Universitat Oberta de Catalunya uoc.edu

# Seguridad en Servidores empresariales.

## Control y Análisis de configuraciones de seguridad y de vulnerabilidades.

**Alumno:** Ramon Illa Gay

**Trabajo Final de Máster:** Máster Universitario e Seguridad en las Tecnologías de la Información y de las comunicaciones (MISTIC)

**Área del Trabajo Final:** Seguridad Empresarial

**Consultor:** Pau del Canto Rodrigo

**Profesor Responsable:** Victor Garcia Font

**Fecha Entrega:** 01/06/2019

**Palabras clave**: SCAP, ‘Server Hardening’, ‘Vulnerability management’

# RESUMEN

La seguridad de los servidores empresariales es de vital importancia para el funcionamiento de las empresas. La no disponibilidad de las aplicaciones alojadas en los servidores puede suponer importantes pérdidas económicas y de prestigio para las empresas. Por este motivo es muy importante para las empresas mantener un elevado nivel de seguridad en sus servidores.

El objetivo principal de este trabajo es la definición de los procesos para la validación continua de la seguridad de los servidores, principalmente validando: la correcta configuración de seguridad de los mismos y sus posibles vulnerabilidades por versiones de sistema operativo o aplicaciones instaladas no actualizadas.

Este trabajo se realiza en la sucursal española de una empresa multinacional, que tiene definidas a nivel corporativo políticas de seguridad basadas en la ISO27001. Uno de los controles pendientes de implementar hace referencia a la seguridad de los servidores, y se alinea totalmente con los objetivos del trabajo. En la empresa existen unos 100 servidores virtuales, la mayoría de los cuales utilizan como sistema operativo alguna versión de Windows server.

Se realizará un estudio de mercado para seleccionar las posibles soluciones a utilizar para el control de vulnerabilidades y configuraciones de seguridad. Se evaluarán soluciones de distribución libre y también comerciales.

Una vez seleccionadas las soluciones se procederá a probarlas, configurarlas y definir el proceso para el control continuo de la seguridad de los servidores.

Para este proyecto se utilizará una metodología en cascada, con fases secuenciadas una detrás de otra. Se ha decidido utilizar esta metodología pues al ser ejecutado por una única persona no hay un beneficio especial en paralelizar actividades, y permite documentar el proyecto a medida que se van cerrando fases (cerrada una fase no habrá cambios significativos).

# ABSTRACT

Enterprise server's security is critical for enterprise operation. The non-availability of applications hosted on servers can cause significant economic and prestige impact for the companies. For this reason, it is very important for companies to maintain a high level of security in their servers.

The main objective of this work is the definition of the processes for the continuous validation of the security of the servers, mainly validating the correct security configuration and their possible vulnerabilities due operating system versions or installed applications not updated.

This work is done in the Spanish branch of a multinational company, which has corporate security policies based on ISO27001. One of the pending controls to implement refers to the security of the servers, which is completely aligned with the objectives of this work. There are about 100 virtual servers in the company, most of which use a version of Windows server as their operating system.

A market study will be conducted to select the possible solutions to be used for the vulnerability and security configuration control. Open Source and commercial solutions will be evaluated.

Once the solutions have been selected, they will be tested, configured and a process will be defined for the continuous control of server security.

For this project, a cascade methodology will be used, with phase's sequenced one after the other. It has been decided to use this methodology because when executed by a single person there is no special benefit in parallelizing activities, and it allows documenting the project as phases are closed (once a phase is closed there will be no significant changes).

# Índice

# 1. Introducción

## 1.1 Contexto y justificación del Trabajo

**Necesidad:** Una empresa multinacional con políticas de seguridad de la información basadas en ISO27001 tiene pendiente desarrollar de forma 'consistente' uno de los controles de seguridad de la información, 'Hardening guidelines should be developed for all systems in use':

- Asegurar la correcta configuración de los servidores en el momento de su bastionado: configurados correctamente a nivel de seguridad (perfiles de seguridad) y libres de vulnerabilidades.
- Auditoria continua de los servidores existentes para asegurar que siguen libres de vulnerabilidades y la configuración de los parámetros de seguridad sigue alineada con los perfiles predefinidos. Actualmente existen unos 100 servidores virtuales (85% Windows server, 15% distribuciones Linux)

**Solución Actual:** Actualmente la necesidad/control no se está realizando, por lo que urge la implementación del mismo. Anteriormente se utilizaba la solución de Microsoft MBSA, pero esta solución ha sido discontinuada por Microsoft.

En cualquier caso, validar el bastionado de servidores y la auditoria continua de los mismos con MBSA suponía una carga de trabajo elevada y no se cubrían todas las necesidades (No se controlaban los servidores Linux y no se controlaban las vulnerabilidades)

**Resultados a Obtener:** Dada la extensión y variedad de servidores en la empresa, en este TFM no se pretende realizar el desarrollo completo de este control de seguridad. El resultado principal tendría que ser la definición del proceso y la elección de la solución para la implementación del control de 'servers hardening' mediante la **elaboración de un prototipo con un grupo reducido de servidores.**

## 1.2 Objetivos del Trabajo

- Obtener conocimiento de las especificaciones SCAP para la automatización del control de las configuraciones o perfiles de seguridad de los servidores (tanto en el momento del bastionado como durante su vida útil):
- Obtener conocimiento de soluciones en el mercado que pueden trabajar con el protocolo SCAP
- Utilización especificaciones y soluciones SCAP para el control de la configuración de los servidores según las normas de seguridad de la empresa.
- Utilización soluciones SCAP para el control de vulnerabilidades de los servidores.
- Validación que las soluciones SCAP permiten cubrir de forma satisfactoria y fiable el control de seguridad 'Hardening guidelines should be developed for all systems in use'.

## 1.3 Enfoque y método seguido

Para realizar este TFM uno de los puntos clave será la selección de las soluciones que puedan trabajar con protocoles SCAP.

Básicamente hay dos posibilidades:

- Utilizar una solución de distribución libre (OpenSCAP)
- Utilizar una solución comercial de pago.

En este caso, realizado un primer estudio de mercado, se llegan a las siguientes conclusiones que nos permitirán definir la estrategia para este TFM:

- La solución OpenSCAP permite cubrir todas las necesidades relacionadas con SCAP, pero la ejecución en un entorno con múltiples servidores es complicada por la carga de trabajo o dificultad de automatización
- Las soluciones comerciales, aportan un extra referente a la implantación en entornos con múltiples servidores. Las soluciones más evolucionadas añaden cuadros de mandos que permiten mayor control y un registro histórico en el tiempo de la evolución de la seguridad de los servidores y de las acciones realizadas.

Por lo explicado anteriormente, se decide realizar este TFM con dos soluciones SCAP:

- OpenSCAP: Se considera interesante a nivel del conocimiento que puede aportar la solución de distribución libre. Seguramente alguna de sus herramientas puede ser de utilidad (como la de edición de ficheros de reglas SCAP)
- Una solución comercial: Se realizará un estudio de mercado para seleccionar la solución que parezca más interesante por su equilibrio entre funcionalidades y precio. La empresa tiene un remanente de la partida presupuestaria para temas de seguridad que será utilizada para este propósito.

## 1.4 Planificación del Trabajo

**RECURSOS**: Los recursos principales que serán necesarios para el desarrollo de este TFM, serán los sistemas donde instalar las distintas soluciones y herramientas SCAP. Como mínimo un sistema Windows y otro Linux. En fases adelantadas del proyecto quizás serán necesarios otros sistemas o servidores para probar la validación de servidores durante su bastionado.

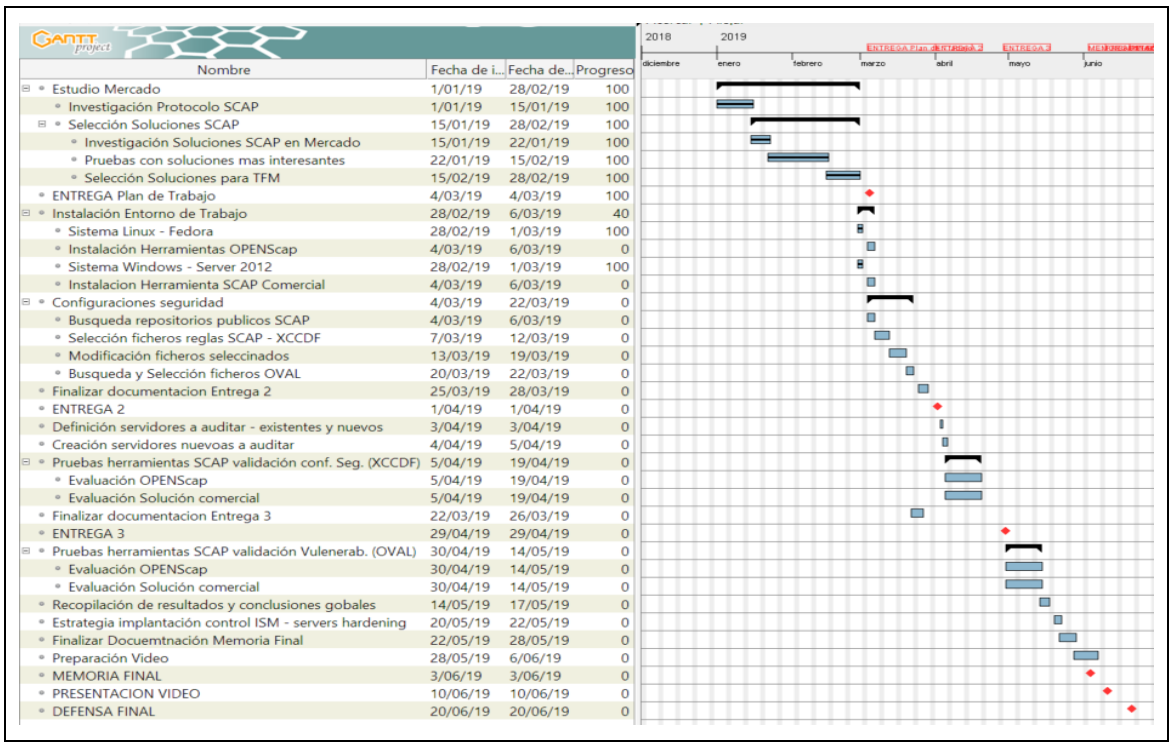
En cualquier caso, todos los sistemas necesarios se crearán en la granja VMWARE de la empresa ubicada en data center propio. La mayoría de los servidores de la empresa están replicados en un data center secundario (como parte del DRP). Estos servidores se crearán en un volumen especifico que no ser replica en el data center secundario.

- Sistema LINUX: Pendiente decidir si se usa CentOS o se escoge Fedora 29 Workstation, en función de las funcionalidades OpenSCAP que permita ejecutar cada sistema
- Sistema Windows: Microsoft Windows Server 2012 R2 (64-bit)

**TAREAS:**

- Estudio de Mercado y selección de las soluciones SCAP a utilizar durante el TFM. (*Nota: Este estudio se ha realizado durante los meses de enero y febrero una vez ya se había confirmado la adjudicación del TFM*)
- Obtención especificaciones de seguridad SCAP para la empresa:
    - Definición de las reglas de seguridad que tienen que cumplir los servidores empresariales (basadas en las políticas de seguridad corporativas)
    - Búsqueda y selección de grupos de reglas de seguridad más apropiadas para auditar los servidores de la empresa. Se utilizarán repositorios públicos como 'NIST' donde encontrar las reglas de Seguridad (Ficheros XCCDF) que se acerquen más a los requerimientos de Seguridad definidos por las políticas corporativas y la tipología de servidores existentes.
    - Edición de las reglas seleccionadas para ajustarlas a las necesidades propias de la empresa.
- Búsqueda y selección de ficheros OVAL con definiciones de vulnerabilidades para testear soluciones SCAP
- Pruebas con OpenSCAP y con la solución SCAP comercial seleccionada:
    - Definición servidores a auditar (existentes y nuevos)
    - Instalación y configuración Herramientas OpenSCAP
    - Instalación y configuración Solución Scap comercial
    - Validación servidores Nuevos y existentes contra reglas de Seguridad (XCCDF) y posibles vulnerabilidades (OVAL)
- Conclusiones: Recopilación de los resultados, y decisiones estratégicas para la implantación del control de seguridad al resto de servidores de la empresa:

**Programación de Tareas:** A continuación, se presenta un diagrama Gantt con la programación de Tareas



| Nombre | Fecha de i... | Fecha de... | Progreso |
|---|---|---|---|
| Estudio Mercado | 1/01/19 | 28/02/19 | 100 |
| Investigación Protocolo SCAP | 1/01/19 | 15/01/19 | 100 |
| Selección Soluciones SCAP | 15/01/19 | 28/02/19 | 100 |
| Investigación Soluciones SCAP en Mercado | 15/01/19 | 22/01/19 | 100 |
| Pruebas con soluciones mas interesantes | 22/01/19 | 15/02/19 | 100 |
| Selección Soluciones para TFM | 15/02/19 | 28/02/19 | 100 |
| ENTREGA Plan de Trabajo | 4/03/19 | 4/03/19 | 100 |
| Instalación Entorno de Trabajo | 28/02/19 | 6/03/19 | 40 |
| Sistema Linux - Fedora | 28/02/19 | 1/03/19 | 100 |
| Instalación Herramientas OPENScap | 4/03/19 | 6/03/19 | 0 |
| Sistema Windows - Server 2012 | 28/02/19 | 1/03/19 | 100 |
| Instalacion Herramienta SCAP Comercial | 4/03/19 | 6/03/19 | 0 |
| Configuraciones seguridad | 4/03/19 | 22/03/19 | 0 |
| Busqueda repositorios publicos SCAP | 4/03/19 | 6/03/19 | 0 |
| Selección ficheros reglas SCAP - XCCDF | 7/03/19 | 12/03/19 | 0 |
| Modificación ficheros seleccinados | 13/03/19 | 19/03/19 | 0 |
| Busqueda y Selección ficheros OVAL | 20/03/19 | 22/03/19 | 0 |
| Finalizar documentacion Entrega 2 | 25/03/19 | 28/03/19 | 0 |
| ENTREGA 2 | 1/04/19 | 1/04/19 | 0 |
| Definición servidores a auditar - existentes y nuevos | 3/04/19 | 3/04/19 | 0 |
| Creación servidores nuevoas a auditar | 4/04/19 | 5/04/19 | 0 |
| Pruebas herramientas SCAP validación conf. Seg. (XCCDF) | 5/04/19 | 19/04/19 | 0 |
| Evaluación OPENScap | 5/04/19 | 19/04/19 | 0 |
| Evaluación Solución comercial | 5/04/19 | 19/04/19 | 0 |
| Finalizar documentacion Entrega 3 | 22/03/19 | 26/03/19 | 0 |
| ENTREGA 3 | 29/04/19 | 29/04/19 | 0 |
| Pruebas herramientas SCAP validación Vulenerab. (OVAL) | 30/04/19 | 14/05/19 | 0 |
| Evaluación OPENScap | 30/04/19 | 14/05/19 | 0 |
| Evaluación Solución comercial | 30/04/19 | 14/05/19 | 0 |
| Recopilación de resultados y conclusiones gobales | 14/05/19 | 17/05/19 | 0 |
| Estrategia implantación control ISM - servers hardening | 20/05/19 | 22/05/19 | 0 |
| Finalizar Docuemtnación Memoria Final | 22/05/19 | 28/05/19 | 0 |
| Preparación Video | 28/05/19 | 6/06/19 | 0 |
| MEMORIA FINAL | 3/06/19 | 3/06/19 | 0 |
| PRESENTACION VIDEO | 10/06/19 | 10/06/19 | 0 |
| DEFENSA FINAL | 20/06/19 | 20/06/19 | 0 |

### 1.5 Productos obtenidos

En este Trabajo final de Master se realizan dos entregables principales: La memoria final y una presentación en formato video. Para un mayor control del trabajo se realizan también unos entregables parciales utilizando el formato de la memoria final.

- **Entrega 1:**
  - Capítulo 1: Plan de trabajo con su calendario de actividades.
  - Capítulo 2: Investigación del protocolo SCAP y de las soluciones de mercado disponibles para la evaluación de seguridad de servidores mediante protocolo SCAP.
- **Entrega 2:**
  - Capítulo 3: Búsqueda de repositorios con configuraciones de Seguridad SCAP. Selección de ficheros (XCCDF) con configuraciones de seguridad a utilizar para la validación de servidores. Modificación de los ficheros XCCDF para que incluyan las configuraciones de seguridad definidas por la política corporativa empresarial.
- **Entrega 3:**
  - Capítulo 4: Validación de la configuración de seguridad de los servidores con las soluciones seleccionadas (Nessus y OpenSCAP) y los ficheros XCCDF con la configuración de seguridad definida previamente.
  - Capítulo 5: Implementación automatizada y centralizada de las políticas y configuraciones de seguridad mediante GPO del Controlador de Dominio empresarial.
  - Capítulo 6: Búsqueda de servidores con vulnerabilidades de seguridad por versiones de sistema operativo o software obsoletas
- **Entrega 4:** Memoria Final, a la que se añaden
  - Capítulo 7: Evaluación de la posibilidad de utilizar los procedimientos y soluciones utilizados en este TFM para evaluar la seguridad del parque de ordenadores personales de la empresa.
  - Resumen del trabajo y las conclusiones globales
- **Entrega 5:** Video con audio: Presentación resumen (Power Point) del TFM que incluye alguna demostración de las soluciones implementadas.

# 2. Estudio de Mercado

### 2.1 Protocolo SCAP (Security Content Automation Protocol)

[1] SCAP) es un conjunto de especificaciones para la automatización del control de seguridad de los sistemas informáticos, es utilizado básicamente para:

- Evaluar el cumplimiento de la configuración de seguridad de los sistemas según determinadas reglas
- Detectar la presencia de versiones vulnerables de software.

El mismo contenido de SCAP puede ser usado por distintas herramientas o soluciones para realizar una evaluación de cumplimiento o detección de vulnerabilidades descrita por el contenido.

Versiones: En estos momentos la última versión de especificaciones es la SCAP 1.3 liberada el 14/02/2018. (de todas formas, la mayoría de especificaciones que se pueden encontrar en repositorios públicos están definidas en SCAP 1.2) La primera versión es la SCAP 1.0 liberada el 28/04/2011.

Ya se está trabajando en la versión SCAP 2.0. Una de las principales novedades es la inclusión explicita de equipos de red, IoT, dispositivos móviles y la automatización de recopilación de información de los mismos.

### 2.2 Especificaciones SCAP:

SCAP incluye varias especificaciones. Para este proyecto nos centraremos y utilizaremos básicamente las dos primeras (XCCDF y OVAL):

- Extensible Configuration Checklist Description Format (XCCDF): es un lenguaje de especificación para escribir listas de verificación de seguridad. Un documento XCCDF representa una colección estructurada de reglas de configuración de seguridad para algún conjunto de sistemas de destino. La especificación está diseñada para admitir el intercambio de información, la generación de documentos, las pruebas de cumplimiento automatizadas y la calificación del cumplimiento. La especificación también define un modelo de datos y un formato para almacenar los resultados de las pruebas de conformidad de referencia. La intención de XCCDF es proporcionar una base uniforme para la expresión de listas de verificación de seguridad, puntos de referencia y otras pautas de configuración, y así fomentar una aplicación más generalizada de buenas prácticas de seguridad.
- Open Vulnerability Assesment Language (OVAL): [3] El lenguaje estandariza los tres pasos principales del proceso de evaluación: representación de la información de la configuración de los sistemas para pruebas; analizar el sistema para detectar la presencia de estados específicos (vulnerabilidad, configuración, estado de parche, etc.); y reportando los resultados de esta evaluación.
- Common Platform Enumeration (**CPE**): es un método estandarizado para describir e identificar las clases de aplicaciones, sistemas operativos y dispositivos de hardware presentes entre los activos informáticos de una empresa.

- **Asset Identification**: Esta especificación proporciona las construcciones necesarias para identificar de forma única los activos en función de identificadores conocidos y / o información conocida sobre los activos.
- Asset Reporting Format **(ARF):** Es un modelo de datos para expresar el formato de intercambio de información sobre activos.
- Open Checklist Interactive Language **(OCIL):** Define un marco para expresar un conjunto de preguntas que se presentarán a un usuario y los procedimientos correspondientes para interpretar las respuestas a estas preguntas. Aún que este estándar puede ser utilizado para interactuar con el usuario en cualquier campo, en el caso de la automatización de la seguridad puede ser utilizado para ayudar a manejar los casos en que los idiomas de verificación de nivel inferior, como OVAL, no pueden automatizar una verificación en particular.
- Software Identification **(SWID)** Tagging: Las etiquetas SWID proporcionan una manera transparente para que las organizaciones rastreen el software instalado en sus dispositivos administrados.
- Trust Model for Security Automation Data **(TMSAD):** Se compone de recomendaciones sobre cómo utilizar las especificaciones existentes para representar firmas, hashes, información clave e información de identidad en el contexto de un documento XML dentro del dominio de automatización de seguridad.

### 2.3 Soluciones que pueden trabajar con SCAP

Para el desarrollo de este proyecto, es importante identificar que productos y soluciones pueden trabajar con las especificaciones SCAP.

El NIST (National Institute of Stnadards and Technology) tiene un programa para validar y probar los productos para el uso de las características y funcionalidades de SCAP. [4] Actualmente la lista de productos validos por este programa no es muy extensa y se puede consultar en la página web de NIST.

### 2.4 Selección de las soluciones/ productos a utilizar en este TFM:

Durante los meses de enero y febrero se ha realizado un estudio de la mayoría de herramientas SCAP validadas por NIST. Dado que la mayoría de productos son comerciales, se han utilizado versiones de prueba (con licencia temporal). No ha sido posible evaluar todos los productos listados por NIST por diversos motivos: en algunos casos no se han conseguido productos de evaluación, en otros casos por limitación de tiempo y la complejidad de configurar el entorno de evaluación. A continuación (Siguiente página), se presenta una tabla con los productos evaluados y principales conclusiones.

Finalmente se decide utilizar para este TFM las siguientes soluciones:

- Nessus profesional: Se selecciona por su facilidad de uso para cualquier plataforma a auditar, precio asumible e independiente del número de plataformas a auditar. Se valora la posibilidad futura de ampliar a Nessus security center (mayor coste), pero que aporta cuadro de mandos con el estado de los sistemas y el histórico de la evolución de la seguridad de los mismos.
- OPENScap: Se selecciona por ser de uso libre. Interesa ver que pueden aportar sus herramientas. Se intentará aplicarla también al entorno Windows

| Producto | Seleccionado | Licencia | Primeras conclusiones con pruebas básicas |
|---|---|---|---|
| **Rapid7 Nexpose** | **NO** | Mínimo 3.500 $ anuales para 128 ips. | Funcionalidades:<br>Escaneo de Vulnerabilidades continuo con asignación prioridades según riesgo<br>Monitorización de nuevos dispositivos conectados a la red<br>Escaneo de políticas (hardening)<br>Cuadro de mandos e Informes de acciones de remediación priorizados<br>Validado por NIST en plataformas Windows y Red HAT. Se descarta por precio |
| **OPENSCAP** | **SI** | Distribución Libre | Funcionalidades: Set de herramientas de distribución libre que permite:<br>Validación cumplimiento seguridad (escaneo de políticas)<br>Escaneo de Vulnerabilidades<br>Pensada básicamente para entornos evaluar y auditar entornos LINUX. Tiene múltiples sets de políticas de LINUX para auditar sistemas. No tiene funcionalidades de cuadro de mandos, automatizaciones.<br>NIST solo lo ha testeado en plataformas RedHAT.<br>Se selecciona por ser de uso libre. Interesa ver que nos puede aportar sus herramientas. Intentaremos aplicarla también al entorno Windows.<br>Las primeras pruebas en entorno LINUX sorprenden por la facilidad de uso y tener también entornos con GUI. |
| **THREATGUARD** | **NO** | 3.600 $ anuales por 200 ips | Funcionalidades:<br>Escaneo de Vulnerabilidades continuo con asignación prioridades según riesgo<br>Escaneo de políticas (hardening)<br>Monitorización y escaneo de nuevos dispositivos conectados a la red<br>Cuadro de Mandos con acciones a realizar y tendencias<br>La solución es fácil de entender y ejecutar (comprobación políticas y escaneo vulnerabilidades). Validado por NIST en |

| | | | |
|---|---|---|---|
| | | | plataformas Windows y Red HAT. Finalista, aún que al final se selecciona Nessus. Sin la parte de consolidación (cuadro de mandos) se prefiere Nessus. La parte de consolidación se licencia por IPs y dispara el precio. |
| **IBM BigFix** | **NO** | | Funcionalidades:<br>Escaneo de Vulnerabilidades continuo<br>Escaneo de políticas (hardening)<br>Monitorización y escaneo de nuevos dispositivos conectados a la red<br>Acciones automatizadas para remediación<br>Se ha contactado con IBM, pero no se ha conseguido versión de prueba. Aún que tenemos el producto a nivel corporativo para distribución de parches de seguridad, los responsables corporativos nos han notificado que no hay planes de añadir la parte de cumplimiento (XCCDF) |
| **SPAWAR** | **NO** | | Restringida a organizaciones gubernamentales de USA. |
| **MS SYSTEM CENTER** | **NO** | | Funcionalidades en entorno Microsoft:<br>Escaneo de políticas (hardening) y vulnerabilidades<br>Monitorización y escaneo de nuevos dispositivos conectados a la red<br>Acciones automatizadas para remediación y aplicación de las políticas de seguridad<br>Se descarta por el coste licenciamiento, y el solape con IBM Big fix para la distribución de software i parches seguridad. |
| **QUALYS SCAP AUDITOR** | **NO** | | Funcionalidades:<br>Escaneo de Vulnerabilidades<br>Escaneo de políticas (hardening)<br>Cuadro de Mandos con acciones a realizar y tendencias<br>Realiza la prueba con versión de Demo, se descarta por su complejidad de configuración y uso |
| **Nessus** | **SI** | 2.300 $ anuales sin | Funcionalidades: |

| | | | |
|---|---|---|---|
| | | limite ips. | Escaneo de Vulnerabilidades<br>Escaneo de políticas (hardening)<br>Nessus es una solución pensada sobre todo para auditores. En la prueba se confirma que es muy fácil e intuitiva de utilizar y genera unos informes muy entendibles. (De hecho, son calcados a informes que nos han entregado en algunas auditorias de seguridad externas).<br>Tiene una solución tenable.sc (de mayor coste) que incluye cuadro de mandos y permite comprobar evolución seguridad de los activos y priorizar las acciones.<br>Se selecciona el producto Nessus por su facilidad de uso para cualquier plataforma a auditar. Si hay presupuesto en el futro se plantearía el tenable.sc que contiene cuadro de mandos con evolución seguridad equipos. |
| **BMC SERVER AUTOAMTION** | **NO** | | Se contacta con agente. Es una solución para automatización y cuadro de Mandos. Necesita otras soluciones por debajo como MS SCCM, Nessus u otros productos de BMC. Se descarta por complejidad y precio. |

### 2.5 Conclusiones

1. Se confirma que el protocolo SCAP es útil para la implementación del control de seguridad 'servers hardening', en concreto sus especificaciones 'Extensible Configuration Checklist Description Format (XCCDF)' que nos permiten definir configuraciones y evaluaciones de seguridad y 'Open Vulnerability Assesment Language (OVAL)' que permite analizar el sistema para detectar la presencia del estados específicos (vulnerabilidad, configuración, estado del parche, etc.); y reportando los resultados de esta evaluación.
2. Se decide utilizar las soluciones OpenSCAP y NESSUS profesional para evaluar los sistemas empresariales con el protocolo y especificaciones SCAP.

# 3. Obtención Especificaciones de seguridad SCAP.

### 3.0 Objetivo:

El objetivo de este capítulo es la obtención de las especificaciones de seguridad SCAP a utilizar en el bastionado y auditoria de los servidores empresariales. Para ello hay que trabajar básicamente en dos puntos:

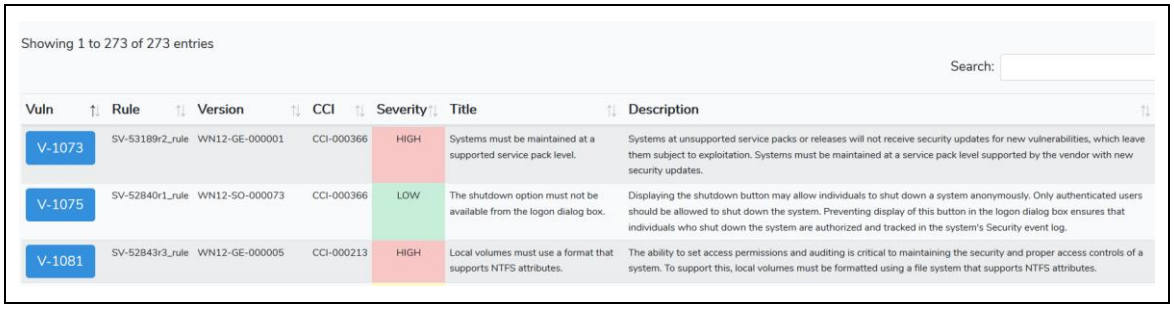
- Definición de las reglas de seguridad que tienen que cumplir los servidores empresariales (basadas en las políticas de seguridad corporativas)
- Búsqueda de grupos de reglas de seguridad SCAP estándares que se puedan adaptar fácilmente a las necesidades empresariales.

### 3.1 Búsqueda repositorios de especificaciones de seguridad SCAP/XCCDF.

Se inicia una búsqueda de repositorios de ficheros XCCDF. Un documento XCCDF representa una colección estructurada de reglas de configuración de seguridad para un sistema determinado.

Sorprende que hay pocos repositorios públicos con documentos XCCDF, y el contenido de los mismos es prácticamente el mismo. A continuación, destaco los principales repositorios encontrados. Durante el proyecto en principio se utilizará el primer repositorio (NIST), por estar más actualizado y ser más amigable de utilizar.

- https://nvd.nist.gov/ncp/repository:buen buscador y con distintos filtros y más actualizado.
- https://cyber.trackr.live/scap: muestra lo mismo que en el repositorio de NIST pero con actualizaciones periódicas. El buscador tiene menos opciones. Como punto fuerte para cada fichero XCCDF tiene un visualizador que permite ver, ordenar o buscar reglas específicas.




- OPENSCAP (políticas LINUX): Una vez instalado el producto, en un directorio local (/usr/share/xml/scap/ssg/content/) se pueden encontrar distintos ficheros XCCDF para diversas distribuciones LINUX.

### 3.2 Definición de las reglas de seguridad que tienen que cumplir los servidores empresariales W2012

En este caso se realiza la investigación para definir las reglas de seguridad para los servidores empresariales Windows server 2012 y 2012 R2.

Más adelante se definirán, siguiendo la misma metodología, las reglas para los servidores Windows 2008R2 y Windows 2016.

Se investigan repositorios públicos para identificar guías de implementación de seguridad en sistemas. Se comprueba que en muchos casos se referencian las guías de implementación 'STIG' (Guías de implementación técnica de seguridad del departamento de defensa de USA).

Se decide utilizar estas guías pues marcan de forma muy clara la Prioridad de las reglas de seguridad (Alta o nivel I, Media o nivel II y Baja o nivel III).

Se han intentado consultar otras fuentes como CN-CERT (centro cristológico nacional), pero es necesario tener una subscripción para poder bajar las guías.

En el caso de Windows 12 se utiliza la guía STIG que se encuentra en 'Cyber Track' [5]. En ella se encuentran definidas 273 reglas de seguridad: 27 de categoría 1, 198 de categoría 2, 48 de categoría 3.

Finalmente, para definir las reglas a comprobar en el bastionado de servidores y en la auditoria continua a nivel empresarial se decide:

- Incorporar todas las reglas de seguridad críticas que son 27 (Categoría Alta o nivel 1).
- Añadir algunas reglas adicionales para cumplir con las reglas de seguridad definidas en la política corporativa de la empresa. Se repasan el resto de reglas de categoría 2 y 3, y se seleccionan las necesarias (24).

Una vez realizado el proceso se seleccionan las 51 reglas listadas en la siguiente tabla:

| Regla | Política |
|---|---|
| SV-53189r2 | El service pack tiene que estar oficialmente soportado por MS. (MS sigue emitiendo parches de seguridad para el Service Pack activo) |
| SV-52843r3 | Los volúmenes locales tienen que soportar atributos NTFS (para garantizar el control apropiado de acceso y seguridad) |
| SV-52847r1 | Restricción para evitar que un anonymous logon pueda listar recursos del sistema (cuentas y shares) |
| SV-52108r3 | No se debe asignar a ninguna cuenta la propiedad de actuar como parte del sistema operativo |
| SV-52864r3 | El acceso anónimo al 'registro' del sistema tiene qu estar restringido |
| SV-52865r1 | La autenticación 'LanMan' se tiene que configurar para usar solo el protocolo NTLMv2, prohibiendo protocolos menos seguros como NTLM o LM |
| SV-52880r1 | Se tiene que deshabilitar la encriptación 'reversible' de password, por ser muy poco segura |

| | |
|---|---|
| SV-52879r2 | Autoplay tiene que estar deshabilitado. (es un riesgo y no tiene ningún sentido en un servidor) |
| SV-51138r2 | Acceso anónimo a los 'Named Pipes' tiene que estar restringido |
| SV-52883r2 | Acceso remoto a los directorios donde está el registry tiene que estar restringido |
| SV-52884r1 | Acceso anónimo a las carpetas compartidas tiene que estar restringido |
| SV-52885r1 | La solicitud de asistencia remota tiene que estar deshabilitada |
| SV-52886r1 | No se pueden permitir cuentas locales sin password |
| SV-52892r2 | Evitar que el sistema almacene el HASH del LAN Manager password |
| SV-52931r2 | Acceso no autorizado remoto a los carpetas y sub carpetas donde está el registro de windows tiene que estar deshabilitado |
| SV-52937r1 | Acceso anónimo a los 'Named Pipes' y carpetas compartidas tiene que estar deshabilitado |
| SV-51175r3 | Permisos apropiados para los ficheros del directorio de ficheros. |
| SV-52115r3 | Los programas de debug solo tienen que poderse ejecutar con usuario administrador |
| SV-53126r2 | Autoplay se tiene que deshabilitar para cualquier recurso que no sea un volumen de sistema |
| SV-53124r2 | Por defecto el comportamiento 'autorun' se tiene que configurar para evitar comandos autorun |
| SV-53123r4 | Los usuarios estándar (no administrador) solo tienen que tener permisos de lectura al registry WINLOGON |
| SV-53122r1 | No se tiene que permitir el listado des de conexión anónima de las cuentas del sistema |
| SV-52113r3 | El permiso de crear 'objetos token' no tiene que ser asignado a ningún grupo de usuarios |
| SV-52956r3 | Los usuarios estándar (no administrador) solo tienen que tener permisos de lectura a la sección del registry (active setup / installed componenets) |
| SV-52954r1 | La opción que el instalador de windows siempre instale con privilegios 'elevados' se tiene que estar deshabilitada |
| SV-51752r1 | EL cliente de Windows remote Management no tiene que utilizar autentificación básica |
| SV-51755r2 | EL Servicio de Windows remote Management no tiene que utilizar autentificación básica |
| SV-52848r1 | Limite número passwords incorrectos |
| SV-52849r2 | Reseteo contador passwords fallidos como mínimo 15 minutos |
| SV-52850r2 | Desbloqueo automático cuenta (cuando habilitado) por passwords fallidos no inferior a 15 minutos |
| SV-52851r1 | Duración máxima password |

| | |
|---|---|
| SV-52852r1 | Duración mínima password |
| SV-52863r2 | Política complejidad de password tiene que estar activada |
| SV-52855r1 | Cuenta invitado tiene que estar deshabilitada |
| SV-52930r1 | Una vez salta el protector de pantalla, al cabo de pocos segundos se tiene que pedir contraseña para quitar el protector de pantalla |
| SV-52938r2 | Longitud mínima passwords |
| SV-52941r1 | No presentar el ultimo usuario que ha accedido en la pantalla de logon. |
| SV-53129r1 | Deshabilitar logs del acceso a objetos globales del sistema, para evitar excesivos logs. |
| SV-52943r1 | Deshabilitar logs para cada fichero que se hace backup o restore, para evitar excesivos logs. |
| SV-52947r1 | En caso petición elevación, se generará dialogo para confirmación del administrador |
| SV-52949r1 | En caso detección instalación aplicaciones, el sistema tiene que pedir la confirmación elevación privilegios y credenciales de cuenta con derechos adminstrador |
| SV-52958r1 | No permitir grabar password en escritorio remoto |
| SV-53014r2 | No permitir un network bridge (puente) |
| SV-53132r1 | Es necesario autentificarse al despertar el sistema. |
| SV-52236r2 | El servicio de FAX tiene que estar deshabilitado si está instalado |
| SV-52237r4 | El servicio de FTP tiene que estar deshabilitado si está instalado ( a no ser que sea necesario) |
| SV-52238r2 | El servicio de pear networking tiene que estar deshabilitado si está instalado |
| SV-52239r2 | El servicio simple TCP tiene que estar deshabilitado si está instalado |
| SV-52240r2 | El servicio simple Telnet tiene que estar deshabilitado si está instalado |
| SV-51609r2 | El acceso a la tienda windows tiene que estar deshabilitado |
| SV-51747r4 | Windows SmartScreen tiene que estar activo |

### 3.3 Configuración del fichero XXCDF con la selección de grupos de reglas de seguridad más apropiadas para auditar los servidores de la empresa.

Una vez definidas las reglas de seguridad STIG a utilizar para auditar los servidores de la empresa, se procede a descargar el fichero XCCDF con todas las 262 reglas especificadas por STIG para Windows server 2012/R2.

Se utiliza el mismo fichero XCCDF disponible en misma página de cyber trackr [5] donde están descritas todas las reglas:
U_MS_Windows_2012_and_2012_R2_MS_V2R15_STIG_SCAP_1-2_Benchmark.xml.

Antes de poder editar el fichero XCCDF V2R15, para añadir el perfil de seguridad 'profile' con las 51 reglas a auditar, se necesita comprender la estructura básica del lenguaje XCCDF.

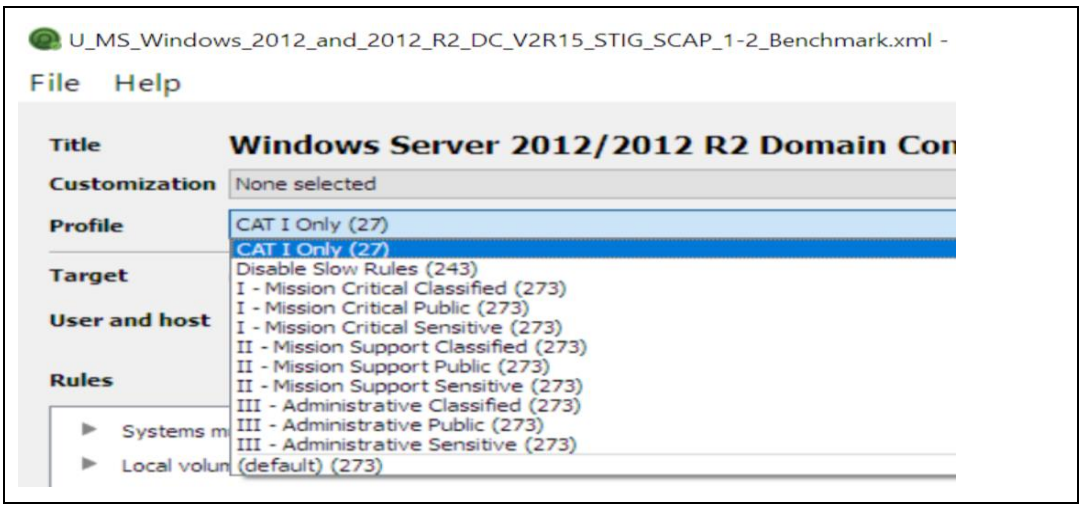
#### 3.3.1 Estructura Básica fichero XCCDF [6][7]

El fichero XCCDF es un fichero estructurado en 'xml'. Para personalizar este fichero es importante conocer al menos tres tipos de secciones que nos encontraremos en el: reglas (rules), parámetros (values) y perfiles (profiles)

- **Reglas y Grupos de Reglas** (rules & groups): Las reglas son cada una de las validaciones específicas de seguridad a realizar. Por ejemplo, comprobar que el sistema tiene un Service Pack aun soportado por el fabricante. Las reglas tienen algunos parámetros importantes:
    - Severity: Nos dice el nivel del riesgo en caso de no cumplir la regla (Nivel High o 1, Medium o 2, Low o 3)
    - Selected: Si por defecto se validará la regla o no. En el fichero V2R15 este parámetro no está informado y todas las reglas se ejecutan por defecto.
    - Groups: Un grupo puede contener varias reglas. Esto permite des de un perfil incluir reglas específicas o todo un grupo de reglas. En el caso del fichero V2R15 curiosamente cada uno de los grupos contienen únicamente regla.
- **Perfiles (Profiles):** Incluyen todas las reglas o grupos de reglas a validar. Es decir, si un fichero xccdf contiene 200 reglas de seguridad, podemos crear un perfil que incluya un sub-conjunto especifico de estas 200 reglas. Un fichero xccdf puede contener varios perfiles.

  Esto permite tener perfiles diferentes de seguridad (cada uno con sus reglas) en función del tipo del sistema o servidor a validar.

  **Como ejemplo** en el fichero xccdf publicado en NIST para Windows 2012: U_MS_Windows_2012_and_2012_R2_MS_V2R15_STIG_SCAP_1-2_Benchmark.xml se definen varios perfiles:
    - Perfil con las reglas de nivel 1 (High) – 27 reglas seleccionadas
    - Perfil con todas las reglas a excepción de las que toman un tiempo largo en su evaluación (slow) – 243 reglas seleccionadas.
    - Varios Perfiles en función del uso del servidor: con información clasificada, sensible y publica combinado con la importancia del servidor (critico o soporte). Curiosamente todos estos perfiles tienen todas las reglas disponibles seleccionadas (273).




- **Parámetros (Values):** Los parámetros son utilizados por las reglas para evaluar determinadas especificaciones de seguridad. Por ejemplo, para especificar los segundos que pasan des de que se activa el protector de pantalla hasta que se activa la protección con password.

  Si, utilizamos un parámetro, cada **perfil** puede definir un valor especifico de este parámetro para que se evalúe la regla seleccionada con el valor determinado. En este caso, en un perfil concreto, podríamos especificar un valor en segundos para este parámetro (value), o podríamos utilizar alguno de sus valores opcionales predefinidos (selectors)

```
<xccdf:Value id="xccdf_mil.disa.stig_value_screen_saver_grace_period_var" type="number" operator="equals">
  <xccdf:title>MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires
  (0 recommended)</xccdf:title>
  <xccdf:description>Setting Added to Registry to Make Screensaver Password Protection Immediate The default
  grace period allowed for user movement before the screen  saver lock takes effect is five seconds. Leaving
  the grace period in the default setting makes your computer vulnerable to a potential attack from someone
  walking up to the console to attempt to log onto the system before the lock takes effect. An entry to the
  registry can be made to adjust the length of the grace period.</xccdf:description>
  <xccdf:value>5</xccdf:value>
  <xccdf:value selector="zero_seconds">0</xccdf:value>
  <xccdf:value selector="5_seconds">5</xccdf:value>
</xccdf:Value>
```

### 3.3.2 Edición fichero XCCDF para incluir el perfil con las reglas de seguridad empresarial para servidores W2012

Se procede realizar una copiar del fichero STIG con las reglas para Windows 2012: U_MS_Windows_2012_and_2012_R2_MS_V2R15_STIG_SCAP_1-2_Benchmark.xml con el nombre: Mycompany_2012_Benchmark-xccdf para editarlo posteriormente añadiendo el perfil de seguridad empresarial (51 reglas seleccionadas)

Para editar el fichero se utiliza el programa notepad++

Se añade en el fichero xccdf un nuevo perfil nombrado
xccdf_mil.disa.stig_profile_MyCompany12

```
<xccdf:Profile id="xccdf_mil.disa.stig_profile_MyCompany12">
        <xccdf:title>My Company std server 2012-2012R</xccdf:title>
        <xccdf:description>This profile includes rules for my company
                        policy</xccdf:description>
```

Las 51 reglas seleccionadas, que se quieren incluir en el perfil de política empresarial incluyen las 27 reglas de nivel I. Por esto motivo se crea el perfil Mycompany12 en el fichero xml como una copia del perfil existente xccdf_mil.disa.stig_profile_CAT_I_Only.

En este fichero xccdf ninguna regla tiene el parámetro 'selected' informado. Ello quiere decir que, por defecto, en cualquier perfil se ejecutará cada una de las 273 reglas de seguridad presentes. Esto se comprueba en el perfil xccdf_mil.disa.stig_profile_CAT_I_Only que especifica 246 reglas que no hay que ejecutar (con lo que se ejecutaran las 27 reglas restantes)

```
<xccdf:Profile id="xccdf_mil.disa.stig_profile_CAT_I_Only">
  <xccdf:title>CAT I Only</xccdf:title>
  <xccdf:description>This profile only includes rules that are Severity Category I.</
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51140r3_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51141r2_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51142r2_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51143r2_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51144r1_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51145r1_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51146r1_rule" selected="false" />
  <xccdf:select idref="xccdf_mil.disa.stig_rule_SV-51147r1_rule" selected="false" />
```

Una vez copiado el perfil CAT_1_ONLY sobre el Mycompany12, se procede a añadir las 24 reglas faltantes. Para ello tendria dos opciones:

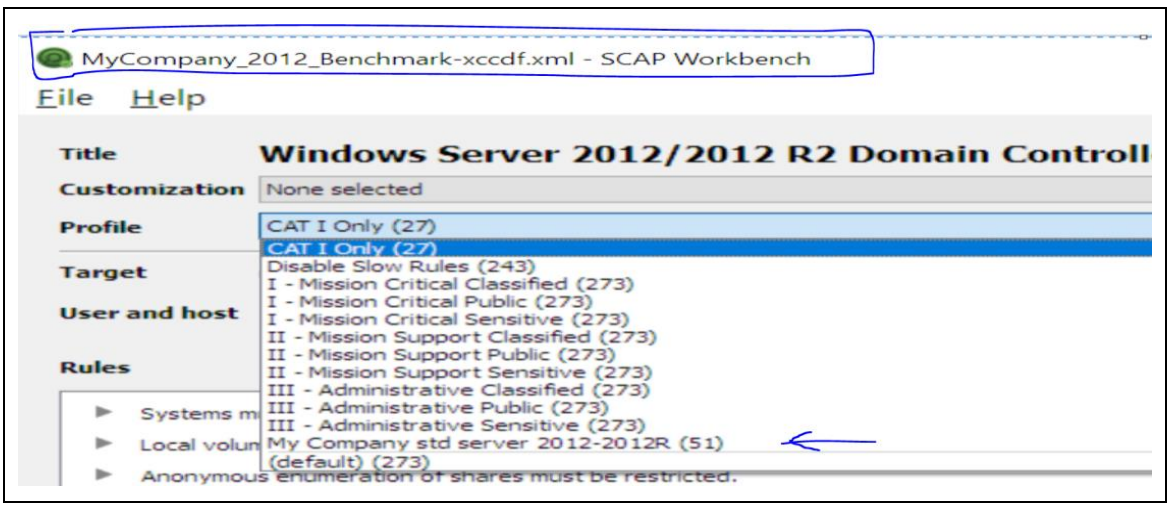
- Borrar en el perfil las líneas (con selected=false) de las 24 reglas adicionales que se quiere que se ejecuten
- Cambiar el parámetro (selected=true) en las 24 reglas adicionales.

En este caso se opta por la segunda opción que facilita encontrar de una forma rápida en el fichero xml las 24 reglas añadidas.

### 3.3.3 Comprobación correcta edición fichero XCCDF

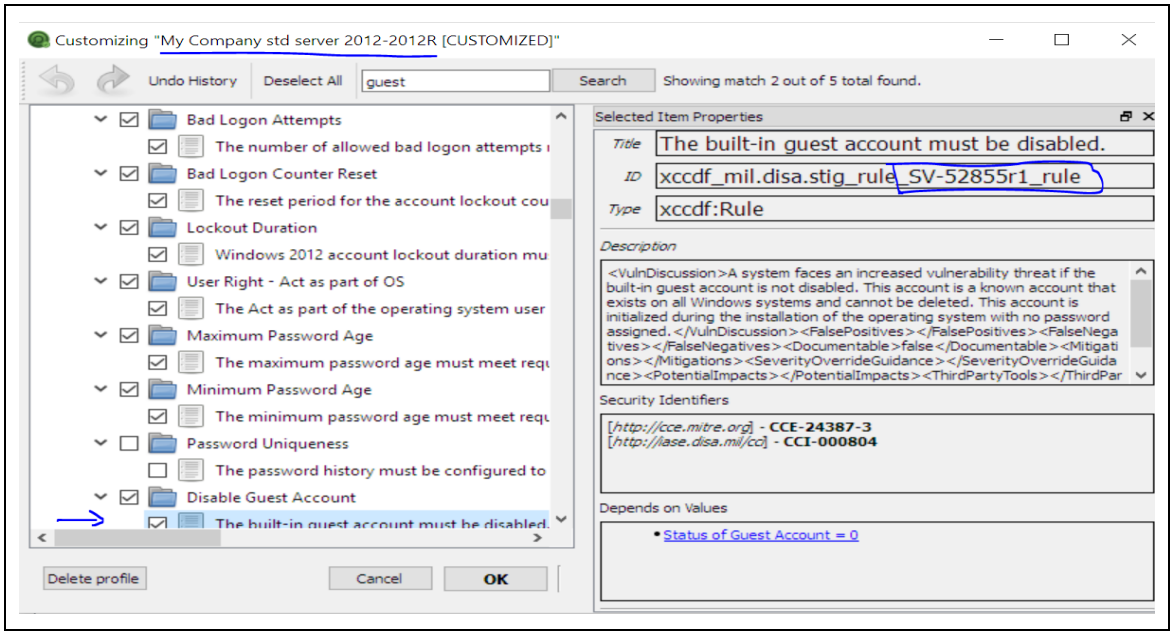
Para comprobar que se ha editado correctamente el fichero XCCDF Mycompany_2012_Benchmark-xccdf Incluyendo un nuevo perfil MyCompany12 que incluye las 51 reglas de seguridad empresarial, se procede a visualizarlo con la aplicación OpenSCAP Workbench.

Se comprueba que hay un nuevo perfil 'My Company std server' con 51 reglas de seguridad. *Nota: En este selector del OpenSCAP se muestra la descripción del perfil de seguridad y no su 'id' o nombre.*



Se entra en la opción para customizar el perfil Mycompany12 para comprobar que las 51 políticas son las deseadas. Por ejemplo, una de las políticas añadidas sobre las 27 de nivel 1, es la referente a las cuentas de invitados:

| | | |
|---|---|---|
| Política empresarial - cuentas invitado | xccdf_mil.disa.stig_rule_SV-52855r1_rule | Cuenta invitado tiene que estar deshabilitada |




### 3.4 Definición políticas de seguridad y ficheros XCCDF para servidores W2008 y W2016

Para el resto de sistemas operativos Microsoft instalados en los servidores de la empresa (Windows Server 2008/R2 y Windows Server 2016), se procede a realizar las mismas actividades ya realizadas para Windows Server 2012:

- Definición de las políticas de seguridad empresariales para cada versión de sistema operativo
- Selección y edición del fichero XCCDF para que contenga un perfil de seguridad 'MyCompany' con las políticas definidas.
- Validación del fichero.

Se realiza una búsqueda en los mismos repositorios utilizados anteriormente, Cyber Track y NIST, para localizar las últimas versiones de ficheros XCCDF con reglas de seguridad para W2008 y W2016.

En la siguiente tabla se detallan la versión seleccionada de fichero XCCDF para cada sistema operativo, y el número de reglas incluidas en cada uno de ellos.

| | Windows Server 2008 / 2008 R2 | Windows Server 2012 / 2012 R2 | Windows Server 2016 |
|---|---|---|---|
| Versión | V001.031R1 | V002.015R2 | V001.008R1 |
| Fecha Última versión | 26.10.2018 | 25.01.2019 | 25.01.2019 |
| Número reglas de Categoría 1 | 22 | 27 | 19 |
| Número Total de Reglas | 246 | 273 | 205 |

Windows 2012 / 2012 R2 es el que tiene más reglas de seguridad, y más reglas de seguridad de nivel 1.

1. Interpreto que en Windows server 2012 se añadieron diversas funcionalidades versus Windows server 2008 que obligaron a definir más reglas de seguridad para estas nuevas funcionalidades o características.
2. Interpreto que en Windows server 2016 se realizaron algunas decisiones a nivel de diseño para priorizar la seguridad, no siendo necesario en algunas áreas comprobar ciertas restricciones de seguridad que ya existen por diseño. Por ejemplo, los logs de sistema están más protegidos que en Windows 2012/R2, donde es importante implementar ciertas reglas o precauciones.

Posteriormente se procede a analizar las reglas de cada sistema operativo, para seleccionar las reglas necearías para cumplir la política empresarial (en cualquier caso, siempre se incluyen las reglas de categoría 1).

A continuación, se lista en una tabla comparativa el número de reglas de seguridad seleccionadas para cada sistema operativo, aplicando la misma filosofía: seleccionando las reglas de categoría 1 y añadiendo el resto de reglas necesario para cumplir la política de seguridad empresarial.

| | Windows Server 2008 / 2008 R2 | Windows Server 2012 / 2012 R2 | Windows Server 2016 |
|---|---|---|---|
| Número reglas de Categoría 1 | 22 | 27 | 19 |
| Reglas añadidas | 24 | 24 | 18 |
| Número Total de Reglas | 46 | 51 | 37 |

En el **ANEXO I** de esta memoria, se lista una tabla detallada con las reglas seleccionadas para cada sistema operativo. A continuación, se presentan algunos ejemplos para distintos grupos de reglas e seguridad.

- **Regla presente en todos los sistemas operativos**. En la categoría de cuentas y contraseñas se puede ver una regla de categoría 1, presente en los 3 sistemas operativos. La única diferencia, es la numeración de la regla en cada sistema operativo. Números más altos para sistemas operativos más modernos.

| Categoría | Regla W2008R2 | Regla W2012 | Regla W2016 | Política |
|---|---|---|---|---|
| Cuentas Y contraseñas | SV-32319r1_rule | SV-52892r2_rule | SV-88351r1_rule | Evitar que el sistema almacene el HASH del LAN Manager password |

- **Reglas presentes en todos los sistemas operativo, pero con distinta categoría.** Sorprende encontrar unos pocos casos en que la categoría de la regla es distinta. En Windows server 2012 y 2016 está definida como categoría 1, pero en Windows server 2008 está definida de categoría 2.

| Categoría | Regla W2008R2 | Regla W2012 | Regla W2016 | Política |
|---|---|---|---|---|
| Auto Play | SV-32460r1_rule | SV-53126r2_rule | SV-88209r1_rule | Autoplay deshabilitado para cualquier recurso que no sea un volumen de sistema. En Windows 2008R2 la regla no está marcada como de Nivel 1. |

- **Reglas no presentes en algún sistema operativo**. En algunos casos hay reglas de seguridad que no existen en Windows server 2016 porque el diseño de seguridad del sistema operativo ya no lo hace necesario. Este es el caso de la siguiente regla de permisos de acceso al registro de Windows.

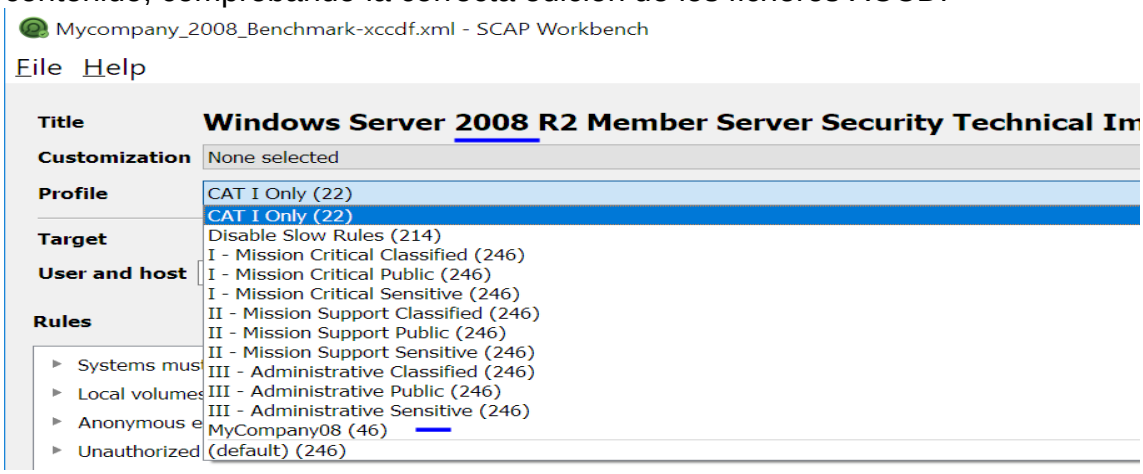
| Categoría | Regla W2008R2 | Regla W2012 | Regla W2016 | Política |
|---|---|---|---|---|
| Permisos Registro de windows | SV-33310r3_rule | SV-53123r4_rule | N/A | Los usuarios estándar (no administrador) solo tienen que tener permisos de lectura al registry WINLOGON |

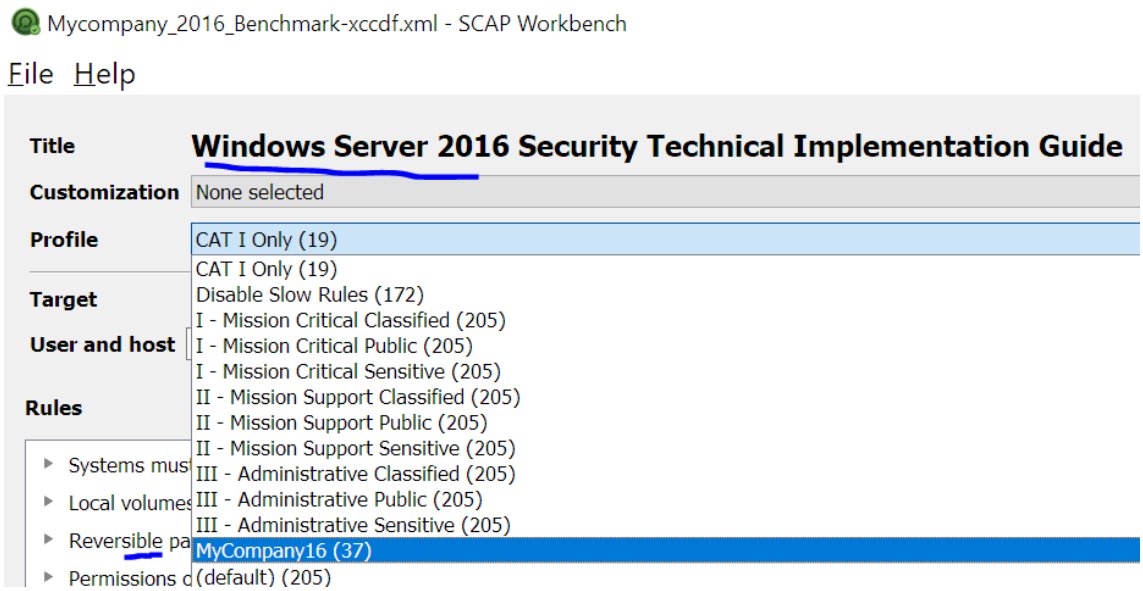
- Ejemplos categorías de reglas: A continuación, se listan ejemplos para las principales categorías de reglas incluidas en la política: Servicios innecesarios, accesos anónimos, cuentas y contraseñas, derechos de acceso, acceso remoto y 'debug & logs'.

| Categoría | Regla W2008R2 | Regla W2012 | Regla W2016 | Política |
|---|---|---|---|---|
| Servicios innecesarios | SV-33731r1_rule | SV-52239r2_rule | SV-87945r1_rule | El servicio de Simple TCP tiene que estar deshabilitado si está instalado (w2008 y w2012) / No tiene que estar instalado (W2016) |
| Permisos | SV- | SV- | SV- | Restricción para evitar que un |

| | | | | |
|---|---|---|---|---|
| accesos anónimos | 32283r1_rule | 52847r1_rule | 88333r1_rule | anonymous logon pueda listar recursos del sistema (cuentas y shares) |
| Cuentas Y contraseñas | SV-32369r1_rule | SV-52938r2_rule | SV-87973r1_rule | Longitud mínima passwords |
| Asignación Derechos de acceso | SV-32287r2_rule | SV-52108r3_rule | SV-88399r1_rule | No se debe asignar a ninguna cuenta la propiedad de actuar como parte del sistema operativo |
| Acceso Remoto | N/A | SV-51755r2_rule | SV-88263r1_rule | EL Servicio de Windows remote Management no tiene que utilizar autentificación básica |
| Debug y Logs | SV-32444r3_rule | SV-52115r3_rule | SV-88419r1_rule | Los programas de debug solo tienen que poderse ejecutar con usuario administrador |

**Edición ficheros XCCDF con las reglas y perfil empresarial:** Finalmente, para cada sistema operativo, se edita el fichero XCCDF seleccionado, añadiendo un perfil empresarial 'MyCompany' con las reglas de seguridad previamente seleccionadas. Con el OpenSCAP workbench se valida su contenido, comprobando la correcta edición de los ficheros XCCDF



### 3.5 Conclusiones

Se definen para los sistemas operativos Windows server 2008 / 2012 /2016 ficheros XCCDF con las verificaciones de configuraciones de seguridad a realizar para cada uno de ellos.

1. Para ello se utilizan los repositorios públicos de NIST para obtener ficheros XCCDF con todas las posibles reglas de seguridad para cada sistema operativo.
2. Se editan los ficheros XCCDF añadiendo un perfil de validación de seguridad customizado seleccionando las reglas críticas y aquellas reglas adicionales necesarias para cumplir la política de seguridad empresarial
3. Se verifica la correcta edición de los ficheros XCCDF con la solución de OpenSCAP ‘SCAP Workbench’.

# 4. Validación Especificaciones de seguridad SCAP.

## 4.0 Objetivo

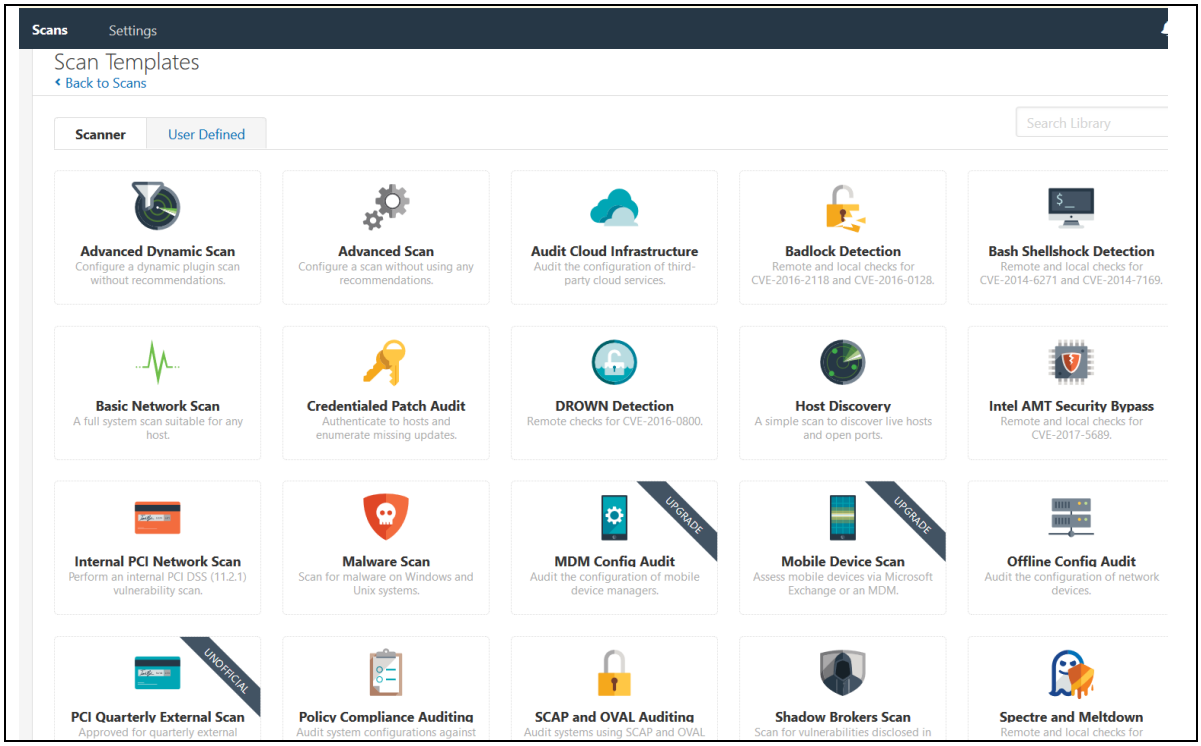
El objetivo de este capítulo, es comprobar que las especificaciones de seguridad SCAP definidas en el capítulo anterior permiten comprobar la correcta configuración de seguridad de los servidores. Para ello se utilizará la siguiente estrategia:

1. Para validar las herramientas y el método, inicialmente se auditará un único servidor ya existente en la empresa con el S.O. Windows server 2016. Se escoge un servidor poco crítico que tiene la ip 10.226.185.91
2. Se validará las especificaciones de seguridad de este servidor contra las especificaciones definidas en el perfil 'MyCompany16' que hemos definido en un fichero xccdf en el apartado anterior. Este perfil contiene 37 reglas de seguridad a validar.
3. Para la validación se utilizará las dos soluciones seleccionadas anteriormente: Nessus y OpenSCAP.

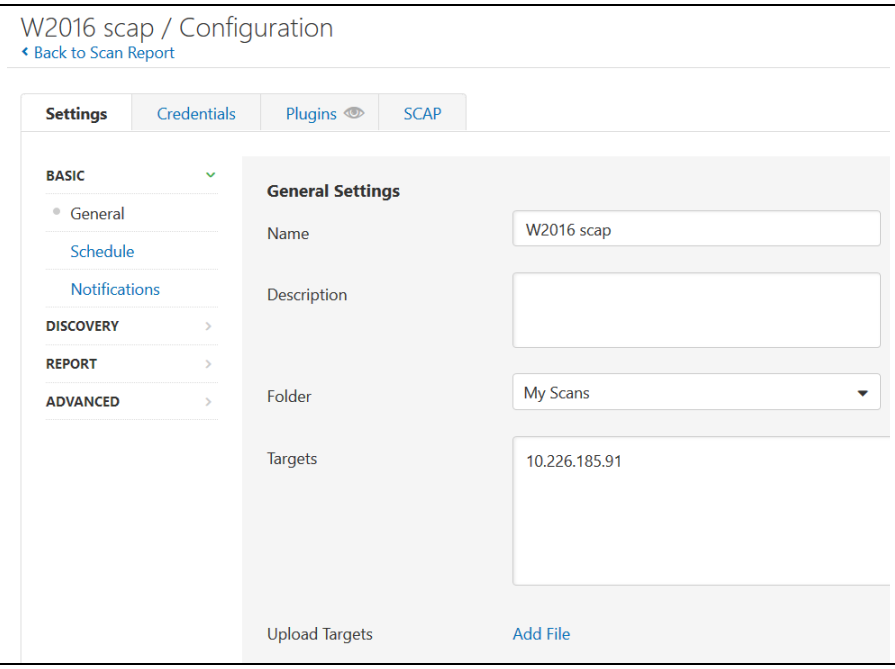
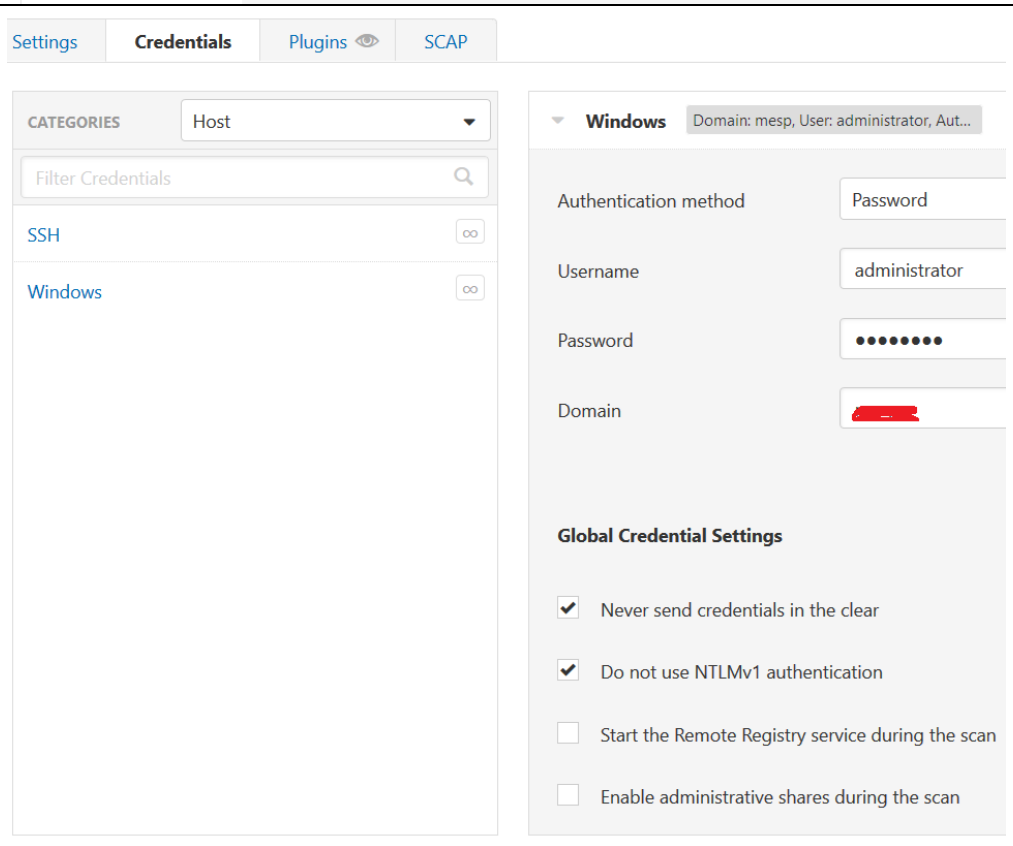
## 4.1 Validación con Nessus.

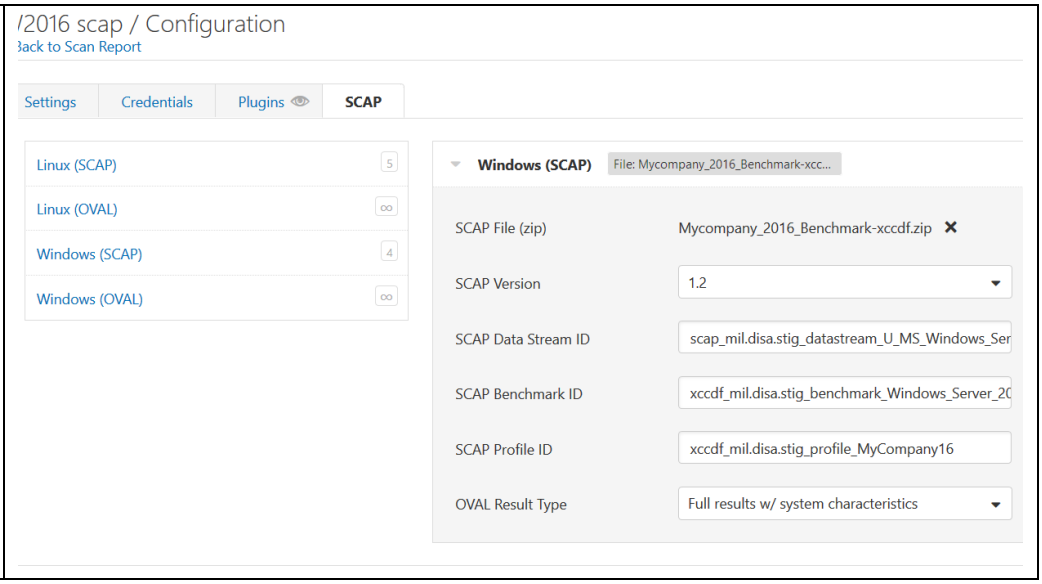
### 4.1.1 Definición Escaneo

Para realizar la validación con Nessus, una vez dentro de la aplicación, se selecciona la función de 'new scan' y aparece la siguiente pantalla con los distintos tipos de escaneos que nos ofrecen Nessus.
En este caso se selecciona el tipo 'SCAP and OVAL Audit' que es el que nos permite utilizar las definiciones de un fichero xccdf.



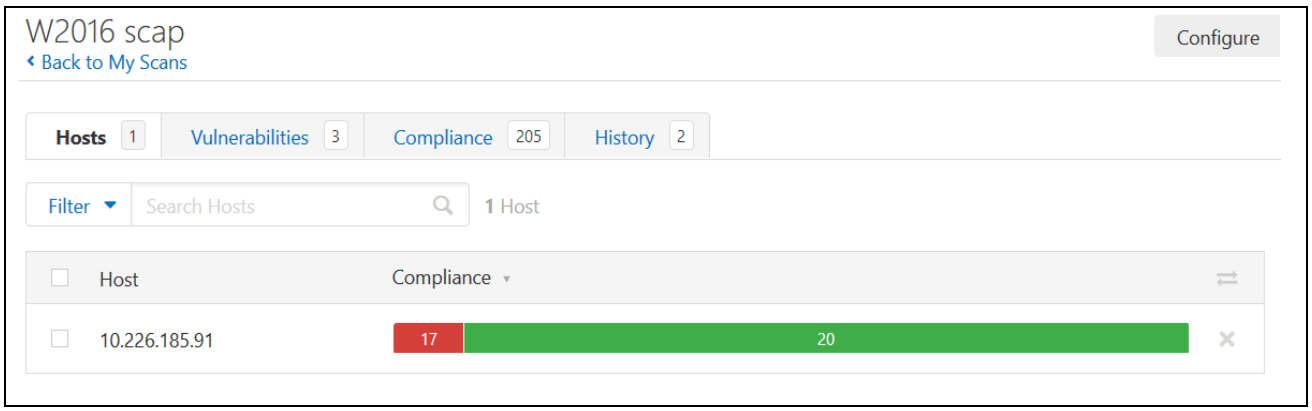
A continuación, hay que definir un conjunto de información para definir las comprobaciones a realizar

| | |
|---|---|
| Se introduce un nombre para identificar el escaneo (W2016 scap) y la dirección IP del servidor a escanear (10.226.185.91) |  |
| Se introducen credenciales con derechos de administrador para escanear la maquina remota. |  |

| | |
|---|---|
| Se carga el fichero xccdf a utilizar y se selecciona el perfil de seguridad a utilizar, en este caso el 'MyCompany16' |  |

### 4.1.1 Resultados Escaneo

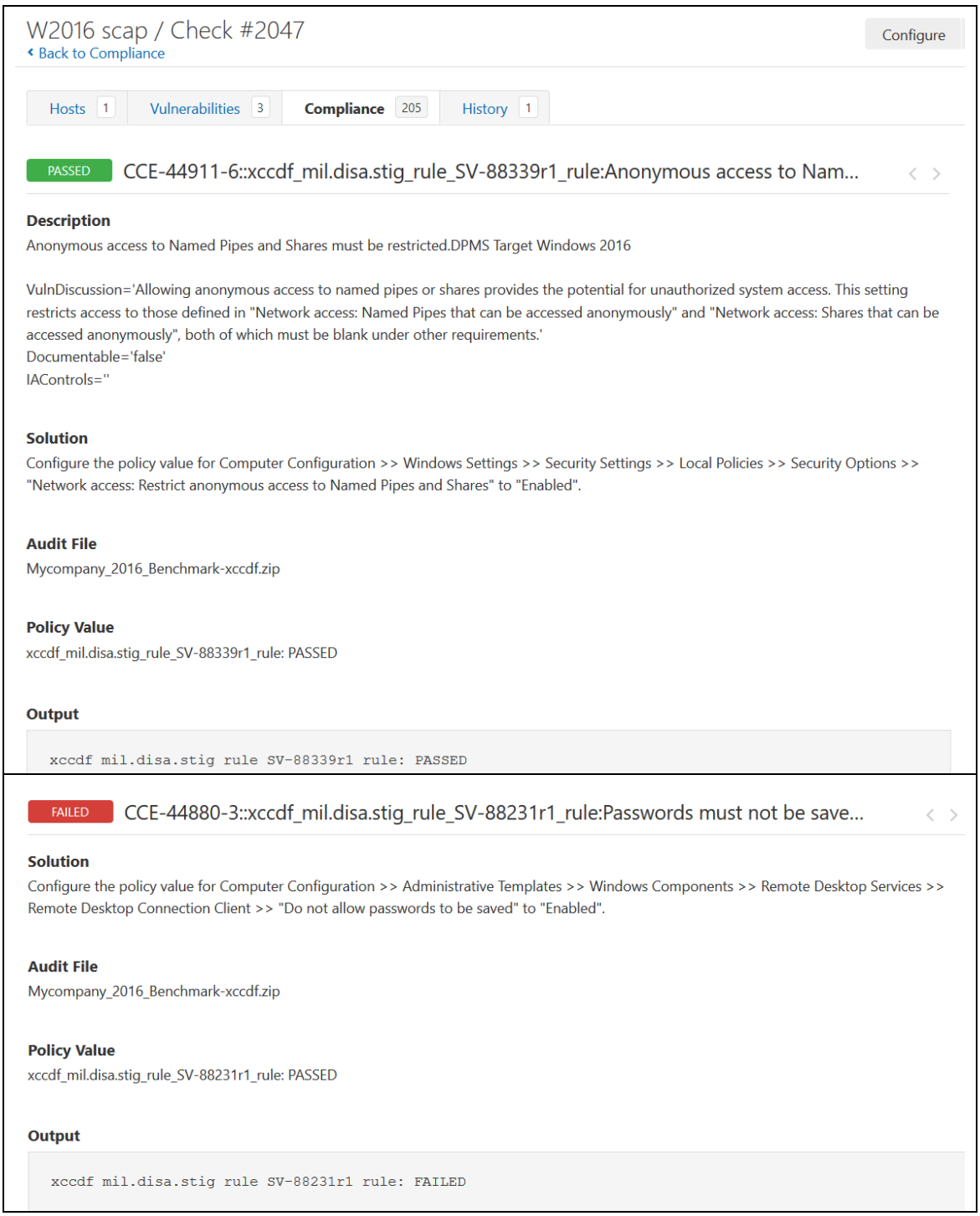
Una vez definido el escaneo, se ejecuta y se visualizan los siguientes resultados:




De las 37 reglas de seguridad:

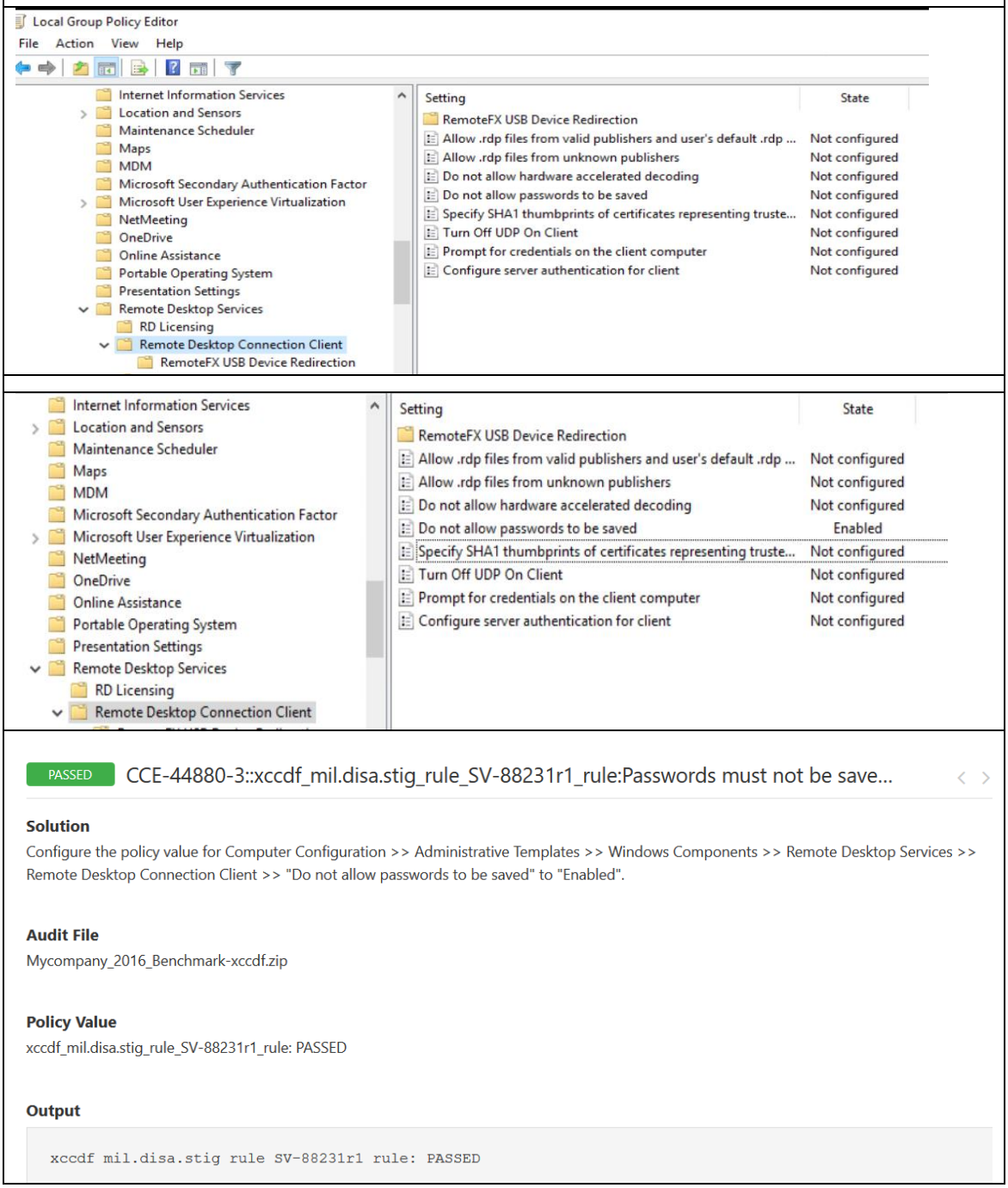
- 17 aparecen como Failed (no cumplimiento)
- 20 aparecen como Passed (cumplimiento)

Para cualquiera de las reglas se puede ver la información detalla, incluyendo las acciones correctoras a realizar en caso de no cumplimiento (Esta información está incluida en el fichero xccdf, y lo único que hace Nessus es mostrarla de una forma amigable. A continuación, se muestran dos ejemplos para dos reglas concretas (Una el que se detecta cumplimiento y otra em ña que se detecta incumplimiento).




En capítulos posteriores se analizará la forma más óptima de propagar las configuraciones de seguridad a varios servidores. Pero en este caso, y con el fin de comprobar el correcto funcionamiento de las instrucciones, se decide corregir la configuración de seguridad reportada como Failed en la imagen anterior (No permitir guardar contraseñas en el cliente de escritorio remoto).
Para ello se accede al servidor 10.226.185.191 y con el editor de políticas (gpedit.msc) se modifica el parámetro sugerido, se escanea de nuevo el servidor y se comprueba que el servidor tiene esta regla configurada correctamente. Se muestran las acciones y resultado en las siguientes capturas de pantalla.

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Connection Client >> "Do not allow passwords to be saved" to "Enabled".




## 4.2 Validación con OpenSCAP.

### 4.1.2 Definición Escaneo

OpenSCAP no permite validar la configuración de seguridad de sistemas remotos si no se ha instalado previamente en la maquina remota el 'OpenSCAP Base' que incluye la aplicación/ejecutable oscap.

Aún que existe una utilidad grafica llamada 'OpenSCAP workbech', en este caso se utilizará directamente la utilidad 'oscap' por línea de comandos. El motivo es que si se quiere automatizar el escaneo y validación de políticas (escaneos periódicos o lanzados remotamente), es necesario realizarlo por línea de comandos.

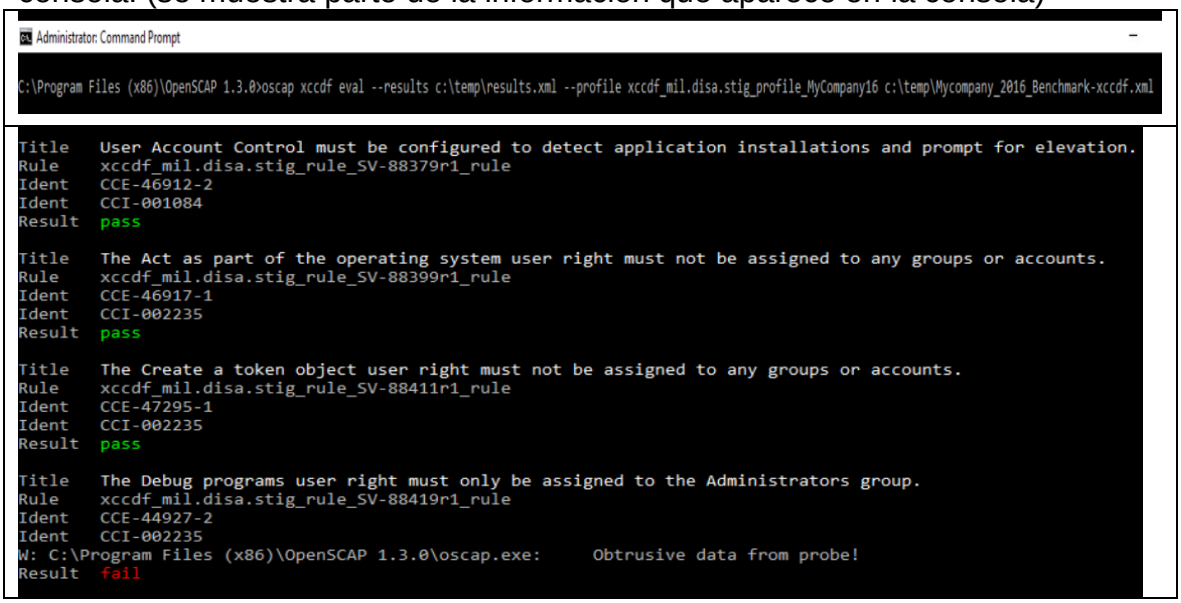
Consultada la documentación en el portal de OpenSCAP, se genera la siguiente línea de comandos que es la que se utilizará para la validación de las reglas de seguridad:

```
oscap  xccdf eval --results c:\temp\results.xml
--profile xccdf_mil.disa.stig_profile_MyCompany2016
c:\temp\Mycompany_2016_Benchmark-xccdf.xml
```

Se puede comprobar que en esta línea de comandos se indica donde guardar los resultados (results.xml), que perfil de seguridad utilizar para la validación (Mycompany16) y la ubicación y nombre del fichero xccdf a utilizar.
Como se puede comprobar se utiliza el mismo fichero xccdf y perfil de seguridad utilizado previamente con Nessus.

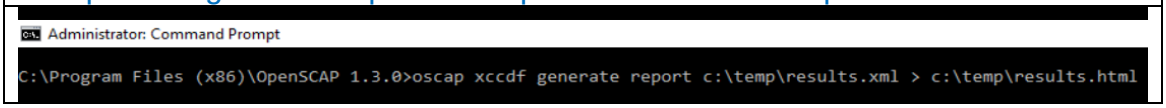
### 4.2.2 Resultados Escaneo

Una vez definido el escaneo se ejecuta y se visualizan los resultados en la consola. (se muestra parte de la información que aparece en la consola)



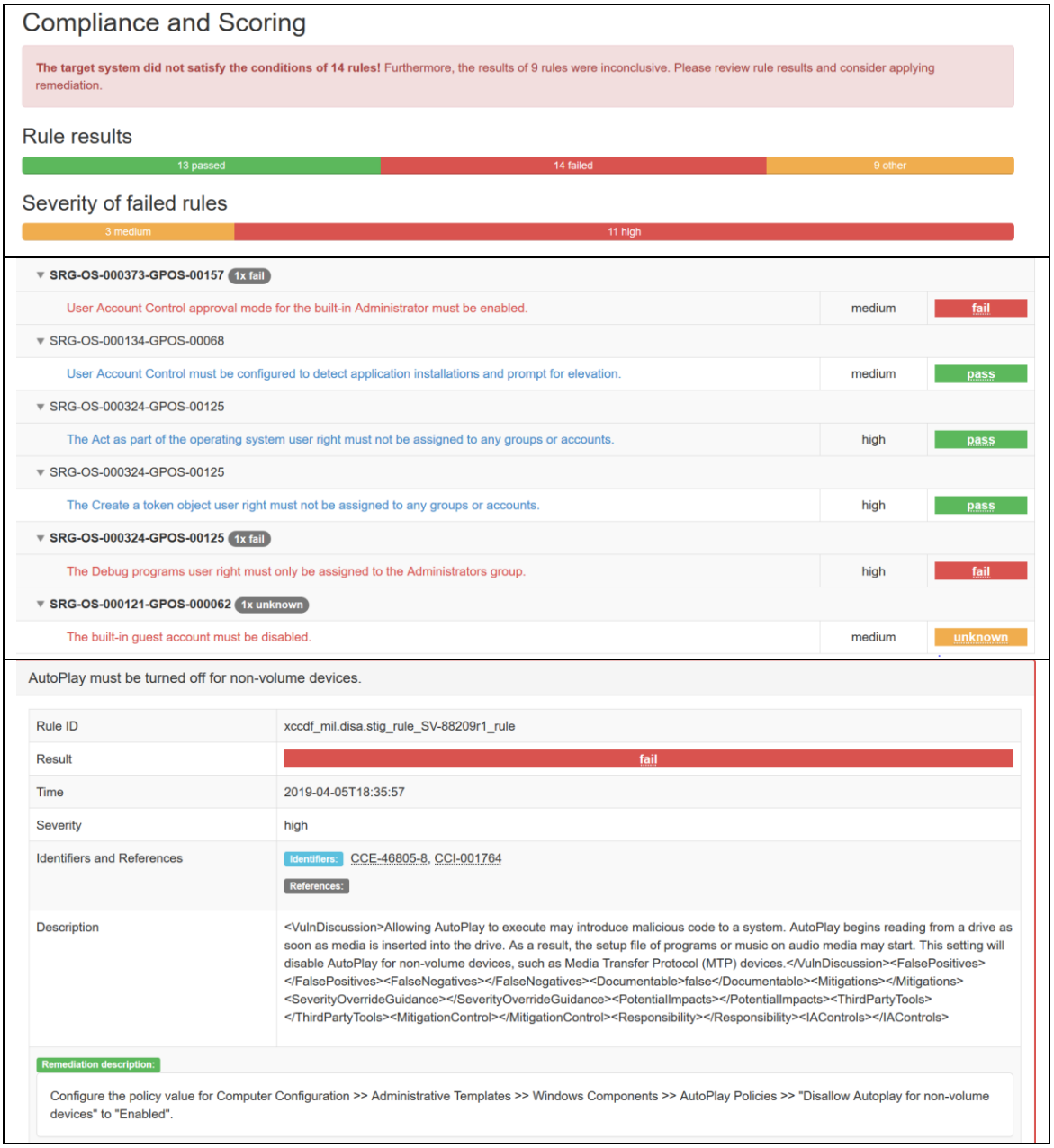

Para visualizar de una forma más comprensible e interactiva los resultados, se utiliza el fichero xml de resultados para generar un informe en formato html con el siguiente comando:

```
oscap  xccdf generate report c:\temp\results.xml > c:\temp\results.html
```




A continuación, se muestra algunas partes del informe html obtenido, como se puede ver:

- La información presentada por OpenSCAP, tanto la resumida como detallada, se parece mucho a la presentada por Nessus
- Algunas reglas de seguridad (9 de 37) aparecen en status ‘Unkonwn’. Esto quiere decir que OpenSCAP no ha podido valorar si la regla de seguridad esta implementada o no. Esto es debido a que OpenSCAP permite analizar sistemas Windows solo recientemente y aún no funciona para el 100% de los casos y reglas a valorar. (originalmente solo funcionaba en sistemas Linux).




### 4.3 Conclusiones y Comparación Nessus vs OpenSCAP.

Se valida que las especificaciones SCAP definidas en el capítulo 3 nos permiten validar la correcta configuración de seguridad de un servidor. Las principales diferencias para analizar y validar políticas de seguridad de sistemas Windows entre Nessus y OpenSCAP son:

- Nessus permite analizar sistemas Windows remotos sin la instalación de software adicional (solo necesita credenciales con derechos de administrador), mientras que OpenSCAP obliga a instalar el software en cada sistema a analizar.
- Nessus soporta al 100% el análisis de las reglas de seguridad de sistemas Windows, mientras que OpenSCAP no es capaz de analizar todas las reglas de seguridad (en el ejemplo anterior no se han podido validar 9 reglas de 37)

Por ese motivo, se decide utilizar Nessus para analizar de forma central y periódica la configuración de seguridad del conjunto de servidores Microsoft de la empresa.

# 5. Implementación centralizada de políticas de seguridad.

## 5.0 Objetivo

Definidas las reglas y configuraciones de seguridad que deben cumplir los servidores empresariales, no es suficiente implementar un control de las configuraciones automático y centralizado, sino que surge la necesidad de encontrar un método automatizado para propagar a los servidores las configuraciones de seguridad deseadas.

El objetivo de este capítulo es definir un método práctico que permita distribuir las reglas de seguridad en los múltiples servidores empresariales. En el caso actual nos encontramos con dos problemáticas a resolver,

1. Distribución de reglas a servidores en el Dominio empresarial
2. Distribución de reglas a servidores fuera del Dominio empresarial (DMZ)

Como se ha explicado en el apartado 4.1.1, una forma de configurar las reglas de seguridad en los servidores, es hacerlo localmente en cada servidor mediante el editor de políticas gpedit.msc. Realizar-lo de esta forma tiene dos inconvenientes principales:

- **Carga de trabajo y posibilidad de errores**: En un entorno empresarial con múltiples servidores, este método obliga a entrar en cada servidor para editar cada una de las reglas de seguridad. Este método supone una carga de trabaja elevada y la posibilidad de cometer errores al ser un método manual.
- **Imposibilidad de editar algunas políticas localmente**: En servidores empresariales que estén controlados por un servidor de dominio, es posible que algunas políticas de seguridad estén forzadas des del controlador de dominio, no permitiendo la modificación local de las mismas.

## 5.1 Distribución de reglas a servidores en el Dominio empresarial

[8][11] Para definir y distribuir las configuraciones de seguridad a todos los servidores en dominio de la empresa, se plantean diversas posibilidades.

**Para la definición de las configuraciones de seguridad se plantean dos opciones:**

1. Definir una GPO (Group Policy Object) para cada sistema operativo. En esta GPO se definirán todas las configuraciones para cumplir las reglas de seguridad empresariales (definidas en los capítulos anteriores).
    a. En una única GPO se tiene la visión de todas las configuraciones de seguridad de los servidores para un sistema operativo concreto.
2. Definir un GPO con las configuraciones de seguridad comunas a los 3 sistemas operativos, y definir una GPO adicional para cada sistema operativo con las configuraciones específicas de cada uno de ellos.
    a. En caso de necesitar modificar configuraciones de seguridad comunes, solo hay que modificar una única GPO y no las 3 para cada sistema operativo.

Finalmente, se decide optar por la primera opción (única GPO para cada sistema operativo), valorando especialmente la visión de todas las configuraciones de seguridad para un sistema operativo en una única GPO

**Para la distribución de las configuraciones definidas en una GPO se plantean dos opciones:**

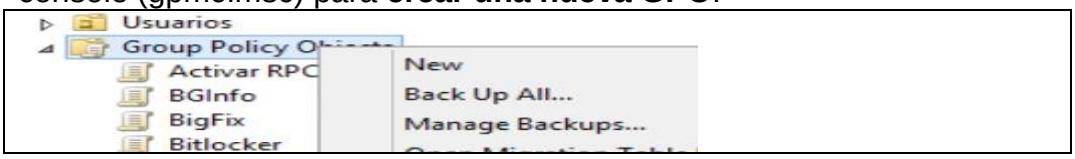
1. Asignar los servidores a distintas OU (unidades organizativas) en función del sistema operativo y asociar cada GPO a la OU especifica.
    a. Aplicación de la GPO a los servidores en poco tiempo o de forma inmediata si se fuerza con 'Gpudate /force'
2. Asociar los servidores a distintos Grupos de Seguridad en función del sistema operativo, y aplicar las GPOs solo a los servidores asociados a los mencionados grupos de seguridad (utilizando la opción 'security filtering' en la GPO)
    a. La aplicación de la GPO se puede retrasas bastante tiempo hasta que el servidor no refresque su pertenencia al grupo de seguridad

Se decide utilizar la Opción 1 asignando la GPO a una OU específica para cada sistema operativo. La opción 1 tiene la ventaja de que la aplicación de la GPO es inmediata, y esto simplifica el despliegue actual en fase de piloto y prototipo. La opción 1, permite agilizar la inclusión o exclusión de servidores en las distribuciones de configuraciones de seguridad vía GPO.
Una vez se tenga confianza que la política no genera ningún problema con la explotación de los servidores, se optará por la opción 2). Utilizar un filtro por grupo de seguridad tiene la ventaja que no necesita colocar los servidores en una OU especifica en función de su sistema operativo.

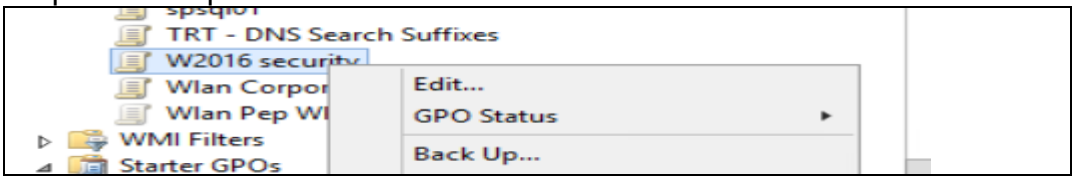
Así pues, se distribuirán las configuraciones de seguridad con una única GPO por sistema operativo, asociandola a una OU especifica donde estarán ubicados los servidores de ese sistema operativo.

A continuación, se explica y muestra el proceso seguido para distribuir las políticas a servidores Windows server 2016.

1. En el controlador de dominio se utiliza la utilidad Group Polilcy management console (gpmc.msc) para **crear una nueva GPO**.



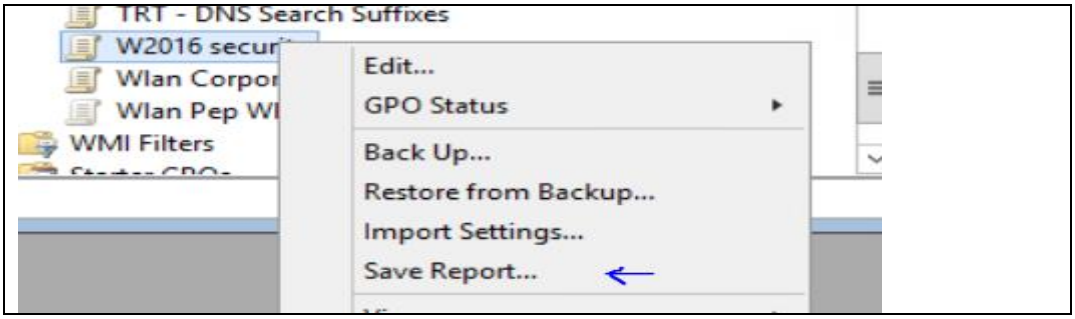

2. **Se define una GPO llamada 'W2016 security'** sin asociarla a ninguna Unidad Organizativa.
3. Se edita la GPO 'W2016 security' **añadiendo todas configuraciones de seguridad para cumplir las reglas de seguridad** definidas previamente en la política empresarial.

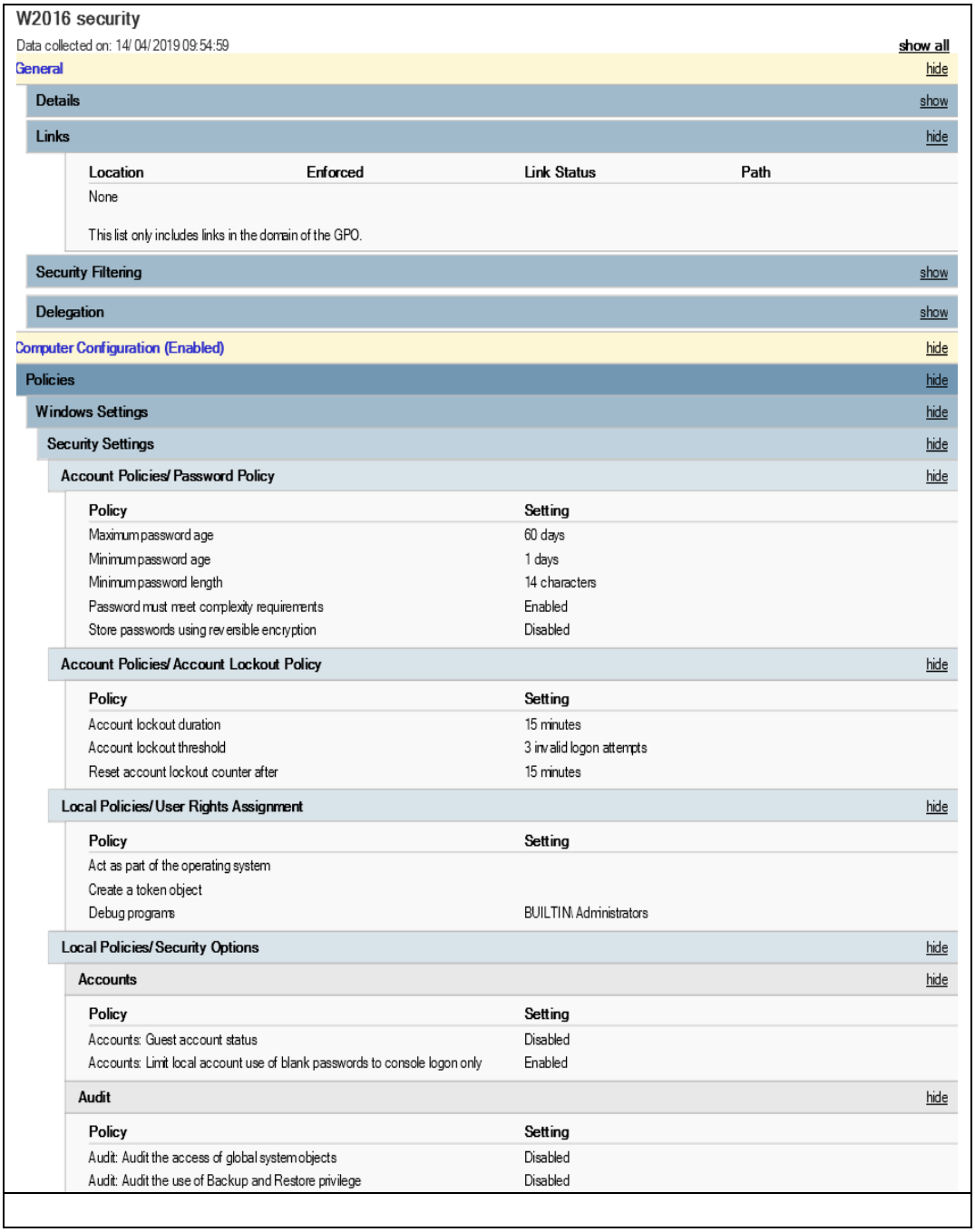



Nota: La política empresarial para Windows server 2016 tiene 37 reglas de seguridad. Unas pocas no se pueden definir en la GPO, pues no son configuraciones de seguridad. Por ejemplo, algunas reglas se refieren a no

tener servicios instalados como FTP o Telnet. Estos casos no se pueden configurar vía GPO. Simplemente los monitorizaremos con Nessus y en caso que se detecte uno de estos servicios innecesarios se desinstalará.

4. **Se valida la GPO creada**. Para ello se utiliza la opción 'Save report' para generar un informe con el contenido de la GPO y se valida que el contenido es el correcto



W2016 security

Data collected on: 14/04/2019 09:54:59 — show all

General — hide

Details — show

Links — hide

| Location | Enforced | Link Status | Path |
|---|---|---|---|
| None | | | |

This list only includes links in the domain of the GPO.

Security Filtering — show

Delegation — show

Computer Configuration (Enabled) — hide

Policies — hide

Windows Settings — hide

Security Settings — hide

Account Policies/Password Policy — hide

| Policy | Setting |
|---|---|
| Maximum password age | 60 days |
| Minimum password age | 1 days |
| Minimum password length | 14 characters |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |

Account Policies/Account Lockout Policy — hide

| Policy | Setting |
|---|---|
| Account lockout duration | 15 minutes |
| Account lockout threshold | 3 invalid logon attempts |
| Reset account lockout counter after | 15 minutes |

Local Policies/User Rights Assignment — hide

| Policy | Setting |
|---|---|
| Act as part of the operating system | |
| Create a token object | |
| Debug programs | BUILTIN\Administrators |

Local Policies/Security Options — hide

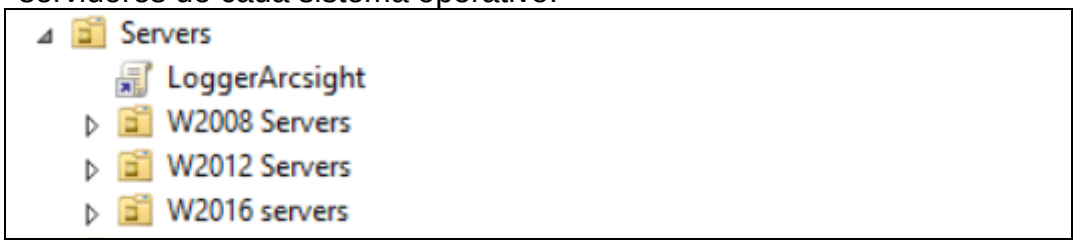
Accounts — hide

| Policy | Setting |
|---|---|
| Accounts: Guest account status | Disabled |
| Accounts: Limit local account use of blank passwords to console logon only | Enabled |

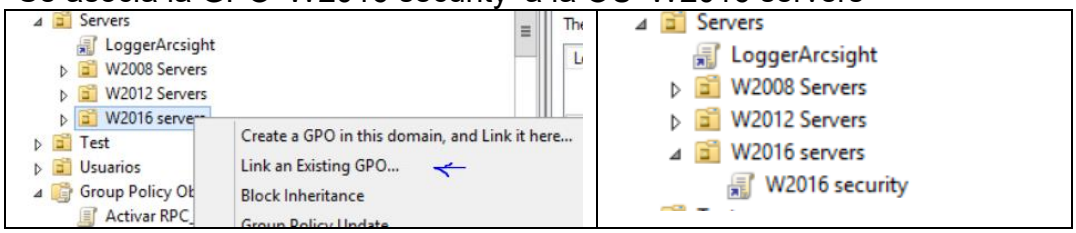
Audit — hide

| Policy | Setting |
|---|---|
| Audit: Audit the access of global system objects | Disabled |
| Audit: Audit the use of Backup and Restore privilege | Disabled |

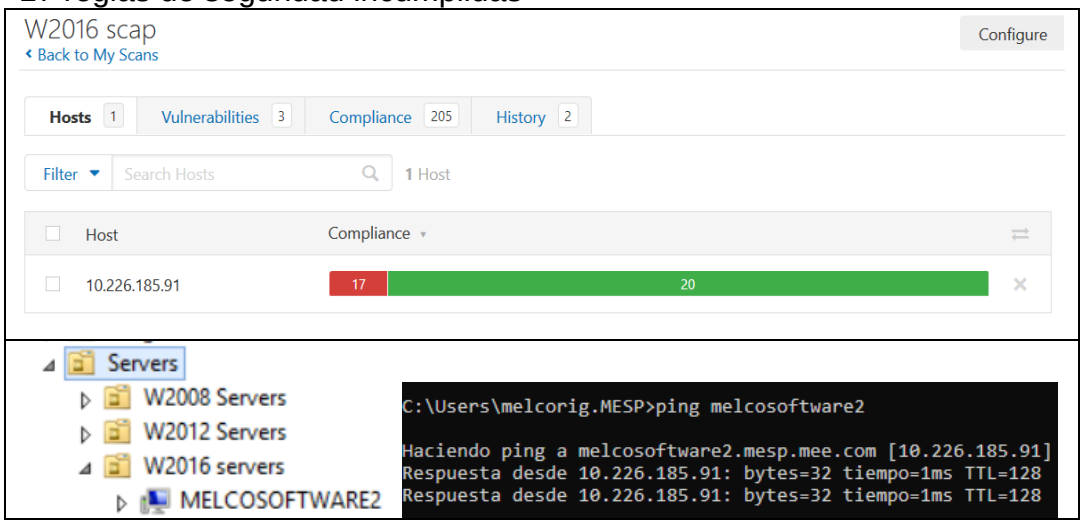
5. Se crea en el directorio activo una OU donde se colocarán los servidores de cada sistema operativo.



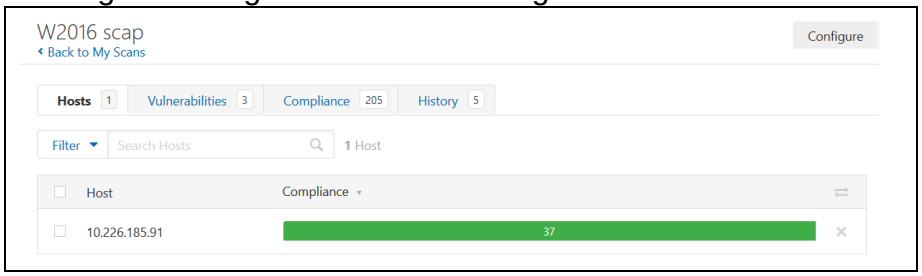

6. Se asocia la GPO 'W2016 security' a la OU 'W2016 servers'




7. Una vez realizada esta acción cualquier servidor ubicado en la OU W2016 servers, se le aplicarán automáticamente las reglas de seguridad empresariales. Para validarlo se mueve el servidor '10.226.185.191' que hemos analizado previamente con Nessus y OpenSCAP y que aún tiene 17 reglas de seguridad incumplidas




8. Una vez realizado se entra en el servidor a analizar y se fuerza la actualización de políticas de seguridad con el comando 'gpudate /force'. También se podría haber esperado un tiempo a que el DC propagase las políticas automáticamente.
9. Se vuelve a realizar el escaneo con Nessus y se comprueba que todas las reglas de seguridad se han configurado correctamente

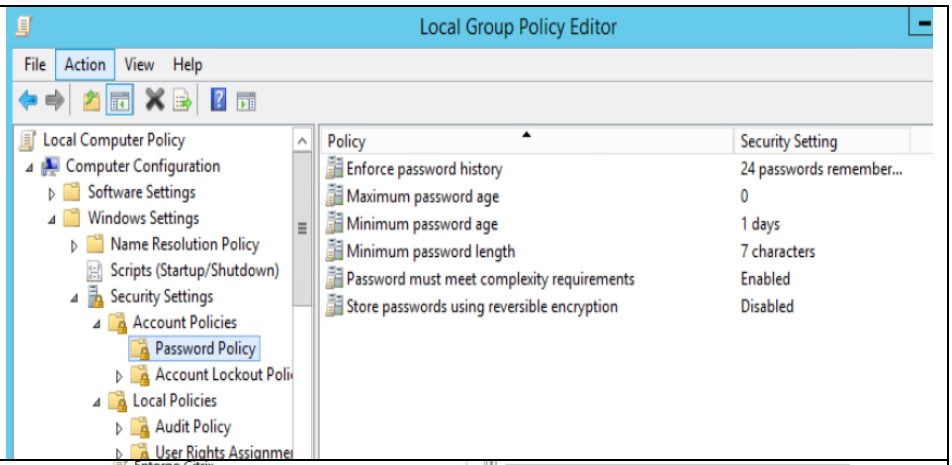
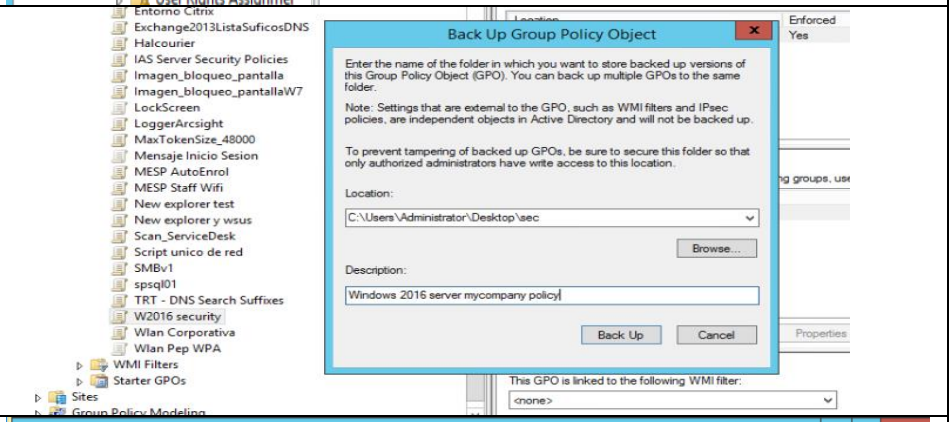
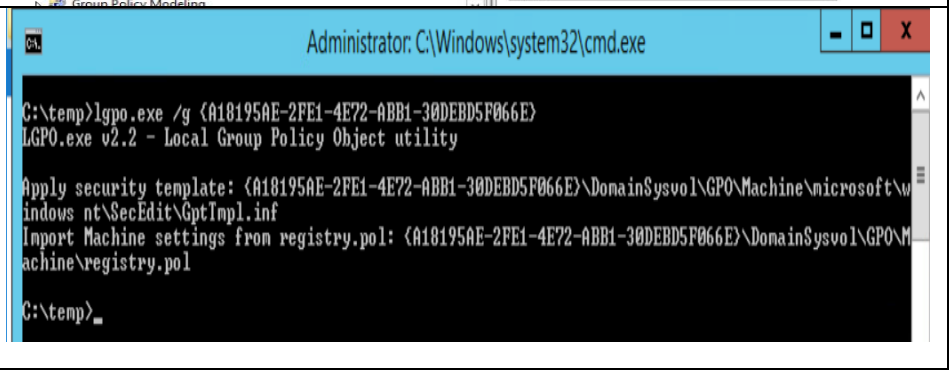


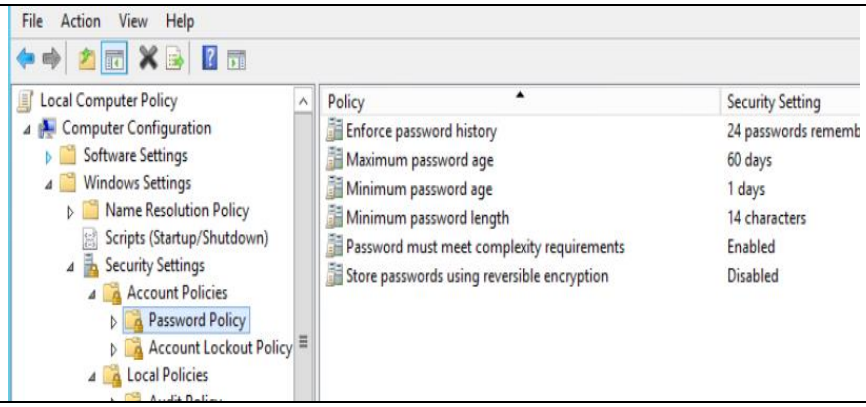
## 5.2 Distribución de reglas a servidores fuera del Dominio empresarial

[9][10] La empresa tiene algunos servidores en la DMZ, que están fuera de dominio. Para estos servidores es necesario encontrar alguna solución práctica que permita cargar las configuraciones de seguridad. Se decide utilizar la siguiente estrategia:

1. Realizar copia de seguridad en un fichero de la GPO 'W2016 Security' ya existente en el controlador de dominio.
2. Copiar el fichero con la copia de seguridad de la GPO en los servidores fuera de dominio
3. Importar la GPO con la utilidad lgpo.exe

A continuación, se muestra las capturas de pantalla del proceso seguido para cargar las políticas de seguridad en un servidor fuera del controlador de dominio. Este servidor no tiene todas las políticas de seguridad configuradas según la normativa corporativa. Se comprueba que una vez importado el backup de la GPO se cumplen correctamente las normativas corportativas.

| | |
|---|---|
| Ejemplo politicas de seguridad de passwords configuradas antes de importar la politica |  |
| Backup GPO |  |
| Importación GPO en servidor fuera de dominio. |  |

| | |
|---|---|
| Ejemplo politicas de seguridad de passwords configuradas correctamente después de importar la politica |  |

### 5.3 Conclusiones

Se define un proceso que permite de una forma fácil y automatizada distribuir las configuraciones de seguridad a los servidores empresariales:

1. En el caso de los servidores en el dominio empresarial:
    a. Se define una GPO para cada sistema operativo con las configuraciones de seguridad
    b. Se crea una OU (unidad organizativa) para cada sistema operativo, donde se sitúan los servidores correspondientes
    c. Se asigna la GPO de cada sistema operativo a la OU correspondiente
2. En el caso de los servidores fuera del Dominio se define un proceso semi-manual que permite la carga de las configuraciones de seguridad:
    a. Se exporta a un fichero la GPO definida en el controlador de dominio para el sistema operativo del servidor a configurar. (utilizando la opción de backup)
    b. Se importa con una utilidad de Microsoft la GPO al servidor.

# 6. Control Vulnerabilidades Servidores

## 6.0 Objetivo

Para garantizar la seguridad de los servidores, no solo es necesario tener la configuración y políticas de seguridad correctamente aplicadas, sino que es muy importante asegurar que los servidores no tienen vulnerabilidades de seguridad. En general las vulnerabilidades de seguridad están generadas por:

- Versiones de sistema operativo o aplicaciones instaladas obsoletas
- Parches de seguridad de sistema operativo o aplicaciones no instalados.

Así pues, el objetivo de este capítulo será encontrar la forma más pragmática para:

- Detectar si algún servidor tiene una vulnerabilidad especifica de seguridad. En casos de emergencias, puede ser muy importante poder encontrar de forma muy rápida que servidores están afectados por una vulnerabilidad especifica de seguridad. Esto nos permitirá realizar acciones inmediatas como aislarlos de la red y fijar la vulnerabilidad lo antes posible.
- Análisis global de vulnerabilidades existentes en servidores. En este caso permitirá detectar los principales problemas de seguridad y realizar un plan para resolverlos en función de la criticidad de las vulnerabilidades y numero de servidores afectados.

Todas las pruebas se realizarán con la herramienta Nessus Profesional. El objetivo es validar que la misma solución que permite controlar la configuración de seguridad de los servidores también permite controlar de forma fácil las vulnerabilidades de seguridad de los mismos.

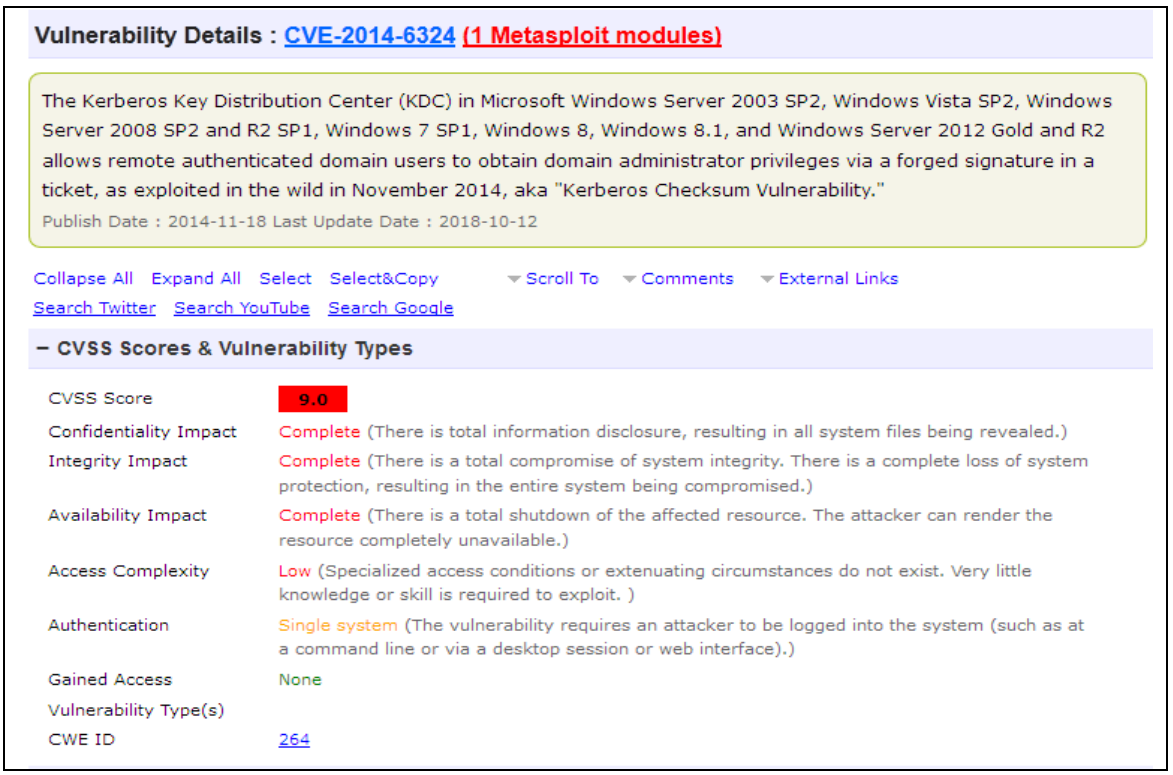
## 6.1 Detección de una Vulnerabilidad especifica en servidores empresariales

### 6.1.1 Definición Escaneo

[12] Para la detección de vulnerabilidades, Nessus utiliza los llamados ‘Nessus Plugins’, que son unos programas escritos en lenguaje de programación propios de Nessus (NASL) para la detección de las vulnerabilidades.
Así pues, para detectar una vulnerabilidad específica, se tendrá que encontrar que plugin hay que utilizar. Como curiosidad, hasta la actualidad Nessus ha publicado 127.079 plugins

Para realizar esta prueba, se busca una vulnerabilidad critica, que puede afectar a varios servidores empresariales y que tenga un exploit. Después de realizar algunas búsquedas en ‘www.cvedetails.com’ se escoge la vulnerabilidad CVE-2014-6234 que afecta a los servidores W2008 y W2012.

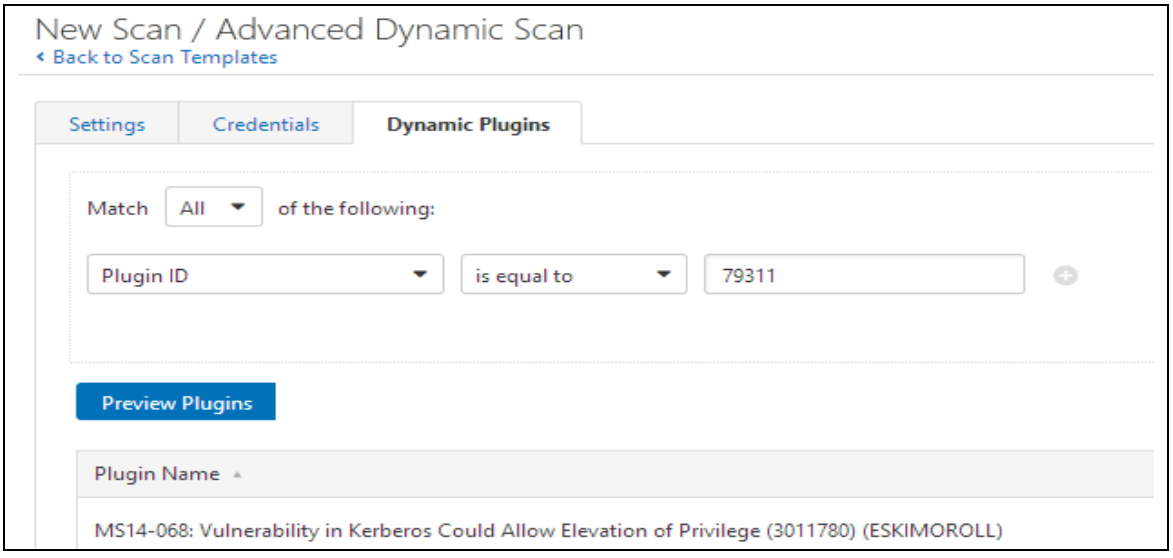
Se busca en la librería de Nessus [12] y se comprueba que la mencionada vulnerabilidad se puede analizar con el plugin ID ‘79311’



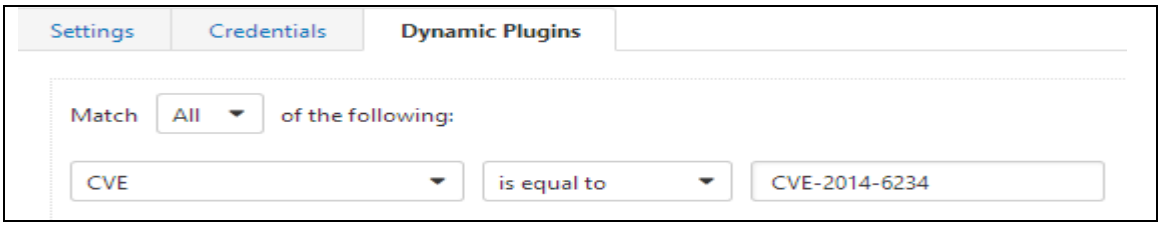


Una vez conocido el Plugin a utilizar, solo falta lanzar un escaneo con credenciales a la red de servidores utilizando este plugin.
Definimos un nuevo escaneo en Nessus, tipo 'New Scan / Advanced Dynamic Scan':

- Definimos como 'target' el rango de IP's de la red de servidores
- Introducimos credenciales con derecho de administrador en los servidores
- En la pestaña 'Dynamic plugins' seleccionamos el plugin 79311.

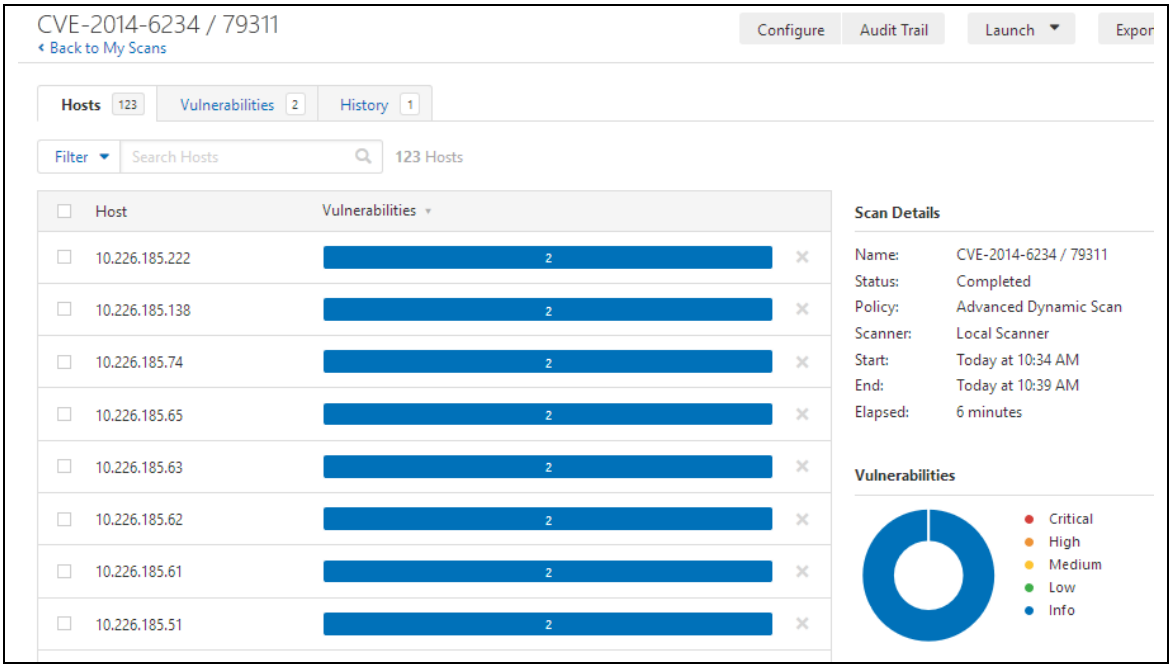


Nota: En un mismo escaneo Nessus permite utilizar varios plugins. También permite definir directamente el código CVE de la vulnerabilidad. En este caso, Nessus buscará automáticamente el Plugin a utilizar para detectar la vulnerabilidad.

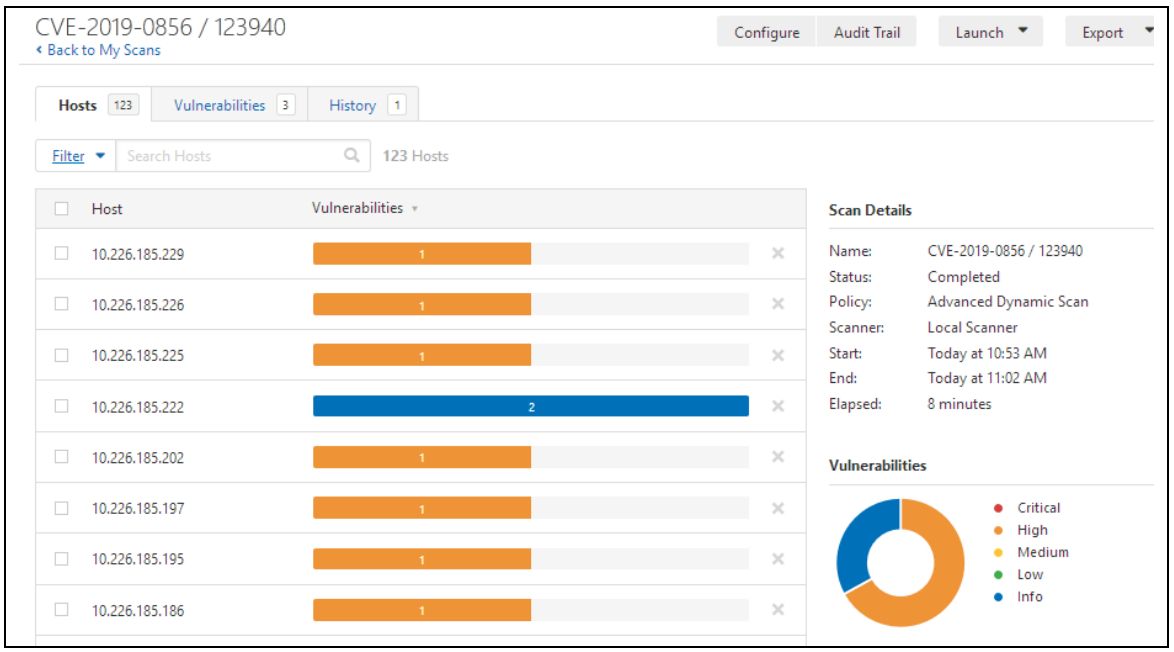



### 6.1.2 Ejecución Escaneo

Una vez ejecutado el escaneo sobre 123 servidores, se comprueba que ninguno de ellos tiene la vulnerabilidad crítica. Esto tiene sentido, pues el parche de la vulnerabilidad fue distribuido en 2014, y todos los servidores se han actualizado posteriormente.
Como curiosidad, se comprueba que el escaneo sobre 123 servidores de una vulnerabilidad especifica tarda solo 6 minutos.




Para confirmar que el proceso es el correcto y detecta vulnerabilidades, se busca una vulnerabilidad más reciente. Se selecciona la vulnerabilidad CVE-2019-0856, que se puede validar con el plugin 123940. Esta Vulnerabilidad y su parche por parte de Microsoft están publicadas en el mes de abril de 2019.
Se configura un nuevo escaneo de Nessus de la misma forma que el caso anterior. En este caso, se comprueba que el 66% de los servidores están afectados (dando que aún no se han actualizado con el 'April security update')




Si consultamos el informe detallado de Nessus para alguno de los servidores afectados, se confirma que se ha utilizado el plugin 123940 que hemos configurado para el escaneo y que el servidor está afectado por la vulnerabilidad CVE-2019-0856. Al final del informe también se detalla el parche a instalar para resolver la vulnerabilidad.

### 6.2 Detección global de vulnerabilidades en servidores empresariales.

Visto en el apartado anterior como comprobar si los servidores empresariales están expuestos a alguna vulnerabilidad específica, lo más importante es realizar una detección global de las vulnerabilidades a que están expuestos los servidores empresariales. En general las vulnerabilidades vendrán ocasionadas por tres motivos:

- Versiones de sistema operativo, o aplicaciones sin soporte por fabricante
- Parches de sistema operativo o aplicaciones no instalados.
- Configuración del servidor

Para realizar un escaneo global, se realiza la misma estrategia que en el caso anterior, pero se selecciona todos los grupos de plugins de Nessus que interesan:

- Windows (4.247 plugins ): Básicamente validaciones de aplicaciones que se pueden instalar en entornos Windows, por ejemplo: Acrobat reader, winrar, etc.
- Windows Microsoft bulletins (1.547 plugins): validaciones de los parches de seguridad de windows
- Otros: Plugins específicos para validar servicios que pueden estar instalados en el servidor: DNS, FTP, Webservers, Denial of Service, Databases, Backdoors

Una vez realizado el escaneo (34 Minutos), se visualiza el estado del parque de servidores:

- Solo hay un 20% de servidores sin ninguna vulnerabilidad
- Hay 10% servidores con vulnerabilidades críticas.

Se comprueba que el informe de las vulnerabilidades detectadas se puede visualizar de dos formas distintas, ambas muy interesantes:

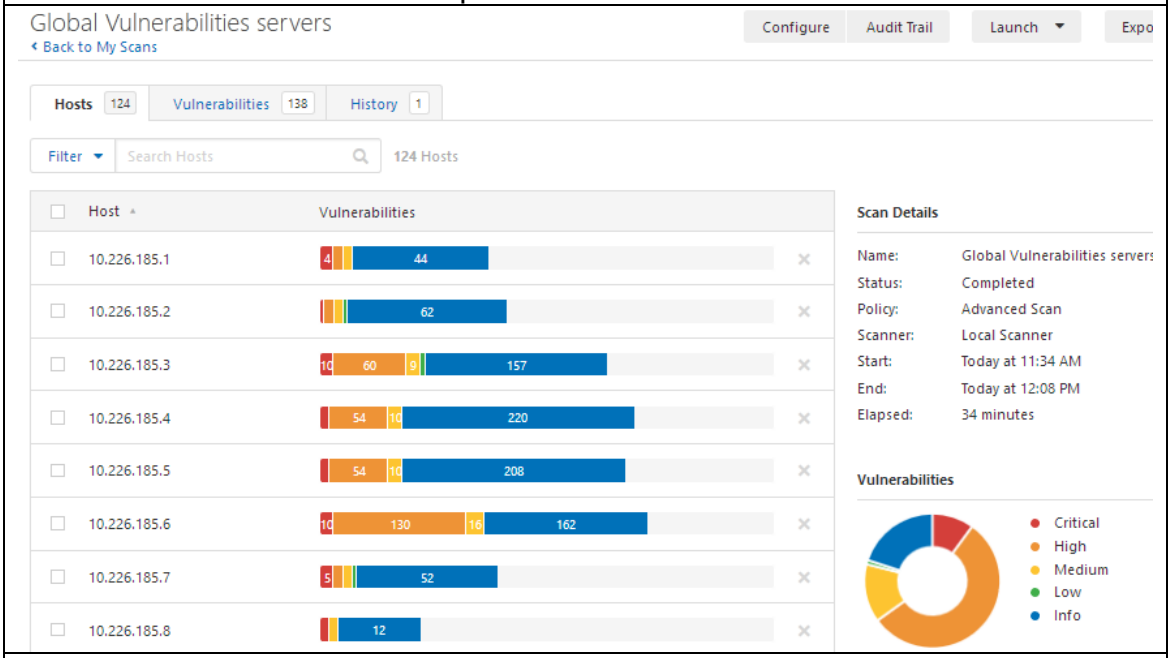
- Análisis servidor a servidor, viendo las vulnerabilidades detectadas clasificadas por criticidad. Para cada vulnerabilidad se puede ver la información detallada y las acciones necesarias para su resolución. Este informe es muy interesante, si nos queremos centrar primero en resolver los problemas de seguridad de los servidores más críticos.

- Análisis por vulnerabilidad (ordenadas por número de servidores afectados): Para cada vulnerabilidad, se puede ver que servidores están afectados y la información detallada de la vulnerabilidad. Este informe es muy interesante, si nos queremos centrar en resolver los problemas de seguridad que afectan a más número de servidores.

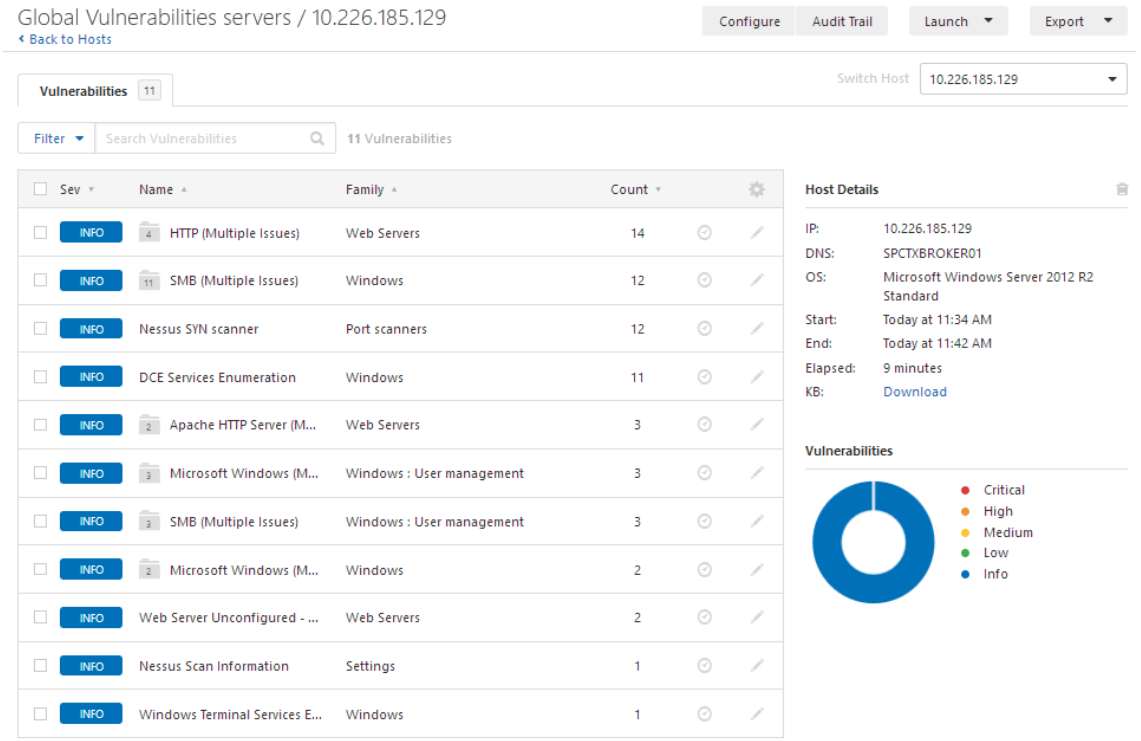
NOTA: En caso que nos interese, Nessus permite cambiar la criticidad de una vulnerabilidad (para todos los servidores) o para uno en concreto de forma permanente. Para ello está la opción ‘modify’ con el icono del lápiz al lado de la vulnerabilidad. Hay otra opción ‘snooze’ que permite eliminar durante un tiempo que definamos una vulnerabilidad concreta de los informes.

A continuación, se muestran capturas de pantalla de lo que se ha descrito en los apartados anteriores.

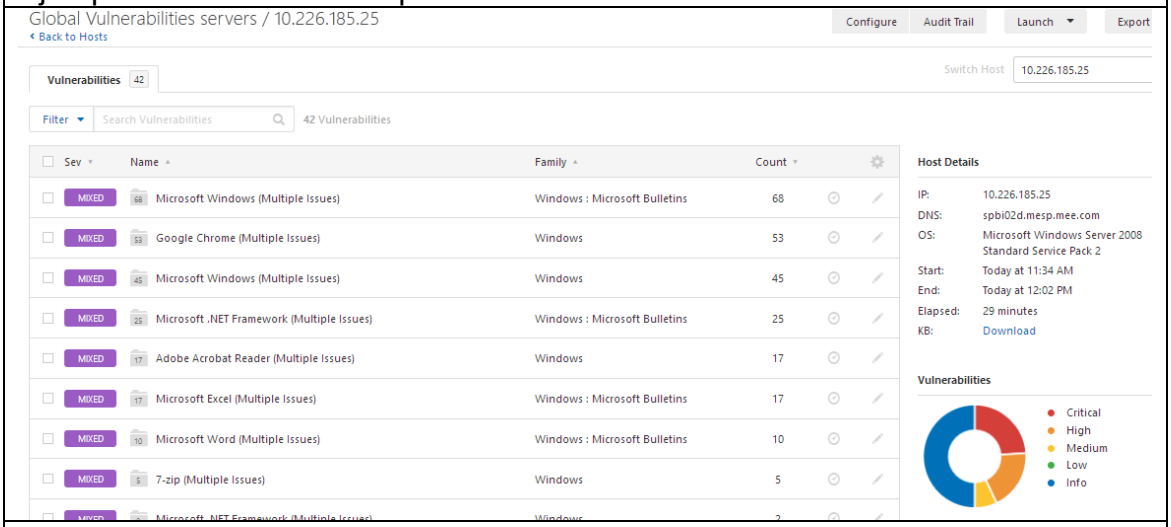
Visualización Vulnerabilidades por Servidores



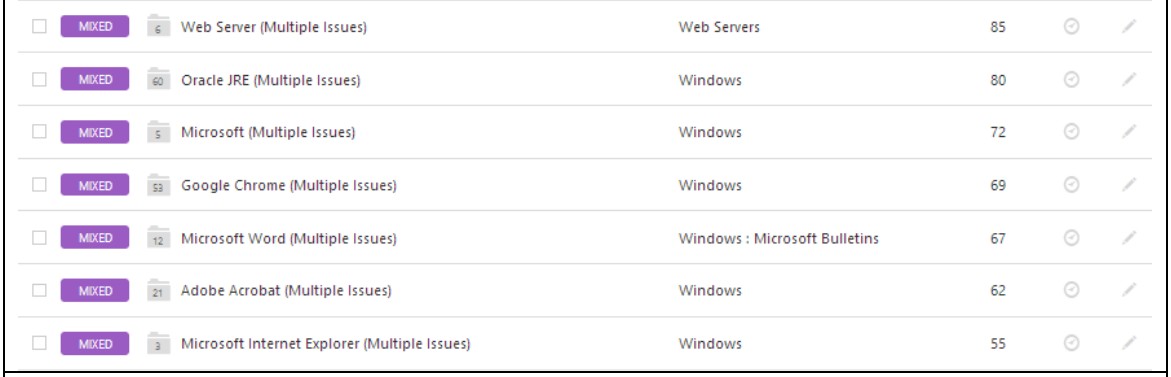

Visualización Servidor Libre de Vulnerabilidades



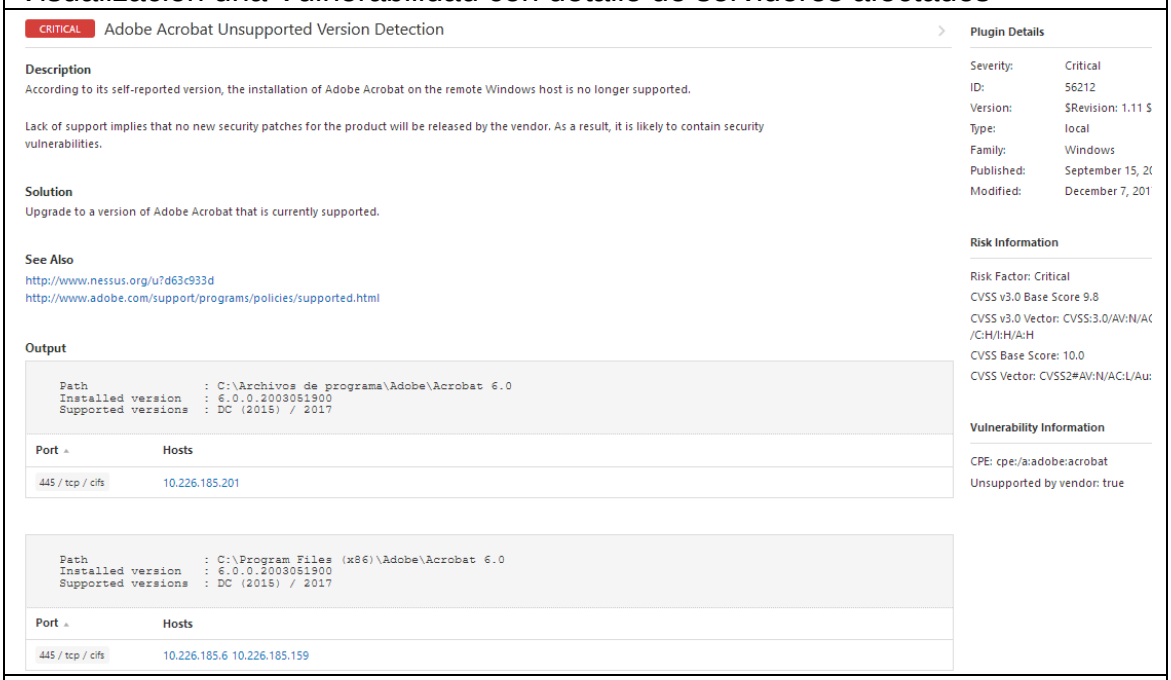
## Ejemplo Servidor con Múltiples Vulnerabilidades




## Visualización Vulnerabilidades por Vulnerabilidad




## Visualización una Vulnerabilidad con detalle de servidores afectados



### 6.3 Conclusiones

Nessus es una solución idónea para la evaluación continua de las posibles vulnerabilidades de los servidores empresariales.

Se ha utilizado el escaneo con credenciales ‘advanced scan’ que permite utilizar plugins (programas de Nessus) para detectar las vulnerabilidades conocidas de:

- sistema operativo
- programas instalados
- configuraciones erróneas.

Seleccionando un único plugin podemos buscar una vulnerabilidad especifica o seleccionando familias de plugins podemos hacer un análisis global de vulnerabilidades.

Finalmente, se comprueba que los informes generados por Nessus son muy intuitivos y útiles para gestionar las resoluciones de vulnerabilidades con distintas estrategias:

- Centrarse en los servidores más críticos y resolver todas sus vulnerabilidades
- Centrarse en las vulnerabilidades que afectan más servidores.

**Nota:** Al inicio del TFM se querían utiliza ficheros OVAL para detección de vulnerabilidades específicas, pero finalmente este punto se ha resuelto con la utilización de Nessus y el escaneo por plugins.

# 7. Control Seguridad en Ordenadores empresariales

## 7.0 Objetivo

El Objetivo de este capítulo es validar la posibilidad de utilizar las soluciones analizadas en los capítulos anteriores, orientadas a la seguridad de los servidores, para validar la configuración de seguridad y las vulnerabilidades de los ordenadores empresariales.

La principal diferencia, versus los servidores, es que los ordenadores no están siempre funcionando ni conectados a la red empresarial. Este punto dificultará la estrategia de escaneo de los mismos. Esta dificultad no existía en el control de seguridad de los servidores que pueden escanearse en cualquier momento al estar siempre conectados a la red empresarial y en funcionamiento.

En el caso de la configuración de la seguridad y validación de vulnerabilidades de los ordenadores se presentan dos necesidades distintas:

1. **Validación de las maquetas** utilizadas para el planchado de los nuevos ordenadores. Cada vez que se prepare o actualice una maqueta interesará validar que está correctamente configurada y libre de vulnerabilidades.

2. **Validación de la configuración de seguridad y chequeo de vulnerabilidades de todo el parque de ordenadores**. Aún que un ordenador se haya configurado con una maqueta validada, puede ser que con el paso del tiempo o acciones realizadas por el usuario su configuración no sea la correcta o esté expuesto a vulnerabilidades. Los principales motivos pueden ser:
    a. Modificaciones por parte del usuario de configuraciones de seguridad (sobre todo si el usuario tiene derechos de administración)
    b. Sistema Operativo o aplicaciones instaladas que no han sido actualizados con los últimos parches de seguridad.
    c. Nuevas aplicaciones instaladas por el usuario.

Nota: El objetivo del capítulo 7 es validar la utilidad de la solución Nessus Profesional para la validación de la seguridad de los ordenadores. Entender para que es útil, y sus limitaciones. Por ese motivo, en este capítulo no se entrará ni se documentará en detalle todos los pasos y configuraciones necesarias (que en la mayoría de los casos serían muy repetitivas versus lo ya explicado para los servidores)

## 7.1 Validación seguridad de las maquetas de ordenadores de Usuario.

Para la validación de la seguridad de las maquetas de usuario, se realizará las acciones similares a las realizadas con los servidores:

1. Validación de la configuración de seguridad.
2. Validación que la maqueta está libre de vulnerabilidades

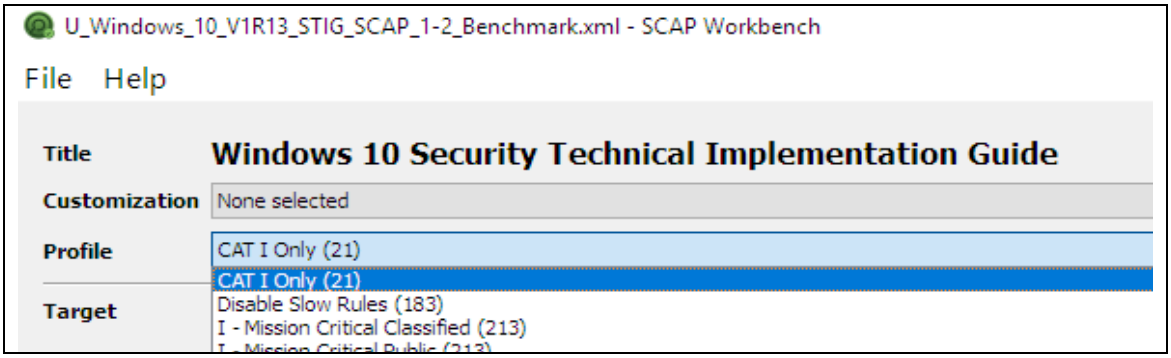
Los mismos escaneos que se definan en este apartado, serán los que se utilizarán en el escaneo del parque de ordenadores.

### 7.1.1 Validación configuración de seguridad maqueta para ordenadores usuarios.

Como en el caso de los servidores, se descarga del mismo repositorio el fichero XCCDF más actualizado con todas las reglas especificadas por STIG para Windows 10. En concreto se baja la versión 'V1R13'.

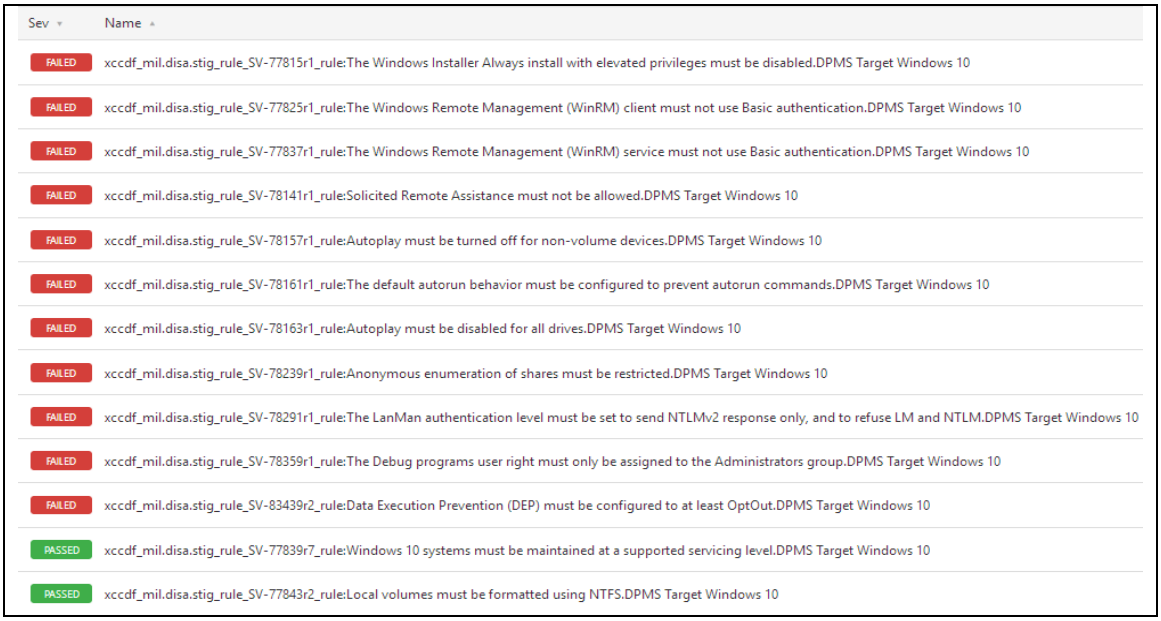
En este caso se comprueba que la versión 'V1R13' tiene definidas 213 reglas de seguridad para Windows 10. De ellas 21 reglas son de categoría 1.

Se decide validar la configuración de seguridad de la maqueta contra el perfil de seguridad 'CAT I only' ya definido en el fichero XCCDF descargado de NIST que incluye las 21 reglas de categoría 1.




Se crea un escaneo de Nessus tipo XCCDF utilizando el perfil 'CAT I only' contra un ordenador recién planchado con la maqueta que se quiere validar.

Realizado el escaneo se detecta que la configuración de la maqueta solo cumple 10 de las 21 reglas de seguridad de categoría 1.
**Acción Interna:** Se decide cambiar la configuración de la maqueta para que cumpla como mínimo todas las 21 reglas de categoría 1.



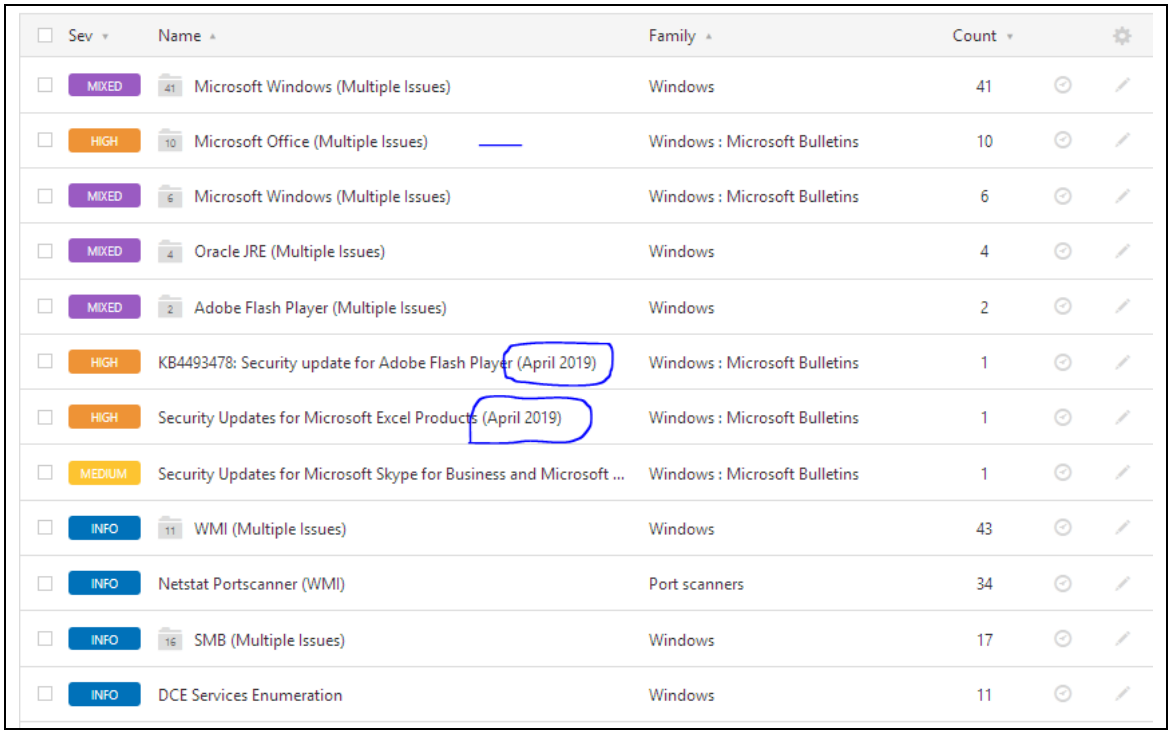
### 7.1.2 Verificación vulnerabilidades de la maqueta para ordenadores usuarios.

Para validar que la maqueta está libre de vulnerabilidades se configura un escaneo de Nessus tipo 'advanced' seleccionando todos los grupos de plugins de Nessus que interesan:

- Windows (4.247 plugins ): Básicamente validaciones de aplicaciones que se pueden instalar en entornos Windows, por ejemplo: Acrobat reader, winrar, etc.
- Windows Microsoft bulletins (1.547 plugins): validaciones de los parches de seguridad de windows
- Otros: Plugins específicos para validar servicios que pueden estar instalados en el ordenador: DNS, FTP, Webservers, Denial of Service, Databases, Backdoors

Se comprueba que el resultado del escaneo de la maqueta es bastante correcto. No hay ninguna vulnerabilidad crítica y unas pocas High y Medium. Las que se reportan como 'mixed', no tienen ninguna vulnerabilidad critica dentro. En muchos casos las vulnerabilidades High corresponden a parches publicados en el mes de abril que aún no han sido incluidos en la maqueta.

En este caso, será importante validar que los ordenadores se actualizan de forma periódica con las actualizaciones de seguridad de aplicaciones y sistema operativo. (siguiente apartado)



| Sev | Name | Family | Count |
|---|---|---|---|
| MIXED | Microsoft Windows (Multiple Issues) | Windows | 41 |
| HIGH | Microsoft Office (Multiple Issues) | Windows : Microsoft Bulletins | 10 |
| MIXED | Microsoft Windows (Multiple Issues) | Windows : Microsoft Bulletins | 6 |
| MIXED | Oracle JRE (Multiple Issues) | Windows | 4 |
| MIXED | Adobe Flash Player (Multiple Issues) | Windows | 2 |
| HIGH | KB4493478: Security update for Adobe Flash Player (April 2019) | Windows : Microsoft Bulletins | 1 |
| HIGH | Security Updates for Microsoft Excel Products (April 2019) | Windows : Microsoft Bulletins | 1 |
| MEDIUM | Security Updates for Microsoft Skype for Business and Microsoft ... | Windows : Microsoft Bulletins | 1 |
| INFO | WMI (Multiple Issues) | Windows | 43 |
| INFO | Netstat Portscanner (WMI) | Port scanners | 34 |
| INFO | SMB (Multiple Issues) | Windows | 17 |
| INFO | DCE Services Enumeration | Windows | 11 |

## 7.2 Validación de la seguridad de todo el parque de ordenadores.

7.2.0 Estrategia escaneo parque ordenadores.

Aún que se pretende utilizar las mismas técnicas aplicadas anteriormente para escanear los ordenadores de usuarios, se plantea la dificultad de como escanear todo el parque de ordenadores.
Los escaneos utilizados en los apartados anteriores con Nessus, necesitan que durante el escaneo el ordenador o servidor esté funcionando y conectado a la red empresarial.
Aún que se pueden seleccionar los mejores momentos para lanzar un escaneo 'online' del parque de ordenadores (viernes por la mañana cuando la mayoría de la fuerza comercial está en la oficina), nunca se podrá escanear el 100% de los ordenadores pues algunos estarán apagados o fuera de la oficina.
Se investiga que opciones ofrece Nessus para solventar este problema. Consultada la documentación se confirma que es posible configurar un escaneo utilizando un Agente instalado en el ordenador. Es decir, es cada ordenador que, de forma periódica, cuando esté conectado a la red empresarial enviará la información del escaneo configurado al servidor Nessus que lo consolidará en el informe del escaneo. Los principales beneficios de utilizar el escaneo por agente son:

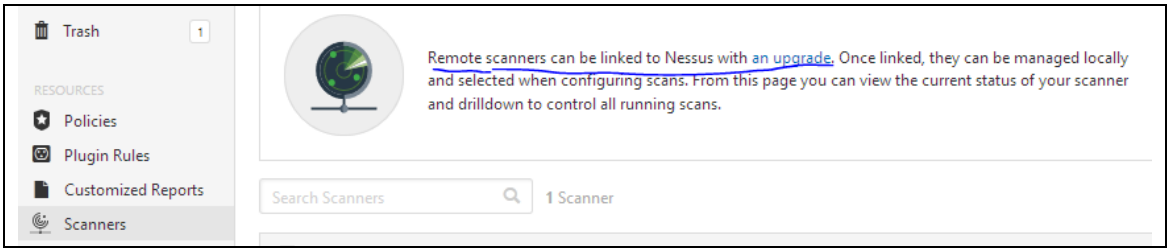
- Se asegura el escaneo de todos los ordenadores empresariales.
- Se minimiza el impacto en tráfico de red al realizar escaneos masivos.

**Agents**

Agents increase scan flexibility by making it easy to scan assets without needing ongoing host credentials or assets that are offline. Additionally, agents enable large-scale concurrent scanning with little network impact.

The **Agents** page displays the Linking Key and a list of linked agents. You can click on a linked agent to view details about that agent. There are four tabs available on the **Agents** page: **Linked Agents**, **Agent Groups**, **Blackout Windows**, and **Agent Settings**.

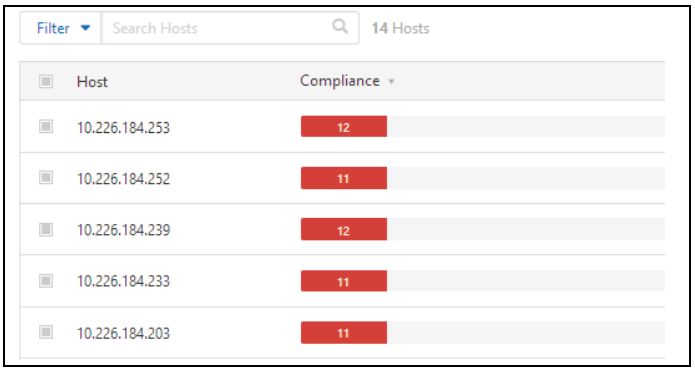
Lamentablemente la versión utilizada de Nessus (Nessus Profesional) que es la más económica no tiene licenciado el uso de escáneres en equipos remotos.
Para ello es necesario actualizar a una versión superior como Nessus Security center (tenable.sc). Es posible que en el futuro se plantee esta opción para tener cubierta esta necesidad completamente. De momento se seguirá utilizando Nessus profesional para realizar 'muestreos' del parque de ordenadores, detectando potenciales problemas y ejecutando las acciones correctivas necesarias como distribución de configuraciones vía GPOs, instalaciones de parches y actualización de versiones de software.



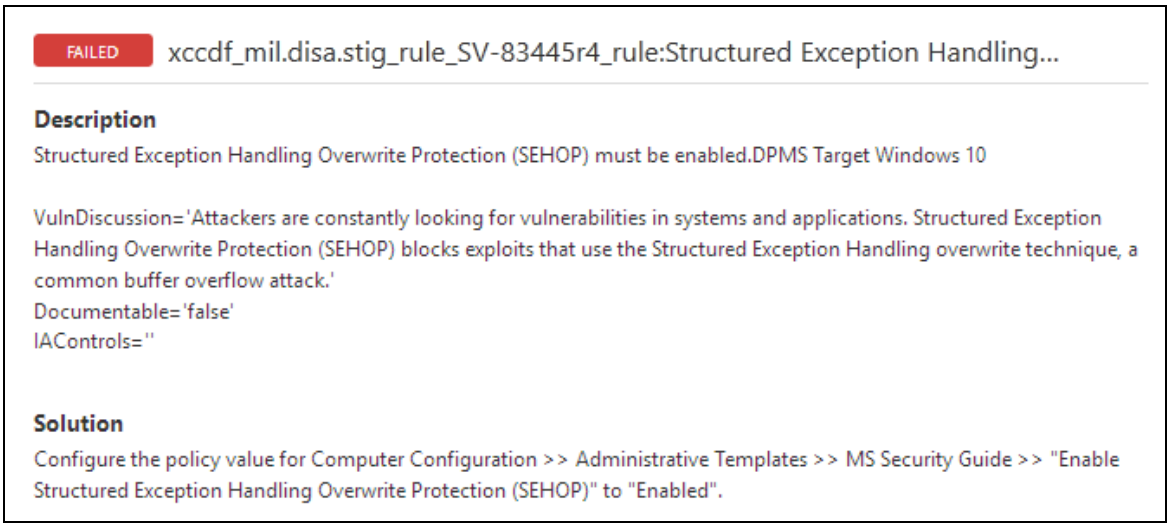
### 7.2.1 Validación configuración de seguridad del parque de ordenadores.

Realizada la comprobación de la configuración de la seguridad de la maqueta para planchar ordenadores, se realiza un escaneo sobre un número limitado de ordenadores para comprobar si su configuración de seguridad ha variado versus la maqueta con el paso del tiempo o por las acciones de los usuarios.

El proceso se realiza un viernes por la tarde con todos los ordenadores encendidos y conectados a la red en ese momento (14 equipos), pocos, pero suficientes para comprobar si la configuración de seguridad ha variado versus la maqueta.
Se comprueba que 8 ordenadores incumplen 11 reglas de seguridad (las mismas reglas que la maqueta) y 6 incumplen 12 reglas de seguridad (una más que la maqueta).
Se comprueba que los ordenadores que incumplen una regla adicional habían sido configurados con una maqueta anterior a la actual.




En concreto la regla de seguridad adicional no implementada en algunos ordenadores es la referente al control SEHOP que no está activado.




**Acción Interna:** Aún que las nuevas maquetas tengan la configuración de seguridad correcta, es necesario propagar las configuraciones de seguridad a los ordenadores actuales y asegurar que se mantendrán correctas con el paso del tiempo.

Se decide crear un GPO para que propague las 21 reglas de categoría 1 a todos los ordenadores Windows 10 el parque empresarial. Con esta acción se resolverán las configuraciones incorrectas actuales (11 o 12 reglas incumplidas) y se evitará el incumplimiento futuro de cualquier de las 21 reglas de categoría 1.
Periódicamente será necesario validar en NIST si se ha actualizado las reglas de seguridad STIG para Windows 10, validando el contenido de las nuevas versiones.

### 7.2.2 Verificación vulnerabilidades del parque de ordenadores.

Para validar el estado de exposición de los ordenadores empresariales a vulnerabilidades se configura un escaneo de Nessus tipo 'advanced' seleccionando todos los grupos de plugins de Nessus que interesan:

- Windows (4.247 plugins ): Básicamente validaciones de aplicaciones que se pueden instalar en entornos Windows, por ejemplo: Acrobat reader, winrar, etc.
- Windows Microsoft bulletins (1.547 plugins): validaciones de los parches de seguridad de windows
- Otros: Plugins específicos para validar servicios que pueden estar instalados en el ordenador: DNS, FTP, Webservers, Denial of Service, Databases, Backdoors

En este caso se lanza un escaneo en un miércoles por la tarde El escaneo que incluye todas las subsedes en España dura más de 6 horas. Se escanean un total de 180 equipos de un total potencial de 300.
Una vez finalizado el escaneo se comprueba que se permite visualizar los resultados estructurados de dos formas, en todas ellas se puede ordenar y filtrar los resultados por varios criterios:

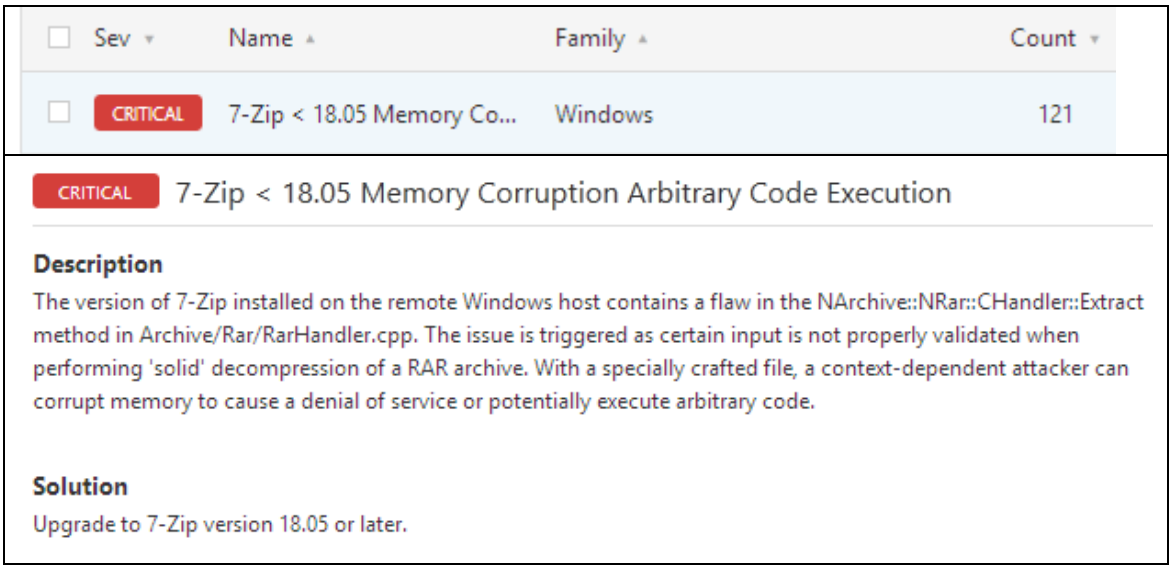
1. Visualización por Ordenador: Interesante para priorizar y buscar aquellos ordenadores que tengan incidencias de severidad critica.
2. Visualización por Vulnerabilidad: Permite filtrar por nivel de vulnerabilidad, y ordenar por número de sistemas afectados por cada vulnerabilidad. Permite priorizar la resolución de problemas que afectan a múltiples ordenadores y dejar para más tarde las vulnerabilidades que afectan a unos pocos ordenadores.

Nessus también permite exportar los resultados a distintos formatos (pdf, html, …) y con distintos niveles de detalle. Es muy útil para realizar informes que puedan ser consultados sin necesidad de acceder a la solución Nessus.

Los resultados aportan conclusiones importantes y obligan a tomar acciones para resolver algunos problemas de seguridad importantes.

1. El sistema operativo de los ordenadores y las aplicaciones Microsoft están actualizadas con los últimos parches de seguridad. Esto es debido a que la empresa tiene una solución centralizada y gestionada por comporte para controlar y distribuir parches de seguridad.
2. Se detectan aplicaciones instaladas en múltiples ordenadores con versiones obsoletas con vulnerabilidades de nivel crítico o alto. Se comprueba que en algunos casos son aplicaciones instaladas en la maqueta inicial y en otros casos son aplicaciones instaladas por el

mismo usuario. Como ejemplo se encuentran versiones obsoletas de Firefox, Chrome, 7ZIP, VLC … A continuación, el ejemplo de vulnerabilidad con más ocurrencias (121 de 180 equipos escaneados), relativa a una versión de 7-ZIP con una vulnerabilidad crítica.




**Acción Interna:** Utilizando la misma solución de parcheado de aplicaciones (IBM Bigfix) que también permite distribución de software, se lanzan tareas globales para desinstalar las aplicaciones obsoletas detectadas e instalar las nuevas versiones.

### 7.3 Conclusiones

La solución actual 'Nesus Profesional' no es la mejor solución para validar de forma continua la configuración de seguridad y el estado de vulnerabilidades de los ordenadroes empresariales.
El hecho de solo analizar los ordenadores en funcionamiento y conectados a la red empresarial en el momento del escaneo impide tener un repositorio global y detallado del estado de todos los ordenadores.
En qualquier caso, sigue siendo un solución que aporta valor pues nos permite realizar muestras significativas sobre ordenadores que esten conectados en un momento determinado, lo que permite la detección de problemas generales y la resolución de los mismos. Tiene el riesgo de no detectar algún problema grabe de seguridad que afecte a uno o pocos ordenadores.
Com se ha visto, se puede solucionar esta limitación utilizando otro producto de Nessus (upgrade) que permite realizar escaneos por agente instalado en cada uno de los ordenadores.

# 8. Conclusiones y Trabajo Futuro

## 8.1 Conclusiones

Actualmente las empresas tienen un elevado o total nivel de dependencia de las aplicaciones informáticas, y por tanto de los servidores donde estas están alojadas. Es por ese motivo, que en un mundo donde los cyber ataques aumentan y se sofistican continuamente es muy importante tener un alto nivel de seguridad de los servidores.

Muchos de los desastres producidos por ataques de seguridad, se podrían haber evitado si no se hubieran descuidado tareas obvias y básicas como el parcheado de los sistemas y la configuración correcta de los servidores. Es decir, a veces, se invierten cantidades elevadas de dinero y tiempo en configurar sistemas de seguridad y se descuidan tareas básicas.

Por esto motivo es muy importante definir procesos y soluciones que automaticen el control continuo en el tiempo de la seguridad de los servidores y sistemas. Este pues, era el objetivo principal de este trabajo: seleccionar y configurar alguna/s soluciones y definir los procesos para garantizar de forma continua la seguridad de los servidores:

- Su correcta configuración a nivel de políticas de seguridad
- La validación de las versiones y parcheado del Sistema operativo y aplicaciones (para asegurar que no tienen vulnerabilidades importantes de seguridad).

Para conseguir el objetivo final, se planteaban 5 objetivos concretos, los que se han conseguido resolver al menos con una solución o proceso.

- **Obtener conocimiento de soluciones en el mercado que pueden trabajar con el protocolo SCAP:** Inicialmente se planteó el estudio 9 distintas soluciones, pero 4 de ellas no se han podido probar por no haber conseguido versiones de prueba o por falta de tiempo. Se ha decidido utilizar para este trabajo 2 de las soluciones probadas: Nessus Profesional y OpenSCAP.
- **Obtener conocimiento de las especificaciones SCAP**: Se ha obtenido conocimiento de las especificaciones SCAP, sobretodo de ‘Extensible Configuration Checklist Description Format (XCCDF)’ que es un lenguaje de especificación para escribir listas de verificación de seguridad.
- **Control Configuración seguridad de los servidores según las normas de seguridad de la empresa.** Se han utilizado repositorios públicos de ficheros XCDDF (NIST), seleccionando los ficheros más actualizados para el sistema operativo a validar, y modificándolos para ajustar la validación de la configuración de seguridad para que este alineada con la política corporativa de seguridad empresarial.
- **Control de vulnerabilidades.** La intención inicial era realizar el control de vulnerabilidades utilizando ficheros OVAL para realizar las validaciones. Finalmente se ha comprobado que lo más útil era utilizar los propios repositorios y plugins suministrados por Nessus, tanto para análisis específicos o globales de vulnerabilidades.

- **Validación que las soluciones SCAP permiten cubrir de forma satisfactoria y fiable la seguridad de los servidores:** Se ha confirmado que mediante la herramienta comercial 'Nessus Profesional' se puede controlar de forma satisfactoria y automatizada la seguridad de los servidores, tanto su configuración de seguridad como potenciales vulnerabilidades. Se comprueba que:
    - La mayoría de los servidores no tienen configuradas correctamente todas las políticas de seguridad. Se empiezan acciones correctoras mediante la distribución automática de las configuraciones necesarias vía GPO's distribuidas por el controlador de dominio.
    - En varios casos las vulnerabilidades más grabes provienen de versiones no actualizadas de aplicaciones, pues en general el sistema operativo esta actualizado con los últimos parches de seguridad. Se empiezan acciones correctivas mediante distribuciones automáticas de software para corregir este problema.

  Referente a la solución de código abierto OpenSCAP, se considera muy interesante, pero sobre todo para entornos LINUX. Hace poco que ofrece la posibilidad de validar entornos Microsoft y aún tiene algunos fallos o carencias que no permite validar el 100% de los controles. Por otro lado, en entornos con un número elevado de servidores es necesario definir procesos para automatizar las validaciones y análisis con OpenSCAP pues la propia aplicación no lo contempla.

En resumen, este ha sido un trabajo muy interesante que ha permitido dar una respuesta válida para desarrollar de forma satisfactoria el control de la seguridad de los servidores empresariales.

### 8.2 Trabajo Futuro

El mundo de la seguridad no es estático, y por tanto se plantean las acciones necesarias para mantener la seguridad de los servidores. A nivel de empresa se toman las siguientes decisiones:

- Revisar de forma semestral, en repositorios públicos (NIST), las novedades de reglas de seguridad recomendadas para los sistemas operativos, por si es necesario actualizar las definiciones de los escaneos y las GPO's para distribuir las configuraciones de seguridad.
- En caso de cambios en las políticas de seguridad corporativa, actualizar las definiciones de los escaneos y las GPO's para distribuir las configuraciones de seguridad.
- Escanear tanto a nivel de configuración de seguridad como de vulnerabilidades todos los servidores de forma mensual, y cualquier servidor en momento de su bastionado para realizar cualquier acción correctora necesaria.

En este proyecto se ha realizado una pequeña investigación no prevista en el plan de proyecto inicial (capitulo 7) para validar si se podía utilizar la misma solución (Nessus Profesional) para validar la seguridad de los ordenadores empresariales.

Se ha comprobado que no es la mejor solución para validar de forma continua la configuración de seguridad y el estado de vulnerabilidades de los ordenadores empresariales. El hecho de que solo se puedan analizar los ordenadores en funcionamiento y conectados a la red empresarial en el momento del escaneo impide tener un repositorio global y detallado del estado de todos los ordenadores.

Un trabajo futuro interesante seria pues encontrar la mejor solución y definir un proceso para validar de forma continua la seguridad de los ordenadores empresariales.
Hay varias soluciones que resuelven de forma satisfactoria este problema, en general todas instalan un agente en los ordenadores a auditar de forma que este envía la información al servidor central al conectarse a la red empresarial.

# 9. Bibliografia


| | | |
|---|---|---|
| [1] | https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol | 03/01/19 |
| [2] | https://csrc.nist.gov/Projects/scap-validation-program/Validated-Products-and-Modules | 03/01/19 |
| [3] | https://oval.mitre.org/about/faqs.html#a1 | 03/01/19 |
| [4] | https://csrc.nist.gov/Projects/scap-validation-program/Validated-Products-and-Modules | 04/01/19 |
| [5] | https://cyber.trackr.live/scap/xccdf_mil.disa.stig_benchmark_Windows_2012_DC_STIG/002.015/2 | 10/03/19 |
| [6] | http://blog.siphos.be/2013/12/xccdf-documenting-a-bit-more-than-just-descriptions/ | 10/03/19 |
| [7] | https://csrc.nist.gov/CSRC/media/Publications/nistir/7275/rev-4/final/documents/nistir-7275r4_updated-march-2012_clean.pdf | 10/03/19 |
| [8] | https://blog.ragasys.es/administracion-de-directivas-de-grupo-gpo-sobre-ms-windows-server-2016 | 01/04/19 |
| [9] | https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/ | 07/04/19 |
| [10] | https://www.rootusers.com/deploy-configurations-to-domain-and-non-domain-joined-servers-with-security-compliance-manager-scm/ | 07/04/19 |
| [11] | http://www.mustbegeek.com/how-to-apply-gpo-to-computer-group-in-active-directory/ | 26/04/19 |
| [12] | https://www.tenable.com/plugins | 01/05/19 |

# 10. Anexos

## 10.1 ANEXO 1 – Tabla comparativa reglas de Seguridad empresarial para distintas versiones de Windows Server.

| Categoría | Regla W2008R2 | Regla W2012 | Regla W2016 | Política |
|---|---|---|---|---|
| Acceso Remoto | xccdf_mil.disa.stig_rule_SV-32318r1_rule | xccdf_mil.disa.stig_rule_SV-52885r1_rule | N/A | La solicitud de asistencia remota tiene que estar deshabilitada |
| Acceso Remoto | N/A | xccdf_mil.disa.stig_rule_SV-51752r1_rule | xccdf_mil.disa.stig_rule_SV-88257r1_rule | EL cliente de Windows remote Management no tiene que utilizar autentificación básica |
| Acceso Remoto | N/A | xccdf_mil.disa.stig_rule_SV-51755r2_rule | xccdf_mil.disa.stig_rule_SV-88263r1_rule | EL Servicio de Windows remote Management no tiene que utilizar autentificación básica |
| Actualización y Versiones seguras | xccdf_mil.disa.stig_rule_SV-32242r3_rule | xccdf_mil.disa.stig_rule_SV-53189r2_rule | xccdf_mil.disa.stig_rule_SV-87891r1_rule | El service pack tiene que estar oficialmente soportado por MS. (MS sigue emitiendo parches de seguridad para el Service Pack activo) |
| Actualización y Versiones seguras | xccdf_mil.disa.stig_rule_SV-32300r1_rule | xccdf_mil.disa.stig_rule_SV-52865r1_rule | xccdf_mil.disa.stig_rule_SV-88355r1_rule | La autenticación 'LanMan' se tiene que configurar para usar solo el protocolo NTLMv2, prohibiendo protocolos menos seguros como NTLM o LM |
| Asignación Derechos de acceso | xccdf_mil.disa.stig_rule_SV-32248r1_rule | xccdf_mil.disa.stig_rule_SV-52843r3_rule | xccdf_mil.disa.stig_rule_SV-87899r1_rule | Los volúmenes locales tienen que soportar atributos NTFS (para garantizar el control apropiado de acceso y seguridad) |
| Asignación Derechos de acceso | xccdf_mil.disa.stig_rule_SV-32287r2_rule | xccdf_mil.disa.stig_rule_SV-52108r3_rule | xccdf_mil.disa.stig_rule_SV-88399r1_rule | No se debe asignar a ninguna cuenta la propiedad de actuar como parte del sistema operativo |

| | | | | |
|---|---|---|---|---|
| Asignación Derechos de acceso | N/A | xccdf_mil.disa.stig_rule_SV-51175r3_rule | N/A | Permisos apropiados para los ficheros del directorio Activo. |
| Auto Play | xccdf_mil.disa.stig_rule_SV-32315r1_rule | xccdf_mil.disa.stig_rule_SV-52879r2_rule | xccdf_mil.disa.stig_rule_SV-88213r1_rule | Autoplay tiene que estar deshabilitado. (es un riesgo y no tiene ningún sentido en un servidor) |
| Auto Play | xccdf_mil.disa.stig_rule_SV-32460r1_rule | xccdf_mil.disa.stig_rule_SV-53126r2_rule | xccdf_mil.disa.stig_rule_SV-88209r1_rule | Autoplay se tiene que deshabilitar para cualquier recurso que no sea un volumen de sistema. En Windows 2008R2 la regla no está marcada como de Nivel 1. |
| Auto Play | xccdf_mil.disa.stig_rule_SV-32467r1_rule | xccdf_mil.disa.stig_rule_SV-53124r2_rule | xccdf_mil.disa.stig_rule_SV-88211r1_rule | Por defecto el comportamiento 'autorun' se tiene que configurar para evitar comandos autorun |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32314r1_rule | xccdf_mil.disa.stig_rule_SV-52880r1_rule | xccdf_mil.disa.stig_rule_SV-87977r1_rule | Se tiene que deshabilitar la encriptación 'reversible' de password,por ser muy poco segura. En Windows 2008R2 la regla no está marcada como de Nivel 1. |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32319r1_rule | xccdf_mil.disa.stig_rule_SV-52886r1_rule | xccdf_mil.disa.stig_rule_SV-88285r1_rule | No se pueden permitir cuentas locales sin password |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32339r1_rule | xccdf_mil.disa.stig_rule_SV-52892r2_rule | xccdf_mil.disa.stig_rule_SV-88351r1_rule | Evitar que el sistema almacene el HASH del LAN Manager password |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32284r2_rule | xccdf_mil.disa.stig_rule_SV-52848r1_rule | xccdf_mil.disa.stig_rule_SV-87963r1_rule | Limite número passwords incorrectos |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32285r3_rule | xccdf_mil.disa.stig_rule_SV-52849r2_rule | xccdf_mil.disa.stig_rule_SV-87965r1_rule | Reseteo contador passwords fallidos como mínimo 15 minutos |

| | | | | |
|---|---|---|---|---|
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32286r3_rule | xccdf_mil.disa.stig_rule_SV-52850r2_rule | xccdf_mil.disa.stig_rule_SV-87961r2_rule | Desbloqueo automático cuenta (cuando habilitado) por passwords fallidos no inferior a 15 minutos |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32288r2_rule | xccdf_mil.disa.stig_rule_SV-52851r1_rule | xccdf_mil.disa.stig_rule_SV-87969r1_rule | Duración máxima password |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32289r2_rule | xccdf_mil.disa.stig_rule_SV-52852r1_rule | xccdf_mil.disa.stig_rule_SV-87971r1_rule | Duración mínima password |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32298r2_rule | xccdf_mil.disa.stig_rule_SV-52863r2_rule | xccdf_mil.disa.stig_rule_SV-87975r1_rule | Política complejidad de password tiene que estar activada |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32360r1_rule | xccdf_mil.disa.stig_rule_SV-52930r1_rule | N / A | Una vez salta el protector de pantalla, al cabo de pocos segundos se tiene que pedir contraseña para quitar el protector de pantalla |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32369r1_rule | xccdf_mil.disa.stig_rule_SV-52938r2_rule | xccdf_mil.disa.stig_rule_SV-87973r1_rule | Longitud mínima passwords |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32371r1_rule | xccdf_mil.disa.stig_rule_SV-52941r1_rule | N / A | No presentar el ultimo usuario que ha accedido en la pantalla de logon. |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32496r1_rule | xccdf_mil.disa.stig_rule_SV-52958r1_rule | xccdf_mil.disa.stig_rule_SV-88231r1_rule | No permitir grabar password en escritorio remoto |
| Cuentas Y contraseñas | xccdf_mil.disa.stig_rule_SV-32428r1_rule | xccdf_mil.disa.stig_rule_SV-53132r1_rule | xccdf_mil.disa.stig_rule_SV-88197r1_rule | Es necesario autentificarse al despertar el sistema. |
| Debug y Logs | xccdf_mil.disa.stig_rule_SV-32444r3_rule | xccdf_mil.disa.stig_rule_SV-52115r3_rule | xccdf_mil.disa.stig_rule_SV-88419r1_rule | Los programas de debug solo tienen que poderse ejecutar con usuario administrador |
| Debug y Logs | xccdf_mil.disa.stig_rul | xccdf_mil.disa.stig_rul | N / A | Deshabilitar logs del acceso a objetos globales del |

| | | | | |
|---|---|---|---|---|
| | e_SV-32372r2_rule | e_SV-53129r1_rule | | sistema, para evitar excesivos logs. |
| Debug y Logs | xccdf_mil.disa.stig_rule_SV-32373r1_rule | xccdf_mil.disa.stig_rule_SV-52943r1_rule | N / A | Deshabilitar logs para cada fichero que se hace backup o restore, para evitar excesivos logs. |
| Internet | N/A | xccdf_mil.disa.stig_rule_SV-51747r4_rule | xccdf_mil.disa.stig_rule_SV-88223r1_rule | Windows SmartScreen tiene que estar activo |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-32283r1_rule | xccdf_mil.disa.stig_rule_SV-52847r1_rule | xccdf_mil.disa.stig_rule_SV-88333r1_rule | Restricción para evitar que un anonymous logon pueda listar recursos del sistema (cuentas y shares) |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-32260r3_rule | xccdf_mil.disa.stig_rule_SV-52864r3_rule | N/A | El acceso anónimo al 'registro' del sistema tiene que estar restringido |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-46295r1_rule | xccdf_mil.disa.stig_rule_SV-51138r2_rule | xccdf_mil.disa.stig_rule_SV-88339r1_rule | Acceso anónimo a los 'Named Pipes' tiene que estar restringido |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-32484r2_rule | xccdf_mil.disa.stig_rule_SV-52883r2_rule | N/A | Acceso remoto a los directorios donde está el registry tiene que estar restringido |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-32317r1_rule | xccdf_mil.disa.stig_rule_SV-52884r1_rule | N/A | Acceso anónimo a las carpetas compartidas tiene que estar restringido |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-46295r1_rule | xccdf_mil.disa.stig_rule_SV-52937r1_rule | N/A | Acceso anónimo a los 'Named Pipes' y carpetas compartidas tiene que estar deshabilitado |

| | | | | |
|---|---|---|---|---|
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-33732r1_rule | xccdf_mil.disa.stig_rule_SV-53122r1_rule | xccdf_mil.disa.stig_rule_SV-88331r1_rule | No se tiene que permitir el listado des de conexión anónima de las cuentas del sistema |
| Permisos accesos anónimos | xccdf_mil.disa.stig_rule_SV-32291r2_rule | xccdf_mil.disa.stig_rule_SV-52855r1_rule | xccdf_mil.disa.stig_rule_SV-88475r1_rule | Cuenta invitado tiene que estar deshabilitada |
| Permisos administración | xccdf_mil.disa.stig_rule_SV-33392r2_rule | xccdf_mil.disa.stig_rule_SV-52113r3_rule | xccdf_mil.disa.stig_rule_SV-88411r1_rule | El permiso de crear 'objetos token' no tiene que ser asignado a ningún grupo de usuarios |
| Permisos administración | xccdf_mil.disa.stig_rule_SV-46220r1_rule | xccdf_mil.disa.stig_rule_SV-52954r1_rule | xccdf_mil.disa.stig_rule_SV-88249r1_rule | La opción que el instalador de windows siempre instale con privilegios 'elevados' se tiene que estar deshabilitada |
| Permisos administración | xccdf_mil.disa.stig_rule_SV-32377r1_rule | xccdf_mil.disa.stig_rule_SV-52947r1_rule | xccdf_mil.disa.stig_rule_SV-88371r1_rule | En caso petición elevación, se generará dialogo para confirmación del administrador |
| Permisos administración | xccdf_mil.disa.stig_rule_SV-32383r1_rule | xccdf_mil.disa.stig_rule_SV-52949r1_rule | xccdf_mil.disa.stig_rule_SV-88379r1_rule | En caso detección instalación aplicaciones, el sistema tiene que pedir la confirmación elevación privilegios y credenciales de cuenta con derechos administrador |
| Permisos Registro de windows | xccdf_mil.disa.stig_rule_SV-32484r2_rule | xccdf_mil.disa.stig_rule_SV-52931r2_rule | xccdf_mil.disa.stig_rule_SV-88021r1_rule | Acceso no autorizado remoto a los carpetas y sub carpetas donde está el registro de windows tiene que estar deshabilitado |
| Permisos Registro de windows | xccdf_mil.disa.stig_rule_SV-33310r3_rule | xccdf_mil.disa.stig_rule_SV-53123r4_rule | N/A | Los usuarios estadard (no administrador) solo tienen que tener permisos de lectura al registry WINLOGON |

| | | | | |
|---|---|---|---|---|
| Permisos Registro de windows | xccdf_mil.disa.stig_rule_SV-42619r2_rule | xccdf_mil.disa.stig_rule_SV-52956r3_rule | N/A | Los usuarios estándar (no administrador) solo tienen que tener permisos de lectura a la sección del registry (active setup / installed componenets) |
| Redes | xccdf_mil.disa.stig_rule_SV-32408r1_rule | xccdf_mil.disa.stig_rule_SV-53014r2_rule | N/A | No permitir un network bridge (puente) |
| Servicios innecesarios | xccdf_mil.disa.stig_rule_SV-33723r1_rule | xccdf_mil.disa.stig_rule_SV-52236r2_rule | xccdf_mil.disa.stig_rule_SV-87939r1_rule | El servicio de FAX tiene que estar deshabilitado si está instalado (w2008 y w2012) / No tiene que estar instalado (W2016) |
| Servicios innecesarios | xccdf_mil.disa.stig_rule_SV-33725r2_rule | xccdf_mil.disa.stig_rule_SV-52237r4_rule | xccdf_mil.disa.stig_rule_SV-87941r1_rule | El servicio de FTP tiene que estar deshabilitado si está instalado (w2008 y w2012) / No tiene que estar instalado (W2016) |
| Servicios innecesarios | xccdf_mil.disa.stig_rule_SV-33729r1_rule | xccdf_mil.disa.stig_rule_SV-52238r2_rule | xccdf_mil.disa.stig_rule_SV-87943r1_rule | El servicio de peer networking tiene que estar deshabilitado si está instalado w2008 y w2012 / EL servicio peer name resolution no tiene que estar instalado (w2016) |
| Servicios innecesarios | xccdf_mil.disa.stig_rule_SV-33731r1_rule | xccdf_mil.disa.stig_rule_SV-52239r2_rule | xccdf_mil.disa.stig_rule_SV-87945r1_rule | El servicio de Simple TCP tiene que estar deshabilitado si está instalado (w2008 y w2012) / No tiene que estar instalado (W2016) |
| Servicios innecesarios | xccdf_mil.disa.stig_rule_SV-33721r1_rule | xccdf_mil.disa.stig_rule_SV-52240r2_rule | xccdf_mil.disa.stig_rule_SV-87947r1_rule | El servicio de telnet tiene que estar deshabilitado si está instalado (w2008 y w2012) / No tiene que estar instalado (W2016) |
| Servicios innecesarios | N/A | xccdf_mil.disa.stig_rule_SV-51609r2_rule | N/A | El acceso a la tienda windows tiene que estar deshabilitado |