UD 2: Implantación de mecanismos de seguridad activa

SAD

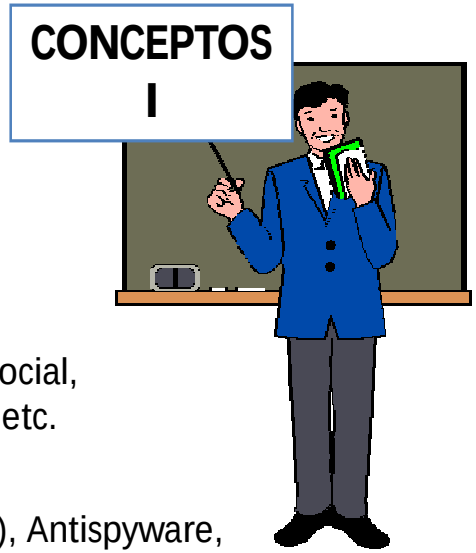
UD 2:
“Implantación de mecanismos de seguridad activa”

RESULTADOS DE APRENDIZAJE

Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

UD 2:
"Implantación de mecanismos de seguridad activa"

- **<u>Ataques y contramedidas en sistemas personales:</u>**
  - Clasificación de los ataques en sistemas personales.
  - Anatomía de ataques.
  - Análisis del software malicioso o malware:
    - Historia del malware.
    - Clasificación del malware: Virus,Gusanos,Troyanos, infostealers, crimeware,grayware,...)
    - Métodos de infección: Explotación de vunerabilidades, Ingeniería social, Archivos maliciosos, Dispositivos extraibles, Cookies maliciosas, etc.
  - Herramientas paliativas. Instalación y configuración.
    - Software antimalware: Antivirus (escritorio, on line, portables, Live), Antispyware, Herramientas de bloqueo web.
  - Herramientas preventivas. Instalación y configuración.
    - Control de acceso lógico (política de contraseñas seguras, control de acceso en la BIOS y gestor de arranque, control de acceso en el sistema operativo, política de usuarios y grupos, actualización de sistemas y aplicaciones)



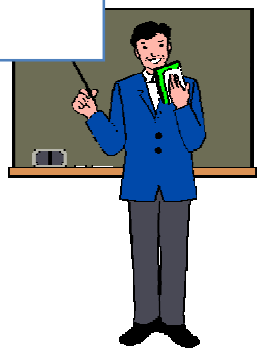
UD 2:
“Implantación de mecanismos de seguridad activa”

- **Seguridad en la conexión con redes públicas:**
  - Pautas y prácticas seguras:
    - *Técnicas de Cifrado:*
      - -Criptografía simétrica.
      - -Criptografía asimétrica.
      - -Criptografía híbrida.
    - *Identificación Digital :*
      - - PKI (Infraestructura de clave pública).
      - - Firma Electrónica y Firma Digital.
      - -Certificado Digital, Autoridad certificadora (CA).
      - - Documento Nacional de Identidad Electrónico (DNIe)
      - - Buenas prácticas en el uso del certificado digital y DNIe.

UD 2:
"Implantación de mecanismos de seguridad activa"

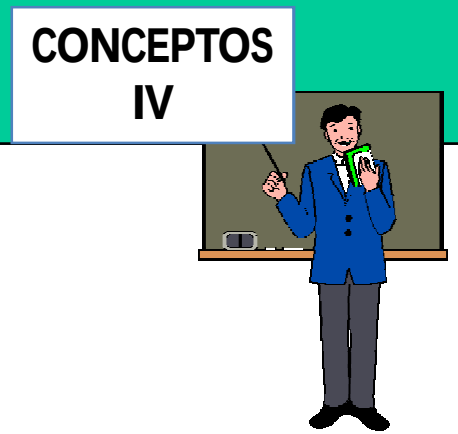
- **Seguridad en la red corporativa:**

CONCEPTOS III



- *Amenazas y ataques en redes corporativas:*
  - * Amenaza interna o corporativa y Amenaza externa o de acceso remoto.
  - * Amenazas: Interrupción, Intercepción, Modificación y Fabricación.
  - * Ataques: DoS, Sniffing, Man in the middle, Spoofing, Pharming.
- *Riesgos potenciales en los servicios de red.*
  - * Seguridad en los dispositivos de red : terminales, switch y router.
  - * Seguridad en los servicios de red por niveles:
    Enlace, Red (IP), Transporte(TCP-UDP) y Aplicación.
- *Monitorización del tráfico en redes: Herramientas.*
- *Intentos de penetración.*
  - * Sistemas de Detección de Intrusos (IDS).
  - * Técnicas de Detección de Intrusos.
  - * Tipos de IDS: (Host IDS, Net IDS).
  - * Software libre y comercial.

UD 2:
“Implantación de mecanismos de seguridad activa”



- **Seguridad en la red corporativa:**
  - *Seguridad en las comunicaciones inalámbricas.*
    - * Sistemas de seguridad en WLAN.
      - Sistema Abierto.
      - WEP.
      - WPA.
    - * Recomendaciones de seguridad en WLAN.

UD 2:

“Implantación de mecanismos de seguridad activa”

Pruebas escritas

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES I

ATAQUES Y CONTRAMEDIDAS EN SISTEMAS PERSONALES:

1. HERRAMIENTAS PALIATIVAS. ANTIMALWARE.

Antivirus. Spyware, Adware , Hijacking, Keyloggers, Stealers, Botnets, Rogue, Criptovirus, autorun.inf, software específico.

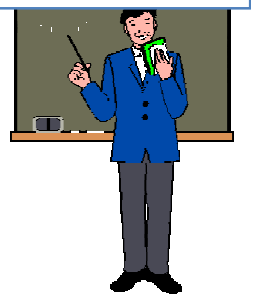
1. Instala en GNU/Linux el antivirus ClamAV, y su versión gráfica Clamtk.

   sudo aptitude install clamav
   sudo aptitude install clamtk
   Escanear modo texto: sudo clamscan –r –i <directorio>
   Escanear modo gráfico: sudo clamtk

2. Investiga en Internet el término : **Spyware**. Cómo puedes eliminar dicho malware. ¿Qué efectos tiene sobre el sistema?. Busca software que evite Spyware.
3. Investiga en Internet el término : **Adware**. Cómo puedes eliminar dicho malware. ¿Qué efectos tiene sobre el sistema?. Busca software que evite Adware.
4. Investiga en Internet el término : **Hijacking**. Cómo puedes eliminar el **"Browser hijacker"**. ¿Qué efectos tiene sobre el sistema?. Cómo puedes eliminar **"Pharming"**. Busca software que evite Hijacking.
5. Investiga en Internet los términos: **Keyloggers y Stealers.** Cómo puedes eliminar dicho malware. ¿Qué efectos tiene sobre el sistema?. Busca software que evite los Keyloggers y Stealers.
6. Investiga en Internet los términos: **Botnets, Rogue, y Criptovirus**. Cómo puedes eliminar dicho malware. ¿Qué efectos tiene sobre el sistema?. Busca software que evite dicho malware.

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES II



ATAQUES Y CONTRAMEDIDAS EN SISTEMAS PERSONALES:

7. Investiga en Internet información sobre el fichero autorun.inf que poseen los dispositivos de almacenamiento y cómo se camufla y opera malware a través de este archivo. Cómo puedes eliminar dicho malware. ¿Qué efectos tiene sobre el sistema?. Busca software que evite dicho malware.
8. Instala y utiliza al menos dos herramientas de análisis antimalware, indicando en un informe que tipo de malware evitas.

- Live AVG Rescue CD que se puede iniciar desde un CD o flash USB.

- SpyBot-Search&Destroy http://www.safer-networking.org

- Software de Microsoft : suite **Sysinternals**. Utiliza entre otros: **Autoruns** y **Process Explorer**
http://technet.microsoft.com/es-es/sysinternals/bb545021

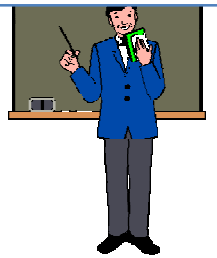
- Herramientas gratuitas de **Trend Micro USA. Utiliza las herramientas: HouseCall, Browser Guard 2011, HiJackThis y RUBotted.**
http://es.trendmicro.com/es/products/personal/free-tools-and-services/

- Software de recuperación de pulsaciones de teclado denominado **Revealer Keylogger.** Piensa como prevenir este software e informa en un documento. Utiliza el software **Malwarebytes para Windows.** ¿Lo detecta?. http://www.malwarebytes.org

- Otro software de compañias antimalware buscado en Internet.

UD 2:
“Implantación de mecanismos de seguridad activa”

EXPOSICIÓN DE TAREAS O ACTIVIDADES III



ATAQUES Y CONTRAMEDIDAS EN SISTEMAS PERSONALES:

2. HERRAMIENTAS PREVENTIVAS.

a) CONTRASEÑAS: BIOS y Gestor de arranque. Recuperación ,modificación y creación de contraseñas seguras. Protección de la cuenta del usuario administrador del sistema. Gestores de contraseñas.

1. Asignar contraseña a la BIOS y observar su vulnerabilidad.
2. Contraseñas en el gestor de arranque: Práctica con GRUB
3. Busca software en Internet para recuperar contraseñas en sistemas Windows y GNU/Linux. (Windows: Ophcrack,... GNU/Linux: John the Ripper,...).
4. Recuperada la contraseña, modifica la misma mediante políticas que permitan contraseñas fuertes y seguras.(Windows: Política de directivas de cuentas, - GNU/Linux: módulo pam_cracklib).
5. En Windows: modifica la contraseña del Administrador y el nombre de dicho usuario.
6. En GNU/Linux: modifica la contraseña de root y el nombre de dicho usuario.
7. Usa un gestor de contraseñas en Windows o GNU/Linux y demuestra su utilización en el sistema elegido. ¿Qué ventajas y vulnerabilidades conlleva la utilización de dicho software?. https://es.wikipedia.org/wiki/Gestor_de_contrase%C3%B1as

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES IV

ATAQUES Y CONTRAMEDIDAS EN SISTEMAS PERSONALES:

2. HERRAMIENTAS PREVENTIVAS.

b) ACCESO A LOS DATOS: Peligro de las distribuciones Live. Cifrado de datos o particiones.

1. Utiliza un DVD con una distribución Live para acceder a las particiones de datos de un sistema: **Ultimate Boot CD – UBCD, Backtrack, Ophcrack, Slax, Wifiway, Wifislax.**
2. Indica como evitar el acceso a los datos de las distribuciones Live en Windows y GNU/Linux.
3. Busca en Internet y utiliza software que permita en Windows o GNU/Linux para cifrar datos o particiones.

c) SISTEMA Y APLICACIONES: Drivers, Utilización de aplicaciones.

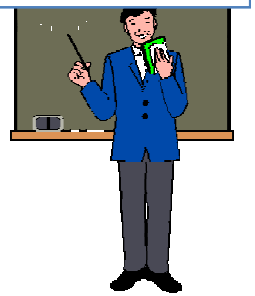
1. Busca aplicaciones que permitan la "congelación de sistema y aplicaciones " en Windows y GNU/Linux y utiliza y demuestra como funcionan. Ejemplo: **DeepFreeze.**
2. Control de usuarios y aplicaciones. Demuestra que un usuario sólo puede utilizar las aplicaciones que se desean en la organización.
   - En Windows: **Política de directivas de seguridad local.**
   - En GNU/Linux: **chmod, chown, chgrp, getfacl, setfacl.**
3. Utiliza un software de copia de seguridad de drivers (Ejemplo: **DriverMax)**.

d) ACCESO A INTERNET: Bloqueo de sitios web maliciosos.

1. Bloquea sitios web utilizando el navegador **Firefox Mozilla.**
2. Bloquear sitios web utilizando el navegador **Chrome.**
3. Bloquear sitios web utilizando el navegador **Internet Explorer.**

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES V



SEGURIDAD EN LA CONEXIÓN CON REDES PÚBLICAS:

3. TÉCNICAS DE CIFRADO: (Trabajo individual o por grupos de dos personas)

a) CIFRADO: Historia.

Realizar CISCO CCNA Security 2.0. Laboratorio : Explorando métodos de cifrado

b) CIFRADO: Funciones HASH--> Integridad y Autenticidad.

(Ver orientaciones prácticas) 1 2

1. Utiliza un programa en Windows o GNU/Linux para simular la **integridad**, utilizando MD5 y SHA1.
2. Utiliza un programa en Windows o GNU/Linux para simular la **autenticidad** utilizando HMAC-MD5, HMAC-SHA1.

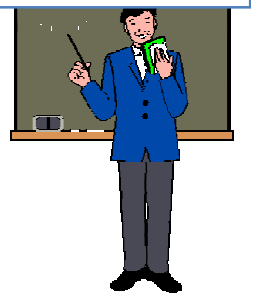
c) CIFRADO: Simétrico y Asimétrico--> Confidencialidad, Integridad y Autenticidad.

(Ver orientaciones prácticas) 4 5 7 8

1. Utiliza un programa en Windows o GNU/Linux para simular la **confidencialidad** mediante "cifrado simétrico".
2. Utiliza un programa en Windows o GNU/Linux para simular la **confidencialidad** mediante "cifrado asimétrico".
3. Utiliza un programa en Windows o GNU/Linux para simular la **autenticidad** mediante "cifrado asimétrico".
4. Utiliza un programa en Windows o GNU/Linux para simular la **"autenticidad"+"confidencialidad"** mediante "cifrado asimétrico".
5. Utiliza un programa en Windows o GNU/Linux para simular una comunicación segura utilizando cifrados híbridos **"autenticidad" + "confidencialidad"+"integridad"** : asimétricos (clave pública) y simétricos (clave privada)

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES VI



SEGURIDAD EN LA CONEXIÓN CON REDES PÚBLICAS:

4. IDENTIDAD DIGITAL (PKI – Infraestructura de clave pública):

a) CERTIFICADOS DIGITALES: Solicitud.

(Ver orientaciones prácticas) 10 11

1. Busca que Autoridades Certificadoras Admitidas de certificados digitales existen en España. **Describe el proceso para la obtención del certificado digital**. Visita la web www.fnmt.es, CERES: http://www.cert.fnmt.es/
2. ¿Es válido para todos los navegadores web? .¿Puede emplearse para firmar otro tipo de archivos?.¿Es posible exportarlo o solamente se puede emplear en un solo equipo?.¿Qué precauciones podemos tener con el certificado digital en cuanto a protección mediante contraseñas a la exportación?
3. Obtener tú **certificado digital software de usuario de CERES**. Solicitar vía Internet, acreditar en la Oficina de Registro de la Agencia Tributaria y descargar certificado.
4. Obtener tú **certificado digital software de usuario con DNIe**.

b) CERTIFICADOS DIGITALES: Uso en INTERNET.

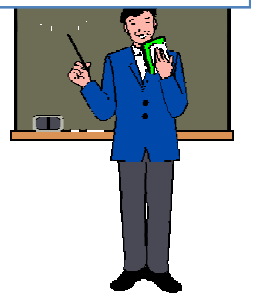
Una vez realizado los trámites para la obtención de tu certificado dígital. ¿Qué caducidad posee?¿Qué estándares utiliza?.

1.- Instalarlo en **Internet Explorer, Firefox y Chrome**.

2.- Accede a la plataforma PAPAs mediante certificado digital.

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES VII



SEGURIDAD EN LA CONEXIÓN CON REDES PÚBLICAS:

4. IDENTIDAD DIGITAL:

c) CERTIFICADOS DIGITALES: Uso en correo electrónico.

1.- Revisa en la web www.camerfirma.com , uno de los usos que tiene el certificado digital para la firma y el envío de correo electrónicos con certificado dígital. Describe el proceso. ¿Qué garantiza?.¿Qué es S- MIME?.

2.- Instala tu certificado digital en tu cliente de correo electrónico y firma tus mensajes de correo.

d) CERTIFICADOS DIGITALES: Uso del DNIe.

(Ver orientaciones prácticas) 12

1.- Actualiza tu DNIe en un Punto de Actualización del DNIe.
2.- Instala un lector de DNIe.
3.- Realiza una búsqueda de los servicios de empresas como bancos, y de la administración pública (Seguridad Social, Hacienda, etc) a los que se puede acceder de forma segura, mediante certificado digital y mediante DNIe.
4.- Acceder a un organismo público en Internet utilizando el Dni-e.

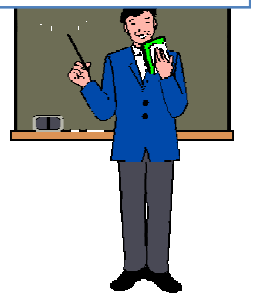
e) FIRMA DIGITAL: Uso en documentos.

(Ver orientaciones prácticas) 9

Utiliza un programa en GNU/Linux o Windows para firmar digitalmente un fichero.

UD 2:
“Implantación de mecanismos de seguridad activa”

EXPOSICIÓN DE TAREAS O ACTIVIDADES VIII



SEGURIDAD EN LA CONEXIÓN CON REDES PÚBLICAS:

4. IDENTIDAD DIGITAL:

f) CERTIFICADOS DIGITALES: Uso Empresarial. (Ver orientaciones prácticas):

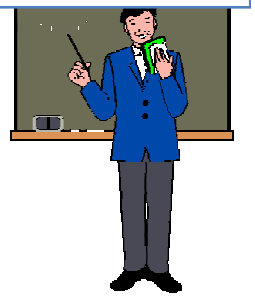
1.- ¿Qué diferencias existen entre la instalación de un certificado en un servidor web y un servidor de certificaciones?.

2.- Busca cómo se instala y qué opciones ofrece el **servidor de certificados digitales (CA) integrados en el servidor Windows 2003/2008/2012 Server de Microsoft.**

3.- Realiza una petición por parte de un cliente (usuario, equipo o aplicación) de un certificado digital a dicho servidor.

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES IX



SEGURIDAD EN LA RED CORPORATIVA:

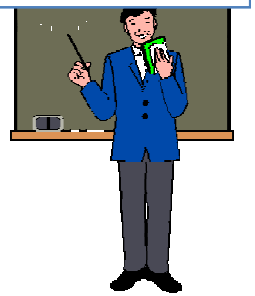
5. AMENAZAS Y ATAQUES EN REDES CORPORATIVAS:

Simulación de amenazas. Análisis de puertos. Amenazas a Bases de Datos . SQL Inyection.

1.- Utiliza software (Windows o GNU/Linux) para "recrear o simular" una amenaza en una red:
   a).- ARP Spoofing /MAC Spoofing /IP Spoofing
   b).- Man in the Midle (MitM) /Sniffing / Pharming.
2. (Host) Uso de netstat para análisis de puertos en Window y GNU/Linux.
3. (Red). Uso de software (Windows o GNU/Linux) para un análisis de puertos de un equipo en la red.
4. (Inyección SQL)
   a).-¿Qué es la inyección de código SQL.
   b).- Buscar enlaces en Internet que indiquen como evitar SQL iInyection.
   c).- Indica como puede utilizar la distribución Backtrack de GNU/Linux para investigar sobre la inyección de código SQL (SQL Inyection) y que te permita obtener las tablas de usuarios y contraseña de las bases de datos de sitios web.
   http://www.backtrack-linux.org/

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES
X



SEGURIDAD EN LA RED CORPORATIVA:

6. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED:

a) ROUTERS. Cisco.

Realizar el laboratorio. CISCO CCNA Security 2.0. Laboratorio: Asegurando routers.

b) SWITCHS. Cisco

Realizar el laboratorio CISCO CCNA Security 2.0. Laboratorio: Asegurando switchs.

7. MONITORIZACIÓN DEL TRÁFICO EN REDES:

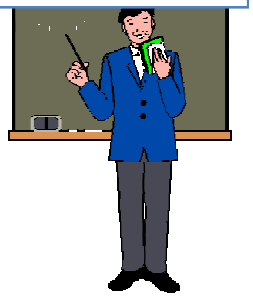
Redes Cableadas. Redes inalámbricas.

a) Descarga e instala software que monitorice y supervise el tráfico de la red y realiza filtrado de servicios de red : **Syslog, SNMP y NetFlow.** para monitorizar sólo el tráfico deseado. – diferente de Wireshark-.

b) Descarga e instala software que monitorice redes inalámbricas y realiza filtrados de red para monitorizar sólo el tráfico deseado.

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES XI



SEGURIDAD EN LA RED CORPORATIVA:

8. INTENTOS DE PENETRACIÓN:

a) SISTEMA DE DETECCIÓN DE INTRUSOS (IDS): HostIDS

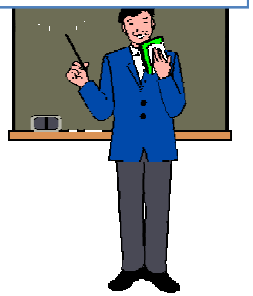
1. **Integridad** en el sistema de ficheros.
   a) Linux: Integridad de un fichero: **md5sum**., **trypwire.**
   b) Windows: Integridad del sistema de ficheros mediante **Xintegrity**.
2. **Honeypot**.
   a) ¿Qué es un Honeypot?.¿Para que se utiliza en seguridad informática?.
   b) Elabora un listado de software Honeypot.
   c) Instalación , configuración , ejecución y prueba en Windows o GNU/Linux software del tipo honeypot

b) SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) : NetIDS

1. **Snort .** Instalación, configuración, ejecución y prueba en GNU/Linux.
   www.snort.org
   (Simula un ataque a dicho equipo para observar como responde Snort)
2. **Routers**. Realizar CISCO CCNA Security 2.0. Laboratorio: Configurando un IPS usando CLI.

UD 2:
"Implantación de mecanismos de seguridad activa"

EXPOSICIÓN DE TAREAS O ACTIVIDADES XII



SEGURIDAD EN LA RED CORPORATIVA:

9. SEGURIDAD EN LAS COMUNICACIONES INALÁMBRICAS.

Entorno. Configuración. Configuración con seguridad. Monitorización y Auditoria.

1. Realiza junto a otros compañeros un "mapa wardriving" de alguna zona de tu localidad o entorno.
2. Configuración de un punto de acceso inalámbrico seguro. Utilizando emuladores:
   TP-LINK: http://www.tp-link.es/support/emulators/
   CISCO Linksys: http://ui.linksys.com/
3. Configuración de un router de acceso inalámbrico CISCO Linksys seguro y un cliente de acceso inalámbrico en Windows y GNU/Linux.
   - Filtro MAC, WPA, Control parental.
4. Realiza una auditoria wireless para medir el nivel de seguridad de una red inalámbrica, utilizando:
   a.- Monitorizar canales y frecuencias de puntos de acceso y routers inalámbricos.
   b.- Una aplicación para monitorizar y recuperar contraseñas inalámbricas WEP (**airodump**, **aircrack**, etc..)
   c.- Una distribución Live para monitorizar y recuperar contraseñas inalámbricas. (**Backtrack**, **Wifiway, Wifislax**, etc)

UD 2:

“Implantación de mecanismos de seguridad activa”

REALIZACIÓN DE TAREAS O ACTIVIDADES POR EL ALUMNO