SEGURIDAD EN WINDOWS 10

EL EQUIPO A

ÍNDICE

1. MECANISMOS DE SEGURIDAD
2. SEGURIDAD OOTB Y HARDENING
3. POLÍTICAS
4. HISTORIAL DE VULNERABILIDADES E INCIDENCIAS

1. MECANISMOS DE DEFENSA

1.1 Introducción

- Interés cambiante de los atacantes:
  - Antes: reputación y prestigio
  - Ahora: capital/otros fines malvados

- Los mecanismos de seguridad de Windows se centran principalmente en:
  1. Eliminar clases enteras de vulnerabilidades
  2. Romper las técnicas de explotación
  3. Contener el daño y evitar la persistencia
  4. Limitar la ventana de oportunidad para explotar

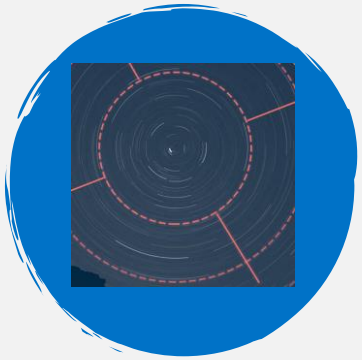
- Microsoft ha desarrollados fuertes mecanismos de defensa
  - Adiós a EMET (Enhanced Mitigation Experience Toolkit)
  - Bienvenido Windows Defender Exploit Guard

1.2 Windows Defender Exploit Guard

Componentes principales

Exploit Protection

Mitigaciones contra exploits comunes



Attack Surface Reduction (ASR)

Conjunto de reglas para evitar llamadas entre aplicaciones

Network protection

Protección de endpoints mediante bloqueo de procesos

Controlled folder access

Comprobación de aplicaciones. Uso de listas de confianza

Exploit Protection

- Aglutina un conjunto de mitigaciones de exploits (sustituye a los de EMET) que puede configurarse fácilmente para proteger su sistema y sus aplicaciones.
- Cierta flexibilidad.
- Componentes principales:
  - Configuración del Sistema.
  - Configuración de Programas.
  - Configuraciones importadas/exportadas
- Configuraciones se realizan en entradas de registros.
  - Están guardadas en la ruta:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ImageFileExecutionOptions\ImageFileName\MitigationOptions)

- Minimiza los lugares vulnerables
  - Reduce la superficie de ataque
- Conjunto de reglas
  - Evita llamadas entre aplicaciones
- Office:
  - Bloquea las macros
- Scripts:
  - Bloquea PowerShell y JavaScripts
    - Potencialmente dañinos
- Emails:
  - Bloquea contenido descargado
    - Proveniente del cliente nativo de correo
- USBs:
  - Bloquea ejecutables no firmados
- Ejemplo de regla:
  - *“Set-MpPreference-AttackSurfaceReductionRulesIds 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B-AttackSurfaceReductionRulesActions Enabled”*

Attack Surface Reduction (ASR)

Office – Scripts – Emails - USBs

Network Protection

SmartScreen

- Windows SmartScreen
  - Protege el endpoint contra las amenazas basadas en la web bloqueando cualquier proceso saliente en el dispositivo hacia hosts/IP no confiables.

- Principal objetivo de las webs maliciosas:
  - Adquirir información u obtener un pago financiero inmediato.
  - Instalar un Malware remoto y robar información, además de expandirse por la red

- Se aplica a:
  - Windows 10 (Integrado en el SO)
  - Microsoft Edge (Navegador más seguro)

- Motor principal: ISG
  - Gráfico de Seguridad Inteligente
  - Operativa inteligente

- Alta compatibilidad

Controlled folder access

- Funcionamiento basado en listas de confianza
- Configurable en cada carpeta
  - Acceso a las carpetas restringido
- Uso de la herramienta Intune
  - Agregar aplicaciones automáticamente
    - Basado en reputación
  - Agregar aplicaciones manualmente
    - No recomendable
- Aplicaciones agregadas por defecto
  - Office
  - Aplicaciones nativas del S.O

2. SEGURIDAD OUT OF THE BOX

2.1 categorías principales

La seguridad OotB se divide en 4 categorías

Presentes en la aplicación Seguridad de Windows

Seguridad dispositivo

Seguridad de componentes principales del equipo

Seguridad red

Seguridad de la red, privada o pública

Antivirus

Protección antimalware y antiransomware

Privacidad

Opciones de privacidad del equipo, como cámara y ubicación

Seguridad dispositivo

Seguridad de componentes principales del equipo

- Aislamiento del núcleo
  - Basado en la virtualización, defiende la memoria del sistema de ataques de malware aislándola del resto de componentes
  - Desactivado por defecto
- Trusted Platform Module (TPM)
  - Procesador de seguridad, se encarga de almacenar claves criptográficas para encriptar datos críticos.
  - Activado por defecto si es compatible
- Disponibilidad
  - Si lo permite el equipo físico

Seguridad red

Seguridad de la red, privada o pública

- Firewall
  - Activado de forma automática al conectar a una red
  - La red puede ser pública, privada o de dominio

Antivirus

Protección antimalware y antiransomware

- Antivirus
  - Instalado por defecto
  - Desactivado si existe otro antivirus instalado
- Antiransomware
  - Desactivado por defecto
- Inteligencia de seguridad
  - Base de datos de malware
  - Actualiza automáticamente

- Permisos de Windows
  - Envío de datos de diagnóstico, id de publicidad, reconocimiento de voz
  - Activados por defecto
- Permisos de aplicaciones
  - Acceso a recursos del equipo, como cámara, micrófono o ubicación
  - Activado por defecto (preinstaladas), a veces lo elige el usuario (nuevas aplicaciones)

Privacidad

Opciones de privacidad del equipo, como cámara y ubicación

- Crear una política de contraseñas seguras.
- Cifrar el disco con BitLocker.
- Restringir los privilegios a las cuentas de los usuarios.
- Crear listas blancas de aplicaciones.
- Hardening y parcheo de aplicaciones.
- Parcheo continuo del sistema operativo.
- Arranque seguro (secure boot).
- Bloqueo de scripts de powershell.

HARDENING

Mecanismos para mejorar la seguridad en Windows 10

3. POLÍTICAS DE GESTIÓN DE INCIDENTES

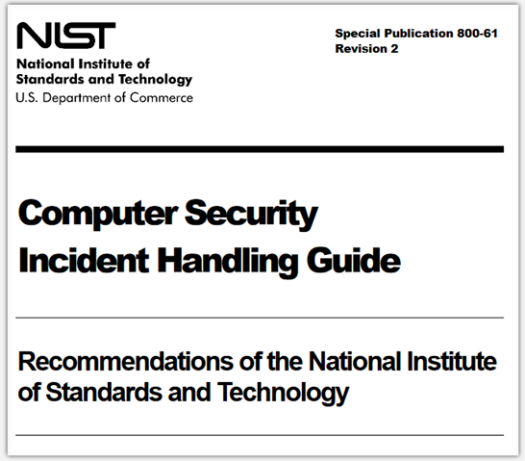
3.1 Introducción

¿Qué son las políticas de gestión de incidentes?

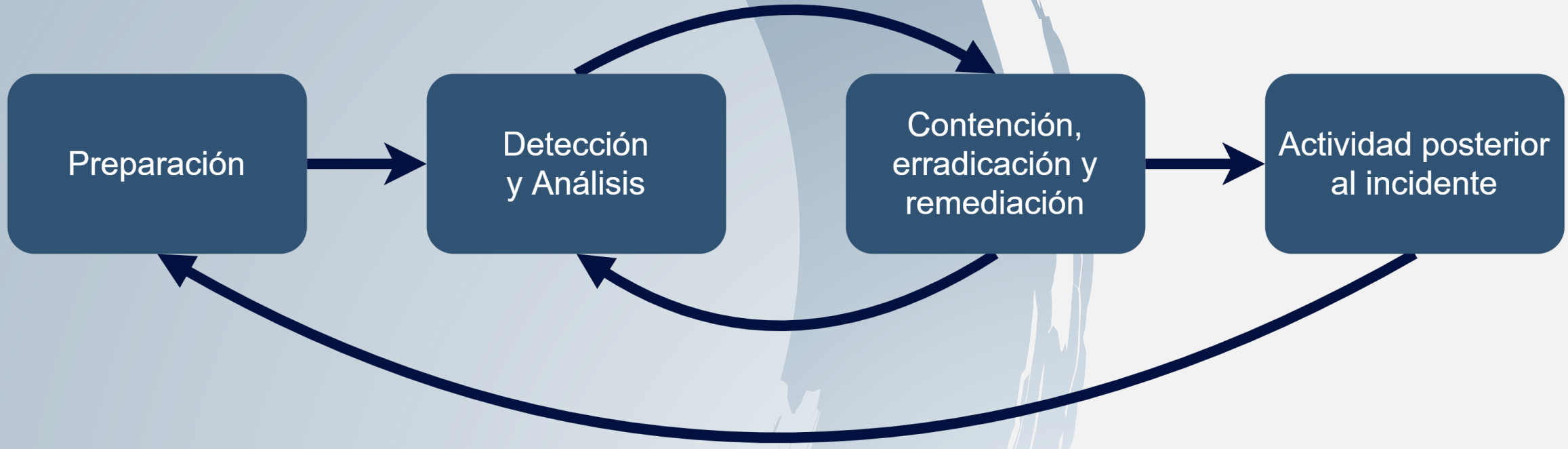
- Es un enfoque organizado para **abordar y gestionar** las secuelas de una brecha de seguridad o **ciberataque**.

- El **objetivo** es manejar la situación de una manera que **limite los daños y reduzca el tiempo y los costes** de recuperación.

- Publicación especial (SP) 800-61 del Instituto Nacional de Estándares y Tecnología (NIST)



3.2 Proceso de gestión de incidentes



Fases de gestión de respuesta NIST 800-61

3.2 Proceso de gestión de incidentes

Preparación

- Se trata de una preparación organizacional que se necesita para poder responder, incluidas herramientas, procesos, competencias y preparación.
  - Los Empleados reciben **capacitación** sobre incidentes de seguridad.
  - Los equipos de desarrollo implementan el **Ciclo de vida de desarrollo de seguridad (SDL)**.
  - **Pruebas de penetración** que evalúa continuamente sus propios sistemas en busca de vulnerabilidades.
- Programa de recompensas de errores de Microsoft (Microsoft Online Services Bug Bounty Program).

3.2 Proceso de gestión de incidentes

Detección y análisis

- **Registra** de forma centralizada los **eventos de seguridad** en el sistema.
- Almacenan en una base de datos central y consolidada.
- Windows Defender puede actuar como **antivirus** que **detecta y recopila muestras y enviarlas**, además de consultar firmas en las bases de datos de Microsoft.

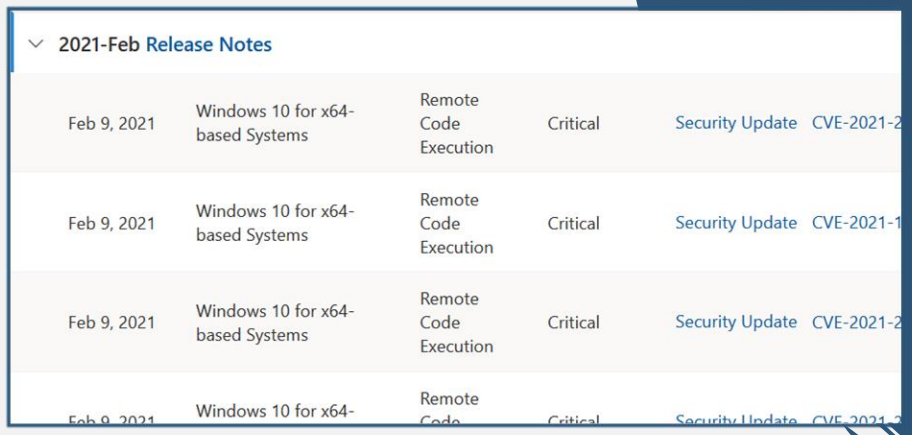
3.2 Proceso de gestión de incidentes

Contención, erradicación y remediación

- Acciones los lleva a cabo el **Centro de respuesta de seguridad de Microsoft (MSRC).**

  - Contención: contener la intrusión antes de que el adversario pueda acceder mas daño.
  - Erradicación: desalojar al adversario del sistema y mitigar la vulnerabilidad (parches de seguridad).
  - Remediación: restauración del sistema por medio de copias de seguridad.

- Si Microsoft determina que ha ocurrido un incidente de seguridad, se lo notifica a sus clientes por diversos medios.
- Página web específica por cada vulnerabilidad conocida en sus productos



3.2 Proceso de gestión de incidentes

Actividad posterior al incidente

- Análisis ***post-mortem***: enumerar la secuencia de eventos que causaron el incidente y crear un resumen técnico del incidente con el respaldo de la evidencia.
    - Este **paso** está **diseñado** para **identificar errores**, errores de procedimiento, errores manuales, errores de proceso y errores de comunicación durante la respuesta al incidente de seguridad.

- En la **documentación se plasma todos los hallazgos** técnicos clave del se capturan en un informe, así como las inversiones en servicios, correcciones en forma de errores, solicitudes de cambio de desarrollo.

3.3 Coordinated Vulnerability Disclosure

- Los **actores que encuentran una vulnerabilidad** la **informan** directamente **a los proveedores** afectados.
- **Esperan** para divulgarla públicamente **hasta que el proveedor haya desarrollado, probado y publicado parches**.
- Esta coordinación **permite al proovedor realizar** una **investigación completa** y **ofrecer actualizaciones** antes de que la vulnerabilidad se comparta públicamente.
- Si se **detectan ataques que utilizan la vulnerabilidad antes** que el proveedor proporcione la **actualización**, deben **coordinarse** para proporcionar una **divulgación** pública **temprana**.

4. HISTORIA DE VULNERABILIDADES E INCIDENCIAS

Vulnerabilidades

Actualizaciones que causan fallos relacionados con el parcheo de funcionalidades y que han generado otras más.

- Solucionar un fallo que afectaba a las funciones de búsqueda:
  - Disparaba el consumo de CPU
    - Afectó al menú de inicio.
    - Barra de búsqueda de Cortana.
- Tras afectar el sonido de algunos juegos:
  - Causaba un consumo excesivo del procesador
    - Provocando fallos en Windows Defender.

Fallos e incidentes relevantes

Actualización 2004 en la que Microsoft parcheó un total de 129 vulnerabilidades en las que 11 eran críticas.

Eternal Darkness

Ejecución de código remoto para obtener control del sistema y causar estragos en el PC.

SMBGhost

Infectar remotamente con programas maliciosos como ransomware y malware.

Wannacry

Malware ransomware para cifrado de archivos a cambio de un rescate.

CVE-2017-0144
12/05/2017

Bugs en SMB - Server Message Block

Common Vulnerabilities and Exposures - CVE

DoS

Denegación de Servicios

Code Execution

Ejecución de código remoto

Overflow

Desbordamiento de Memoria

Memory Corruption

Degradación de la memoria

XSS

Cross Site Scripting

Bypassing Something

Saltar/Evitar accesos

Gain Information

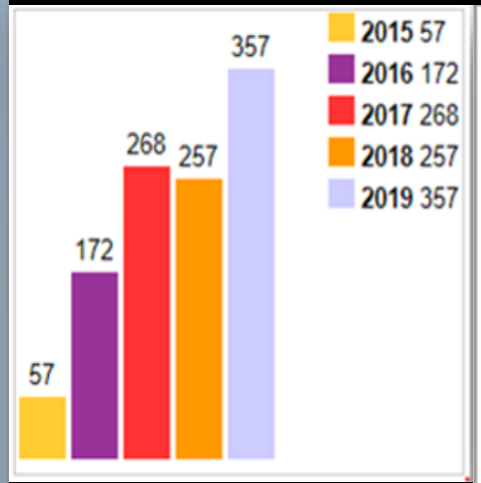
Obtener Información

Gain privileges

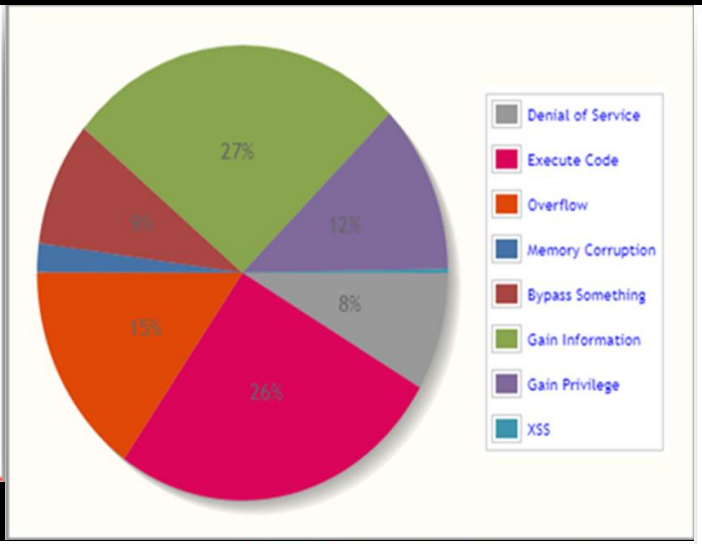
Obtener privilegios

Historial Vulnerabilidades Windows 10

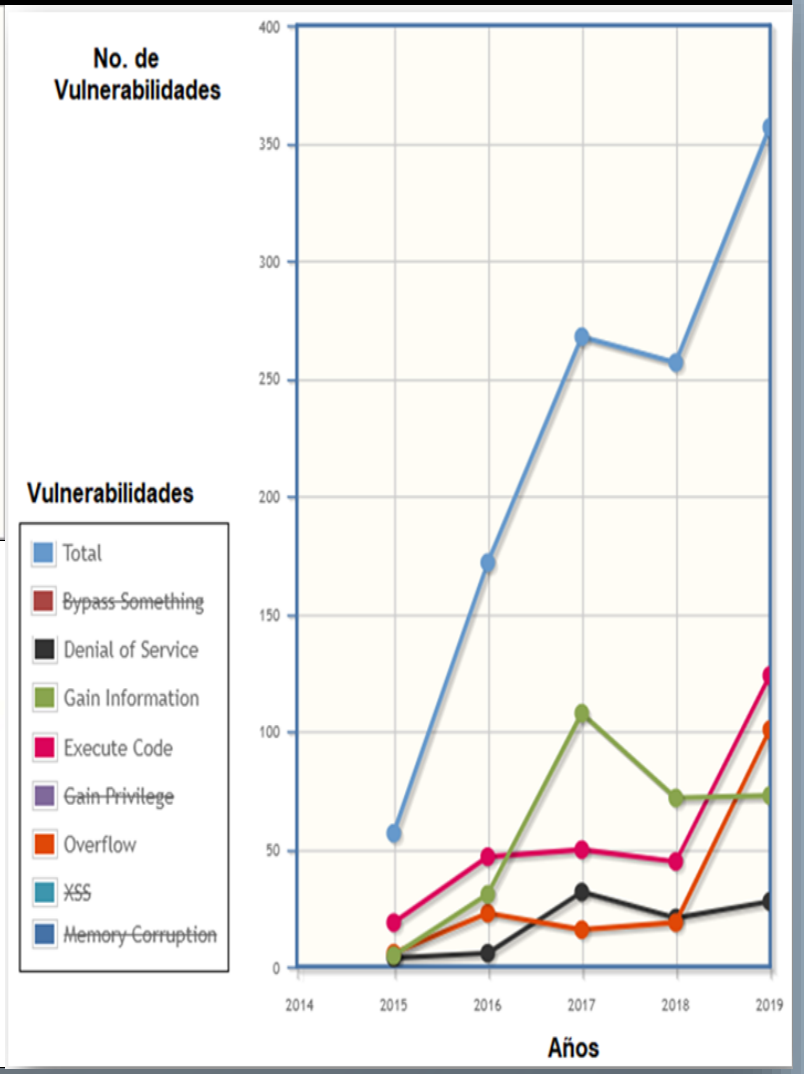
Por año



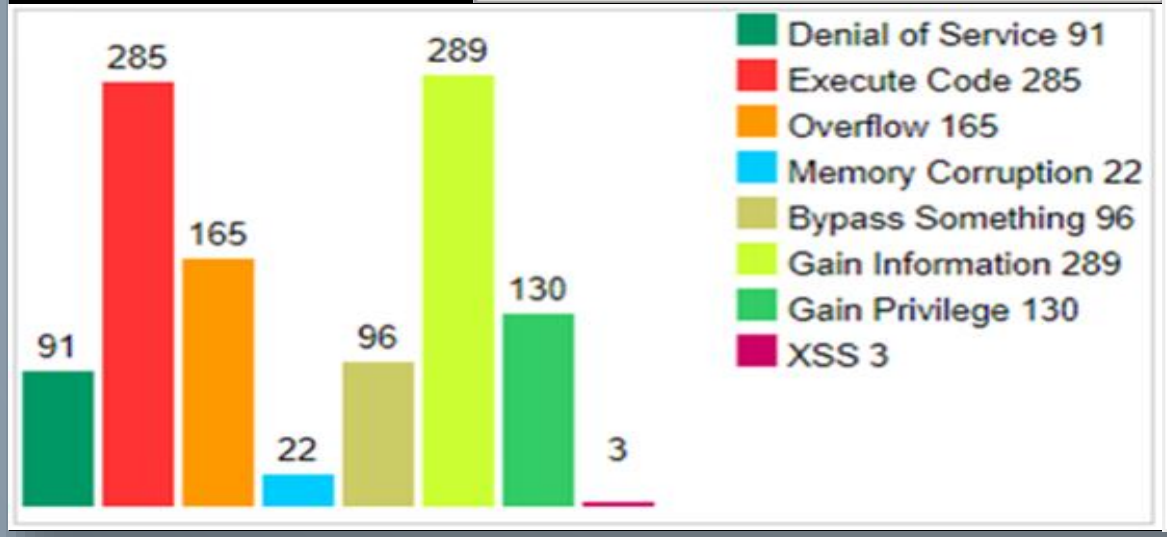
Más relevantes



Por tipo y año



Por tipo



GRACIAS