INFORME TÉCNICO DE ENTREGA DE SOFTWARE Y CAPACITACIÓN

Plataforma de Auditoría: Tenable Nessus Scanner
Fecha de Sesión: 26 de mayo de 2026
Medio de Sesión: Zoho Meeting (meetinglab.zoho.com/jpfe-lqt-xbt)

1. CONTROL DE ASISTENCIA Y ROLES

La sesión de transferencia tecnológica y capacitación práctica contó con la participación activa de los siguientes integrantes del equipo:

- **Mauricio Osorio:** Anfitrión y Director Técnico de la sesión CENTRAL TIC SAS
- **Ing. Javier Ordoñez:** Ingeniero especialista y proveedor de direccionamiento de infraestructura.
- **Cesar Andres Pachon Gordillo:** Ingeniero supervisor de contrato / Equipo técnico.
- **Jorge Molina:** Ingeniero / Equipo técnico de CENTRAL TIC SAS
- **Hilda Garzón:** Personal técnico / Registro y control CENTRAL TIC SAS

2. ALCANCE TÉCNICO DE LA CAPACITACIÓN

El alcance de esta jornada abarcó desde la inicialización de la plataforma hasta el aprovisionamiento avanzado, optimización y análisis de resultados en entornos virtualizados (VMware ESXi) y accesos remotos vía UltraViewer. Se capacito al personal en los siguientes módulos analíticos y de configuración:

A. Inicialización y Gestión de Sesiones

- Acceso seguro a la consola local de Nessus mediante el puerto por defecto de la interfaz web corporativa (https://localhost:8834/#/).
- Diagnóstico de expiración de sesiones (*Session Expired*) y flujos lógicos para el reingreso de credenciales de nivel administrativo bajo el perfil de usuario activo (jncl).

B. Análisis del Catálogo de Plantillas de Escaneo

Se instruyó al equipo en la taxonomía de políticas disponibles en el ecosistema Tenable Nessus, segmentadas según el objetivo táctico:

- **Discovery:** Uso avanzado de *Host Discovery* (descubrimiento simple y mapeo de puertos abiertos) y *Ping-Only Discovery* (mapeo rápido con tráfico mínimo de red).
- **Vulnerabilities:** Configuración de directrices estructurales de escaneo como *Basic Network Scan*, *Credential Validation*, *Advanced Scan* (personalización total sin recomendaciones previas), *Advanced Dynamic Scan*, *Malware Scan*, *Mobile Device Scan*, *Web Application Tests* y *Credentialed Patch Audit*.

3. CONFIGURACIÓN Y PROVISIONAMIENTO DE ESCANEOS (PASO A PASO)

Durante el despliegue práctico, se estructuró un escaneo piloto enfocado en auditoría perimetral e interna:

Paso 1: Definición de Parámetros Básicos y Targets

- **Identificadores:** Se generó un nuevo escaneo de tipo *Host Discovery* titulado "**Directorio activo**" con la descripción "**Prueba**".
- **Direccionamiento IP:** Se parametrizó el segmento objetivo. Se incluyeron explícitamente las direcciones IPv4 de producción 20.10.62.15 y 20.10.62.5 suministradas por el Ingeniero Javier Ordoñez para la exploración de infraestructura. En la consola de Nessus se definió el rango inicial mediante la nomenclatura 20.10.62.1-.

Paso 2: Planificación (Scheduling) y Automatización

- Se instruyó sobre la ventana de ejecución periódica o única. El piloto se programó en modalidad *Once* (una sola ejecución) configurado para iniciar a las **16:30** del **26/05/2026**.

Paso 3: Integración del Motor de Notificaciones (SMTP Server)

Se identificó la alerta del sistema referida a que las notificaciones automatizadas de resultados por correo electrónico requieren la configuración previa del servidor de retransmisión (SMTP). Se procedió a explicar la interfaz de administración:

- Campos de configuración técnica obligatorios: *Host*, *Port*, *From (sender email)*, métodos de cifrado (*Encryption: No Encryption / SSL / TLS*) y mecanismos de autenticación corporativa (*Auth Method: NONE / PLAIN / LOGIN*).

Paso 4: Configuración Avanzada de Descubrimiento (Discovery Customization)

Se evaluaron los sub-módulos críticos del motor de exploración:

- **Scan Type (Tipos de Escaneo):** Explicación detallada del menú desplegable: *Host enumeration*, *OS Identification*, *Port scan (common ports)*, *Port scan (all ports)* y *Custom*.
- **Fingerprinting de Sistemas Operativos:** Selección activa de *OS Identification* para determinar el kernel y distribución de los objetivos sin necesidad de credenciales.

- **Vectores de Red (Ping hosts using):** Activación de sondeos concurrentes mediante protocolos **TCP**, **ARP**, e **ICMP (con un umbral de 2 reintentos)**.

Paso 5: Políticas de Salida (Report) y Tuning de Rendimiento (Advanced)

- **Directivas del Reporte:** Habilitación de la casilla *Allow users to edit scan results* para auditorías dinámicas y *Display hosts that respond to ping*.
- **Performance Options (Control de Congestión):**
    - Habilitación del *throttling* dinámico (*Slow down the scan when network congestion is detected*).
    - *Network timeout*: Configurado estrictamente en **5 segundos** para evitar colas de espera en hosts apagados.
    - *Max simultaneous checks per host*: Limitado a **5 comprobaciones concurrentes**.
    - *Max simultaneous hosts per scan*: Parametrizado en un máximo de **256 hosts simultáneos** para proteger el ancho de banda del canal.

4. FASE DE PRUEBAS EMPÍRICAS Y ANÁLISIS DE RESULTADOS

Para contrastar el comportamiento del motor de escaneo con la infraestructura real, se ejecutaron pruebas de diagnóstico directo:

Conectividad de Red y Diagnóstico ICMP

Desde una terminal Linux (developer@ubuntu:~$), se procedió a realizar un rastreo de red mediante comandos ICMP contra el objetivo:

Bash

developer@ubuntu:~$ ping 20.10.62.15

El diagnóstico de red devolvió paquetes de error procedentes del nodo de enrutamiento intermedio (From 192.168.93.128 icmp_seq=4 Destination Host Unreachable). Esto sirvió como un excelente caso de estudio práctico durante la capacitación para demostrar cómo los firewalls perimetrales o políticas de enrutamiento bloquean las trazas ICMP tradicionales, validando el por qué Nessus requiere técnicas de descubrimiento híbridas (TCP/ARP) para confirmar la disponibilidad real de un activo.

Análisis del Escaneo de Vulnerabilidades Ejecutado

Posteriormente, se verificó el registro e historial de auditorías dentro de la carpeta corporativa *My Scans*, donde se analizó el comportamiento de la tarea "**Escaner vulnerabilidades**":

- **Estado de Ejecución:** El escaneo fue lanzado bajo demanda (*On Demand*), registrando actividad finalizada o en procesamiento a las **4:39 PM**.
- **Análisis del Plugin Técnico #10180 (Ping the remote host):** Se realizó un *deep-dive* en la firma de severidad *Info*. El plugin determinó con éxito que el objetivo remoto se encontraba operativo (*The remote host is up*) gracias a que respondió de manera efectiva a un paquete de eco ICMP directo procesado internamente por el motor de puertos de Nessus.
- **Mapeo de Activos y Superficie de Ataque Abierta:** Se expuso el resultado en tiempo real del host objetivo **10.10.63.39**, el cual presentaba un progreso del **80%** en estado de ejecución (*Running*). El sistema identificó de manera precisa los siguientes puertos y servicios abiertos:

Puerto Local	Protocolo / Servicio Asociado (Enumeración de Puertos)
135	RPC (Remote Procedure Call) - Crítico para gestión de entornos Windows.
137	NetBIOS Name Service - Tráfico de resolución de nombres local.
139	NetBIOS Session Service - Interconexión de recursos compartidos.
445	Microsoft-DS (SMB) - Protocolo de intercambio de archivos (Core de AD).
49664 a 49686	Puertos dinámicos / efímeros asignados para llamadas RPC de sistema.

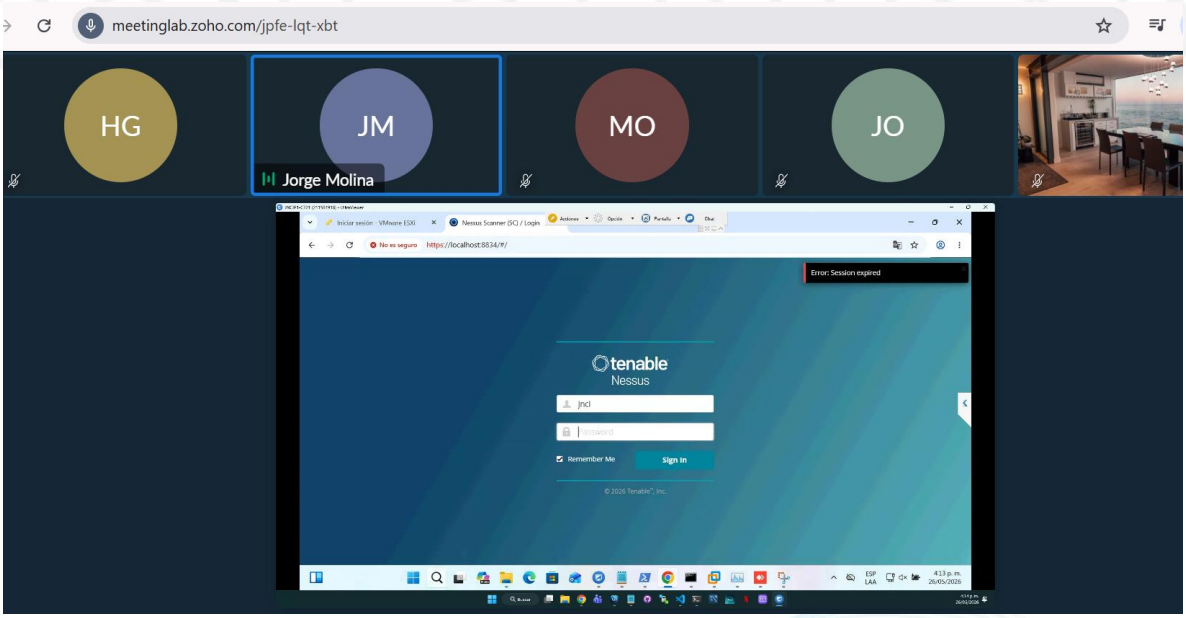
- **Matriz de Riesgo Inicial:** El gráfico sectorial de severidades arrojó un resultado preliminar del **100% en categoría "Info" (Color Azul)**. Esto certifica que el escaneo configurado cumplió exactamente el alcance de descubrimiento y auditoría de puertos sin generar falsos positivos ni alertas críticas de denegación de servicio en la fase de reconocimiento de infraestructura.

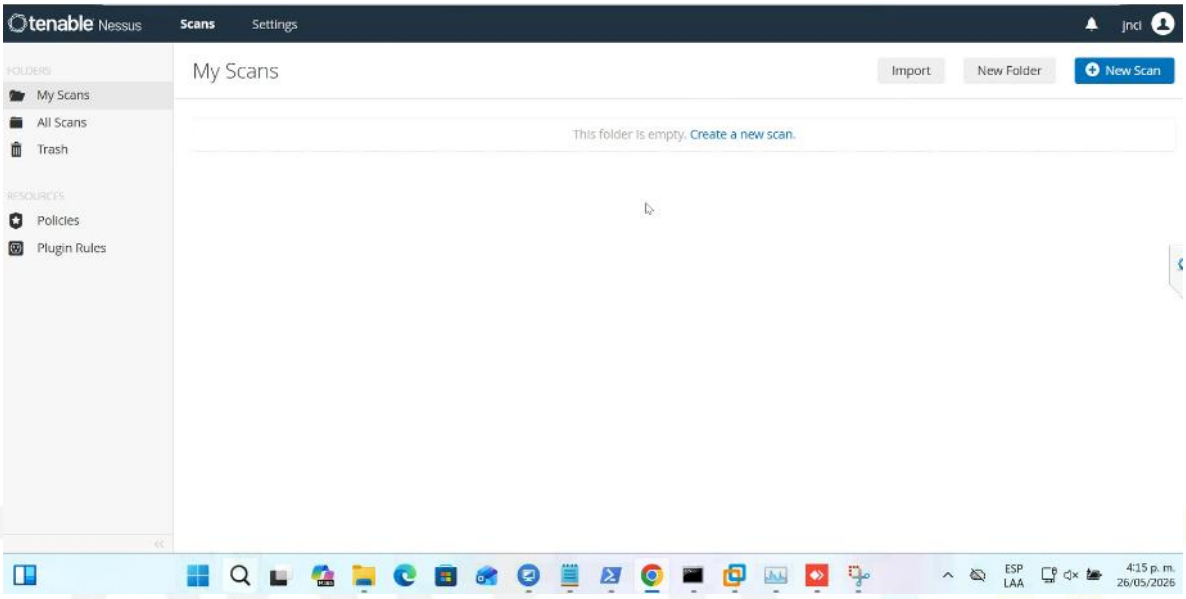
5. CONCLUSIONES DE LA ENTREGA

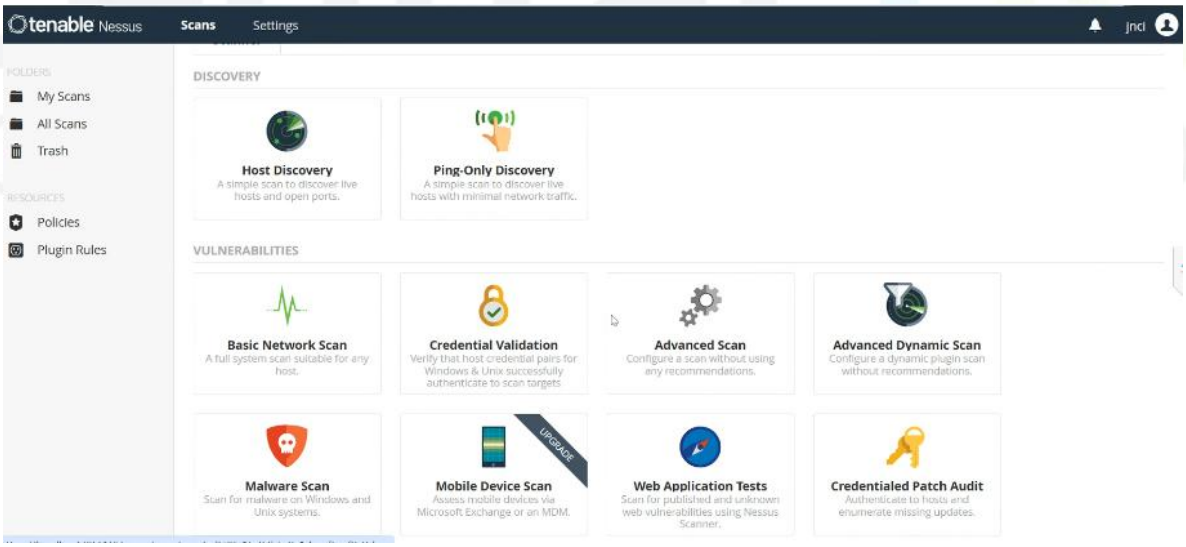
El software Tenable Nessus Scanner se encuentra **completamente instalado, operativo y validado** en la infraestructura. El equipo técnico asistente demostró comprensión total en la manipulación de la interfaz, creación de políticas de host y lectura avanzada de plugins informativos, quedando altamente capacitado para iniciar los ciclos autónomos de auditorías de vulnerabilidades corporativas.

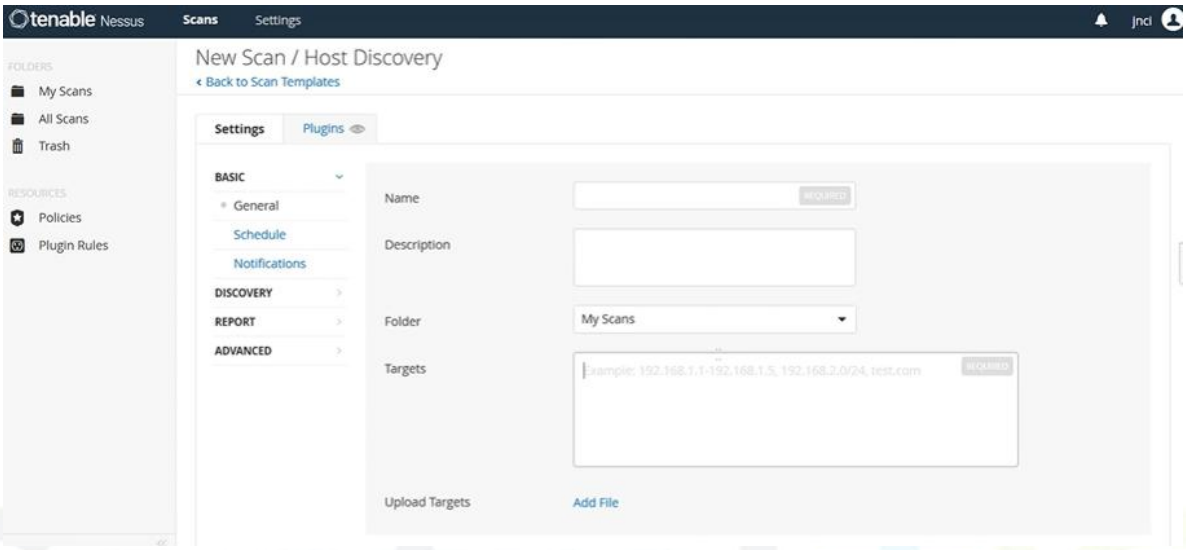
REGISTRO VISUAL



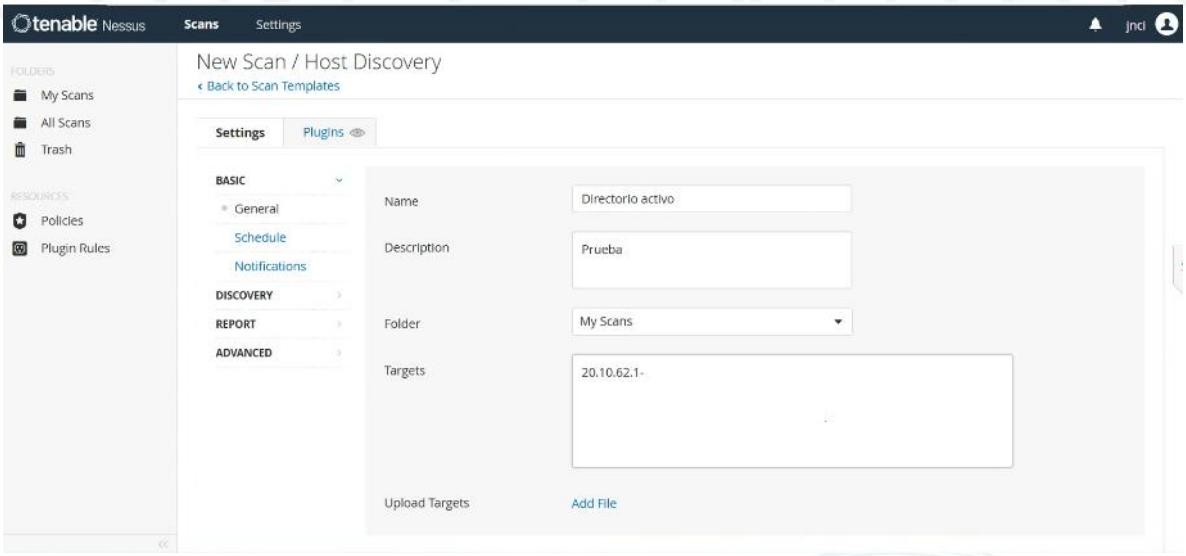


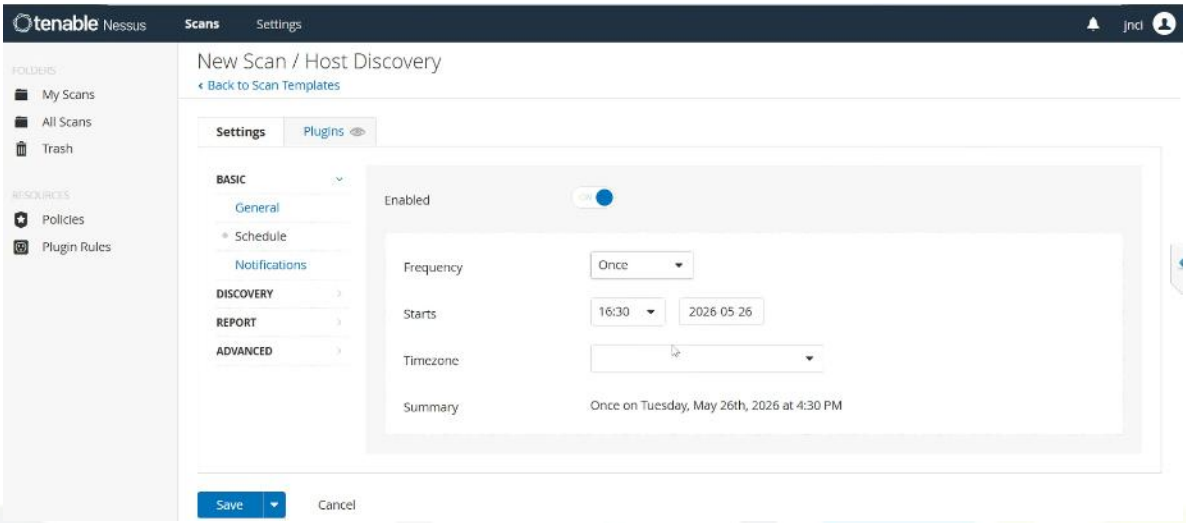

tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.
ESP
LAA
4:15 p. m.
26/05/2026

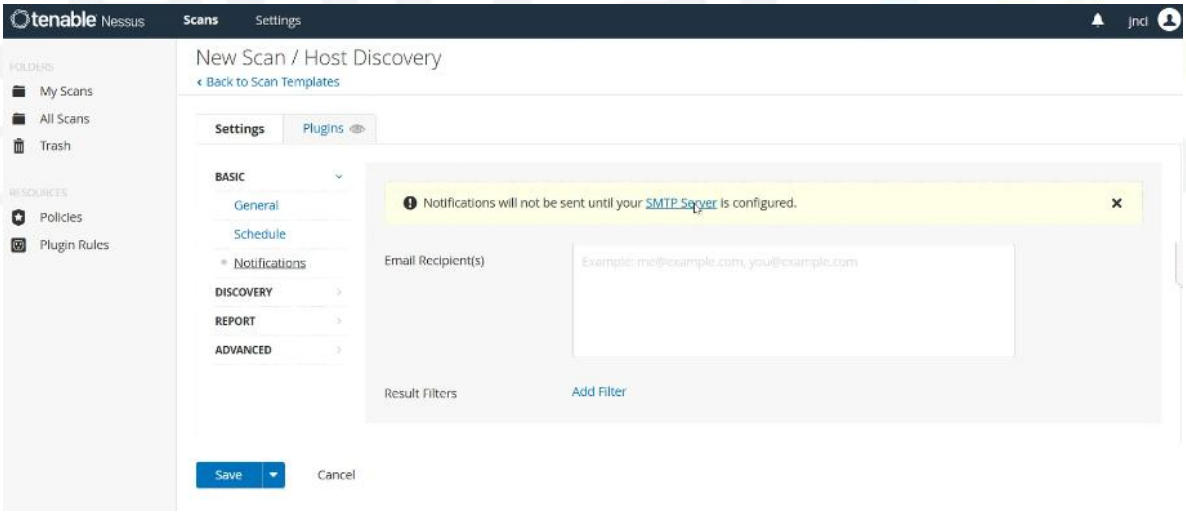

tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

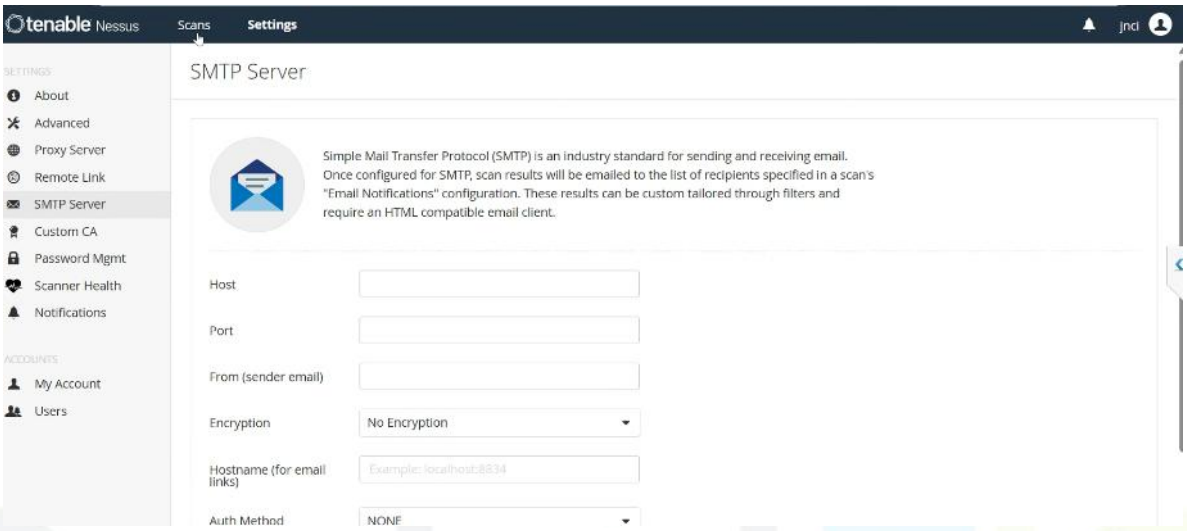


Exploración con la IP 20.10.62.15 y 20.10.62.5 suministrados por Ingeniero Javier Ordoñez.

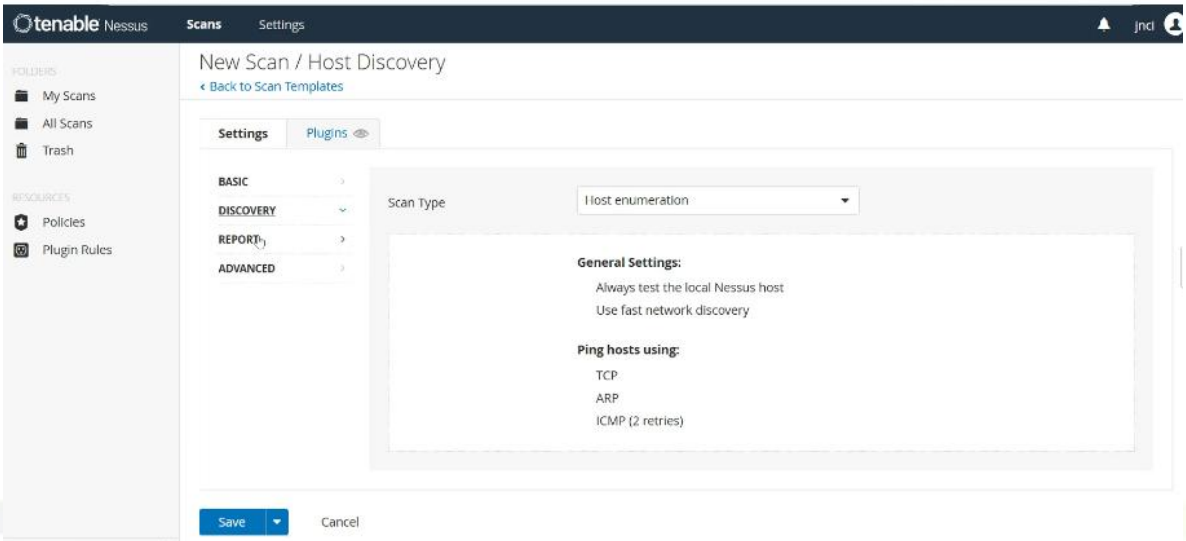


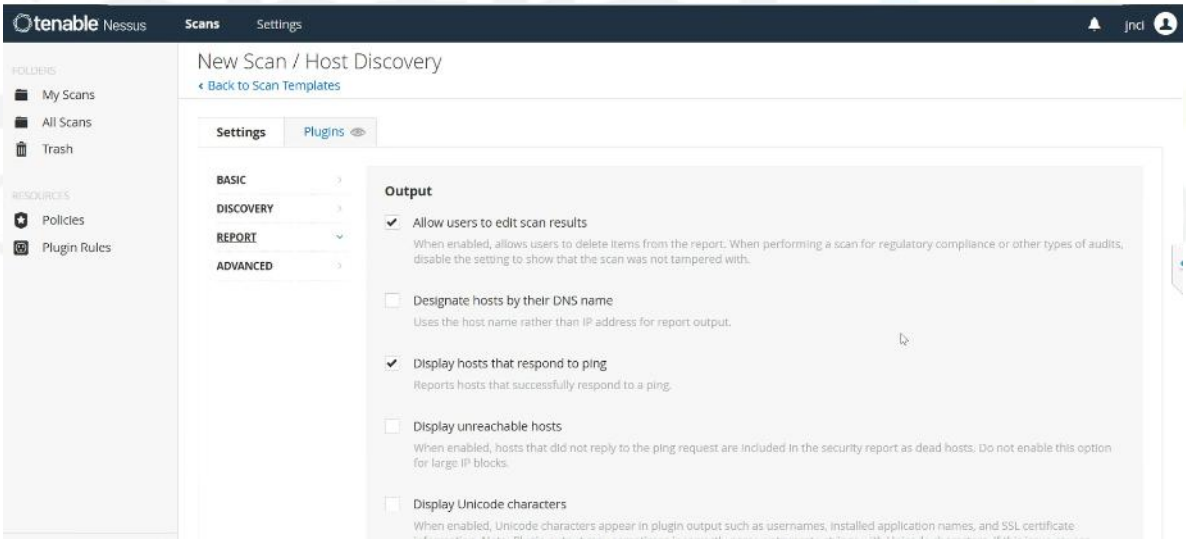

tenable Nessus
Scans
Settings
jncl
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
‹ Back to Scan Templates
Settings
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
REPORT
ADVANCED
Enabled
Frequency
Once
Starts
16:30
2026 05 26
Timezone
Summary
Once on Tuesday, May 26th, 2026 at 4:30 PM
Save
Cancel

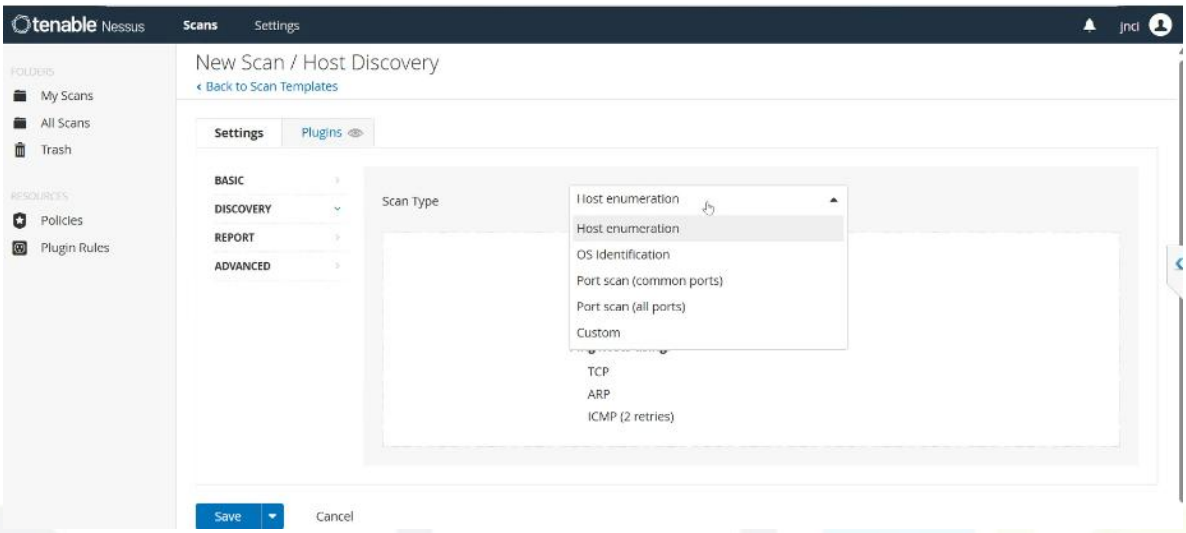

tenable Nessus
Scans
Settings
jncl
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
‹ Back to Scan Templates
Settings
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
REPORT
ADVANCED
Notifications will not be sent until your SMTP Server is configured.
Email Recipient(s)
Example: me@example.com, you@example.com
Result Filters
Add Filter
Save
Cancel

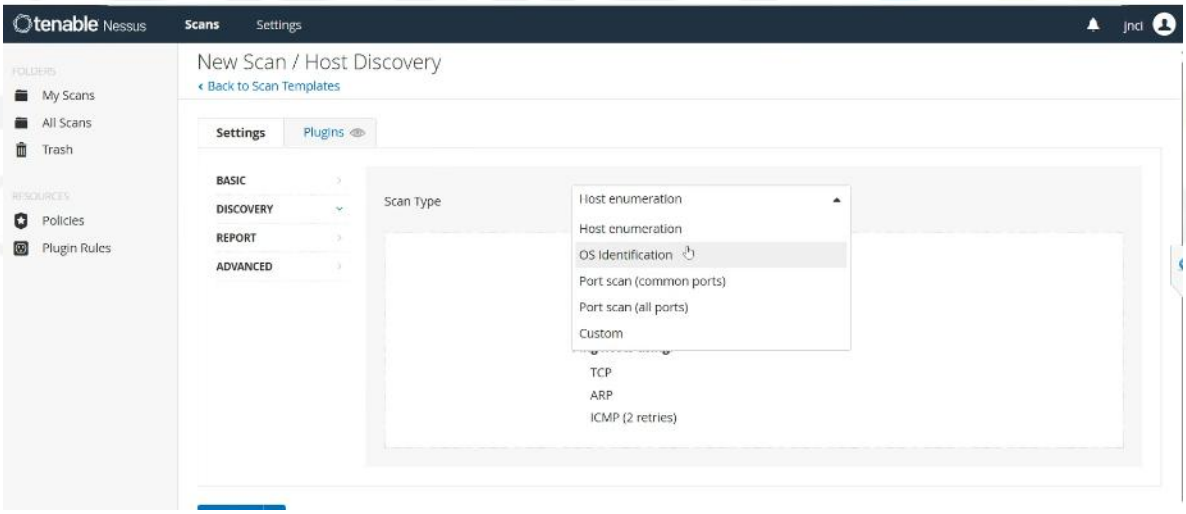


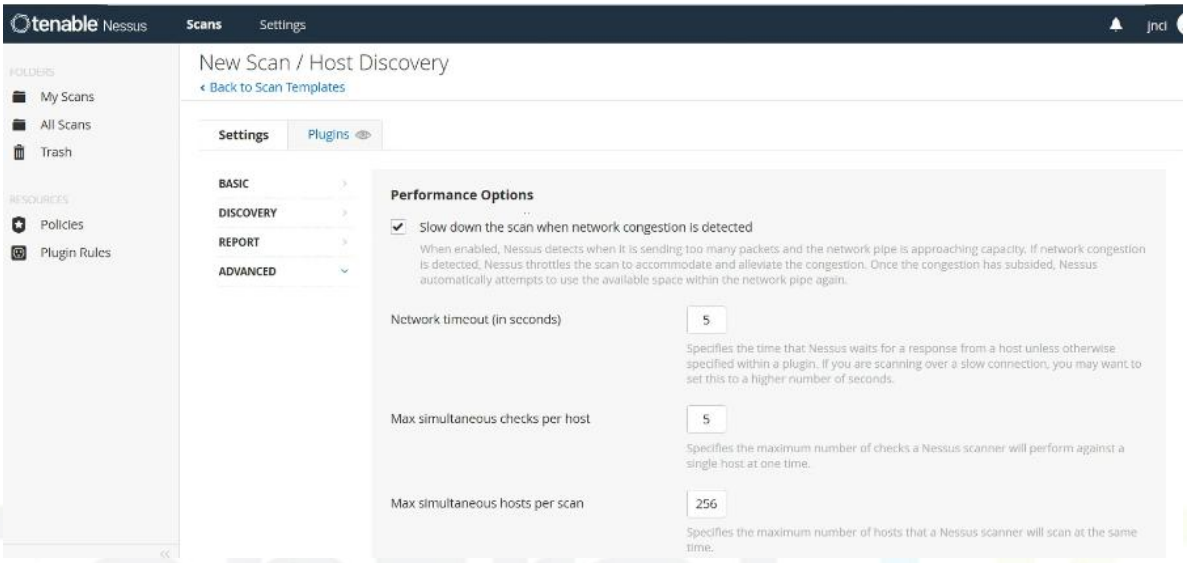
CentralTIC
CONECTIVIDAD


tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
‹ Back to Scan Templates
Settings
Plugins
BASIC
DISCOVERY
REPORT
ADVANCED
Scan Type
Host enumeration
General Settings:
Always test the local Nessus host
Use fast network discovery
Ping hosts using:
TCP
ARP
ICMP (2 retries)
Save
Cancel

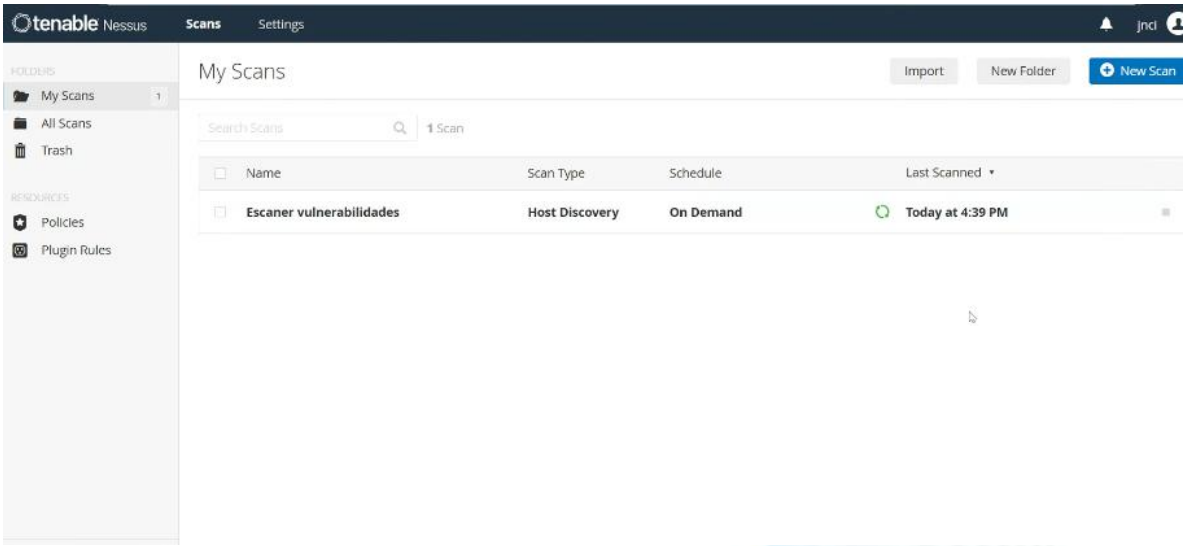

tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
‹ Back to Scan Templates
Settings
Plugins
BASIC
DISCOVERY
REPORT
ADVANCED
Output
Allow users to edit scan results
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
Designate hosts by their DNS name
Uses the host name rather than IP address for report output.
Display hosts that respond to ping
Reports hosts that successfully respond to a ping.
Display unreachable hosts
When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
Display Unicode characters
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate

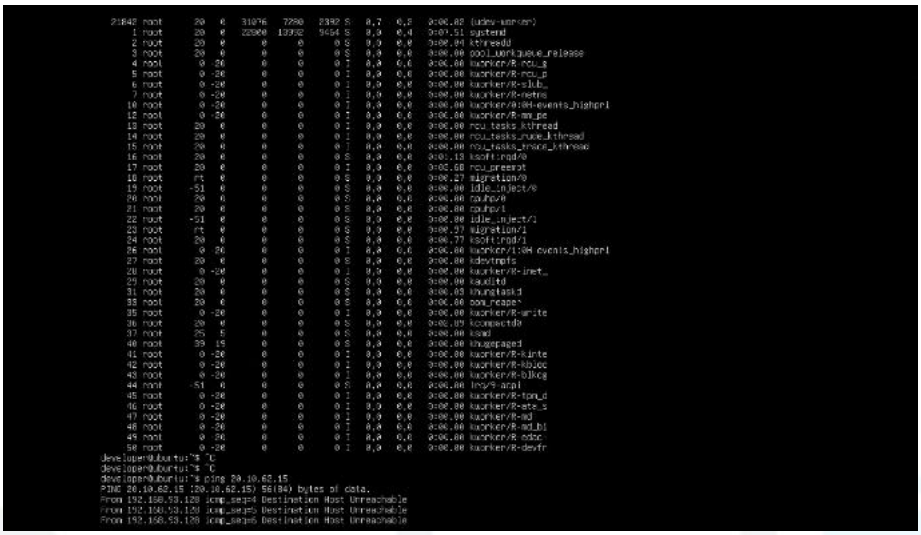

tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
Back to Scan Templates
Settings
Plugins
BASIC
DISCOVERY
REPORT
ADVANCED
Scan Type
Host enumeration
Host enumeration
OS Identification
Port scan (common ports)
Port scan (all ports)
Custom
TCP
ARP
ICMP (2 retries)
Save
Cancel

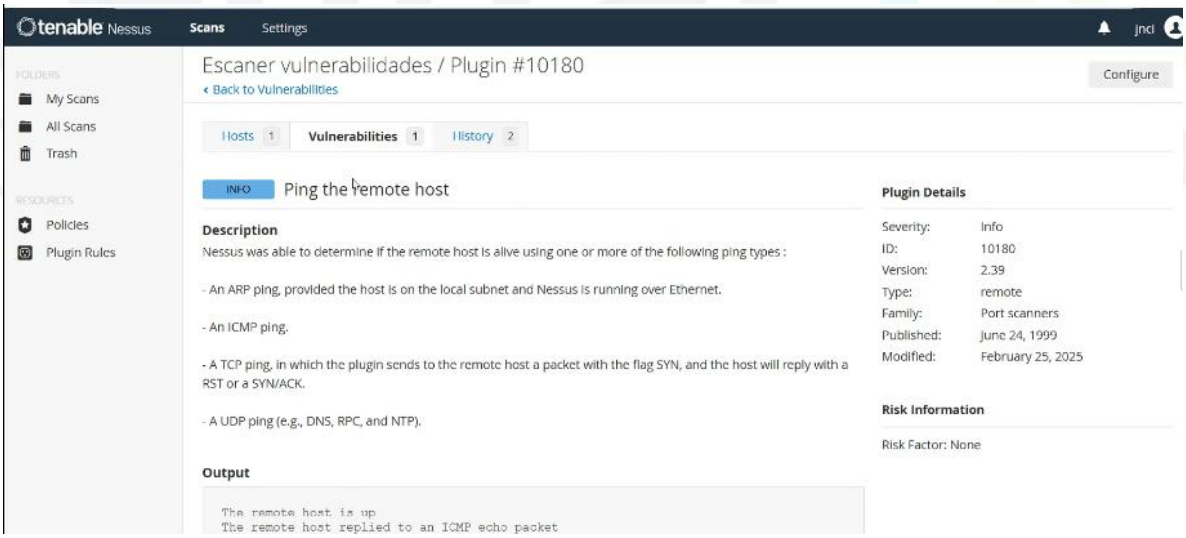

tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
Back to Scan Templates
Settings
Plugins
BASIC
DISCOVERY
REPORT
ADVANCED
Scan Type
Host enumeration
Host enumeration
OS Identification
Port scan (common ports)
Port scan (all ports)
Custom
TCP
ARP
ICMP (2 retries)

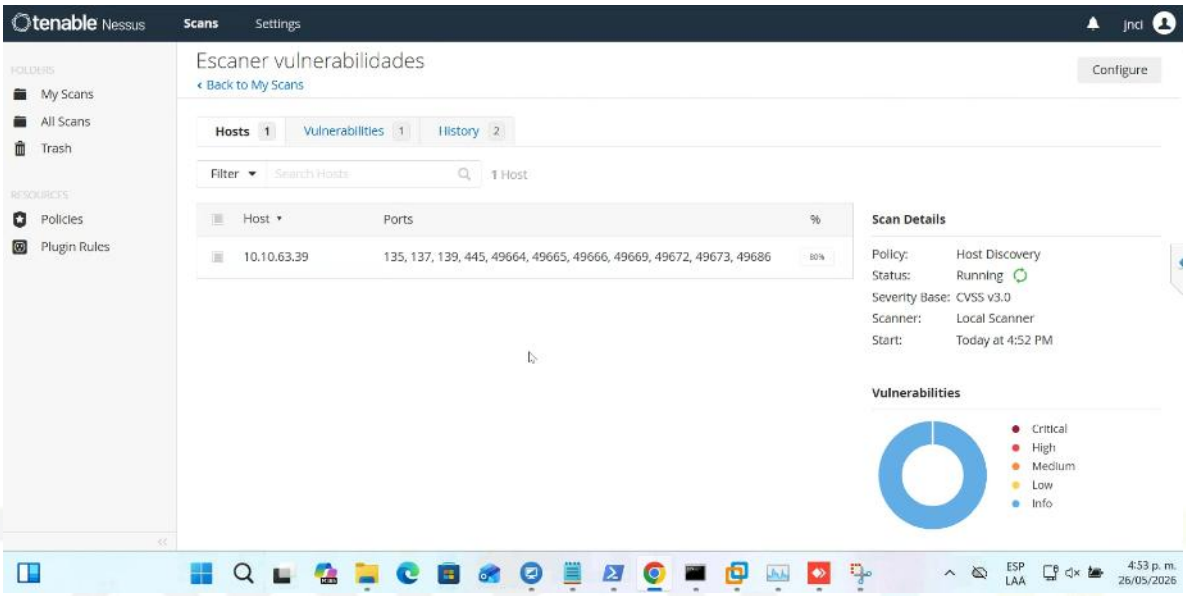

tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
New Scan / Host Discovery
Back to Scan Templates
Settings
Plugins
BASIC
DISCOVERY
REPORT
ADVANCED
Performance Options
Slow down the scan when network congestion is detected
When enabled, Nessus detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, Nessus throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Nessus automatically attempts to use the available space within the network pipe again.
Network timeout (in seconds)
5
Specifies the time that Nessus waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.
Max simultaneous checks per host
5
Specifies the maximum number of checks a Nessus scanner will perform against a single host at one time.
Max simultaneous hosts per scan
256
Specifies the maximum number of hosts that a Nessus scanner will scan at the same time.

Pruebas


tenable Nessus
Scans
Settings
jnci
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
Escaner vulnerabilidades
Host Discovery
On Demand
Today at 4:39 PM


Developer@Ubuntu:~$ ^C
Developer@Ubuntu:~$ ^C
Developer@Ubuntu:~$ ping 20.10.62.15
PING 20.10.62.15 (20.10.62.15) 56(84) bytes of data.
From 192.168.53.128 icmp_seq=4 Destination Host Unreachable
From 192.168.53.128 icmp_seq=5 Destination Host Unreachable
From 192.168.53.128 icmp_seq=6 Destination Host Unreachable


tenable Nessus
Scans
Settings
jncl
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Escaner vulnerabilidades / Plugin #10180
Back to Vulnerabilities
Configure
Hosts 1
Vulnerabilities 1
History 2
INFO
Ping the remote host
Description
Nessus was able to determine if the remote host is alive using one or more of the following ping types :
- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.
- An ICMP ping.
- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.
- A UDP ping (e.g., DNS, RPC, and NTP).
Output
The remote host is up
The remote host replied to an ICMP echo packet
Plugin Details
Severity: Info
ID: 10180
Version: 2.39
Type: remote
Family: Port scanners
Published: June 24, 1999
Modified: February 25, 2025
Risk Information
Risk Factor: None



Central TIC
CONECTIVIDAD