ANALISIS DE VULNERABILIDADES

Enerser

Depto. Infraestructura

Fecha: 4/10/24

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.

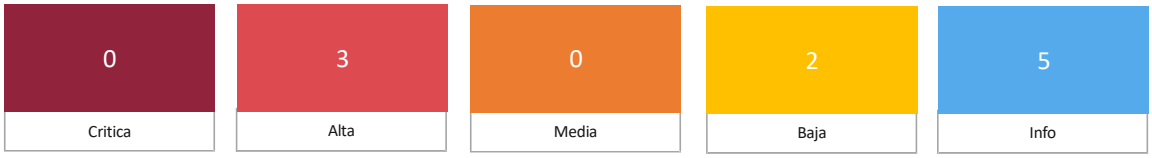
Dichas medidas ayudaran a preservar la continuidad del negocio, por lo cual el realizar de forma periódica dichos analisis es fundamental para conocer el estatus de la infraestructura y en caso de vulnerabilidades emergentes, tener un plan de remediación el cual efectuar y así conservar la confidencialidad,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

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
Fecha de escaneo	25 Sep 2024 - 1:50 pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explotación

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
Fecha de escaneo	25 Sep 2024 -1:53 pm

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Media	5.3	-	-	57608	SMB Signing not required
Baja	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

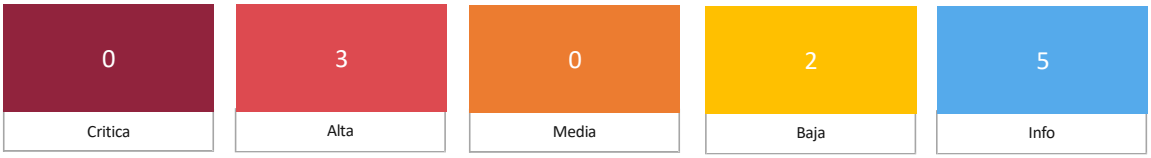
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	25 Sep 2024 - 2:17pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

Pedro Escobedo

Estación	Pedro Escobedo
Dirección	Cuerpo A, Autopista México-Querérato,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
Fecha de escaneo	25 Sep 2024 - 2:21pm

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Media	5.3	-	-	57608	SMB Signing not required
Baja	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

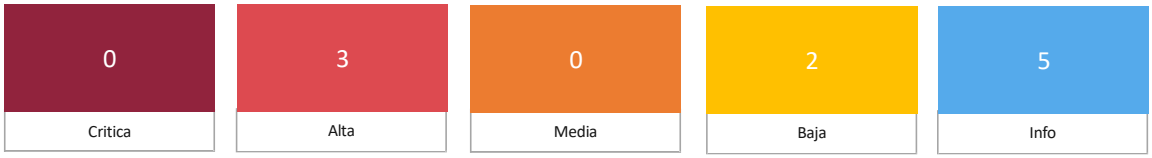
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	25 Sep 2024 - 3:45 pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	25 Sep 2024 - 3:52 pm

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Media	5.3	-	-	57608	SMB Signing not required
Baja	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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explot

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
Fecha de escaneo	26 Sep 2024 - 9:05 am

Vulnerabilidades y sus niveles de riesgo

Critica	Alta	Media	Baja	Info
0	3	0	2	5

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	26 Sep 2024 - 9:15 am

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Media	5.3	-	-	57608	SMB Signing not required
Baja	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

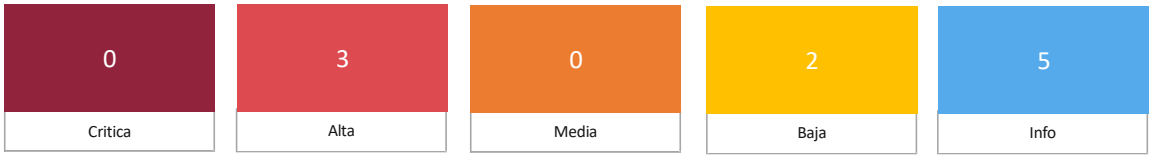
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explot

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
Fecha de escaneo	26 Sep 2024 - 11:27 am

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	26 Sep 2024 - 11:33 am

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Media	5.3	-	-	57608	SMB Signing not required
Baja	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

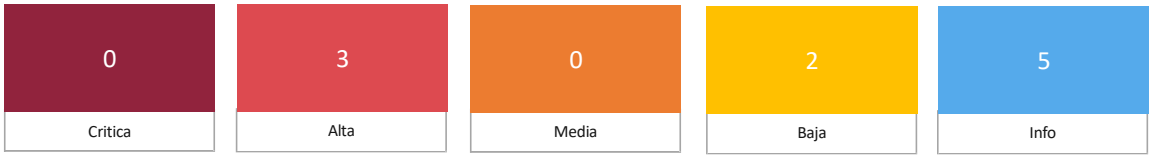
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explot

La Pila

Estación	La Pila
Dirección	Carrt 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
Fecha de escaneo	26 Sep 2024 - 12:01 pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

La Pila

Estación	La Pila
Dirección	Carrt Federal, San Luis Potosi, SLP
Sistema Operativo	Windows 11
Tipo de dispositivo	Desktop
Nombre del equipo	Desktop-H9UPTV1
Direccion IP	192,168.188.4
Fecha de escaneo	26 Sep 2024 - 12:07pm

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Media	5.3	-	-	57608	SMB Signing not required
Baja	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

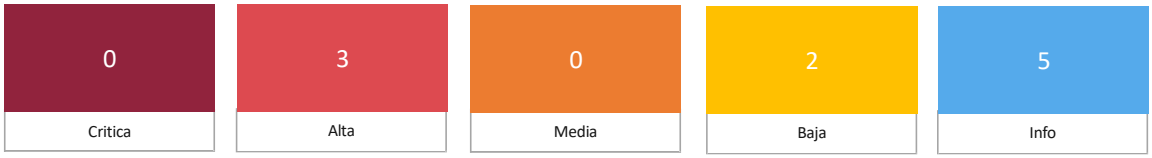
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explot

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
Fecha de escaneo	26 Sep 2024 - 1:30 pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	26 Sep 2024 - 2:27 pm

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Critica	10.0	-	-	108797	Unsupported Windows OS (remote)
Media	5.3	4.2	0.8808	57608	SMB Signing not required
baja	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
baja	N/A	-	-	45590	Common Platform Enumeration (CPE)
baja	N/A	-	-	10736	DCE Services Enumeration
baja	N/A	-	-	54615	Device Type
baja	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
baja	N/A	-	-	10920	Microsoft Windows 'Administrators' Group User List
baja	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
baja	N/A	-	-	17651	Microsoft Windows SMB Log In Possible

Herramientas utilizadas en la prueba de auditoria

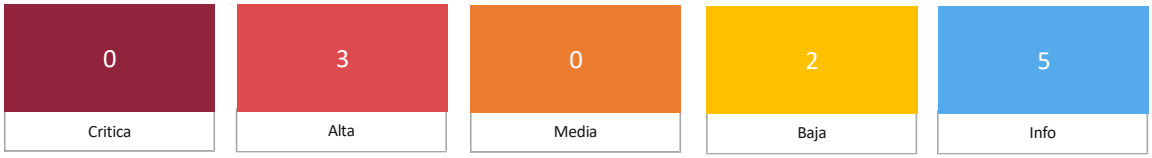
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metasploit:
Analisis de las vulnerabilidades, explotación y post-explot

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
Fecha de escaneo	26 Sep 2024 - 2:33pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	26 Sep 2024 - 9:15 am

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Critica	10.0	-	-	108797	Unsupported Windows OS (remote)
Media	5.3	4.2	0.8808	57608	SMB Signing not required
baja	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
baja	N/A	-	-	45590	Common Platform Enumeration (CPE)
baja	N/A	-	-	10736	DCE Services Enumeration
baja	N/A	-	-	54615	Device Type
baja	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
baja	N/A	-	-	10920	Microsoft Windows 'Administrators' Group User List
baja	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
baja	N/A	-	-	17651	Microsoft Windows SMB Log In Possible

Herramientas utilizadas en la prueba de auditoria

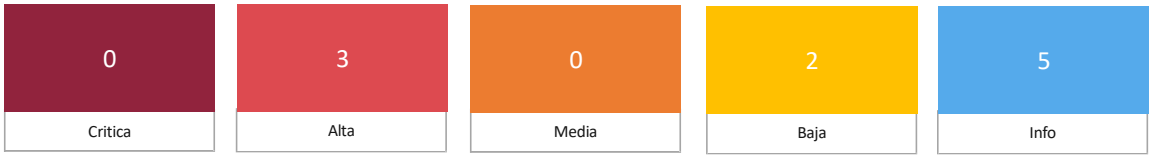
Tenable Nessus:
Software dedicado al escaneo de vulnerabilidades en sistemas informaticos mediante el estandar CVE (Common Vulnerabilities Exposures)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explot

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
Fecha de escaneo	26 Sep 2024 - 4:00 pm

Vulnerabilidades y sus niveles de riesgo



Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Alta	7.5	6.7	0.1591	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
Alta	7.5	6.0	0.0009	202704	Oracle Java SE Multiple Vulnerabilities
Alta	7.4	6.0	0.0009	207298	Oracle Java SE Multiple Vulnerabilities
Baja	3.8	2.4	0.0004	10114	Rocky Linux 9 : glib2 (RLSA-2024:6464)
Baja	2.1*	4.2	0.8808	207298	ICMP Timestamp Request Remote Date Disclosure
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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explotación.

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
Fecha de escaneo	26 Sep 2024 - 4:15 pm

Vulnerabilidades y sus niveles de riesgo

Severidad	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
Critica	10.0	-	-	108797	Unsupported Windows OS (remote)
Media	5.3	4.2	0.8808	57608	SMB Signing not required
baja	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure
baja	N/A	-	-	45590	Common Platform Enumeration (CPE)
baja	N/A	-	-	10736	DCE Services Enumeration
baja	N/A	-	-	54615	Device Type
baja	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
baja	N/A	-	-	10920	Microsoft Windows 'Administrators' Group User List
baja	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
baja	N/A	-	-	17651	Microsoft Windows SMB Log In Possible

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)

Metaslploit:
Analisis de las vulnerabilidades, explotación y post-explot

CONCLUSION

En conclusión, los resultados del escaneo de vulnerabilidades en los segmentos de estaciones han revelado un panorama detallado de las posibles amenazas a las que se encuentra expuesta la infraestructura. Las tablas presentadas a lo largo de este documento evidencian la necesidad de implementar un plan de remediación urgente y eficaz. Es fundamental abordar las vulnerabilidades identificadas para garantizar la integridad y confidencialidad de los datos, así como para prevenir incidentes de seguridad que puedan comprometer la continuidad del negocio.