UD 2: Implantación de mecanismos de seguridad activa

Indice

Ataques y contramedidas en sistemas personales

Seguridad en la conexión con redes públicas

Elaboración de un manual de seguridad y planes de contingencia

Seguridad en la red corporativa

Ataques y contramedidas en sistemas personales

Integridad, confidencialidad y disponibilidad

Clasificación de los ataques I

- **Ataques de ingeniería social**: son métodos de manipualción psicológica que buscan obtener acceso o información mediante el engaño (phishing, vishing y baiting)
- **Ataques de malware**: Consiste en la utilización de software malicioso para dañar o tomar el control del sistema de un usuario. Incluyen virus, gusanos, troyanos, ransomware y spyware.
- **Ataques de fuerza bruta y craqueo de contraseñas**: Implica la utilización de herramientas automatizadas para descifrar contraseñas mediante pruebas exhaustivas. Son comunes en ataques de red y en sistemas que no han implementado restricciones de intentos fallidos y autenticación multifactor. Ejemplos son los ataques con diccionario o ataques al hash de la contraseña.

Clasificación de los ataques II

- **Ataques de denegación de servicios** (DoS) y distribuidos (DDoS): Consiste en saturar un sistema o rede con tráfico innecesario hasta que sus recursos se agotan, volviéndolo inaccesible para usuarios legítimos.
- **Ataques de interceptación** (Man in the Middle o MitM) en castellano el hombre del medio. En este caso, el atacante intercepta y potencialmente altera la comunicación entre dos partes sin que estas lo sepan.

Anatomía de ataques y análisis de software malicioso. Pasos

- Infección inicial: el malware entra en el sistema, ya sea mediante un archivo adjunto en un correo, un enlace malicioso o la descarga de un archivo.
- Expansión: una vez dentro, el malware intenta extenderse dentro del sistema o hacía otros dispositivos conectados en la red. Los gusanos, por ejemplo, se replican y diseminan automáticamente.
- Ejecución de la carga útil: el malware realiza la acción maliciosa para la cual fue diseñado, ya sea cifrar archivos (ransomware), robar datos o espiar las actividades del usuario
- Evasión y persistencia: muchos tipos de malware incluyen mecanismos para evitar la detección y mantenerse activos incluso después de que el sistema sea reiniciado.

Herramientas preventivas

Son las herramientas que previenen ataques en sistemas personales. Existen herramientas de seguridad que permiten reducir el riesgo de infección y la posibilidad de accesos no autorizados.

Instalación y configuración en Windows

- Antivirus y antimalware. Windows cuenta con Windows Defender, pero es recomendable complementarlo con herramientas como Malwarebytes. Se debe configurar para realizar análisis periódicos y activar el escudo en tiempo real.
- Firewall (cortafuegos). Windows integra un firewall que debe estar activo en todo momento. En la configuración avanzada se pueden definir reglas específicas para el tráfico entrante y saliente.
- Actualizaciones automáticas: es fundamental que Windows Update está activo para asegurar que el sistema tenga los últimos parches de seguridad.

Instalación y configuración de Linux

- **ClamAV**: en Linux es un antivirus que ofrece una buena protección. Aunque los ataques de virus son menos comunes, su uso sigue siendo recomendado en entornos multiusuario.
- **Firewall** (cortafuegos): las **Iptables** permite definir reglas de cortafuegos personalizadas para bloquear puertos y proteger servicios. También se puede utilizar **ufw** (uncomplicated firewall, en castellano, cortafuegos “descompilado”) o su versión con interfaz gráfica **gufw**
- **SELinux/AppArmor**: ambas son herramientas de seguridad que añaden capas de control sobre las aplicaciones que se ejecutan en el sistema, limitado los permisos.

Instalación y configuración en macOs

- Xprotect: es el antivirus integrado en macOs, que se actualiza automáticamente y protege contra amenazas conocidas.
- Firewall (cortafuegos): en las opciones de seguridad y privacidad, se puede activar el firewall y definir permisos para aplicaciones específicas.
- Gatekeeper: este sistema evita la ejecución de aplicaciones de desarrolladores no autorizados, minimizando el riesgo de instalar software malicioso.

Práctica entregable

- Configura Windows Defender para realizar análisis periódicos (por ejemplo, todos los días a las 12 de la noche) y activa el escudo en tiempo real para que te avise de posibles ataques en el momento que se producen.
- Configura un servidor web con UFW que permita tráfico HTTP (puerto 80) y HTTPs (puerto 443) pero boquee todo el tráfico no autorizado.

Solución:

Paso	Comando
Habilitar UFW	`sudo ufw enable`
Permitir puertos HTTP y HTTPS	`sudo ufw allow 80` `sudo ufw allow 443`
Permitir SSH desde una IP específica (por seguridad)	`sudo ufw allow from 192.168.1.10 to any port 22`
Verificar la configuración	`sudo ufw status`
Bloquear todo el tráfico restante	`sudo ufw default deny incoming`

Práctica entregable

- Instalar en Linux ClamAV y su opción gráfica para proteger el Linux que tenemos instalado de posibles ataques. Realizar un escaneo de carpetas tanto en modo comando con en modo gráfico.
- Configura el firewall de al menos dos sistemas operativos (Windows, Linux o Mac) y establece reglas para bloquear el tráfico entrante desde puertos no seguros (debes averiguar cuales son esos puertos y que es lo que puede entrar por ellos).

Entrega un documento pdf documentando todos los pasos realizados.

Herramientas paliativas

Son aquellas que ayudan a reducir el impacto de un ataque una vez que esta ya se ha producido. Aunque no previenen el ataque inicial permiten mitigar el daño y facilitar la recuperación del sistema.

Una de las medidas es realizar y guardar copias de seguridad de los datos importantes siguiendo la regla 3, 2, 1

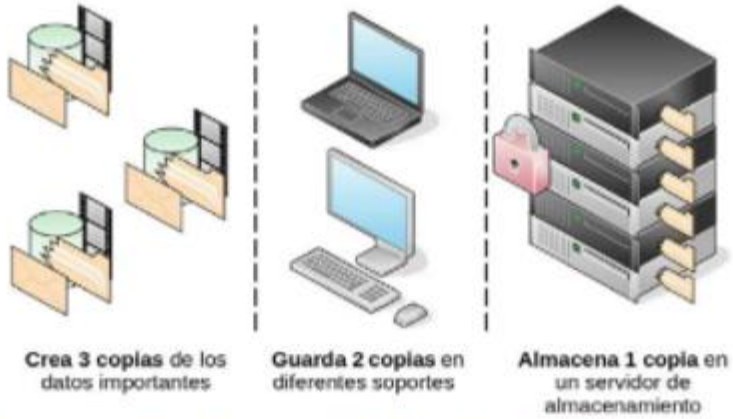
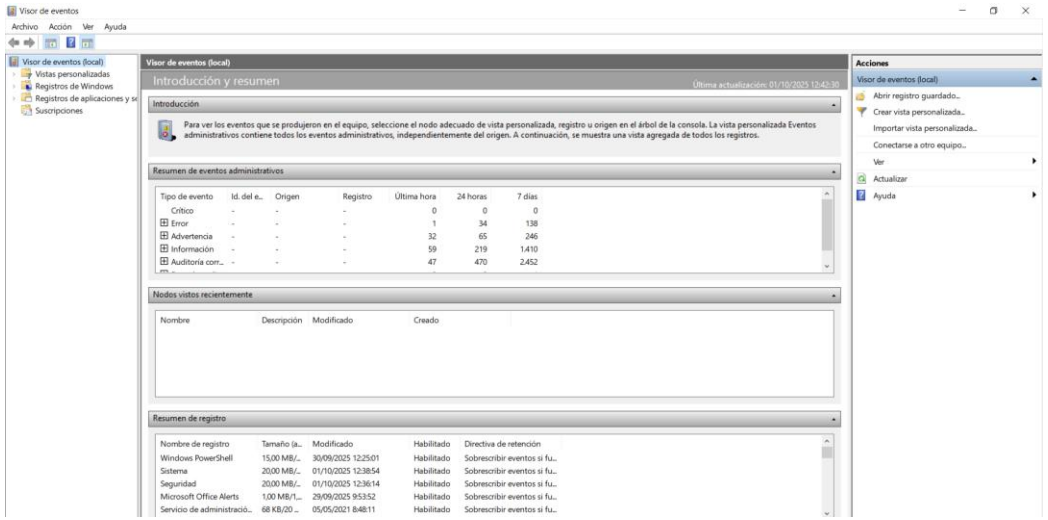


Figura 2.2. Representación de la regla de 3, 2, 1 aplicada al almacenamiento de datos.

Herramientas paliativas en Windows

- **Restauración del sistema**: permite recuperar el estado del sistema a un punto anterior a la infección o el problema
- **Copia de seguridad (backup):** Windows incluye la posibilidad de hacer copias de seguridad automáticas de archivos importantes, así como copias de imagen del sistema para restauración completa.
- **Herramientas de diagnóstico**: unidades como el Visor de eventos ayudan a identificar posibles fuentes de problemas y rastrear actividades sospechosas.



Herramientas paliativas de Linux

- **Backup(Rsync):** permite sincronizar y realizar copias de seguridad de los archivos importantes en diferentes ubicaciones, facilitando la recuperación tras un ataque.
- **Log del sistema**: en Linux los registros se encuentran en la carpeta /var/log y su análisis es esencial para entender cómo se produjo el ataque y qué áreas fueron comprometidas.
- **Chroot jail**: permite ejecutar aplicaciones en un entorno restringido, lo cual minimiza el daño que pueden causar al sistema en caso de infección.

Herramientas paliativas en macOs

- **Time Machine**: es la herramienta de backup de macOS que permite restaurar archivos o todo el sistema a un estado previo.
- **Log console** (consola de registro): ayuda a monitorear eventos y detectar actividades anómalas.
- **Modo seguro** (Safe Boot): permite iniciar el sistema solo con los controladores básicos y ayuda a eliminar archivos maliciosos o a restaurar configuraciones.

Práctica entregable

Configura y prueba una herramienta paliativa en dos de los tres sistemas operativos más usados (Linux, Windows o Mac). Simula una situación de recuperación y entrega un documento pdf documentando todos los pasos realizados.

Actuación de sistemas y aplicaciones

Mantener actualizados el sistema operativo y las aplicaciones es una medida de seguridad muy efectiva contra las vulnerabilidades conocidas. Estas actualizaciones corrigen errores y fallos de seguridad que podrían utilizar los atacantes.

- Windows: las actualizaciones se gestionan desde Windows Update. Es recomendable activar las actualizaciones automáticas.
- Linux: las distribuciones basadas en Debian, como Ubuntu, utilizan el gestor de paquetes apt o apt-get:
  - Apt-get update && apt-get upgrade –y

  Otras distribuciones utilizan herramientas como yum o dnf
- macOs: las actualizaciones se gestionan a través de la App Store o el panel de preferencias del sistema. Se recomienda mantener las actualizaciones automáticas activas.

Seguridad en la conexión con redes públicas

Identificación digital

Permite verificar la identidad de un usuario o sistema en línea. Este proceso es fundamental para autenticar conexiones, validar permisos de acceso y proteger datos personales. Los métodos mas comunes son:

- Autenticación basada en contraseñas: es el método más común, aunque menos seguro. Los usuarios deben utilizar contraseñas robustas y cambiarlas periódicamente.
- Autenticación multifactor (MFA): incluye un segundo método de verificación, como un código SMS o la sincronización con una aplicación-
- Certificados digitales: son documentos electrónicos que validan la identidad del usuario o sistema. Funcionan con un par de claves (una pública y una privada) y son emitidos por una autorizada certificadora (CA)

Firma electrónica y certificado digital

Son componentes esenciales de la seguridad en línea, ya que permiten validar la identidad y la integridad de los documentos.

- Firma electrónica: conjunto de datos que se añaden a un documento para identificar al firmante y garantizar que el documento no ha sido modificado. Existen varios niveles de firma electrónica desde la simple (sin validación) hasta la cualificada (verificada por una entidad acreditada). Se suele usar en transacciones comerciales y firmas de documentos oficiales en el entorno digital.
- Certificado digital: es emitido por una autoridad certificadora (CA) que verifica la entidad del titular y genera una clave criptográfica única para ese usuario o empresa.
- Los certificados digitales son usados tanto en sitios web (HTTPs) como en la firma de documentos y correos electrónicos.

Actividad

Investigar los pasos a seguir para obtener un certificado digital en la web de la FNMT (Fabrica Nacional de La Moneda y Timbre) y lista los documentos necesarios. Averigua que aplicaciones prácticas tiene dicho certificado en la vida cotidiana.

Publicidad y correo no deseado

Las amenazas mas comunes en la publicidad y el correo no deseado son:

- Phising: suplantación de identidad mediante correos fraudulentos que buscan obtener información persona o financiera
- Malware oculto en enlaces o archivos adjuntos: los correos no deseados pueden tener archivos que infectan al sistema al abrirlos.
- Recolección de datos: usan formularios o enlaces engañosos para recopilar datos de los usuarios.

Contramedidas a realizar

- Filtros de correo: configurar filtros antispam en el cliente de correo o en el servidor.
- Evitar abrir correos de remitentes desconocidos y principalmente si tienen enlaces o archivos adjuntos
- Navegación segura: evitar hacer clic en enlaces de sitios poco fiables y mantener actualizado el SO y el navegador.

Otros

- Evitar realizar transacciones sensibles cuando estemos conectados a una red pública (transferencias bancarias o envío de información sensible)
- Usar VPN (Red Privada Virtual) cifra la conexión entre el usuario y el servidor, lo cual aumenta la seguridad al ocultar la actividad en línea y proteger la privacidad del usuario.
- Desactivar el uso compartido de archivos: si desactivamos el uso compartido de archivos y acceso remoto reduce la exposición a ataques.
- Configurar el firewall para restringir el tráfico entrante y evitar accesos no autorizados.

Práctica entregable

Instala y configura una VPN en un dispositivo personal. Analiza cómo el uso de una VPN contribuye a proteger la conexión en una red pública. Si no es posible utilizar una VPN, documenta el proceso de cómo se llevaría a cabo la instalación y la configuración.

Elaboración de un manual de seguridad y planes de contingencia

Manual de seguridad y planes de contingencia

- La creación de un manual de seguridad es esencial para establecer pautas y prácticas que minimicen el riesgo de incidentes.
- Un plan de contingencia por su parte, es un protocolo que permite actuar rápidamente ante un incidente de seguridad para minimizar el impacto en el sistema.
- El manual de seguridad debe incluir los siguientes contenidos:
  - Definición de objetivos y alcance: es fundamental delimitar también las áreas de aplicación y los roles de cada usuario.
  - Medidas preventivas: incluyen la implementación de contraseñas robustas, el uso de autenticación multifactor y la capacitación continua en prácticas de seguridad para los usuarios.
  - Procedimientos ante incidentes: deben definir claramente incluso los contactos de emergencia y las responsabilidades de cada miembro del equipo.
  - Plan de recuperación: define los pasos para restablecer el sistema y asegurar la integridad de los datos tras un incidente. Esto incluye el uso de copias de seguridad y herramientas de recuperación de sistemas

Seguridad en la red corporativa

Protección y monitorización del tráfico de las redes.

Monitorización del tráfico en redes

Permite detectar patrones sospechosos o intrusiones. Es un paso clave para garantizar que la información que circula por la red está protegida y para responder rápidamente ante posibles amenazas.

- Aplicaciones para la captura y análisis del tráfico: consiste en recoger datos que circulan por la red para analízalos y detectar posibles irregularidades. Algunas aplicaciones son:
  - Windows: Wireshark
  - Linux: tcpdunp, nmap y Wireshark
  - macOs: Wireshark y Little Snitch.

Actividades

- Analiza el tráfico HTTP (puerto 80) en la interfaz eth0, capturando solo 20 paquetes y guardando la captura en un archivo para su análisis posterior.
- Realiza un escaneo completo con nmap de un servidor en la red local para identificar servicios, versiones y posibles vulnerabilidades en los puertos comunes.

Aplicaciones para la monitorización de redes y equipos

- Windows: PRTG Network Monitor es una aplicación que permite monitorear el tráfico de red, servidores, dispositivos y aplicaciones. Se usa para generar informes detallados y alertas en caso de actividad inusual.
- Linux: Nagios monitorea tanto la red como los equipos conectados a ella. Permite recibir alertas y reportes detallados en caso de fallos o anomalías.
- macOS: Zabbix es de código abierto y proporciona una interfaz fácil de usar para monitorizar redes, dispositivos y rendimiento de servidores.

Instala Nagios en un sistema Linux y configúralo para monitorear los recursos de la red y del equipo ¿Qué alertas se pueden configurar? ¿Cómo contribuyen a la seguridad de la red?

Seguridad de los protocolos para comunicaciones inalámbricas

Buenas prácticas en las redes inalámbricas:

- Configuración del SSID (nombre de la red): es recomendable no usar nombres que identifiquen a la empresa para evitar posibles atacantes.
- Cambio de contraseñas periódicas: especialmente en entornos corporativos, es necesario cambiar las contraseñas de las redes periódicamente.
- Implementación de autenticación multifactor (MFA): algunas redes permiten la autenticación adicional para usuarios, mejorando el control de acceso.

Riesgos potenciales de los servicios de red

Los riesgos más comunes de los servicios en red son:

- Escaneo de puertos: los atacantes pueden usar herramientas como Nmap para identificar servicios y puertos abiertos y así encontrar vulnerabilidades.
- Inyección de SQL en aplicaciones web: los atacantes envían comandos SQL maliciosos para obtener el acceso a la base de datos.
- Exposición de servicios sin protección: es necesario configurar correctamente el firewall para que el riesgo de intrusiones baje.

¿Cómo protegemos los servicios en red?

- Cerrar los puertos no utilizados. Es esencial cerrar los puertos que no son necesarios para reducir la posibilidad de ataque.
- Parametrizar la entrada a la base de datos con mínimos privilegios para evitar ataque de SQL. Utilizar consultas ya preparadas.
- Usar proxies y cortafuegos eso ayudará a controlar y limitar el tráfico que entra y sale de la red.
- Actualizar constantemente el software para reducir el riesgo de ataques aprovechando vulnerabilidades.

Intentos de penetración (I)

Técnicas utilizadas para explotar vulnerabilidades en la red con el fin de acceder a datos o recursos no autorizados. Algunos son:

- Craqueado de contraseñas que utiliza software para descifrar las credenciales de los usuarios. Algunos métodos de craqueado son:
  - Ataques de diccionario que utilizan una lista de palabras comunes para probar contraseñas. Hay herramientas para generar listados de contraseñas a través de patrones de palabras clave
  - Ataques de fuerza bruta que prueban todas las combinaciones posibles hasta encontrar la contraseña.
  - Ataques de hash que lo que intentan es conseguir el hash de una contraseña y con un listado existente ir comprobando hasta dar con el hash que nos interesa. Si se consigue el hash correspondiente a la contraseña, conoceremos la contraseña.

Intentos de penetración (II)

- Forzado de recursos: son ataque de fuerza bruta dirigidos a acceder a otros recursos de la web como servidores o bases de datos.
- Puertas traseras: son accesos ocultos en el sistema y/o aplicaciones que los desarrolladores pueden dejar para mantenimiento o pruebas de la aplicación. Los atacantes los puede utilizar para acceder sin permiso.
- Pentesting se trata de realizar pruebas de seguridad para evaluar la seguridad de la red y la de sus recursos con técnicas controladas. Se suelen utilizar Kali Linux y ParrotOS porque tienen herramientas especificas para poder realizar las pruebas. Algunas herramientas son: Hydra, John the Ripper y Metasploit.

Sistemas de detección de intrusiones (IDS) I

Permiten identificar comportamientos inusuales o potencialmente maliciosos en la red, dispositivos o sistema operativo, alertando a los administradores para que puedan responder de inmediato.

- Tipos de sistemas de detección de intrusiones:
  - IDS basados en red (NIDS): monitorean el tráfico de red en busca de patrones de actividad sospechosa
  - IDS basados en host (HIDS): se instalan en dispositivos individuales y monitorean la actividad del sistema operativo y las aplicaciones.
  - IDS basados en análisis de firmas: utilizan patrones conocidos de ataques para identificar intrusiones
  - IDS basados en análisis de anomalías: monitorean el comportamiento normal del sistema o la red y detectan desviaciones de este comportamiento.
  - IDS híbridos: combinan características de los IDS basados en firmas y anomalías.

Sistemas de detección de intrusiones (IDS) II

Características comunes de los IDS

- Monitoreo en tiempo real: analizar y responder en tiempo real.
- Alertas y notificaciones: generar alertas cuando se detectan actividades sospechosas
- Registro de eventos: mantener registros de las actividades detectadas para su posterior análisis.
- Integración de otras herramientas de seguridad: trabajar con firewalls, sistemas de gestión de eventos y otras soluciones de seguridad
- Escalabilidad: capacidad para adaptarse a redes o sistemas en crecimiento.

Sistemas de detección de intrusiones (IDS) III

Algunos IDS para los sistemas operativos mas usados son:

- IDS en Windows: Snort o Windows Event Viewer. Registran eventos sospechosos y emiten alertas cuando detectan posibles intrusiones.
- IDS en Linux: Suricata permite la captura y análisis de tráfico y OSSEC se basa en host que se integra bien con otros sistemas de seguridad.
- IDS en macOS: Snort o Little Snitch para monitorear conexiones y detectar intrusiones. Proporcionan alertas en tiempo real y opciones para bloquear accesos no autorizados.