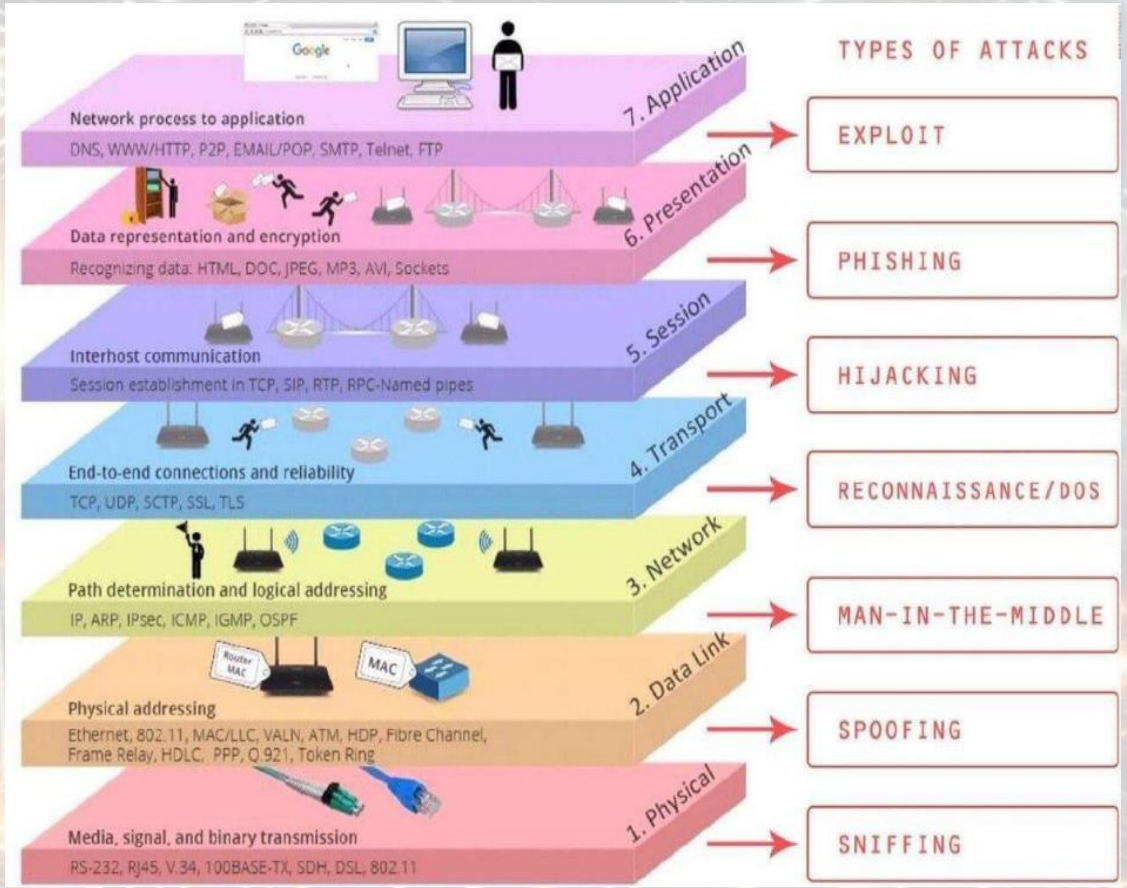
- **Denegación de servicio**: se utiliza técnicas IP Flooding
- **SYN flooding**: abrir conexiones TCP sin utilizarlas
- **Ataques contra el establecimiento de sesiones TCP**: consite en la interceptación de sesiones TCP establecidas para redirigirlas a otros equipos
- **Ataques de reconocimiento**: escaneo de puertos TCP/UDP abiertos para posterior ataque



Vulnerabilidades de los servicios de red

Niveles de sesión, presentación y aplicación: mas **cercano** a los **usuarios** presentan vulnerabilidades que afectan a la **confidencialidad**, **integridad**, **disponibilidad**, **no repudio** o **autenticación.**

- Ataques sobre la confidencialidad (Telnet, FTP)
- Suplantación del servicio de nombres de dominio (suministra una dirección IP falsa)
- Agotamiento de direcciones IP (DHCP starvation)
- Inyección SQL (https://demo.testfire.net/index.jsp)
- Escalada de directorios (acceso a directorios sin permisos) https://demo.testfire.net/index.jsp
- XSS (*Cross Site Scripting*) (inyección código malicioso en sitios web)
- Desbordamiento de búfer (fallo de diseño aplicación y ejecutar código malicioso)



Monitorización

NOC - *Network Operations Center*
Es el responsable de diseñar, instalar, dar mantenimiento correctivo y preventivo a la operación (Gestión, Soporte y monitoreo) de redes de telecomunicaciones de datos.

SOC - *Security Operations Center*
Es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.

Monitorización

NOC - *Network Operations Center*
Es el responsable de monitorizar las redes en función de alarmas o condiciones que requieran atención especial para evitar impacto en el rendimiento de las redes y el servicio a los clientes finales

Monitorización

SOC - *Security Operations Center*
es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.

- Diagnóstico de Vulnerabilidades
- Recuperación de desastres
- Respuesta a incidentes
- Neutralización de ataques
- Programas de prevención
- Administración de riesgos
- Alertas de antivirus informáticos

Herramientas de monitorización

Redes	Seguridad
Wireshark	SolarWinds Security Event Manager
Ettercap	Micro Focus ArcSight Enterprise Security Manager (ESM)
Ntop	Splunk Enterprise Security
HP Openview	LogRhythm Security Intelligence Platform
MRTG	AlienVault Unified Security Management
Cacti	RSA NetWitness
Nagios	FortiSIEM
PandoraFMS	IBM QRadar
Ganglia	McAfee Enterprise Security Manager

Técnicas de protección

- Firewall
- IPtables
- ACL (Access Control List)
- Implementación de políticas de seguridad
- Monitoreo de control y cumplimiento
- Plan de PenTest periódicos
- Capacitación y concientización constante en todos los niveles

Protección en redes inalámbricas

Presentan vulnerabilidades que amenazan la **disponibilidad**, **confidencialidad** e **integridad** de la información

Ataques comunes:

- Ataques de denegación de servicio (DoS): transmisiones de banda de frecuencias
- Escuchas del tráfico de la red (sniffing)
- Inyección de tráfico en la red
- Conexiones no autorizadas a la red
- Ataques de acceso
- Rogue AP (falso AP)

Mecanismos de seguridad en redes inalámbricas

No implementar WEB - Wired Equivalent Privacy
Evitar implementar WPA -Wireless Protected Access
Utilizar WPA2 y WPA2 Enterprice

Además considerar que el filtrados por direcciones MAC y ocultamiento de SSID se consideran falsas medidas de seguridad lo que ocasiona complejidad en la gestión de los mismos sin aportar mayor seguridad

Referencias

- COSTAS SANTOS, J. (2014). Seguridad informática. RA-MA, SA.
- ESCRIVA, G. R. (2013). Seguridad Informática. España: Macmillan Iberia SA .
- Internautas. (07 de 04 de 2020). Internautas. Obtenido de https://www.internautas.org/w-scanonline.php

¿PREGUNTAS?

Actividad de Proceso

- Elaborar la tarea “***C5 - Elaborar Cuadro Comparativo (6 puntos)”***

Realizar la tarea y seguir las instrucciones indicadas en Google Classroom.

Actividad de Proceso

- Elaborar la tarea “***P3 - Evaluación y Análisis de Riesgo (8 puntos)”***

Realizar la tarea y seguir las instrucciones indicadas en Google Classroom.

Muchas Gracias..!!