Ejercicios guiados con Nessus

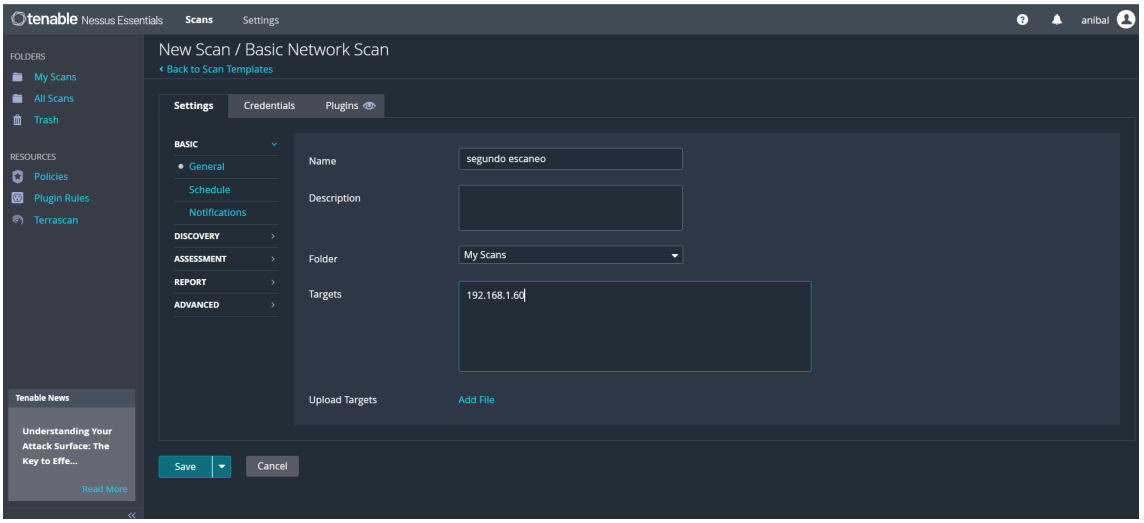
Ejercicio 1: Crear tu primer escaneo básico

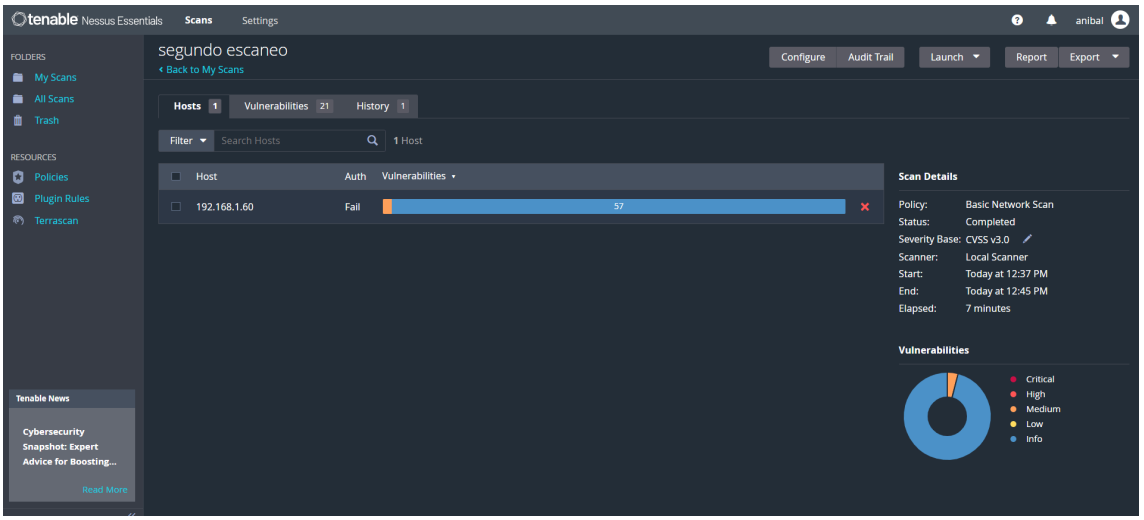
Objetivo: Aprender a crear un escaneo simple para revisar vulnerabilidades en un equipo.

Guía paso a paso:

- Abre tu navegador y entra a Nessus en https://localhost:8834.
- Inicia sesión con tu usuario y contraseña de Nessus.
- En el menú izquierdo, haz clic en **Scans**.
- Haz clic en el botón **New Scan**.
- Selecciona **Basic Network Scan**.
- Ponle un nombre al escaneo (ejemplo: *Mi primer escaneo*).
- En el campo **Targets**, escribe la IP o nombre del equipo que quieres escanear (por ejemplo: 192.168.1.10).
- Haz clic en **Save**.
- Haz clic en el triángulo de **Play** para iniciar el escaneo.

Resultado esperado: El escaneo aparece como *Running* y, al finalizar, se muestra un resumen de vulnerabilidades.





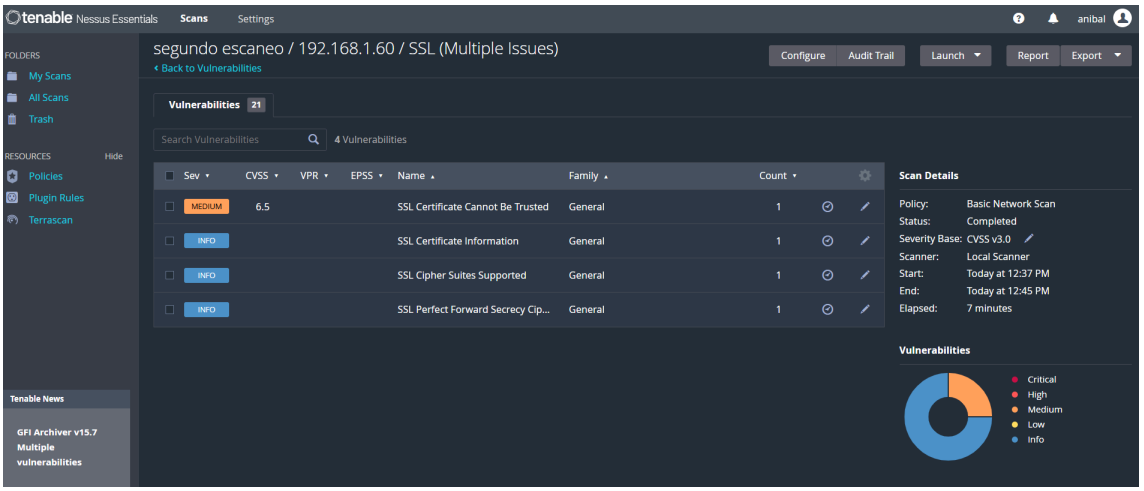
Ejercicio 2: Explorar el reporte de un escaneo

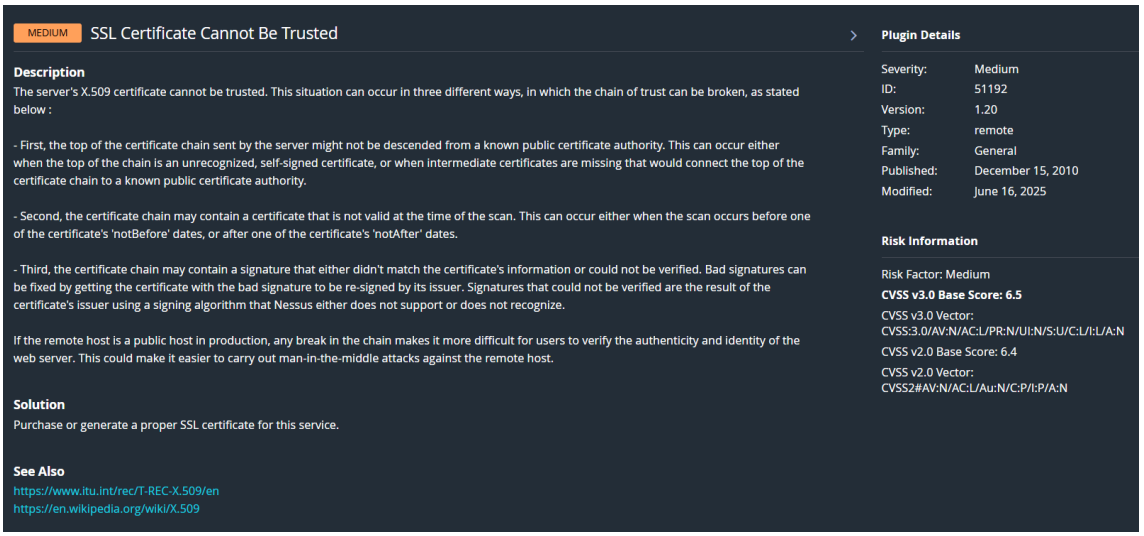
Objetivo: Aprender a interpretar los resultados que Nessus muestra después de un escaneo.

Guía paso a paso:

1. Abre un escaneo que ya hayas realizado.
2. Observa la lista de vulnerabilidades clasificadas por colores (rojo = crítico, naranja = alto, amarillo = medio, azul = bajo).
3. Haz clic sobre una vulnerabilidad para ver más detalles: descripción, solución y enlaces a información oficial.

Resultado esperado: Entiendes qué significa el nivel de severidad y sabes cómo encontrar recomendaciones para solucionarlas.



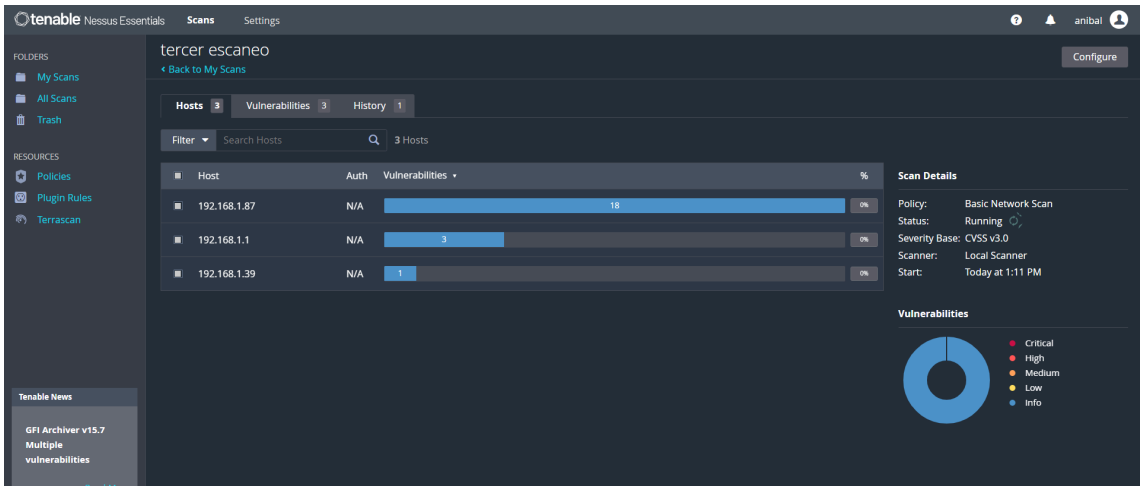


Ejercicio 3: Escaneo de varios dispositivos al mismo tiempo

Objetivo: Configurar un escaneo para revisar varios equipos en tu red de una sola vez.

Guía paso a paso:

1. En **New Scan**, crea otro **Basic Network Scan**.
2. En el campo **Targets**, escribe varias IPs separadas por comas (por ejemplo: 192.168.1.10,192.168.1.11).
3. usa un rango (ejemplo: 192.168.1.10-192.168.1.20).
4. Guarda y ejecuta el escaneo.
5. **Resultado esperado:** El reporte muestra cada dispositivo escaneado por separado con sus vulnerabilidades.



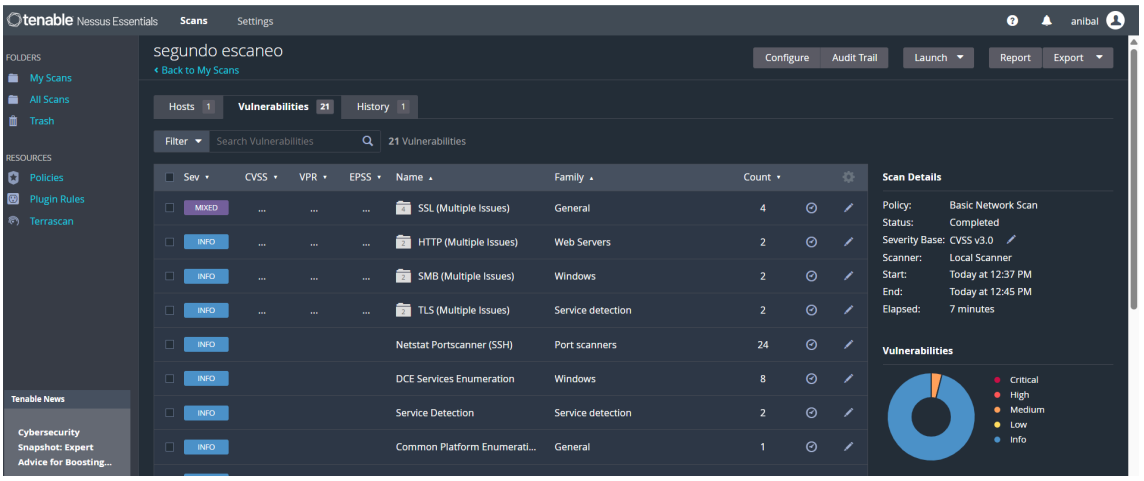
Ejercicio 4: Filtrar vulnerabilidades por severidad

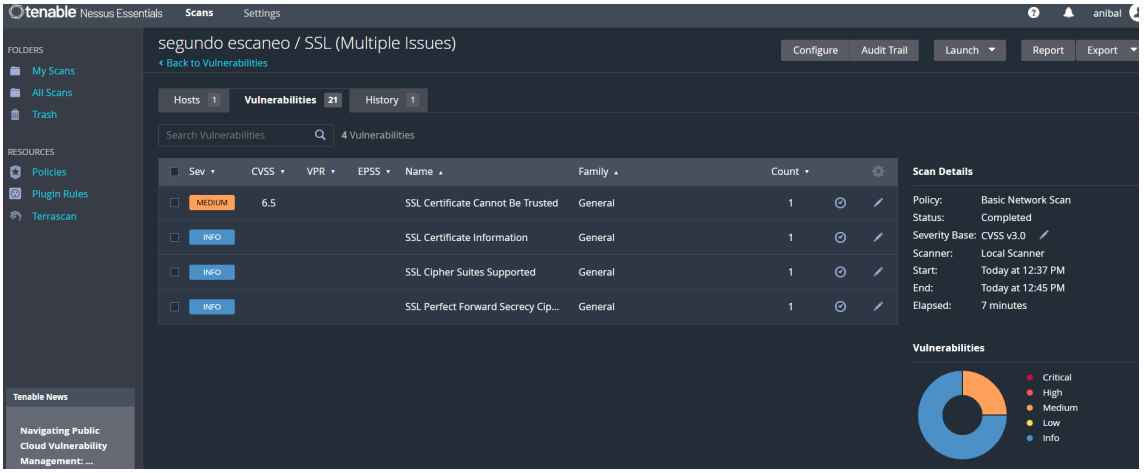
Objetivo: Aprender a priorizar la corrección de problemas graves.

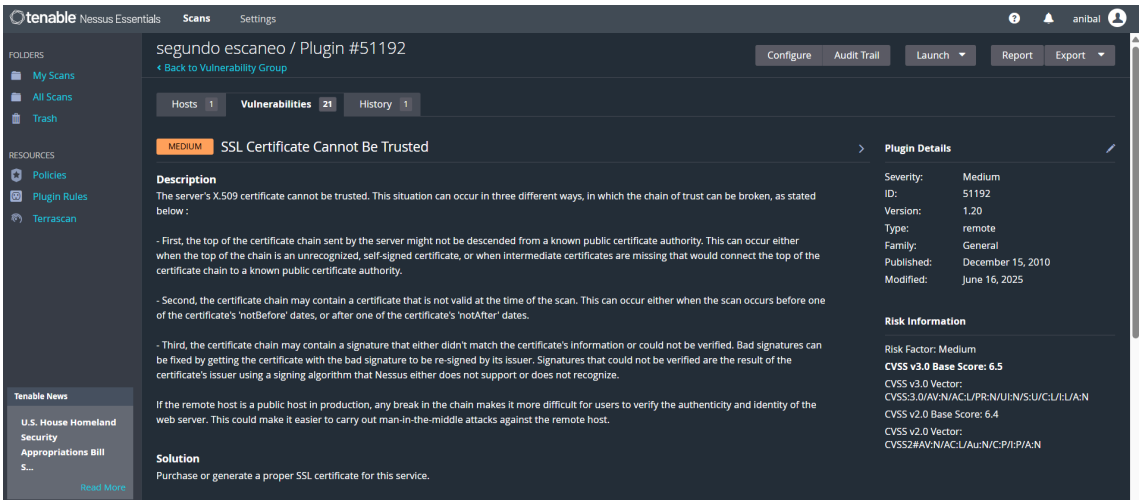
Guía paso a paso:

1. Abre un reporte de escaneo terminado.
2. En la parte superior, usa los filtros para mostrar solo vulnerabilidades de severidad **Critical** o **High**.
3. Haz una lista de estas vulnerabilidades para planificar su corrección.

Resultado esperado: Sabes identificar qué vulnerabilidades son más urgentes.







Vulnerabilidad	Severidad	Descripción resumida	Recomendación técnica
SSL Certificate Cannot Be Trusted	Media	El certificado SSL no es confiable. Puede ser autofirmado o mal encadenado	Usar certificado firmado por CA pública reconocida

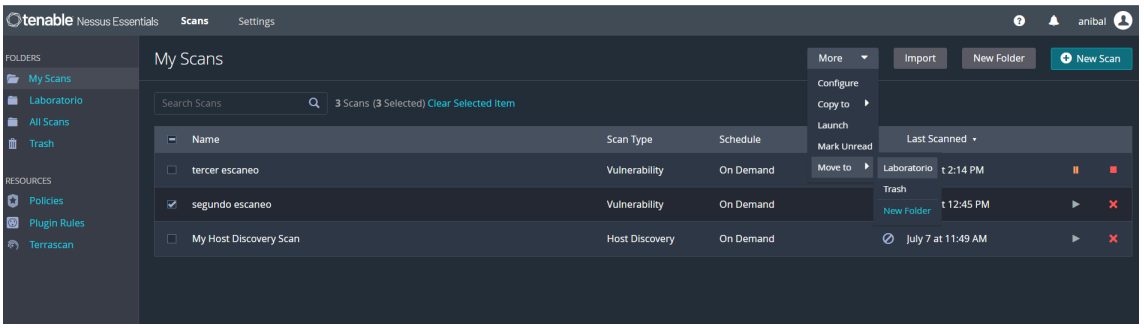
Ejercicio 5: Personalizar el nombre y carpeta de tus escaneos

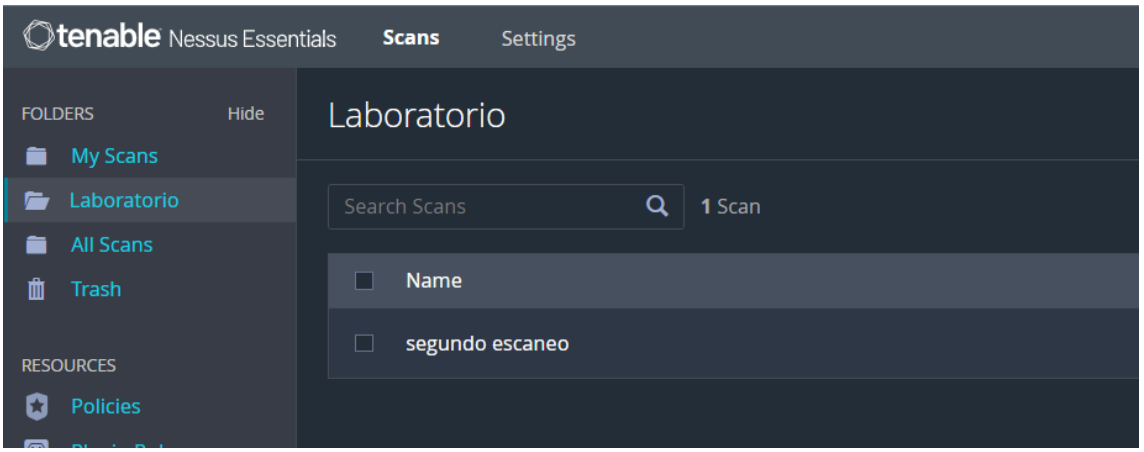
Objetivo: Organizar tus escaneos para que no se mezclen entre sí.

Guía paso a paso:

1. Al crear un escaneo nuevo, cambia el campo **Folder** para agruparlo (por ejemplo, crea una carpeta llamada *Oficina* o *Laboratorio*).
2. Usa nombres descriptivos como *Escaneo_Servidor_X* o *Escaneo_Red_Sucursal*.

Resultado esperado: Escaneos organizados, fáciles de encontrar.





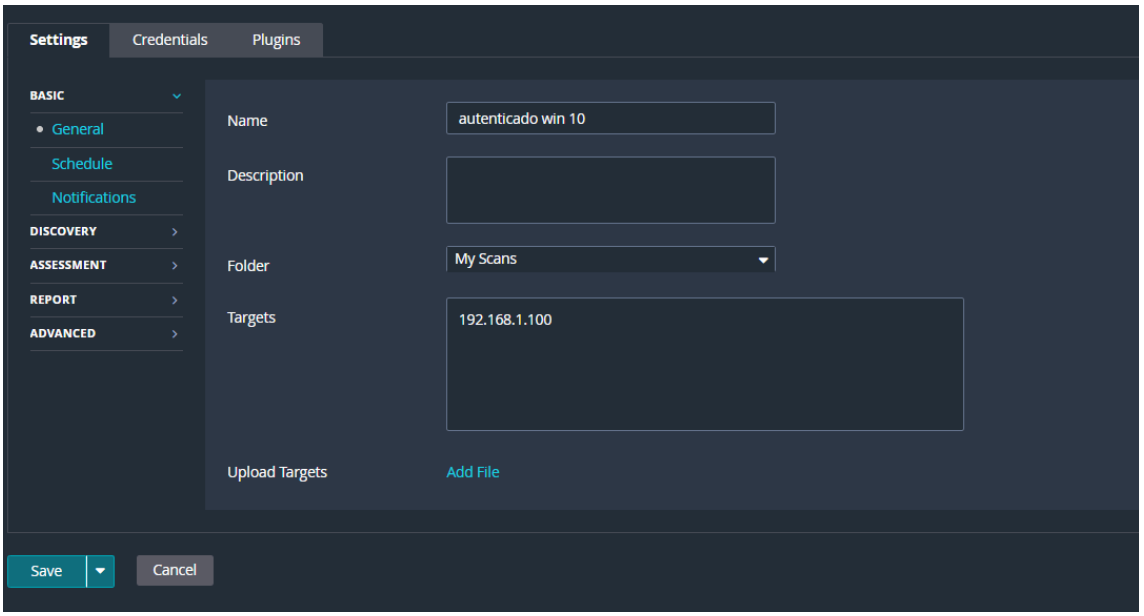
Ejercicio 6: Hacer un escaneo autenticado en Windows

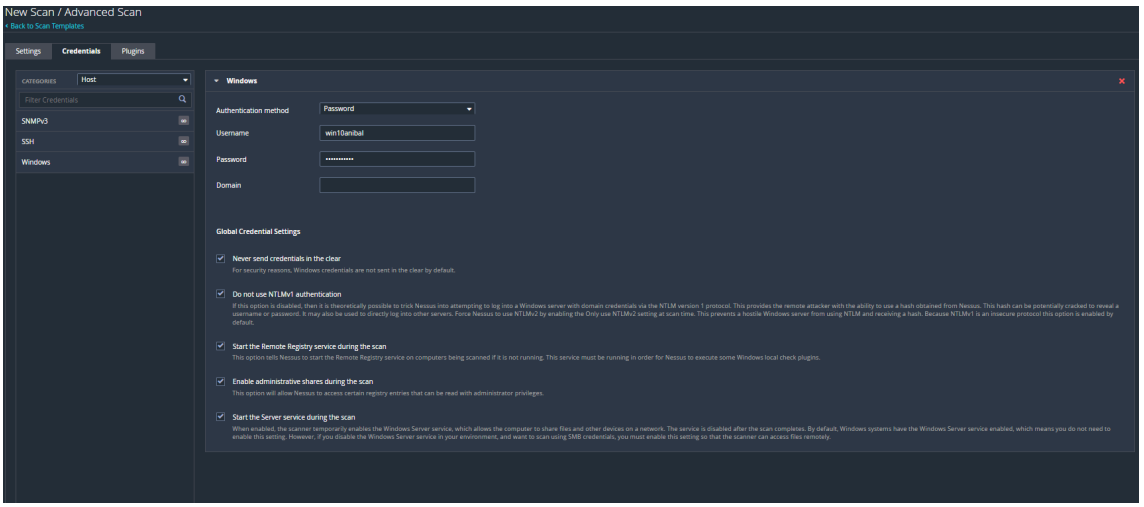
Objetivo: Aprender a usar credenciales de Windows para encontrar vulnerabilidades internas.

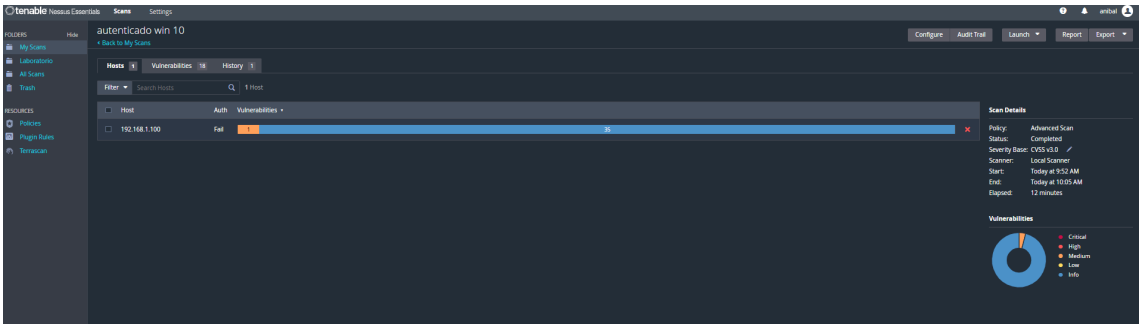
Guía paso a paso:

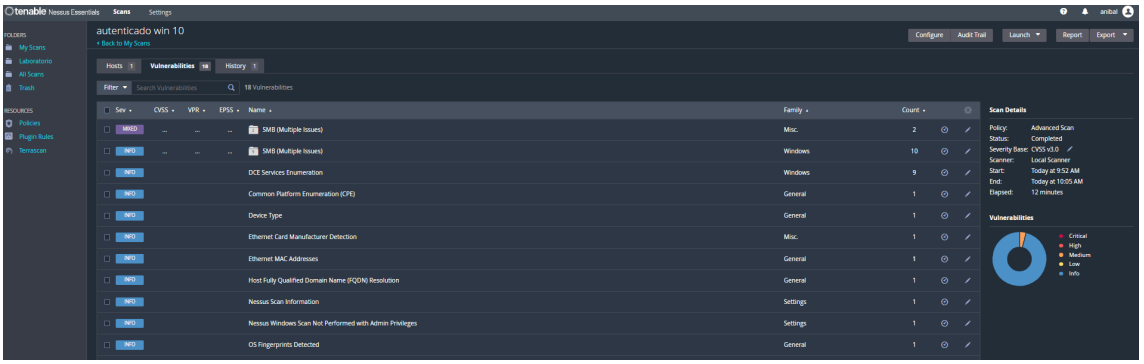
1. En el escaneo, ve a la pestaña **Credentials**.
2. Elige **Windows**.
3. Introduce un usuario y contraseña válidos que existan en el equipo objetivo.
4. Guarda y ejecuta el escaneo.

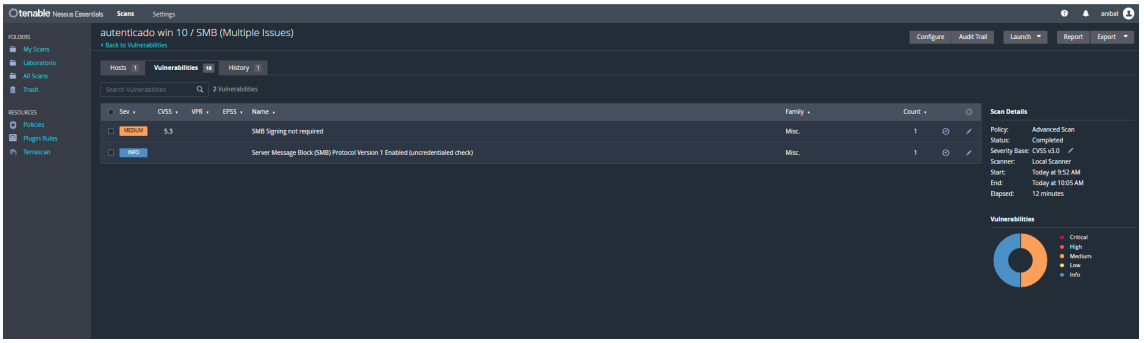
Resultado esperado: El reporte muestra más detalles como parches faltantes o configuraciones inseguras.

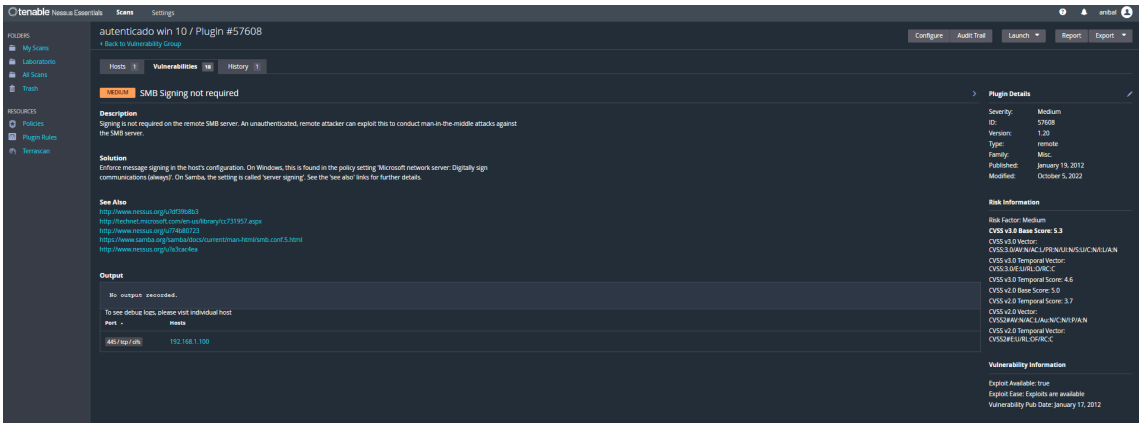

Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
autenticado win 10
Description
Folder
My Scans
Targets
192.168.1.100
Upload Targets
Add File
Save
Cancel


New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
Windows
Authentication method
Password
Username
win10anibal
Password
Domain
Global Credential Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan
Enable administrative shares during the scan
Start the Server service during the scan


autenticado win 10
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts
Vulnerabilities
History
192.168.1.100
Scan Details
Vulnerabilities







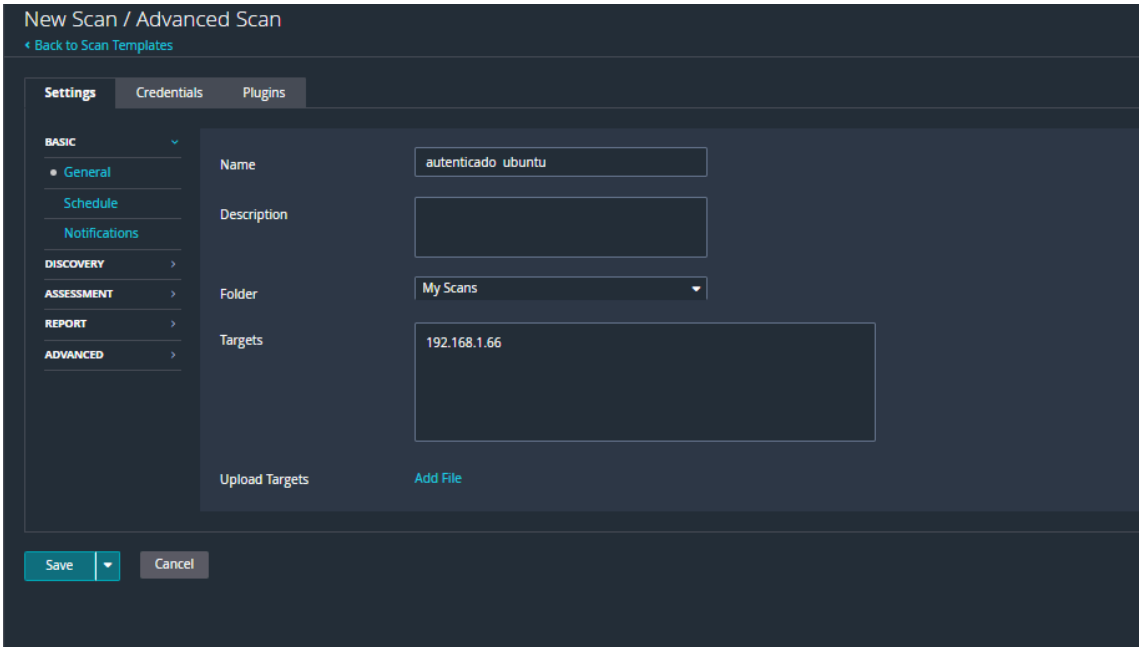
Ejercicio 7: Hacer un escaneo autenticado en Linux

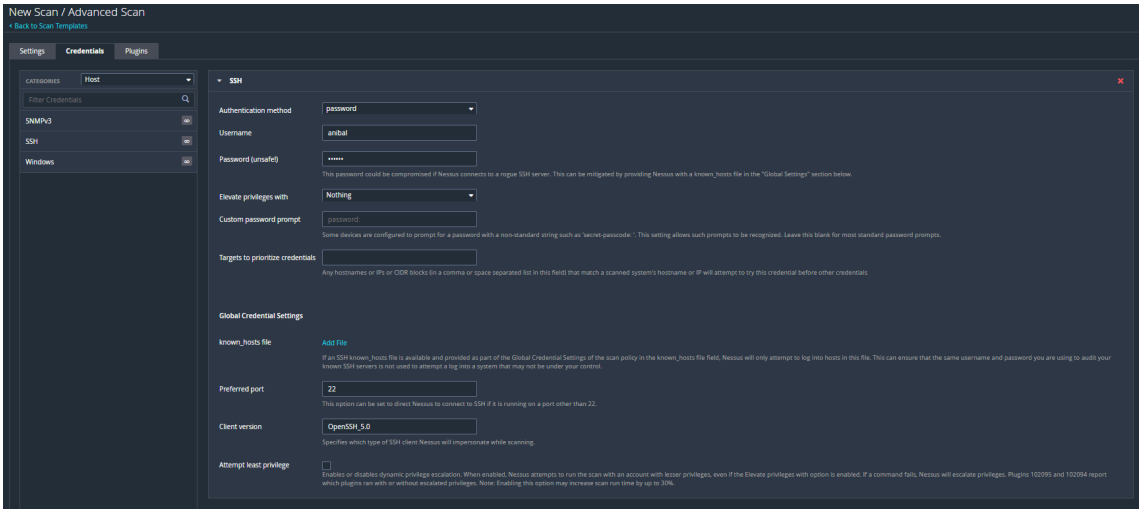
Objetivo: Igual que el anterior, pero para equipos Linux.

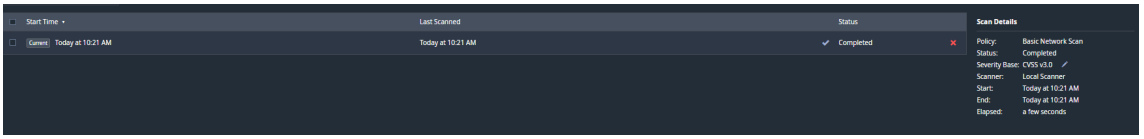
Guía paso a paso:

1. En **Credentials**, selecciona **SSH**.
2. Ingresa un usuario y contraseña con permisos en la máquina Linux objetivo.
3. Guarda y ejecuta el escaneo.

Resultado esperado: Detección de vulnerabilidades específicas de Linux.







Ejercicio 8: Exportar el reporte en PDF

Objetivo: Generar un archivo con los resultados para compartir o guardar como evidencia.

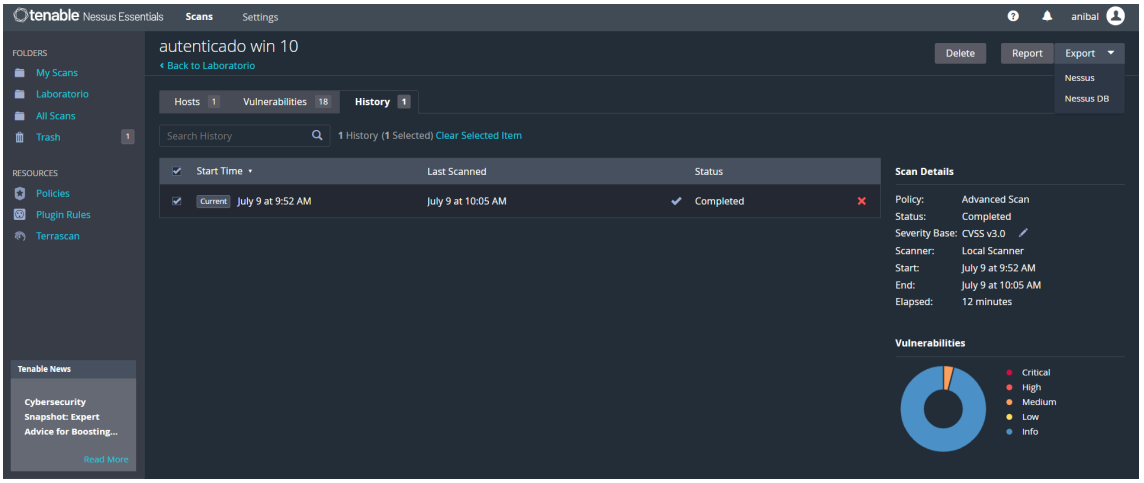
Guía paso a paso:

1. En el reporte de un escaneo, haz clic en **Export** (ícono de disquete o menú desplegable).

2. Elige **PDF**.
3. Descarga el archivo y ábrelo para revisarlo.

Resultado esperado: Un reporte en PDF con todo el detalle del escaneo.

Aclaración: Nessus Essentials no permite pdf.



Ejercicio 9: Comparar antes y después de aplicar parches

Objetivo: Verificar si la corrección de vulnerabilidades fue exitosa.

Guía paso a paso:

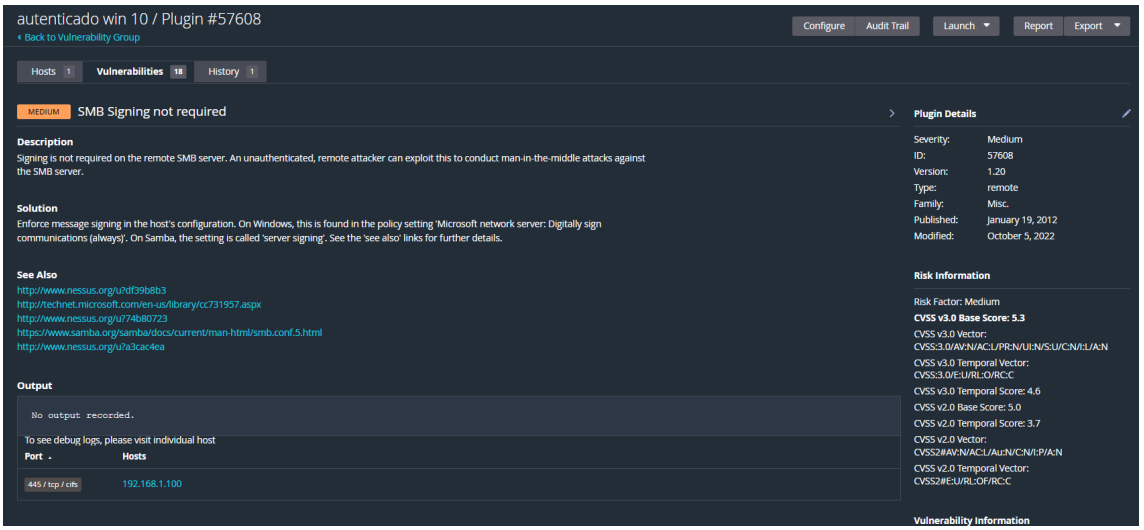
1. Realiza un escaneo inicial y guarda el reporte.
2. Aplica las actualizaciones o corrige vulnerabilidades en el equipo.
3. Realiza un nuevo escaneo al mismo equipo.
4. Compara los dos reportes (en Nessus o con PDFs) para comprobar que desaparecieron vulnerabilidades corregidas.

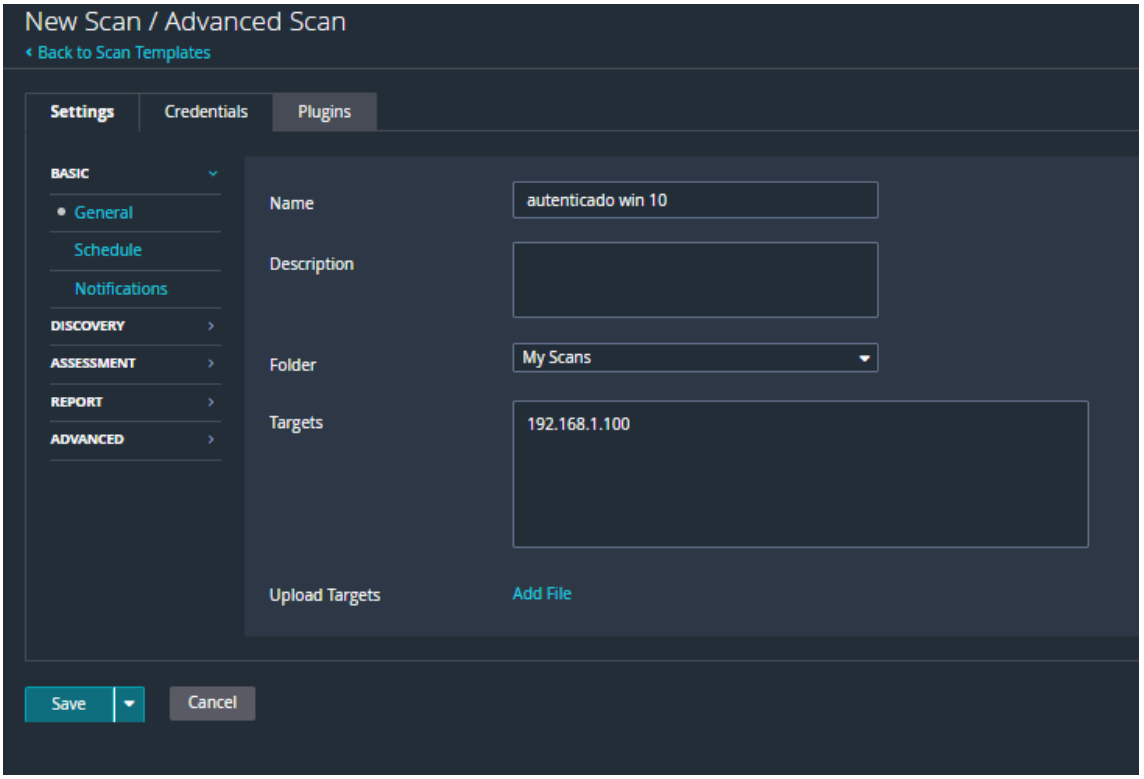
Resultado esperado: Validar que los problemas han sido solucionados.

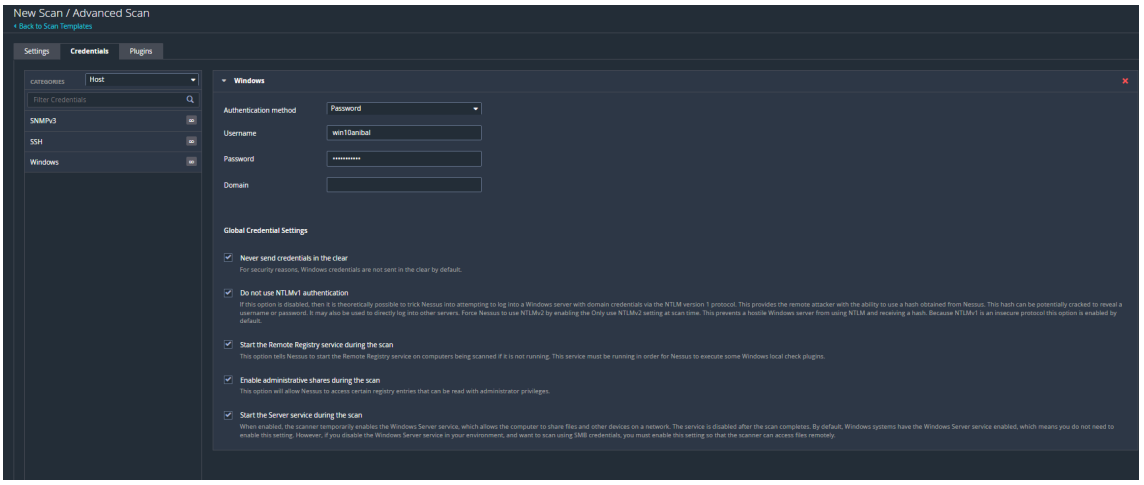
Vulnerabilidad detectada: SMB Signing not required (plugin #57608).

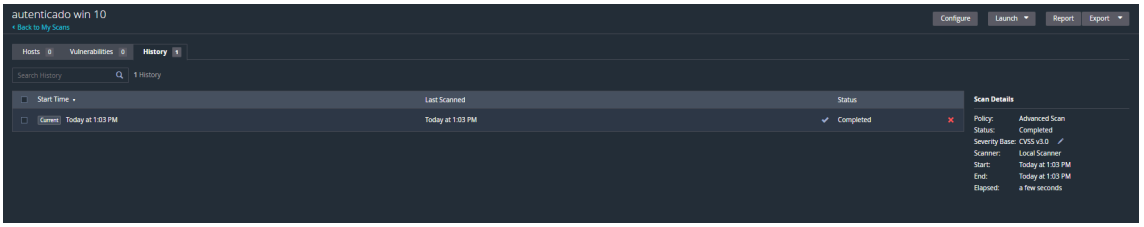
Solución aplicada: Se habilitó la opción de firma digital obligatoria para comunicaciones SMB desde el Editor de directivas locales.

Resultado: En el escaneo posterior, **la vulnerabilidad ya no aparece**, confirmando que fue **corregida con éxito**.


autenticado win 10 / Plugin #57608
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 18
History 1
MEDIUM
SMB Signing not required
Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
See Also
http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea
Output
No output recorded.
To see debug logs, please visit individual host
Port
Hosts
445 / tcp / cifs
192.168.1.100
Plugin Details
Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C
Vulnerability Information


New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
autenticado win 10
Description
Folder
My Scans
Targets
192.168.1.100
Upload Targets
Add File
Save
Cancel





Ejercicio 10: Crear un informe para un jefe o cliente

Objetivo: Aprender a presentar los hallazgos de forma clara para personas no técnicas.

Guía paso a paso:

Usa el reporte exportado (PDF o CSV).

Resalta las vulnerabilidades críticas encontradas.

Escribe en un documento aparte (Word o similar) un resumen en lenguaje sencillo:

- Ejemplo: "En el equipo 192.168.1.10 se encontró una vulnerabilidad crítica que podría permitir a un atacante controlar el sistema."
- Añade la recomendación que da Nessus como solución.
- Añade la recomendación que harías tu.

Resultado esperado: Un informe breve y comprensible, listo para compartir con alguien sin conocimientos técnicos.