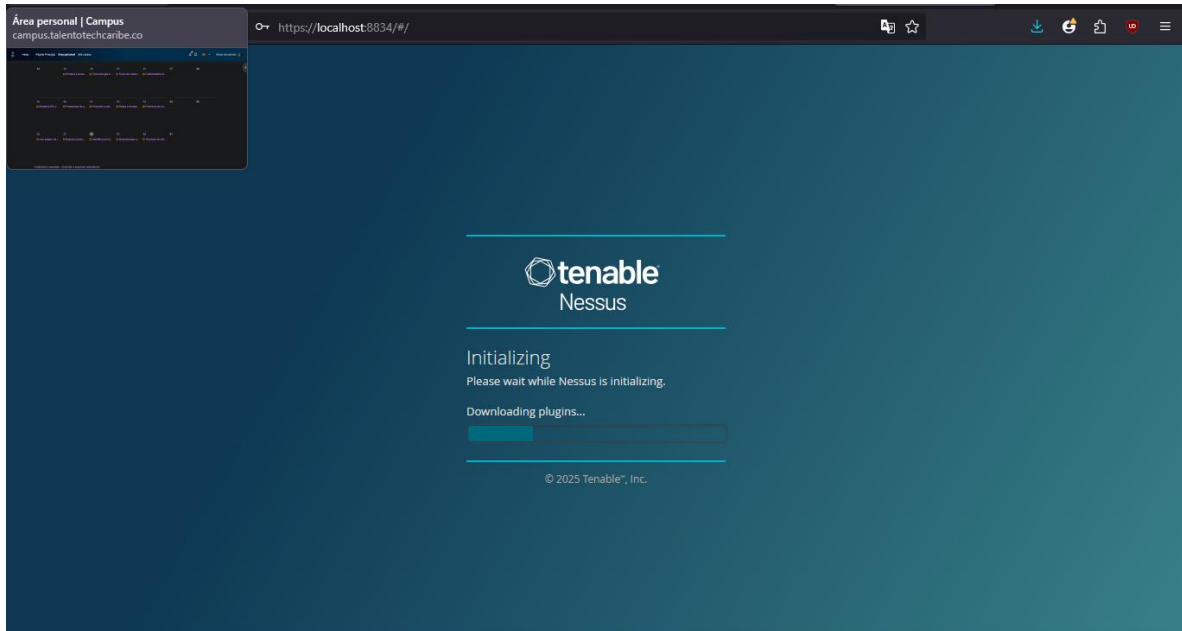


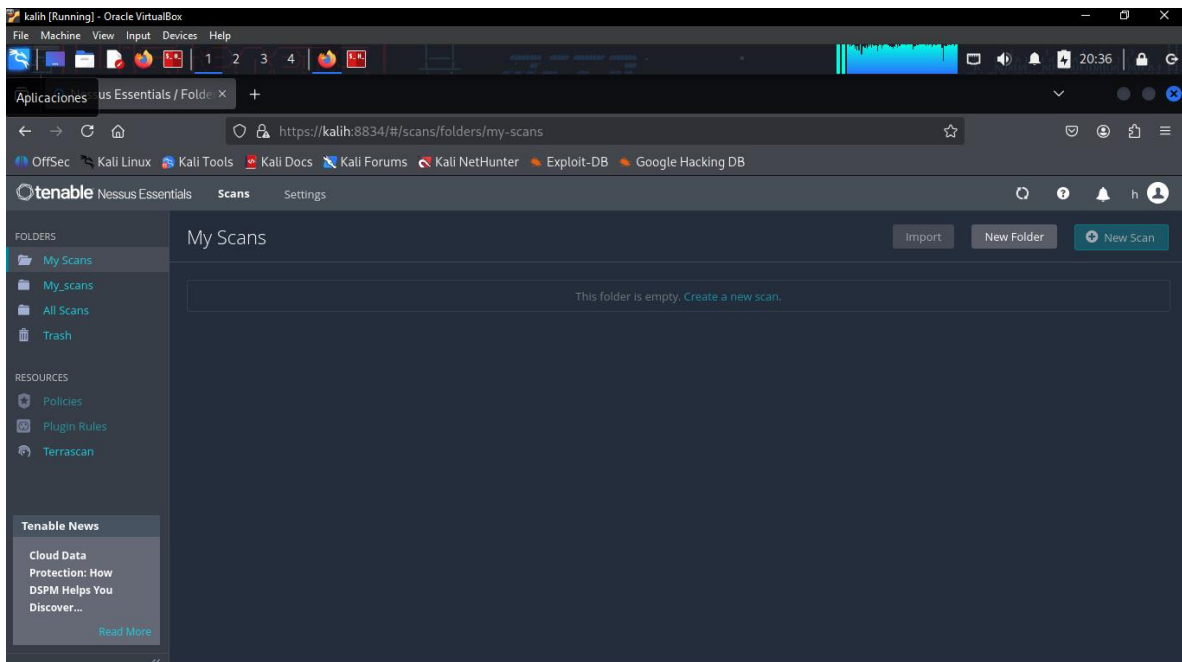
# LABORATORIO 12

HECTOR DIAZ

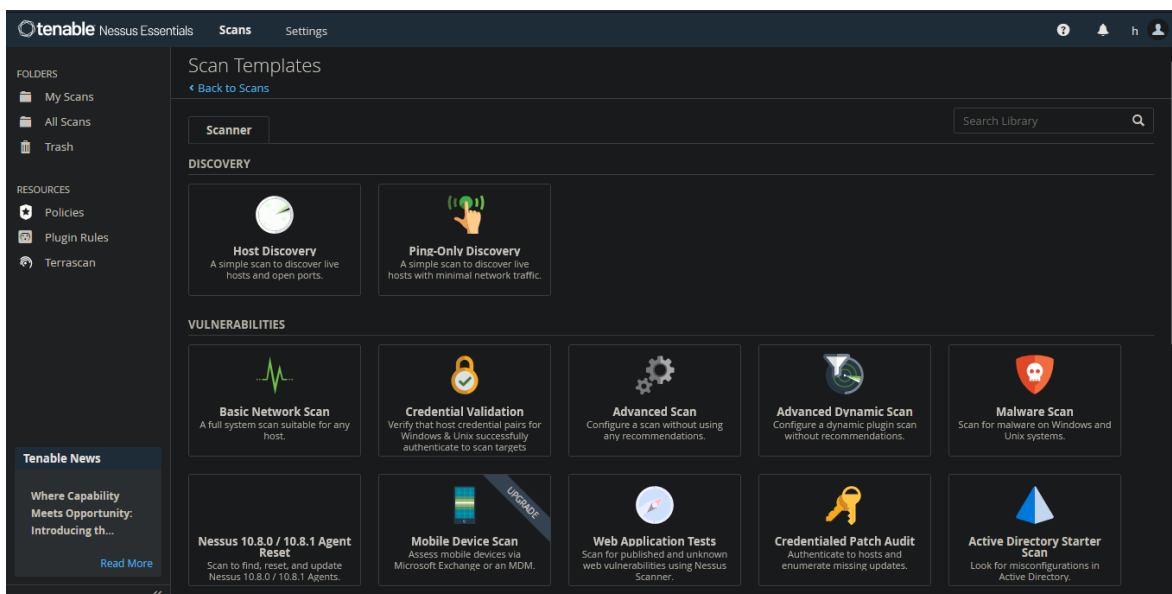
## PASO 3: configuración de herramienta Nessus en windows



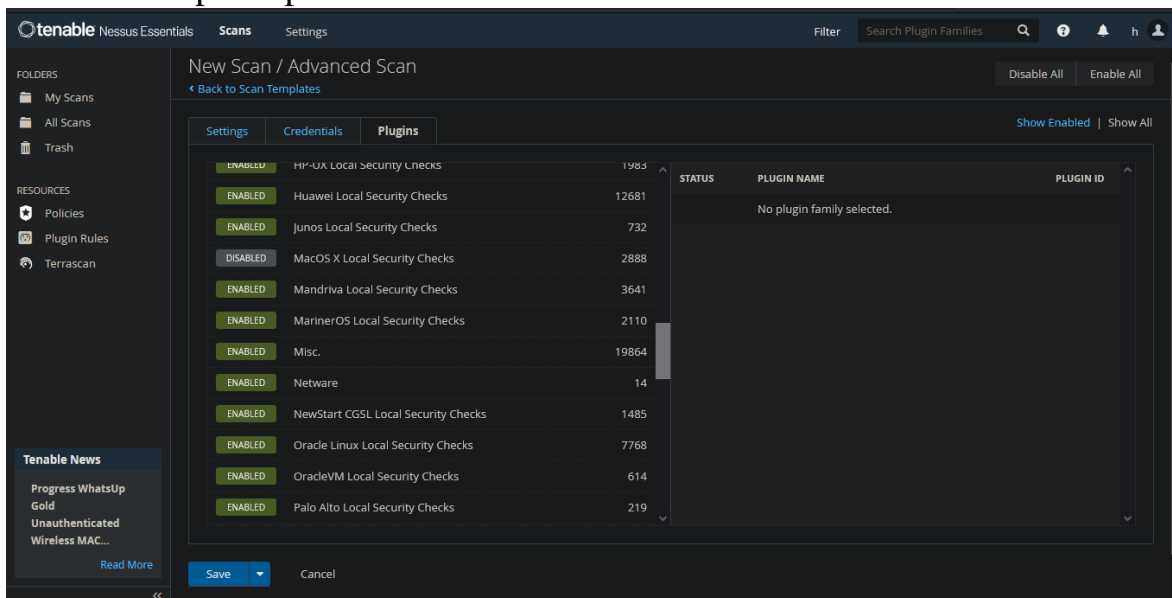
En Linux:



## Configuración de Nessus para escaneos



## Creación de perfil personalizado en Nessus



tenable

Nessus Essentials

Scans

Settings

my\_host

Configure

Audit Trail

Launch

Report

Export

Back to My Scans

Hosts 1

Vulnerabilities 22

History 1

Filter

Search Vulnerabilities

22 Vulnerabilities

Sev	CVSS	VPR	EPSS	Nam...Family	Count		
MEDIUM	5.3			S... Misc.	1		
MIXED	...	...	...	SGGeneral	4		
INFO	...	...	...	SWindows	6		
INFO	...	...	...	HWeb Servers	2		
INFO	...	...	...	MWindows	2		
INFO	...	...	...	TIService detection	2		
INFO	...	...	...	N... Port scanners	31		
INFO	...	...	...	D... Windows	8		
INFO	...	...	...	S... Service detection	3		

Scan Details

Policy:

Advanced Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 9:46 PM

End:

Today at 9:55 PM

Elapsed:

9 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Tenable News

Siemens User Management Component V2.15 Multiple V...

Read More

my\_host / Plugin #57608

Configure
Audit Trail
Launch
Report
Export

Back to Vulnerabilities

Hosts1
Vulnerabilities22
History1

MEDIUM

SMB Signing not required

< >

Plugin Details

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/u7df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u774b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u7a3cac4ea>

Output

No output recorded.

To see debug logs, please visit individual host

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

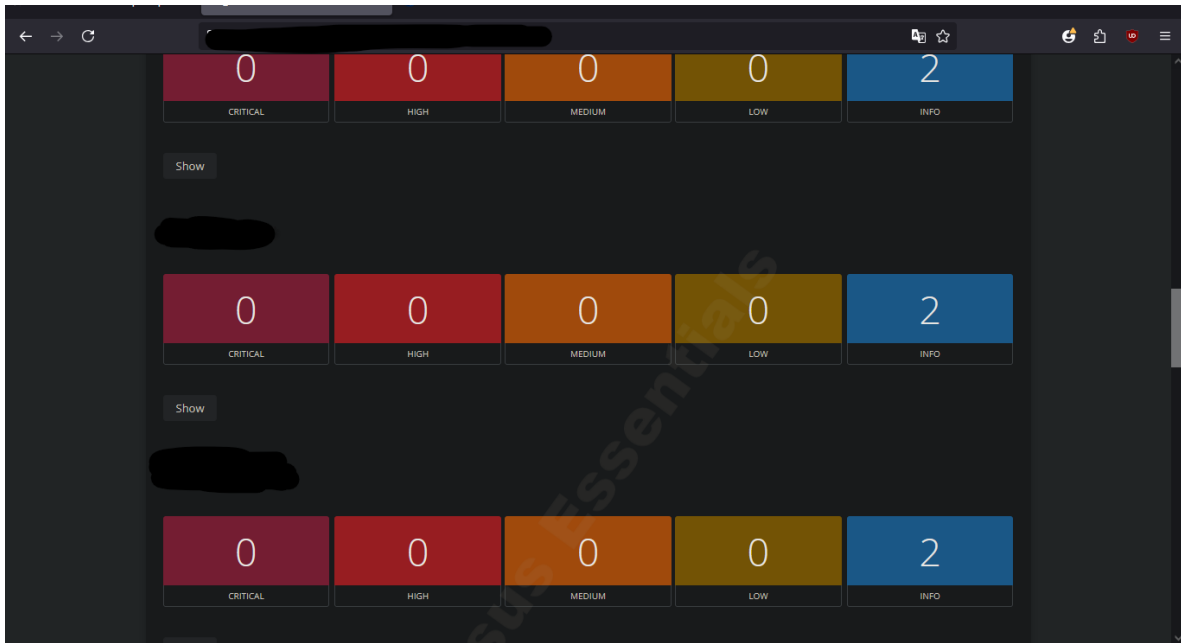
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

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



#### Parte 5: Posible soluciones de vulnerabilidades encontradas:

En el host propio se encontró dos vulnerabilidades de criticidad media, donde nos da una solución en Nessus, en el que se refiere al medio de autenticación en el que se aconseja métodos mas seguros para el servidor de samba.

#### Parte 6: Preparar un informe y recomendaciones para mitigar vulnerabilidades Informe de vulnerabilidades con Nessus:

Se implementó la herramienta Nessus para escaneo de red, como identificación de dispositivos conectados a la red, y un escaneo de vulnerabilidades host.

En el escaneo de dispositivos se logró detectar 14 dispositivos en línea en los que uno llama la atención por tener diferentes puertos abiertos. Se identifica el host en un análisis, determinando que es nuestro host. Se realiza el escaneo de vulnerabilidades anteriormente, en el que nos arroja resultados con novedades, Estas novedades son 2 vulnerabilidades de criticidad media, en el que determinados que es con respecto al servidor SAMBA en el que se utiliza para la transferencia de archivos. Para la mitigación de vulnerabilidades es aconsejable seguir las recomendaciones de la herramienta samba donde nos da una solución en el que se pide mejorar la autenticación hacia el servidor. Como recomendación adicional, se sugiere volver hacer un escaneo al host para confirmación de dichas vulnerabilidades.

