niversidad de San Carlos de Guatemala

Facultad de Ingeniería

Escuela de Estudios de Postgrado

ESCANEO DIRECCIONES IP GUATEMALA

Brandon René Portillo González

Carnet: 999011994

Repositorio: https://github.com/usac201612398/IoT

Guatemala, 28 noviembre 2025

INDICE DE CONTENIDO

INDICE DE TABLAS

1. RESUMEN

Se consolidaron seis escaneos Nmap (reporte1.txt a reporte6.txt, debido a la alta cantidad de direcciones IPngos de IP públicas asociados, en su mayoría, a dominios DSL en Guatemala. En los seis reportes, los puertos ICS consultados aparecen como 'filtered' cuando hay detalle, y la mayoría de hosts fueron omitidos por timeout. No se observaron puertos ICS en estado 'open'. Por lo tanto, con esta evidencia, no se confirman dispositivos ICS expuestos a Internet en los rangos evaluados.

2. INTRODUCCION

La creciente interconexión de sistemas industriales (ICS/OT) con redes corporativas y, en algunos casos, con internet, ha incrementado el riesgo de exposición de dispositivos críticos a amenazas externas. Algunos protocolos como Modbus/TCP, Siemens S7, EtherNet/IP, entre otros, fueron diseñados originalmente para entornos cerrados y carecen de mecanismos robustos de autenticación y cifrado, lo que los convierte en objetivos atractivos para atacantes cuando están accesibles públicamente.

Con el objetivo de evaluar la superficie de ataque en rangos de direcciones IP públicas asociadas a proveedores locales, se realizaron seis escaneos Nmap orientados a puertos comúnmente utilizados por dispositivos ICS y algunos servicios IT complementarios. La metodología incluyó la identificación de hosts activos y la verificación del estado de puertos específicos, aplicando parámetros que piorizan velocidad y cobertura básica.

Este informe consolida los hallazgos obtenidos, analiza los resultados y discute sus implicaciones en términos de seguridad, limitaciones del proceso y recomendaciones para mejorar la precisión en futuras evaluaciones.

3. METODOLOGIA DE LA INVESTIGACION

3.1. Comandos a utilizar

Se ejecuta en cmd la siguiente instrucción para proceder a grabar cada reporte de escaneo realizado por Nmap como sigue:

"C:\Program Files (x86)\Nmap\nmap.exe" -p 502,102,44818,2222,20548,9600,28784,57176,2004,33061433,445 -iL ips1.txt -Pn -sV --max-retries 2 --host-timeout 30s -T4 -oN reporte1.txt

3.2. Herramientas

3.3. Puertos a escanear

Se realiza es escaneo a través de los siguientes puertos para realizar un análisis de cada IP y poder determinar que sucede en las mismas.

- 102 Siemens S7 (iso-tsap)
- 502 Modbus/TCP (mbap)
- 44818 Allen-Bradley EtherNet/IP
- 2222 Allen-Bradley EtherNet/IP (alt)
- 20548 Schleicher XCX 300
- 9600 Omron PLC
- 28784 Koyo Ethernet
- 57176 GE QuickPanels
- 2004 LS
- 3306 MySQL
- 1433 MSSQL

- 445 Microsoft-DS

4. PRESENTACION DE RESULTADOS

4.1. Rangos indicadores del escaneo

El escaneo de direcciones IP reflejó lo siguiente:

Tabla 1.

Resumen de escaneo de IPs

Archivo	IPs	Hosts up
reporte1.txt	512	512
reporte2.txt	256	256
reporte3.txt	256	256
reporte4.txt	8192	8192
reporte5.txt	2048	2048
reporte6.txt	2048	2048

Nota. Elaborado en Word 365 y obtenido de procesamiento mediante php

4.2. ICS expuestos al Internet

El escaneo indica que no hay dispositivos ICS expuestos al internet.

Tabla 2.

Resultados por puerto ICS

Puerto	Protocolo/Servicio	Estado	Conteo de hosts
102	Siemens S7 (iso-tsap)	open	0
102	Siemens S7 (iso-tsap)	closed	5
102	Siemens S7 (iso-tsap)	filtered	326

502	Modbus/TCP (mbap)	open	0
502	Modbus/TCP (mbap)	closed	5
502	Modbus/TCP (mbap)	filtered	326
2222	Allen-Bradley EtherNet/IP (alt)	open	0
2222	Allen-Bradley EtherNet/IP (alt)	closed	5
2222	Allen-Bradley EtherNet/IP (alt)	filtered	326
9600	Omron PLC	open	0
9600	Omron PLC	closed	5
9600	Omron PLC	filtered	326
20548	Schleicher XCX 300	open	0
20548	Schleicher XCX 300	closed	5
20548	Schleicher XCX 300	filtered	326
28784	Koyo Ethernet	open	0
28784	Koyo Ethernet	closed	5
28784	Koyo Ethernet	filtered	326
44818	Allen-Bradley EtherNet/IP	open	0
44818	Allen-Bradley EtherNet/IP	closed	5
44818	Allen-Bradley EtherNet/IP	filtered	326
57176	GE QuickPanels	open	0
57176	GE QuickPanels	closed	5
57176	GE QuickPanels	filtered	326

Nota. Elaborado con Word 365 a partir de análisis de csv con resumen de métricas

Se observa que no se encontraron IPs con puertos ICS abiertos en los seis escaneos analizados.

5. DISCUSION DE RESULTADOS

5.1. Interpretación téctica

El estado filtered significa que el puerto no respondió directamente, pero tampoco está cerrado; esto suele deberse a firewalls o ACLs que bloquean el escaneo. Además los timeouts masivos pueden indicar que los rangos están detrás de NAT, CGNAT o que hay ISP-level filtering.

5.2. Limitaciones del escaneo

Se usó --host-timeout 30s y --max-retries 2, lo que reduce la posibilidad de detectar hosts lentos o con alta latencia. Asimismo, no se incluyó UDP, que es relevante para protocolos ICS como EtherNet/IP implícito.

5.3. Implicaciones

Aunque no se encontraron puertos abiertos, no se puede descartar exposición parcial sin pruebas adicionales (escaneo con mayor tiempo, NSE scripts, otras fuentes). El resultado es positivo desde la perspectiva de seguridad: baja superficie de ataque directa en Internet.

6. CONCLUSIONES

- No se detectaron puertos ICS abiertos en ninguno de los seis rangos analizados.
- Los puertos críticos (102/S7, 502/Modbus, 44818/2222 EtherNet/IP, etc.) aparecen como filtered en los pocos hosts que respondieron, lo que indica presencia de filtrado perimetral o firewalls.
- La mayoría de las IPs fueron omitidas por timeout, lo que sugiere limitaciones de conectividad o políticas de rate-limiting.
- Con la evidencia actual, no hay exposición directa de dispositivos ICS a Internet en los rangos evaluados.

7. RECOMENDACIONES

- Aumentar tiempos y reintentos: --host-timeout 60–120s, --max-retries 4–6; usar -T3 para minimizar rate-limiting.
- Añadir UDP cuando aplique (p.ej., 2222/udp para EtherNet/IP implícito).
- Ejecutar NSE específico (modbus-discover, s7-info, ethernetip-info) para reconocimiento de banners.
- Validar desde otra red/origen para evitar filtros perimetrales dependientes del origen.