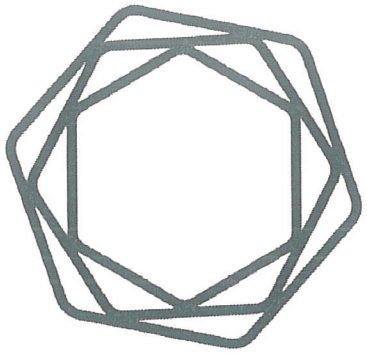
XIGA



ANALISIS DE VULNERABILIDADES

Enerser

Depto. Infraestructura

Fecha: 14/02/25

XIGA

INTRODUCCIÓN

Con el objetivo de fortalecer la postura de seguridad de la infraestructura, se llevará a cabo un escaneo exhaustivo de vulnerabilidades en los segmentos de estaciones. Esta iniciativa permitirá identificar de manera precisa las aplicaciones y servicios expuestos a riesgos, facilitando así la implementación de medidas correctivas y preventivas oportunas.

Dichas medidas ayudaran a preservar la continuidad del negocio, por lo cual el realizar de forma periódica dichos analisis es fundamental para conocer el estatus de la infraestructura y en caso de vulnerabilidades emergentes, tener un plan de remediación el cual efectuar y así conservar la confidencialidad, integridad y disponibilidad de nuestros sistemas de información.

ALCANCE

Evaluar la seguridad de la infraestructura de las 9 estaciones de servicio: **Calzada Independencia PL 1668, Esteban Alatorre PL 1667, El pueblito PL 7171, Epigmeo-Queretaro PL 19175, Pedro Escobedo PL 880, Tepalcapa 18819, Doloores Hidalgo PL 5811, La Pila, PL 5404, San Diego de la Union PL 5915.** Identificando las vulnerabilidades presentes y determinando el nivel de riesgo al que están expuestos los datos.

XIGA

RESUMEN EJECUTIVO

Nombre de la prueba	Análisis de vulnerabilidades - estaciones Chevron
Descripción:	Evaluación de estaciones Chevron.
Tipo:	Evaluación
Tiempo y Duración	Feb 14 2025 10:10 am - Feb 14 2025 2:18 pm

Top Service/App/Sofware

Se representa el top 5 herramientas servicios o software mas vulnerable.

DNS Server detection

Common Platform Enumeration (CPE)

HTTP/2 ClearText Detection

OpenSSH Detection

PostgrSQL Server Detection

Resumen Porcentual de Vulnerabilidades

HOST ANALISIS DE VULNERABILIDADES

Esteban Alatorre

Estación	Esteban Alatorre
Dirección	Calle Esteban Alatorre No. 3002, Col. Libertad,
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	GDL-ESTEBANALATORRE
Direccion IP	192.168.184.1

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	10

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Esteban Alatorre

Estación	Esteban Alatorre
Dirección	Calle Esteban Alatorre No. 3002,
Sistema Operativo	Windows 10 Enterprise
Tipo de dispositivo	Desktop
Nombre del equipo	DESKTOP-MKH4LEV
Direccion IP	192.168.184.4

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	5

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Pedro Escobedo

Estación	Pedro Escobedo
Dirección	Cuerpo A, Autopista México-Querérato,Tramo Palmillas-Quéretaro, Pedro Escobedo, QRO
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	QET-PEDROESCOBEDO
Direccion IP	192.168.112.1

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	10

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Pedro Escobedo

Estación	Pedro Escobedo
Dirección	Cuerpo A, Autopista México-Querétato,Tramo Palmillas-Quéretaro, Pedro Escobedo, QRO
Sistema Operativo	Windows 10 Enterprise
Tipo de dispositivo	Desktop
Nombre del equipo	Jaysee-C
Direccion IP	192.168.112.4

Vulnerabilidades y sus niveles de riesgo

0	0	0	0	5
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

San Diego de la Union

Estación	San Diego de la Union
Dirección	Allende No.1, Centro, San diego de la union
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	GTO-SANDIEGOUNION
Direccion IP	192.168.185.1

Vulnerabilidades y sus niveles de riesgo

0	0	0	0	10
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

San Diego de la Union

Estación	San Diego de la Union
Dirección	Allende No.1, Centro, San diego de la union
Sistema Operativo	Wikndows 10 Enterprise
Tipo de dispositivo	Desktop
Nombre del equipo	DESKTOP-B2BVT28
Direccion IP	192.168.185.4

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	5

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Calzada Independencia

Estación	Calzada Independencia
Dirección	Calz. Independencia Nte No.2920, La Federacha,Guadalajara
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	GDL-CALZADAINDEPENDENCIA
Direccion IP	192,168.196.1

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	10

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Calzada Independencia

Estación	Calzada Independencia
Dirección	Calz. Independencia Nte No.2920, La Federacha,Guadalajara
Sistema Operativo	Windows 11
Tipo de dispositivo	Desktop
Nombre del equipo	DESKTOP-156JKKU
Direccion IP	192,168.196.4

Vulnerabilidades y sus niveles de riesgo

0	0	0	0	5
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Dolores Hidalgo

Estación	Dolores Hidalgo
Dirección	Libramiento Oriente KM 0.20,Dolores Hidalgo Cuna de la Independencia Nacional, GTO
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	GTO-DOLORES
Direccion IP	192.168.186.1

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	10

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	N/A	-	-	181418	Open SSH Detection
Info	N/A	-	-	26024	PostgreSQL Server detection
Info	N/A	-	-	45590	Common Platform Eumeration (CPE)
Info	N/A	-	-	11002	DNS server Detection
Info	N/A	-	-	85805	HTTP/2 ClearText Detection
Info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
Info	N/A	-	-	34098	BIOS Info (SSH)
Info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Dolores Hidalgo

Estación	Dolores Hidalgo
Dirección	Libramiento Oriente KM 0.20,Dolores Hidalgo Cuna de la Independencia Nacional, GTO
Sistema Operativo	Windows 11
Tipo de dispositivo	Desktop
Nombre del equipo	DESKTOP-DRHS44Q
Direccion IP	192.168.186.4

Vulnerabilidades y sus niveles de riesgo

0	0	0	0	5
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

La Pila

Estación	La Pila
Dirección	Carr Federal, San Luis Potosi, SLP
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	SLP-LAPILA
Direccion IP	192,168.188.1

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	10

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

La Pila

Estación	La Pila
Dirección	Carr Federal, San Luis Potosi, SLP
Sistema Operativo	Windows 11
Tipo de dispositivo	Desktop
Nombre del equipo	Desktop-H9UPTV1
Direccion IP	192,168.188.4

Vulnerabilidades y sus niveles de riesgo

0	0	0	0	5
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

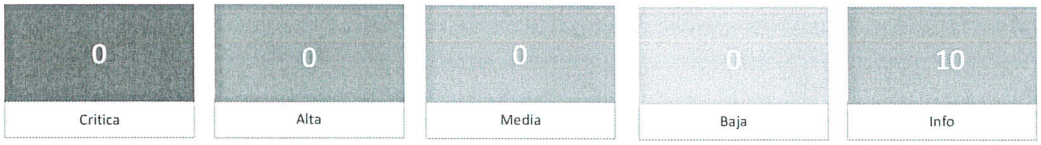
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

El Pueblito

Estación	El Pueblito
Dirección	Camino a Vanegas No. 13,Emiliano Zapata,Corregidora,QRO
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	QET-ELPUEBLITO
Direccion IP	192,168.192.1

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

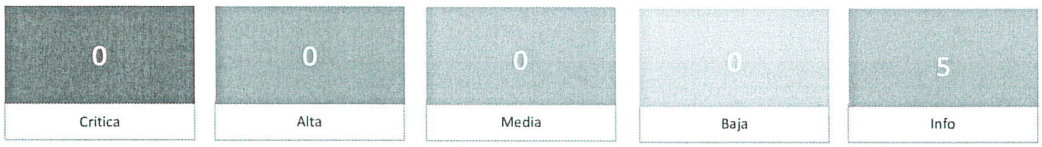
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

El Pueblito

Estación	El Pueblito
Dirección	Camino a Vanegas No. 13,Emiliano Zapata,Corregidora,QRO
Sistema Operativo	Windows 7
Tipo de dispositivo	DESKTOP
Nombre del equipo	DESKTOP-0HNNIKC
Direccion IP	192.168.192.4

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Epigmenio

Estación	Epigmenio
Dirección	Epigmenio González No. 11,San Pablo Tecnológico,Queretaro,QRO
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	QET-EPIGMENIO
Direccion IP	192,168.114.1

Vulnerabilidades y sus niveles de riesgo

0	0	0	0	10
Critica	Alta	Media	Baja	Info

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

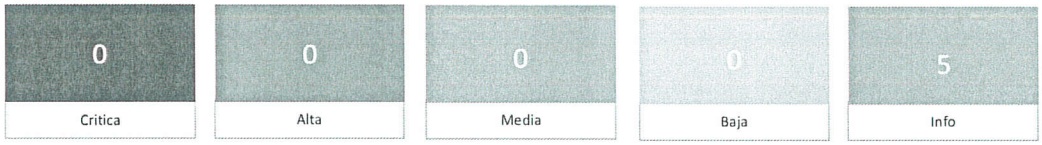
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Epigmenio

Estación	Epigmenio
Dirección	Epigmenio González No. 11,San Pablo Tecnológico,Queretaro,QRO
Sistema Operativo	Windows 7
Tipo de dispositivo	Desktop
Nombre del equipo	DESKTOP-156JKKU
Direccion IP	192,168.196.4

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Tepalcapa

Estación	Tepalcapa
Dirección	Estación Rael, S. de R.L. de C.V.
Sistema Operativo	Rocky Linux 9.4 - Blue Onix
Tipo de dispositivo	Servidor
Nombre del equipo	MEX-TECALCAPA
Direccion IP	192.168.113.1

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	0	0	0	10

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
info	N/A	-	-	181418	Open SSH Detection
info	N/A	-	-	26024	PostgreSQL Server detection
info	N/A	-	-	45590	Common Platform Eumeration (CPE)
info	N/A	-	-	11002	DNS server Detection
info	N/A	-	-	85805	HTTP/2 ClearText Detection
info	N/A	-	-	156000	Apache Log4j Installed (Linux / Unix)
info	N/A	-	-	34098	BIOS Info (SSH)
info	N/A	-	-	39520	Backported Security Patch Detection (SSH)
info	N/A	-	-	45590	Common Platform Enumeration (CPE)
info	N/A	-	-	182774	Curl Installed (Linux / Unix)

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

XIGA

Tepalcapa

Estación	Tepalcapa
Dirección	Estación Rael, S. de R.L. de C.V.
Sistema Operativo	Windows 7
Tipo de dispositivo	Desktop
Nombre del equipo	Tepalcapa-PC
Direccion IP	192.168.113.4

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Info	5.3	-	-	57608	SMB Signing not required
Info	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
Info	N/A	-	-	45590	Common Platform Enumeration (CPE)
Info	N/A	-	-	10107	HTTP Server Type and Version
Info	N/A	-	-	54615	Device Type

Herramientas utilizadas en la prueba de auditoria

Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)