**Auditoría/Informe del proyecto del equipo Gryffindor CIT31-01**

# ÍNDICE

[ÍNDICE 2](#_heading=h.lnxbz9)

[ÍNDICE DE FIGURAS 3](#_heading=h.35nkun2)

[ENUNCIADO 4](#_heading=h.1ksv4uv)

[RED PROPUESTA 5](#_heading=h.44sinio)

[AUDITORÍA 7](#_heading=h.2jxsxqh)

[1.](#_heading=h.z337ya) Enumeración de redes, componentes, topologías y protocolos 7

[2.](#_heading=h.3j2qqm3) Identificación de los sistemas operativos instalados 7

[3.](#_heading=h.1y810tw) Análisis de servicios y aplicaciones 8

[4.](#_heading=h.4i7ojhp) Detección, comprobación y evaluación de vulnerabilidades 9

[5.](#_heading=h.2xcytpi) Medidas específicas de corrección 10

[6.](#_heading=h.1ci93xb) Recomendaciones sobre implantación de medidas preventivas. 11

[REFERENCIAS 14](#_heading=h.3whwml4)

# ÍNDICE DE FIGURAS

[Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022). 6](#_heading=h.2et92p0)

# ENUNCIADO

Usted trabaja para una empresa de SmartBuildings. Ante la emergencia de Coronavirus se le pide desplegar un sistema de SmartCities para comunicar en tiempo real a los miembros del sistema sanitario. Para ello despliega en dos edificios sistemas basados en gateways Linux (puede escoger la distribución más apropiada). Dichos sistemas permiten enviar información mediante una interfaz web a una base de datos alojada en uno de los edificios. A dicha base de datos y servicio web solo se puede acceder desde la intranet del edificio. Además, en el servidor, debe alojar una plataforma web para que todo el público pueda enviar consultas y otra información para permitir servicios de telemedicina.

Debe planificar un sistema seguro que permita a los gateway enviar los datos al servidor, que además debe estar accesible a los habitantes del edificio y cualquier usuario doméstico (todos ellos usuarios de Windows). Dichos usuarios se conectan desde Intranet donde se dispone de una LAN WiFi que mantiene conectados los equipos mencionados y, además, dispositivos móviles.

Adicionalmente, el profesor dijo que tratáramos de hacer nuestro proyecto de mensajería sin alterar la infraestructura original.

# RED PROPUESTA

Inicialmente nos centramos por un diseño como el mencionado en el enunciado, tanto por simplicidad como por petición del enunciado, en el que se comunica el exterior con el interior mediante una VPN para evitar tener que alterar la infraestructura original de la empresa, incluyendo firewalls. La red VPN tiene la ventaja de cifrar el tráfico durante el establecimiento de conexión con los servidores, lo que hace que ya no aparezca texto en claro sensible con datos del usuario que pueda ser fácilmente expuesto en redes Wi-fi no muy seguras y dificulta que un ataque man-in-the-middle pueda acceder a estos, algo vital para el servicio de mensajería.

Al comienzo tratamos de usar la VPN preinstalada de Windows, pero por comodidad decidimos emplear el software profesional OpenVPN. Según las instrucciones de instalación (WunderTech, 2022), hemos decidido que nuestra VPN es 192.168.60.0/24 es la VPN, llamada OpenVPN Servidor, la Clave pre-compartida es “SorbeteDeLimon” y el resto queda por defecto. Estos parámetros los utilizamos para el Firewall de su edificio también. El usuario es SSR con nombre completo “Albus Dumbledore”.

El edificio remoto tiene red 192.168.57.0/24, el edificio de la empresa 192.168.56.0/24 y la internet la simulamos con la 100.200.0.0/24, inicialmente tratamos de hacer una conexión entre dos ordenadores físicos virtualizando los edificios y con un módem físico entre medias, pero no funcionó así que pasamos a virtualizarlo todo en una máquina y quitarnos el router de en medio.

Hemos supuesto que en la infraestructura original los gateways son del tipo pfSense y utilizan un único firewall por edificio de política restrictiva hacia adentro, para mayor seguridad (menos funcionalidades supone menos potenciales vulnerabilidades), permitiendo la entrada por el puerto 443 y 80 (también está el 3306 para el mySQL pero para acceso local); y sin suponer mayor profundidad en la red, para permitir virtualizar varias máquinas.

La BBDD es SQL (MariaDB) mediante xampp, se debe tener una IP de la LAN y contraseña.

El material de nuestra red puede encontrarse en el github:

https://github.com/tardisfromtornspace/ProyectoGryffindorCIT31-01.git

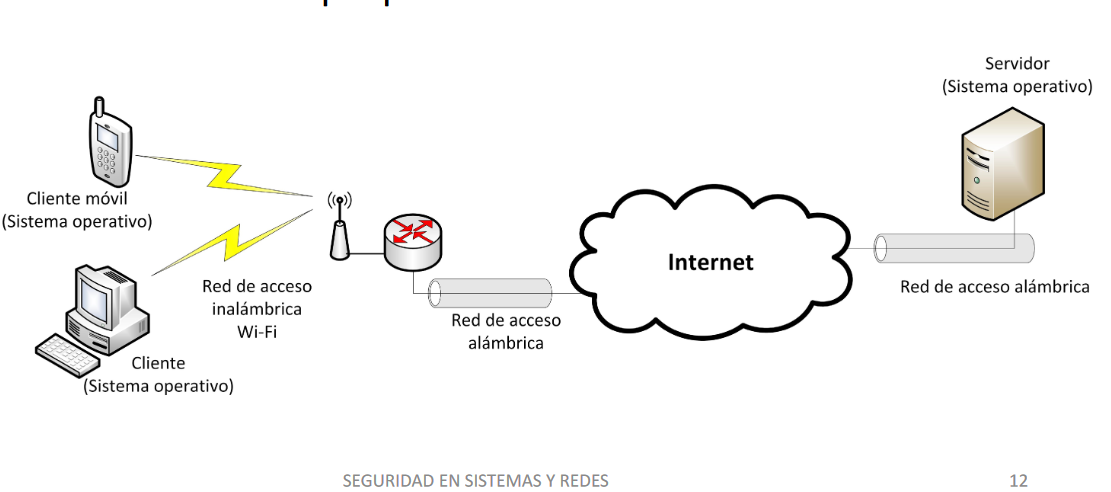


Figura 1: Modelo esquemático de la red propuesta **(Sánchez, 2022)**.

# AUDITORÍA

Hemos decidido emplear una auditoría de caja blanca por falta de tiempo y para mayor eficiencia, con un conocimiento total de la red.

*Los ataques se hacen desde 3 sitios, edificio de la empresa, edificio remoto y desde la internet, con una Kali Linux o Windows donde corresponda*

## Enumeración de redes, componentes, topologías y protocolos

Hay 3 redes, mencionadas en el apartado red propuesta:

**LANA** – La red del edificio de la empresa 192.168.56.0/24 tiene configurada una VPN. Tiene una máquina servidor (192.168.56.10) y el router pfSense1 (192.168.56.1)

**LANB** – La red edificio remoto 192.168.57.0/24. Tiene una máquina clienteRemoto (192.168.57.2) y el router pfSense2 (192.168.57.1)

**WAN** – Simulación del internet 100.200.0.0/24. Tiene los dos routers (pfSense1 con 100.200.0.1 y pfSense2 con 100.200.0.2).

Todos ellos emplean topología en estrella, menos la conexión de WAN, simulada con un P2P. Todos ellos emplean máscara /24 por simplicidad.

Routers:

**pfSense1:** es el que conecta LANA con WAN

**pfSense2:** es el que conecta LANB con WAN

-Ambos actúan con el mismo tipo de firewall: política permisiva desde LAN y restrictiva desde WAN.

Usamos protocolo TCP/IP para las conexiones, salvo OpenVPN, que se especializa en el uso de UDP.

## Identificación de los sistemas operativos instalados

1. **pfSense1 (#R1):** pfSense 2.6.0-RELEASE FreeBSD 64-bit 12.3-STABLE
2. **pfSense2 (#R2)**: pfSense 2.5.2-RELEASE FreeBSD 64-bit 12.2-STABLE
3. **ClienteRemoto** **(#LANB1**): ~~Windows XP 32-bit con parche Service Pack 3~~ *No hemos usado el Windows XP por su gran número de vulnerabilidades conocidas y la imposibilidad de actualizar o parchear gran parte de ellas, así que hemos empleado un* Windows 7 Ultimate 32-bit bit 6.1.7601 Service Pack 1 Build 7601
4. **Servidor (#LANB2):** Windows 10 Education 64-bit, versión 1903, versión del SO 18362.592

## Análisis de servicios y aplicaciones

*NOTA: Previo a esto hemos ido eliminando aplicaciones innecesarias en el Servidor.*

|  |
| --- |
| **pfSense1 (#R1)**  Nmap LAN   * PORT STATE SERVICE VERSION * **80**/tcp open http nginx * **443**/tcp open ssl/https?   Dispone solamente del servicio http en el puerto 80 para la configuración del pfsense. Lo mismo ocurre con el puerto 443, para la conexión por https que ha sido configurada en el pfSense1.  Nmap WAN  PORT STATE SERVICE VERSION  El puerto 1194 se encuentra abierto para la comunicación  por VPN, aunque Nmap no lo ha detectado.  Lista de servicios (todos los servicios locales de pfSense1, no hecha por Nmap sino al verlo nosotros en caja blanca):   * dpinger (Gateway Monitoring Daemon) * openvpn (OpenVPN server: VPN Servidor) * syslogd (System Logger Daemon) * unbound (DNS Resolver)   **pfSense2 (#R2)**:  Nmap LAN  PORT STATE SERVICE VERSION   * **53**/tcp open domain Unbound * **80**/tcp open http nginx * **443**/tcp open ssl/http nginx   Similar a pfSense1, pero en este caso el puerto 53 se encuentra abierto.  Este servicio se utiliza para comunicar tramas DNS.  Nmap WAN  PORT STATE SERVICE VERSION  El puerto 1194 se encuentra abierto para la comunicación  por VPN, aunque Nmap no lo ha detectado.  Lista de servicios (todos los servicios locales de pfSense2, no hecha por Nmap sino al verlo nosotros en caja blanca):   * dpinger (Gateway Monitoring Daemon) * pcscd (PC/SC Smart Card Daemon) * syslogd (System Logger Daemon) * unbound (DNS Resolver)   **ClienteRemoto** **(#LANB1**):  Resultados del nmap  PORT STATE SERVICE VERSION   * **135**/tcp open msrpc Microsoft Windows RPC * **139**/tcp open netbios-ssn Microsoft Windows netbios-ssn * **445**/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) * **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) * **49152**/tcp open msrpc Microsoft Windows RPC * **49153**/tcp open msrpc Microsoft Windows RPC * **49154**/tcp open msrpc Microsoft Windows RPC * **49155**/tcp open msrpc Microsoft Windows RPC * **49156**/tcp open msrpc Microsoft Windows RPC * **49157**/tcp open msrpc Microsoft Windows RPC   Lista de aplicaciones**:**   1. (Las estándar del paquete Microsoft para la versión de Windows) 2. Microsoft.NET Framework 4.7.03062 3. Mozilla Firefox x86 (es-ES) 101.0.1 4. Mozilla Maintenance Service 101.0.1.8194 5. OpenVPN x86 2.5.021 6. Oracle VM VirtualBox Guest Additions 6.1.0 (*No se va a contar para vulnerabilidades*)   Lista de servicios (todos los servicios locales de windows, no hecha por Nmap, por lo que no se tendrá tan en cuenta):   * 1. Name   2. ActiveX Installer (AxInstSV)   3. Adaptive Brightness   4. Application Experience   5. Application Identity   6. Application Information   7. Application Layer Gateway Service   8. Application Management   9. ASP.NET State Service   10. Background Intelligent Transfer Service   11. Base Filtering Engine   12. BitLocker Drive Encryption Service   13. Block Level Backup Engine Service   14. Bluetooth Support Service   15. BranchCache   16. Certificate Propagation   17. CNG Key Isolation   18. COM+ Event System   19. COM+ System Application   20. Computer Browser   21. Credential Manager   22. Cryptographic Services   23. DCOM Server Process Launcher   24. Desktop Window Manager Session Manager   25. DHCP Client   26. Diagnostic Policy Service   27. Diagnostic Service Host   28. Diagnostic System Host   29. Diagnostics Tracking Service   30. Disk Defragmenter   31. Distributed Link Tracking Client   32. Distributed Transaction Coordinator   33. DNS Client   34. Encrypting File System (EFS)   35. Extensible Authentication Protocol   36. Fax   37. Function Discovery Provider Host   38. Function Discovery Resource Publication   39. Group Policy Client   40. Health Key and Certificate Management   41. HomeGroup Listener   42. HomeGroup Provider   43. Human Interface Device Access   44. IKE and AuthIP IPsec Keying Modules   45. Interactive Services Detection   46. Internet Connection Sharing (ICS)   47. Internet Explorer ETW Collector Service   48. IP Helper   49. IPsec Policy Agent   50. KtmRm for Distributed Transaction Coordinator   51. Link-Layer Topology Discovery Mapper   52. Media Center Extender Service   53. Microsoft .NET Framework NGEN v2.0.50727\_X86   54. Microsoft .NET Framework NGEN v4.0.30319\_X86   55. Microsoft iSCSI Initiator Service   56. Microsoft Software Shadow Copy Provider   57. Mozilla Maintenance Service   58. Multimedia Class Scheduler   59. Net.Msmq Listener Adapter   60. Net.Pipe Listener Adapter   61. Net.Tcp Listener Adapter   62. Net.Tcp Port Sharing Service   63. Netlogon   64. Network Access Protection Agent   65. Network Connections   66. Network List Service   67. Network Location Awareness   68. Network Store Interface Service   69. Offline Files   70. OpenVPN Interactive Service   71. Parental Controls   72. Peer Name Resolution Protocol   73. Peer Networking Grouping   74. Peer Networking Identity Manager   75. Performance Logs & Alerts   76. Plug and Play   77. PnP-X IP Bus Enumerator   78. PNRP Machine Name Publication Service   79. Portable Device Enumerator Service   80. Power   81. Print Spooler   82. Problem Reports and Solutions Control Panel Support   83. Program Compatibility Assistant Service   84. Protected Storage   85. Quality Windows Audio Video Experience   86. Remote Access Auto Connection Manager   87. Remote Access Connection Manager   88. Remote Desktop Configuration   89. Remote Desktop Services   90. Remote Desktop Services UserMode Port Redirector   91. Remote Procedure Call (RPC)   92. Remote Procedure Call (RPC) Locator   93. Remote Registry   94. Routing and Remote Access   95. RPC Endpoint Mapper   96. Secondary Logon   97. Secure Socket Tunneling Protocol Service   98. Security Accounts Manager   99. Security Center   100. Server   101. Shell Hardware Detection   102. Smart Card   103. Smart Card Removal Policy   104. SNMP Trap   105. Software Protection   106. SPP Notification Service   107. SSDP Discovery   108. Superfetch   109. System Event Notification Service   110. Tablet PC Input Service   111. Task Scheduler   112. TCP/IP NetBIOS Helper   113. Telephony   114. Themes   115. Thread Ordering Server   116. UPnP Device Host   117. User Profile Service   118. Virtual Disk   119. VirtualBox Guest Additions Service   120. Volume Shadow Copy   121. WebClient   122. Windows Audio   123. Windows Audio Endpoint Builder   124. Windows Backup   125. Windows Biometric Service   126. Windows CardSpace   127. Windows Color System   128. Windows Connect Now - Config Registrar   129. Windows Defender   130. Windows Driver Foundation - User-mode Driver Framework   131. Windows Error Reporting Service   132. Windows Event Collector   133. Windows Event Log   134. Windows Firewall   135. Windows Font Cache Service   136. Windows Image Acquisition (WIA)   137. Windows Installer   138. Windows Management Instrumentation   139. Windows Media Center Receiver Service   140. Windows Media Center Scheduler Service   141. Windows Media Player Network Sharing Service   142. Windows Modules Installer   143. Windows Presentation Foundation Font Cache 3.0.0.0   144. Windows Remote Management (WS-Management)   145. Windows Search   146. Windows Time   147. Windows Update   148. WinHTTP Web Proxy Auto-Discovery Service   149. Wired AutoConfig   150. WLAN AutoConfig   151. WMI Performance Adapter   152. Workstation   153. WWAN AutoConfig   **Servidor (#LANB2):**  Resultados del nmap  PORT STATE SERVICE VERSION   * **80**/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m * PHP/8.1.2) * **443**/tcp open ssl/http Apache httpd 2.4.52 ((Win64) * OpenSSL/1.1.1m PHP/8.1.2) * **3306**/tcp open mysql? (MariaDB) * **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)   Los puertos 80 y 443 para la conexión http y https respectivamente.  En el puerto 3306 podemos encontrar la conexión a la base de datos  mysql. El puerto 5357 se utiliza para detectar redes y dispositivos plug &  play.  Lista de aplicaciones (sacadas desde Aplicaciones y características porque tanto WMIC CONO Get-itemProperty solo nos dicen los que hemos instalado nosotros**):**   1. Alarms & Clock 10.1910.3121.0 2. App Installer 1.0.32912.0 3. Camara 2019.926.20.0 4. Extensión de Imagen HEIF 1.0.23292.0 5. Extensiones de Imagen Webp 1.0.22753.0 6. Fotos de Microsoft 2019.19081.22010.0 7. Get Help 10.1909.22691.0 8. Maps 5.1909.2813.0 9. Microsoft Edge 44.18362.449.0 10. Microsoft Store 120001.1001.0 11. Microsoft Update Health Tools 2.84.0.0 12. Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30135 13. Mozilla Firefox (x86 es-ES) 100.0.2 <- ACTUALIZAR 14. Mozilla Maintenance Service 71.0 15. Oracle VM VirtualBox Guest Additions 6.1.0 (*No se va a contar para vulnerabilidades*) 16. Paquete de experiencia local en español (España) 18362.47.133.0 17. People 10.2105.4.0 18. USBPcap 1.5.4.0 <- VER SI PODEMOS BORRAR ESTE 19. XAMPP 8.1.2-0 20. Xbox Game Bar 3.36.6003.0 21. Your Phone 1.19122.89.0   Todas las aplicaciones de Microsoft Windows se encuentran actualizadas al parche  VER SI PODEMOS LISTAR LAS “CARACTERISTICAS OPCIONALES” Y BORRAR LAS EXTRA  Lista de servicios (todos los servicios de windows locales, no hecha por Nmap, por lo que no se tendrá tan en cuenta):   * 1. Acceso a datos de usuarios\_45406   2. Actualizador de zona horaria automática   3. Adaptador de rendimiento de WMI   4. Administración de aplicaciones   5. Administración de autenticación de Xbox Live   6. Administración de capas de almacenamiento   7. Administración remota de Windows (WS-Management)   8. Administrador de conexiones automáticas de acceso remoto   9. Administrador de conexiones de acceso remoto   10. Administrador de conexiones de Windows   11. Administrador de configuración de dispositivos   12. Administrador de credenciales   13. Administrador de cuentas de seguridad   14. Administrador de cuentas web   15. Administrador de identidad de redes de mismo nivel   16. Administrador de mapas descargados   17. Administrador de pagos y NFC/SE   18. Administrador de sesión local   19. Administrador de usuarios   20. Adquisición de imágenes de Windows (WIA)   21. Agent Activation Runtime\_45406   22. Agente de conexión de red   23. Agente de detección en segundo plano de DevQuery   24. Agente de directiva IPsec   25. Agente de eventos de tiempo   26. Agente de eventos del sistema   27. Agente de supervisión en tiempo de ejecución de Protección del sistema   28. Agrupación de red del mismo nivel   29. Aislamiento de claves CNG   30. Almacenamiento de datos de usuarios\_45406   31. Aplicación auxiliar de NetBIOS sobre TCP/IP   32. Aplicación auxiliar IP   33. Aplicación del sistema COM+   34. Archivos sin conexión   35. Asignador de detección de topologías de nivel de vínculo   36. Asignador de extremos de RPC   37. Asistente para la conectividad de red   38. Audio de Windows   39. Autenticación natural   40. Ayuda del Panel de control de Informes de problemas y soluciones   41. Ayudante para el inicio de sesión de cuenta Microsoft   42. BranchCache   43. Captura de SNMP   44. CaptureService\_45406   45. Carpetas de trabajo   46. Centro de seguridad   47. Cliente de directiva de grupo   48. Cliente de seguimiento de vínculos distribuidos   49. Cliente DHCP   50. Cliente DNS   51. Cliente web   52. Cola de impresión   53. Compilador de extremo de audio de Windows   54. Comprobador puntual   55. Conexión compartida a Internet (ICS)   56. Conexiones de red   57. Configuración automática de dispositivos conectados a la red   58. Configuración automática de redes cableadas   59. Configuración automática de WLAN   60. Configuración automática de WWAN   61. Configuración de Escritorio remoto   62. ConsentUX\_45406   63. Contenedor de Microsoft Passport   64. Control parental   65. Coordinador de transacciones distribuidas   66. Copias de seguridad de Windows   67. CoreMessaging   68. CredentialEnrollmentManagerUserSvc\_45406   69. Datos de contactos\_45406   70. Detección de hardware shell   71. Detección SSDP   72. DeviceAssociationBroker\_45406   73. DevicePicker\_45406   74. DevicesFlow\_45406   75. Diagnostic Execution Service   76. Directiva de extracción de tarjetas inteligentes   77. Disco virtual   78. Dispositivo host de UPnP   79. DLL de host del Contador de rendimiento   80. Energía   81. Enrutamiento y acceso remoto   82. Estación de trabajo   83. Eventos de adquisición de imágenes estáticas   84. Experiencia de calidad de audio y vídeo de Windows (qWave)   85. Extensiones y notificaciones de impresora   86. Fax   87. Firewall de Windows Defender   88. GraphicsPerfSvc   89. Hora de la red de telefonía móvil   90. Hora de Windows   91. Host de proveedor de detección de función   92. Host de sistema de diagnóstico   93. Host del servicio de diagnóstico   94. Identidad de aplicación   95. Información de la aplicación   96. Iniciador de procesos de servidor DCOM   97. Inicio de sesión secundario   98. Instalador de ActiveX (AxInstSV)   99. Instalador de módulos de Windows   100. Instantáneas de volumen   101. Instrumental de administración de Windows   102. Interfaz de servicio invitado de Hyper-V   103. KTMRM para DTC (Coordinador de transacciones distribuidas)   104. Llamada a procedimiento remoto (RPC)   105. MessagingService\_45406   106. Microsoft App-V Client   107. Microsoft Passport   108. Microsoft Update Health Service   109. Modo incrustado   110. Módulos de creación de claves de IPsec para IKE y AuthIP   111. Mostrar el servicio de directivas   112. Motor de filtrado de base   113. Mozilla Maintenance Service   114. Net Logon   115. OpenSSH Authentication Agent   116. Optimización de distribución   117. Optimizar unidades   118. Partida guardada en Xbox Live   119. Plug and Play   120. Preparación de aplicaciones   121. PrintWorkflow\_45406   122. Programador de tareas   123. Propagación de certificados   124. Protección de software   125. Protocolo de autenticación extensible   126. Protocolo de resolución de nombres de mismo nivel   127. Proveedor de instantáneas de software de Microsoft   128. Publicación de recurso de detección de función   129. Reconoc. ubicación de red   130. Recopilador de eventos de Windows   131. Redirector de puerto en modo usuario de Servicios de Escritorio remoto   132. Registrador de configuración de Windows Connect Now   133. Registro de eventos de Windows   134. Registro remoto   135. Registros y alertas de rendimiento   136. Servicio Administrador de funcionalidad de acceso   137. Servicio Asistente para la compatibilidad de programas   138. Servicio AssignedAccessManager   139. Servicio AVCTP   140. Servicio biométrico de Windows   141. Servicio Cifrado de unidad BitLocker   142. Servicio de administración de aplicaciones de empresa   143. Servicio de administración de radio   144. Servicio de administración de Windows   145. Servicio de administrador de conexiones con servicios Wi-Fi Direct   146. Servicio de administrador de licencias de Windows   147. Servicio de almacenamiento   148. Servicio de Antivirus de Windows Defender   149. Servicio de asistente para perfil local   150. Servicio de asociación de dispositivos   151. Servicio de caché de fuentes de Windows   152. Servicio de cierre de invitado de Hyper-V   153. Servicio de compatibilidad con Bluetooth   154. Servicio de configuración de red   155. Servicio de configuración de traslación de IP   156. Servicio de datos del sensor   157. Servicio de datos espacial   158. Servicio de detección automática de proxy web WinHTTP   159. Servicio de directivas de diagnóstico   160. Servicio de dispositivo de interfaz humana   161. Servicio de enrutador de AllJoyn   162. Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos   163. Servicio de enumeración de dispositivos de tarjeta inteligente   164. Servicio de experiencia de idioma   165. Servicio de geolocalización   166. Servicio de historial de archivos   167. Servicio de host HV   168. Servicio de implementación de AppX (AppXSVC)   169. Servicio de infraestructura de tareas en segundo plano   170. Servicio de inscripción de administración de dispositivos   171. Servicio de inspección de red de Antivirus de Windows Defender   172. Servicio de instalación de dispositivos   173. Servicio de instalación de Microsoft Store   174. Servicio de intercambio de datos de Hyper-V   175. Servicio de latido de Hyper-V   176. Servicio de licencia de cliente (ClipSVC)   177. Servicio de lista de redes   178. Servicio de mejora de visualización   179. Servicio de notificación de eventos de sistema   180. Servicio de Panel de escritura a mano y teclado táctil   181. Servicio de percepción de Windows   182. Servicio de perfil de usuario   183. Servicio de plataforma de dispositivos conectados   184. Servicio de Protección contra amenazas avanzada de Windows Defender   185. Servicio de protocolo de túnel de sockets seguros   186. Servicio de prueba comercial   187. Servicio de publicación de nombres de equipo PNRP   188. Servicio de puerta de enlace de audio de Bluetooth   189. Servicio de puerta de enlace de nivel de aplicación   190. Servicio de red de Xbox Live   191. Servicio de repositorio de estado   192. Servicio de sensores   193. Servicio de simulación de percepción de Windows   194. Servicio de sincronización de hora de Hyper-V   195. Servicio de solución de problemas recomendado   196. Servicio de soporte técnico de usuario de Bluetooth\_45406   197. Servicio de supervisión de sensores   198. Servicio de transferencia inteligente en segundo plano (BITS)   199. Servicio de uso compartido de datos   200. Servicio de uso compartido de puertos Net.Tcp   201. Servicio de uso compartido de red del Reproductor de Windows Media   202. Servicio de usuario de difusión y GameDVR\_45406   203. Servicio de usuario de notificaciones de inserción de Windows\_45406   204. Servicio de usuario de plataforma de dispositivos conectados\_45406   205. Servicio de usuario del portapapeles\_45406   206. Servicio de virtualización de Escritorio remoto de Hyper-V   207. Servicio de virtualización de la experiencia de usuario   208. Servicio de Windows Insider   209. Servicio de zona con cobertura inalámbrica móvil de Windows   210. Servicio del iniciador iSCSI de Microsoft   211. Servicio del módulo de copia de seguridad a nivel de bloque   212. Servicio del sistema de notificaciones de inserción de Windows   213. Servicio enrutador de SMS de Microsoft Windows.   214. Servicio enumerador de dispositivos portátiles   215. Servicio FrameServer de la Cámara de Windows   216. Servicio host de proveedor de cifrado de Windows   217. Servicio Informe de errores de Windows   218. Servicio Interfaz de almacenamiento en red   219. Servicio Orquestador de actualizaciones   220. Servicio PowerShell Direct de Hyper-V   221. Servicio PushToInstall de Windows   222. Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)   223. Servicio Seguridad de Windows   224. Servicio telefónico   225. Servicio Volumetric Audio Compositor   226. Servicios de cifrado   227. Servicios de Escritorio remoto   228. Servidor   229. Shared PC Account Manager   230. Sincronizar host\_45406   231. Sistema de cifrado de archivos (EFS)   232. Sistema de eventos COM+   233. SMP de Espacios de almacenamiento de Microsoft   234. Solicitante de instantáneas de volumen de Hyper-V   235. SysMain   236. Tarjeta inteligente   237. Telefonía   238. Telemetría y experiencias del usuario conectado   239. Temas   240. Ubicador de llamada a procedimiento remoto (RPC)   241. Uso de datos   242. VirtualBox Guest Additions Service   243. WalletService   244. WarpJITSvc   245. Windows Installer   246. Windows Search   247. Windows Update   248. Windows Update Medic Service   249. Xbox Accessory Management Service |
|  |
|  |

## Detección, comprobación y evaluación de vulnerabilidades

*NOTA: En las buscadas manualmente solo hemos incluido aquellas vulnerabilidades que afectan al servicio / aplicación / S.O. / Sistema con el SW utilizado. Aquellas vulnerabilidades que ya hubieran sido parcheadas o bien no se incluyen, o solo se cuentan si tenemos dos versiones de la misma aplicación / servicio / S.O. Algunas vulnerabilidades relacionadas con el HW no se han podido evaluar en profundidad (puesto que son máquinas virtuales y cada miembro del equipo emplea un HW diferente).*

|  |  |  |
| --- | --- | --- |
| Para cada servicio y/o aplicación en cada una de las máquinas • Si la máquina es un S.O. o un dispositivo móvil, hay que utilizar las herramientas vistas en cada una de las unidades (p.ej. vulscan, ZAP, Sqlmap)  Vulscan  git clone https://github.com/scipag/vulscan scipag\_vulscan  ln -s `pwd`/scipag\_vulscan /usr/share/nmap/scripts/vulscan  cd scipag\_vulscan  nmap -sV --script=vulscan/vulscan.nse <domain>  Sqlmap  https://sqlmap.org/  • Para servicios WEB se puede usar la metodología OWASP como vimos • También análisis generales como de denegación de servicio con Apache Benchmarking  **pfSense1 (#R1):**  Búsqueda manual:   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. 2. **CVE-2020-26147, CVE-2020-24588, CVE-2020-26144**, de problemas de seguridad con la agregación y fragmentación de frames del 802.11 junto a la falta de validación de la longitud del SSID. (FreeBSD, 2022) 3. **CVE-2022-0778:** un error en la función BN\_mod\_sqrt() encargada de calcular una raíz cuadrada modular causa que se forme un bucle infinito si el módulo no es primo (FreeBSD, 2022). 4. **CVE-2022-23084, CVE-2022-23085** un proceso en una jaula puede influenciar al entorno huésped si se indica que el netmap (empleado en máquinas virtuales o en mensajes de usuarios cliente-kernel) esté incluido en el devfs\_ruleset. El impacto es potencialmente moderado pero poco común. (FreeBSD, 2022). 5. **CVE-2022-23088:** un heap overflow en el Wi-Fi permite que si nuestro router actúa como cliente, al escanear, un frame de baliza maliciosa puede permitir sobreescribir el kernel y conllevar una ejecución remota de código (FreeBSD, 2022) 6. **CVE-2022-23086** ciertos handlers de disco mpr, mps y mpt (que deciden cuál unidad de almacenamiento está en uso) pueden permitir a un usuario del grupo root escalar en privilegios aún más (FreeBSD, 2022). 7. **CVE-2021-29632** un problema con la consola causa que si se usa un búffer de marcado mientras el texto de consola se mueve, se puedan sobreescribir estructuras de datos de la consola y memoria del kernel, creando comportameintos inesperados e inestabilidad del sistema (FreeBSD, 2022). 8. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS) 9. ESTO PUEDE AYUDAR https://www.cvedetails.com/vulnerability-list.php?vendor\_id=6&product\_id=0&version\_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&cweid=0&order=1&trc=405&sha=9b79e6967ee01508829f232edda61e8907c9e090 10. Además, hubo una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense). **Se corrigió antes de hacer el análisis (nueva contraseña es “Lapatata87pocha”) y por lo tanto no se ha tenido en cuenta en el apartado 5.** 11. También hubo una vulnerabilidad, y es usar un certificado autofirmado para el webConfigurator de conexión segura. Este se ha resuelto mediante el paso a autoridad de certificación propia generada y difundida por nosotros y que los navegadores de esa red la importaran para confiar en dicha autoridad de certificación, y en el nuevo certificado de servidor para conexión firmado por ésta. **Se corrigió antes de hacer el análisis y por lo tanto no se ha tenido en cuenta en el apartado 5.**   Resultados vulscan:   1. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS)   Resultados Apache Benchmarking   1. (cuantos clientes puede soportar el router)   **pfSense2 (#R2)**:  Búsqueda manual:   1. **53/tcp open domain Unbound** -> Potencial vulnerabilidad de dejar un puerto innecesario abierto, con todo lo que conlleva. 2. **FreeBSD 12.3 se considera deprecado** -> Potenciales vulnerabilidades que no vayan a ser parcheadas en un futuro. 3. **CVE-2020-26147, CVE-2020-24588, CVE-2020-26144** 4. **CVE-2022-0778:** 5. **CVE-2022-23084, CVE-2022-23085** 6. **CVE-2022-23088:** 7. **CVE-2022-23086** 8. **CVE-2021-29632** 9. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS) 10. Además, hubo una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense). **Se corrigió antes de hacer el análisis (nueva contraseña es “junio2020”) y por lo tanto no se ha tenido en cuenta en el apartado 5.** 11. También hubo una vulnerabilidad, y es que el conectar al firewall para configurarlo no se hacía en conexión segura, por lo que se podría fácilmente interceptar el mensaje y obtener la contraseña y clave no cifradas. Por lo tanto, pasamos a SSL/TLS y generamos un certificado a de otra CA propia generada y difundida por nosotros y que los navegadores de esa red la importaran para confiar en dicha autoridad de certificación, y en el nuevo certificado de servidor para conexión firmado por ésta. **Se corrigió antes de hacer el análisis y por lo tanto no se ha tenido en cuenta en el apartado 5.**   Resultados vulscan:   1. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS)   Resultados Apache Benchmarking   1. (cuantos clientes puede soportar el router)   **ClienteRemoto** **(#LANB1**):  Búsqueda manual:   1. Microsoft Windows RPC - (HAY VULNERABILIDADES CON ESTO, PROGRESAD CON EL SW) 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. Windows 7)   Resultados vulscan:   1. (lista de servicios acá y vulnerabilidades detectados por vulscan)   *No se han realizado ataques al cliente con Apache Benchmarking ya que tras sopesarlo se considera que el cliente no es un objetivo importante para los atacantes, no soporta ningún papel de servidor en un principio y está bien oculto tras una LAN o con el tráfico redirigido por la VPN en su totalidad.*  **Servidor (#LANB2):**  Búsqueda manual:   1. **5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)** -> 1º es una versión más antigua de HTTP que la empleada para la versión actual de nuestro servidor, que solo debe hacer lo mínimo pedido. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. 2. **mod\_sed: Read/write beyond bounds (**[**CVE-2022-23943**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943)**)** 3. **HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier (**[**CVE-2022-22720**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720)**)** 4. **mod\_proxy\_ajp: Possible request smuggling (**[**CVE-2022-26377**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26377)**)** 5. **La version 1903 de Windows 10 dejó de tener soportes de seguridad desde 8-12-2020** (Microsoft, 2020) 6. **Windows 10 permite extraer las contraseñas con hash de NTLM de todas las cuentas de un dispositivo debido a políticas demasiado permisivas (**[**CVE-2021-36934**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36934)**)** (Microsoft, 2021)y además **pueden instalarse drivers “Point and Print” sin permiso.** 7. **Windows 10 antes del 9-11-2021 permitía a Windows Installer subir de privilegios y poder borrar cualquier archivo - aunque no permitía al usuario verlos ni modificarlos (**[**CVE-2021-41379**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41379)**)** (Microsoft, 2021). 8. **AV1 Video Extension Remote Code Execution Vulnerability (**[**CVE-2022-30193**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30193)**)** (Microsoft, 2022). 9. **Windows SMB Denial of Service Vulnerability** ([CVE-2022-32230](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32230)) (Microsoft, 2022). 10. **Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability** ([CVE-2022-30190](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190)) (Microsoft, 2022). 11. **Windows Hyper-V Remote Code Execution Vulnerability** ([CVE-2022-30163](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30163)) (Microsoft, 2022).  En Firefox 100.0.2 (Sacados de (Mozilla Foundation Security Advisory 2022-20, 2022) que en el momento de hacer el proyecto es la versión más reciente):  |  | | --- | | [(CVE-2022-31736) Cross-Origin resource's length leaked](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/" \l "CVE-2022-31736): A malicious website could have learned the size of a cross-origin resource that supported Range requests.([CVE-2022-31737) Heap buffer overflow in WebGL](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31737): A malicious webpage could have caused an out-of-bounds write in WebGL, leading to memory corruption and a potentially exploitable crash.([CVE-2022-31738): Browser window spoof using fullscreen mode](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31738): When exiting fullscreen mode, an iframe could have confused the browser about the current state of fullscreen, resulting in potential user confusion or spoofing attacks.([CVE-2022-31739): Attacker-influenced path traversal when saving downloaded files](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31739): When downloading files on Windows only, the % character was not escaped, which could have lead to a download incorrectly being saved to attacker-influenced paths that used variables such as %HOMEPATH% or %APPDATA%.([CVE-2022-31740): Register allocation problem in WASM on arm64](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31740): On arm64, WASM code could have resulted in incorrect assembly generation leading to a register allocation problem, and a potentially exploitable crash.([CVE-2022-31741): Uninitialized variable leads to invalid memory read](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31741): A crafted CMS message could have been processed incorrectly, leading to an invalid memory read, and potentially further memory corruption.([CVE-2022-31742): Querying a WebAuthn token with a large number of allowCredential entries may have leaked cross-origin information](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31742): An attacker could have exploited a timing attack by sending a large number of allowCredential entries and detecting the difference between invalid key handles and cross-origin key handles. This could have led to cross-origin account linking in violation of WebAuthn goals.([CVE-2022-31743): HTML Parsing incorrectly ended HTML comments prematurely](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31743): Firefox's HTML parser did not correctly interpret HTML comment tags, resulting in an incongruity with other browsers. This could have been used to escape HTML comments on pages that put user-controlled data in them.([CVE-2022-31744): CSP bypass enabling stylesheet injection](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31744): An attacker could have injected CSS into stylesheets accessible via internal URIs, such as resource:, and in doing so bypass a page's Content Security Policy.([CVE-2022-31745): Incorrect Assertion caused by unoptimized array shift operations](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31745): If array shift operations are not used, the Garbage Collector may have become confused about valid objects.([CVE-2022-1919): Memory Corruption when manipulating webp images](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-1919): An attacker could have caused an uninitialized variable on the stack to be mistakenly freed, causing a potentially exploitable crash.([CVE-2022-31747](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31747)) and ([CVE-2022-31748): Memory safety bugs fixed in Firefox 101](https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31748): Versiones anteriores tenían un problema con memoria corrompible que podía ser explotable con un poco de esfuerzo. |  1. **En XAMPP 8.1.2-0** (Vulmon, 2022):  |  | | --- | | * **(CVE-2022-29376)** Xampp para Windows v8.1.4 y más antiguos permite ejecutar código malicioso ya que su directorio de instalación no está protegido adecuadamente y los atacantes podrían sobreescribir sus archivos binarios (Vulmon, 2022). |  1. (lista de servicios acá y vulnerabilidades de las aplicaciones… también incluyan vulnerabilidades conocidas de la versión del S.O. Windows 10)   Resultados vulscan:  PORT STATE SERVICE VERSION   1. 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) 2. | vulscan: VulDB - https://vuldb.com: 3. | [104986] Apache CXF 2.4.5/2.5.1 WS-SP UsernameToken Policy weak authentication 4. | **[67184] Apache HTTP Server 2.4.5/2.4.6 mod\_cache denial of service** 5. | **[9683] Apache HTTP Server 2.4.5 mod\_session\_dbd denial of service** 6. | [176770] Apache HTTP Server up to 2.4.46 on Windows denial of service 7. | [176769] Apache HTTP Server up to 2.4.46 MergeSlashes unknown vulnerability 8. | [176768] Apache HTTP Server up to 2.4.46 mod\_session heap-based overflow 9. | [176767] Apache HTTP Server up to 2.4.46 mod\_session null pointer dereference 10. | [176766] Apache HTTP Server up to 2.4.46 mod\_proxy\_http null pointer dereference 11. | [176765] Apache HTTP Server up to 2.4.46 mod\_proxy\_wstunnel improper authentication 12. | [176764] Apache HTTP Server up to 2.4.46 mod\_auth\_digest stack-based overflow 13. | [159399] Apache HTTP Server up to 2.4.43 HTTP2 Request privilege escalation 14. | [159376] Apache HTTP Server up to 2.4.43 mod\_http2 privilege escalation 15. | [159375] Apache HTTP Server 2.4.24 mod\_remoteip/mod\_rewrite IP Address weak authentication 16. | [159374] Apache HTTP Server up to 2.4.44 mod\_proxy\_uwsgi memory corruption 17. | [152665] Apache HTTP Server up to 2.4.41 mod\_proxy\_ftp Uninitialized Resource 18. | [152664] Apache HTTP Server up to 2.4.41 mod\_rewrite Redirect 19. | [142325] Apache HTTP Server up to 2.4.39 mod\_remoteip denial of service 20. | [142324] Apache HTTP Server up to 2.4.39 mod\_proxy cross site scripting 21. | [142323] Apache HTTP Server up to 2.4.39 HTTP2 Session memory corruption 22. | [142187] Apache HTTP Server up to 2.4.39 mod\_rewrite Redirect 23. | [136374] Apache HTTP Server up to 2.4.38 Slash denial of service 24. | [136373] Apache HTTP Server 2.4.34/2.4.35/2.4.36/2.4.37/2.4.38 HTTP2 privilege escalation 25. | [136372] Apache HTTP Server up to 2.4.38 HTTP2 memory corruption 26. | [133112] Apache HTTP Server up to 2.4.38 mod\_auth\_digest race condition 27. | [133111] Apache HTTP Server 2.4.37/2.4.38 mod\_ssl privilege escalation 28. | [130341] Apache HTTP Server 2.4.37 mod\_ssl privilege escalation 29. | [130330] Apache HTTP Server up to 2.4.37 mod\_session Expired weak authentication 30. | [130329] Apache HTTP Server 2.4.37 mod\_http2 Slowloris denial of service 31. | [122569] Apache HTTP Server up to 2.4.33 HTTP2 Request denial of service 32. | [121910] Apache HTTP Server 2.4.33 mod\_md denial of service 33. | [115061] Apache HTTP Server up to 2.4.29 HTTP Digest Authentication Challenge weak authentication 34. | [115060] Apache HTTP Server up to 2.4.29 mod\_cache\_socache information disclosure 35. | [115059] Apache HTTP Server up to 2.4.29 HTTP2 denial of service 36. | [115058] Apache HTTP Server up to 2.4.29 memory corruption 37. | [115057] Apache HTTP Server up to 2.4.29 mod\_session privilege escalation 38. | [115039] Apache HTTP Server up to 2.4.29 FilesMatch privilege escalation 39. | [114258] Apache HTTP Server up to 2.4.22 mod\_cluster privilege escalation 40. | [103521] Apache HTTP Server 2.4.26 HTTP2 Free memory corruption 41. | [94627] Apache HTTP Server up to 2.4.24 mod\_auth\_digest privilege escalation 42. | [94626] Apache HTTP Server up to 2.4.24 mod\_session\_crypto Padding weak encryption 43. | [94625] Apache HTTP Server up to 2.4.24 Response Split Data Processing Error 44. | [93958] Apache HTTP Server up to 2.4.23 mod\_http2 h2\_stream.c privilege escalation 45. | [89669] Apache HTTP Server up to 2.4.23 RFC 3875 Namespace Conflict privilege escalation 46. | [88747] Apache HTTP Server 2.4.17/2.4.18 mod\_http2 denial of service 47. | [88667] Apache HTTP Server up to 2.4.20 mod\_http2 privilege escalation 48. | [76733] Apache HTTP Server 2.4.7/2.4.8/2.4.9/2.4.10/2.4.12 ap\_some\_auth\_required privilege escalation 49. | [76732] Apache HTTP Server 2.4.7/2.4.8/2.4.9/2.4.10/2.4.12 Request apr\_brigade\_flatten privilege escalation 50. | [76731] Apache HTTP Server 2.4.12 ErrorDocument 400 denial of service 51. | [74367] Apache HTTP Server up to 2.4.12 mod\_lua lua\_request.c wsupgrade privilege escalation 52. | [73106] Apache Hadoop up to 2.4.0 privilege escalation 53. | [68575] Apache HTTP Server up to 2.4.10 LuaAuthzProvider mod\_lua.c privilege escalation 54. | [62417] Apache CXF 2.4.7/2.4.8/2.5.3/2.5.4/2.6.1 privilege escalation 55. | [68435] Apache HTTP Server 2.4.10 mod\_proxy\_fcgi.c handle\_headers memory corruption 56. | [67185] Apache HTTP Server up to 2.4.9 mod\_status race condition 57. | [67183] Apache HTTP Server up to 2.4.9 mod\_proxy privilege escalation 58. | [67182] Apache HTTP Server up to 2.4.9 mod\_deflate denial of service 59. | [67181] Apache HTTP Server up to 2.4.9 mod\_cgid denial of service 60. | [67180] Apache HTTP Server up to 2.4.9 WinNT MPM denial of service 61. | [13300] Apache HTTP Server 2.4.1/2.4.2 mod\_wsgi setuid privilege escalation 62. | [13299] Apache HTTP Server 2.4.1/2.4.2 mod\_wsgi information disclosure 63. | [12667] Apache HTTP Server 2.4.7 mod\_log\_config.c log\_cookie privilege escalation 64. | [9673] Apache HTTP Server up to 2.4.4 mod\_dav mod\_dav.c privilege escalation 65. | [7202] Apache HTTP Server 2.4.2 on Oracle Solaris ld\_library\_path privilege escalation 66. | [6092] Apache HTTP Server 2.4.0/2.4.1/2.4.2 mod\_proxy\_ajp.c information disclosure 67. | [6090] Apache HTTP Server 2.4.0/2.4.1/2.4.2 mod\_proxy\_http.c information disclosure 68. | 69. | MITRE CVE - https://cve.mitre.org: 70. | [CVE-2013-2249] mod\_session\_dbd.c in the mod\_session\_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors. 71. | [CVE-2012-2378] Apache CXF 2.4.5 through 2.4.7, 2.5.1 through 2.5.3, and 2.6.x before 2.6.1, does not properly enforce child policies of a WS-SecurityPolicy 1.1 SupportingToken policy on the client side, which allows remote attackers to bypass the (1) AlgorithmSuite, (2) SignedParts, (3) SignedElements, (4) EncryptedParts, and (5) EncryptedElements policies. 72. | [CVE-2012-4558] Multiple cross-site scripting (XSS) vulnerabilities in the balancer\_handler function in the manager interface in mod\_proxy\_balancer.c in the mod\_proxy\_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string. 73. | [CVE-2012-3502] The proxy functionality in (1) mod\_proxy\_ajp.c in the mod\_proxy\_ajp module and (2) mod\_proxy\_http.c in the mod\_proxy\_http module in the Apache HTTP Server 2.4.x before 2.4.3 does not properly determine the situations that require closing a back-end connection, which allows remote attackers to obtain sensitive information in opportunistic circumstances by reading a response that was intended for a different client. 74. | [CVE-2012-3499] Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod\_imagemap, (2) mod\_info, (3) mod\_ldap, (4) mod\_proxy\_ftp, and (5) mod\_status modules. 75. | [CVE-2012-3451] Apache CXF before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote attackers to execute unintended web-service operations by sending a header with a SOAP Action String that is inconsistent with the message body. 76. | [CVE-2012-2687] Multiple cross-site scripting (XSS) vulnerabilities in the make\_variant\_list function in mod\_negotiation.c in the mod\_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list. 77. | [CVE-2012-2379] Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1, when a Supporting Token specifies a child WS-SecurityPolicy 1.1 or 1.2 policy, does not properly ensure that an XML element is signed or encrypted, which has unspecified impact and attack vectors. 78. | [CVE-2012-0883] envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD\_LIBRARY\_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl. 79. | [CVE-2011-2516] Off-by-one error in the XML signature feature in Apache XML Security for C++ 1.6.0, as used in Shibboleth before 2.4.3 and possibly other products, allows remote attackers to cause a denial of service (crash) via a signature using a large RSA key, which triggers a buffer overflow. 80. | 81. | SecurityFocus - https://www.securityfocus.com/bid/: 82. | [42102] Apache 'mod\_proxy\_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability 83. | [27237] Apache HTTP Server 2.2.6, 2.0.61 and 1.3.39 'mod\_status' Cross-Site Scripting Vulnerability 84. | [15413] PHP Apache 2 Virtual() Safe\_Mode and Open\_Basedir Restriction Bypass Vulnerability 85. | [15177] PHP Apache 2 Local Denial of Service Vulnerability 86. | [6065] Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability 87. | [5816] Apache 2 mod\_dav Denial Of Service Vulnerability 88. | [5486] Apache 2.0 CGI Path Disclosure Vulnerability 89. | [5485] Apache 2.0 Path Disclosure Vulnerability 90. | [5434] Apache 2.0 Encoded Backslash Directory Traversal Vulnerability 91. | [5256] Apache httpd 2.0 CGI Error Path Disclosure Vulnerability 92. | [4057] Apache 2 for Windows OPTIONS request Path Disclosure Vulnerability 93. | [4056] Apache 2 for Windows php.exe Path Disclosure Vulnerability 94. | 95. | IBM X-Force - https://exchange.xforce.ibmcloud.com: 96. | [75211] Debian GNU/Linux apache 2 cross-site scripting 97. | 98. | Exploit-DB - https://www.exploit-db.com: 99. | [31052] Apache <= 2.2.6 'mod\_negotiation' HTML Injection and HTTP Response Splitting Vulnerability 100. | [30901] Apache HTTP Server 2.2.6 Windows Share PHP File Extension Mapping Information Disclosure Vulnerability 101. | [30835] Apache HTTP Server <= 2.2.4 413 Error HTTP Request Method Cross-Site Scripting Weakness 102. | [28424] Apache 2.x HTTP Server Arbitrary HTTP Request Headers Security Weakness 103. | [28365] Apache 2.2.2 CGI Script Source Code Information Disclosure Vulnerability 104. | [27915] Apache James 2.2 SMTP Denial of Service Vulnerability 105. | [27135] Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution 106. **| [26710] Apache CXF prior to 2.5.10, 2.6.7 and 2.7.4 - Denial of Service** 107. | [24590] Apache 2.0.x mod\_ssl Remote Denial of Service Vulnerability 108. | [23581] Apache 2.0.4x mod\_perl Module File Descriptor Leakage Vulnerability 109. | [23482] Apache 2.0.4x mod\_php Module File Descriptor Leakage Vulnerability (2) 110. | [23481] Apache 2.0.4x mod\_php Module File Descriptor Leakage Vulnerability (1) 111. | [23296] Red Hat Apache 2.0.40 Directory Index Default Configuration Error 112. | [23282] apache cocoon 2.14/2.2 - Directory Traversal vulnerability 113. | [22191] Apache Web Server 2.0.x MS-DOS Device Name Denial of Service Vulnerability 114. | [21854] Apache 2.0.39/40 Oversized STDERR Buffer Denial of Service Vulnerability 115. | [21719] Apache 2.0 Path Disclosure Vulnerability 116. | [21697] Apache 2.0 Encoded Backslash Directory Traversal Vulnerability 117. | [20272] Apache 1.2.5/1.3.1,UnityMail 2.0 MIME Header DoS Vulnerability 118. | [19828] Cobalt RaQ 2.0/3.0 Apache .htaccess Disclosure Vulnerability 119. | [18984] Apache Struts <= 2.2.1.1 - Remote Command Execution 120. | [18329] Apache Struts2 <= 2.3.1 - Multiple Vulnerabilities 121. | [17691] Apache Struts < 2.2.0 - Remote Command Execution 122. | [15319] Apache 2.2 (Windows) Local Denial of Service 123. | [14617] Apache JackRabbit 2.0.0 webapp XPath Injection 124. | [11650] Apache 2.2.14 mod\_isapi Dangling Pointer Remote SYSTEM Exploit 125. | [8458] Apache Geronimo <= 2.1.3 - Multiple Directory Traversal Vulnerabilities 126. | [5330] Apache 2.0 mod\_jk2 2.0.2 - Remote Buffer Overflow Exploit (win32) 127. | [3996] Apache 2.0.58 mod\_rewrite Remote Overflow Exploit (win2k3) 128. | [2237] Apache < 1.3.37, 2.0.59, 2.2.3 (mod\_rewrite) Remote Overflow PoC 129. | [1056] Apache <= 2.0.49 Arbitrary Long HTTP Headers Denial of Service 130. | [855] Apache <= 2.0.52 HTTP GET request Denial of Service Exploit 131. | [132] Apache 1.3.x - 2.0.48 - mod\_userdir Remote Users Disclosure Exploit 132. | [38] Apache <= 2.0.45 APR Remote Exploit -Apache-Knacker.pl 133. | [34] Webfroot Shoutbox < 2.32 (Apache) Remote Exploit 134. | [11] Apache <= 2.0.44 Linux Remote Denial of Service Exploit 135. | [9] Apache HTTP Server 2.x Memory Leak Exploit 136. | 137. | OpenVAS (Nessus) - http://www.openvas.org: 138. | [855524] Solaris Update for Apache 2 120544-14 139. | [855077] Solaris Update for Apache 2 120543-14 140. | [100858] Apache 'mod\_proxy\_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability 141. | [72626] Debian Security Advisory DSA 2579-1 (apache2) 142. | [71551] Gentoo Security Advisory GLSA 201206-25 (apache) 143. | [71550] Gentoo Security Advisory GLSA 201206-24 (apache tomcat) 144. | [71485] Debian Security Advisory DSA 2506-1 (libapache-mod-security) 145. | [71256] Debian Security Advisory DSA 2452-1 (apache2) 146. | [71238] Debian Security Advisory DSA 2436-1 (libapache2-mod-fcgid) 147. | [70724] Debian Security Advisory DSA 2405-1 (apache2) 148. | [70235] Debian Security Advisory DSA 2298-2 (apache2) 149. | [70233] Debian Security Advisory DSA 2298-1 (apache2) 150. | [69988] Debian Security Advisory DSA 2279-1 (libapache2-mod-authnz-external) 151. | [69338] Debian Security Advisory DSA 2202-1 (apache2) 152. | [65131] SLES9: Security update for Apache 2 oes/CORE 153. | [64426] Gentoo Security Advisory GLSA 200907-04 (apache) 154. | [61381] Gentoo Security Advisory GLSA 200807-06 (apache) 155. | [60582] Gentoo Security Advisory GLSA 200803-19 (apache) 156. | [58745] Gentoo Security Advisory GLSA 200711-06 (apache) 157. | [57851] Gentoo Security Advisory GLSA 200608-01 (apache) 158. | [56246] Gentoo Security Advisory GLSA 200602-03 (Apache) 159. | [55392] Gentoo Security Advisory GLSA 200509-12 (Apache) 160. | [55129] Gentoo Security Advisory GLSA 200508-15 (apache) 161. | [54739] Gentoo Security Advisory GLSA 200411-18 (apache) 162. | [54724] Gentoo Security Advisory GLSA 200411-03 (apache) 163. | [54712] Gentoo Security Advisory GLSA 200410-21 (apache) 164. | [54689] Gentoo Security Advisory GLSA 200409-33 (net=www/apache) 165. | [54677] Gentoo Security Advisory GLSA 200409-21 (apache) 166. | [54610] Gentoo Security Advisory GLSA 200407-03 (Apache) 167. | [54601] Gentoo Security Advisory GLSA 200406-16 (Apache) 168. | [54590] Gentoo Security Advisory GLSA 200406-05 (Apache) 169. | [54582] Gentoo Security Advisory GLSA 200405-22 (Apache) 170. | [54529] Gentoo Security Advisory GLSA 200403-04 (Apache) 171. | [54499] Gentoo Security Advisory GLSA 200310-04 (Apache) 172. | [54498] Gentoo Security Advisory GLSA 200310-03 (Apache) 173. | [11092] Apache 2.0.39 Win32 directory traversal 174. | [66081] SLES11: Security update for Apache 2 175. | [66074] SLES10: Security update for Apache 2 176. | [66070] SLES9: Security update for Apache 2 177. | [65893] SLES10: Security update for Apache 2 178. | [65888] SLES10: Security update for Apache 2 179. | [65510] SLES9: Security update for Apache 2 180. | [65249] SLES9: Security update for Apache 2 181. | [65230] SLES9: Security update for Apache 2 182. | [65228] SLES9: Security update for Apache 2 183. | [65207] SLES9: Security update for Apache 2 184. | [65136] SLES9: Security update for Apache 2 185. | [65017] SLES9: Security update for Apache 2 186. | 187. | SecurityTracker - https://www.securitytracker.com: 188. | [1008196] Apache 2.x on Windows May Return Unexpected Files For URLs Ending With Certain Characters 189. | [1007143] Apache 2.0 Web Server May Use a Weaker Encryption Implementation Than Specified in Some Cases 190. | [1006444] Apache 2.0 Web Server Line Feed Buffer Allocation Flaw Lets Remote Users Deny Service 191. | [1005963] Apache Web Server 2.x Windows Device Access Flaw Lets Remote Users Crash the Server or Possibly Execute Arbitrary Code 192. | [1004770] Apache 2.x Web Server ap\_log\_rerror() Function May Disclose Full Installation Path to Remote Users 193. | 194. | OSVDB - http://www.osvdb.org: 195. | [20897] PHP w/ Apache 2 SAPI virtual() Function Unspecified INI Setting Disclosure 196. |\_ 197. **|\_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2** 198. **443/tcp open ssl/http Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.2)** 199. | vulscan: VulDB - https://vuldb.com: 200. | [104986] Apache CXF 2.4.5/2.5.1 WS-SP UsernameToken Policy weak authentication 201. | [67184] Apache HTTP Server 2.4.5/2.4.6 mod\_cache denial of service 202. | [9683] Apache HTTP Server 2.4.5 mod\_session\_dbd denial of service 203. | [176770] Apache HTTP Server up to 2.4.46 on Windows denial of service 204. | [176769] Apache HTTP Server up to 2.4.46 MergeSlashes unknown vulnerability 205. | [176768] Apache HTTP Server up to 2.4.46 mod\_session heap-based overflow 206. | [176767] Apache HTTP Server up to 2.4.46 mod\_session null pointer dereference 207. | [176766] Apache HTTP Server up to 2.4.46 mod\_proxy\_http null pointer dereference 208. | [176765] Apache HTTP Server up to 2.4.46 mod\_proxy\_wstunnel improper authentication 209. | [176764] Apache HTTP Server up to 2.4.46 mod\_auth\_digest stack-based overflow 210. | [159399] Apache HTTP Server up to 2.4.43 HTTP2 Request privilege escalation 211. | [159376] Apache HTTP Server up to 2.4.43 mod\_http2 privilege escalation 212. | [159375] Apache HTTP Server 2.4.24 mod\_remoteip/mod\_rewrite IP Address weak authentication 213. | [159374] Apache HTTP Server up to 2.4.44 mod\_proxy\_uwsgi memory corruption 214. | [152665] Apache HTTP Server up to 2.4.41 mod\_proxy\_ftp Uninitialized Resource 215. | [152664] Apache HTTP Server up to 2.4.41 mod\_rewrite Redirect 216. | [142325] Apache HTTP Server up to 2.4.39 mod\_remoteip denial of service 217. | [142324] Apache HTTP Server up to 2.4.39 mod\_proxy cross site scripting 218. | [142323] Apache HTTP Server up to 2.4.39 HTTP2 Session memory corruption 219. | [142187] Apache HTTP Server up to 2.4.39 mod\_rewrite Redirect 220. | [136374] Apache HTTP Server up to 2.4.38 Slash denial of service 221. | [136373] Apache HTTP Server 2.4.34/2.4.35/2.4.36/2.4.37/2.4.38 HTTP2 privilege escalation 222. | [136372] Apache HTTP Server up to 2.4.38 HTTP2 memory corruption 223. | [133112] Apache HTTP Server up to 2.4.38 mod\_auth\_digest race condition 224. | [133111] Apache HTTP Server 2.4.37/2.4.38 mod\_ssl privilege escalation 225. | [130341] Apache HTTP Server 2.4.37 mod\_ssl privilege escalation 226. | [130330] Apache HTTP Server up to 2.4.37 mod\_session Expired weak authentication 227. | [130329] Apache HTTP Server 2.4.37 mod\_http2 Slowloris denial of service 228. | [122569] Apache HTTP Server up to 2.4.33 HTTP2 Request denial of service 229. | [121910] Apache HTTP Server 2.4.33 mod\_md denial of service 230. | [115061] Apache HTTP Server up to 2.4.29 HTTP Digest Authentication Challenge weak authentication 231. | [115060] Apache HTTP Server up to 2.4.29 mod\_cache\_socache information disclosure 232. | [115059] Apache HTTP Server up to 2.4.29 HTTP2 denial of service 233. | [115058] Apache HTTP Server up to 2.4.29 memory corruption 234. | [115057] Apache HTTP Server up to 2.4.29 mod\_session privilege escalation 235. | [115039] Apache HTTP Server up to 2.4.29 FilesMatch privilege escalation 236. | [114258] Apache HTTP Server up to 2.4.22 mod\_cluster privilege escalation 237. | [103521] Apache HTTP Server 2.4.26 HTTP2 Free memory corruption 238. | [94627] Apache HTTP Server up to 2.4.24 mod\_auth\_digest privilege escalation 239. | [94626] Apache HTTP Server up to 2.4.24 mod\_session\_crypto Padding weak encryption 240. | [94625] Apache HTTP Server up to 2.4.24 Response Split Data Processing Error 241. | [93958] Apache HTTP Server up to 2.4.23 mod\_http2 h2\_stream.c privilege escalation 242. | [89669] Apache HTTP Server up to 2.4.23 RFC 3875 Namespace Conflict privilege escalation 243. | [88747] Apache HTTP Server 2.4.17/2.4.18 mod\_http2 denial of service 244. | [88667] Apache HTTP Server up to 2.4.20 mod\_http2 privilege escalation 245. | [76733] Apache HTTP Server 2.4.7/2.4.8/2.4.9/2.4.10/2.4.12 ap\_some\_auth\_required privilege escalation 246. | [76732] Apache HTTP Server 2.4.7/2.4.8/2.4.9/2.4.10/2.4.12 Request apr\_brigade\_flatten privilege escalation 247. | [76731] Apache HTTP Server 2.4.12 ErrorDocument 400 denial of service 248. | [74367] Apache HTTP Server up to 2.4.12 mod\_lua lua\_request.c wsupgrade privilege escalation 249. | [73106] Apache Hadoop up to 2.4.0 privilege escalation 250. | [68575] Apache HTTP Server up to 2.4.10 LuaAuthzProvider mod\_lua.c privilege escalation 251. | [62417] Apache CXF 2.4.7/2.4.8/2.5.3/2.5.4/2.6.1 privilege escalation 252. | [68435] Apache HTTP Server 2.4.10 mod\_proxy\_fcgi.c handle\_headers memory corruption 253. | [67185] Apache HTTP Server up to 2.4.9 mod\_status race condition 254. | [67183] Apache HTTP Server up to 2.4.9 mod\_proxy privilege escalation 255. | [67182] Apache HTTP Server up to 2.4.9 mod\_deflate denial of service 256. | [67181] Apache HTTP Server up to 2.4.9 mod\_cgid denial of service 257. | [67180] Apache HTTP Server up to 2.4.9 WinNT MPM denial of service 258. | [13300] Apache HTTP Server 2.4.1/2.4.2 mod\_wsgi setuid privilege escalation 259. | [13299] Apache HTTP Server 2.4.1/2.4.2 mod\_wsgi information disclosure 260. | [12667] Apache HTTP Server 2.4.7 mod\_log\_config.c log\_cookie privilege escalation 261. | [9673] Apache HTTP Server up to 2.4.4 mod\_dav mod\_dav.c privilege escalation 262. | [7202] Apache HTTP Server 2.4.2 on Oracle Solaris ld\_library\_path privilege escalation 263. | [6092] Apache HTTP Server 2.4.0/2.4.1/2.4.2 mod\_proxy\_ajp.c information disclosure 264. | [6090] Apache HTTP Server 2.4.0/2.4.1/2.4.2 mod\_proxy\_http.c information disclosure 265. | 266. | MITRE CVE - https://cve.mitre.org: 267. | [CVE-2013-2249] mod\_session\_dbd.c in the mod\_session\_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors. 268. | [CVE-2012-2378] Apache CXF 2.4.5 through 2.4.7, 2.5.1 through 2.5.3, and 2.6.x before 2.6.1, does not properly enforce child policies of a WS-SecurityPolicy 1.1 SupportingToken policy on the client side, which allows remote attackers to bypass the (1) AlgorithmSuite, (2) SignedParts, (3) SignedElements, (4) EncryptedParts, and (5) EncryptedElements policies. 269. | [CVE-2012-4558] Multiple cross-site scripting (XSS) vulnerabilities in the balancer\_handler function in the manager interface in mod\_proxy\_balancer.c in the mod\_proxy\_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string. 270. | [CVE-2012-3502] The proxy functionality in (1) mod\_proxy\_ajp.c in the mod\_proxy\_ajp module and (2) mod\_proxy\_http.c in the mod\_proxy\_http module in the Apache HTTP Server 2.4.x before 2.4.3 does not properly determine the situations that require closing a back-end connection, which allows remote attackers to obtain sensitive information in opportunistic circumstances by reading a response that was intended for a different client. 271. | [CVE-2012-3499] Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod\_imagemap, (2) mod\_info, (3) mod\_ldap, (4) mod\_proxy\_ftp, and (5) mod\_status modules. 272. | [CVE-2012-3451] Apache CXF before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote attackers to execute unintended web-service operations by sending a header with a SOAP Action String that is inconsistent with the message body. 273. | [CVE-2012-2687] Multiple cross-site scripting (XSS) vulnerabilities in the make\_variant\_list function in mod\_negotiation.c in the mod\_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list. 274. | [CVE-2012-2379] Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1, when a Supporting Token specifies a child WS-SecurityPolicy 1.1 or 1.2 policy, does not properly ensure that an XML element is signed or encrypted, which has unspecified impact and attack vectors. 275. | [CVE-2012-0883] envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD\_LIBRARY\_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl. 276. | [CVE-2011-2516] Off-by-one error in the XML signature feature in Apache XML Security for C++ 1.6.0, as used in Shibboleth before 2.4.3 and possibly other products, allows remote attackers to cause a denial of service (crash) via a signature using a large RSA key, which triggers a buffer overflow. 277. | 278. | SecurityFocus - https://www.securityfocus.com/bid/: 279. | [42102] Apache 'mod\_proxy\_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability 280. | [27237] Apache HTTP Server 2.2.6, 2.0.61 and 1.3.39 'mod\_status' Cross-Site Scripting Vulnerability 281. | [15413] PHP Apache 2 Virtual() Safe\_Mode and Open\_Basedir Restriction Bypass Vulnerability 282. **| [15177] PHP Apache 2 Local Denial of Service Vulnerability** 283. | [6065] Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability 284. | [5816] Apache 2 mod\_dav Denial Of Service Vulnerability 285. | [5486] Apache 2.0 CGI Path Disclosure Vulnerability 286. | [5485] Apache 2.0 Path Disclosure Vulnerability 287. | [5434] Apache 2.0 Encoded Backslash Directory Traversal Vulnerability 288. | [5256] Apache httpd 2.0 CGI Error Path Disclosure Vulnerability 289. | [4057] Apache 2 for Windows OPTIONS request Path Disclosure Vulnerability 290. | [4056] Apache 2 for Windows php.exe Path Disclosure Vulnerability 291. | 292. | IBM X-Force - https://exchange.xforce.ibmcloud.com: 293. | [75211] Debian GNU/Linux apache 2 cross-site scripting 294. | 295. | Exploit-DB - https://www.exploit-db.com: 296. | [31052] Apache <= 2.2.6 'mod\_negotiation' HTML Injection and HTTP Response Splitting Vulnerability 297. | [30901] Apache HTTP Server 2.2.6 Windows Share PHP File Extension Mapping Information Disclosure Vulnerability 298. | [30835] Apache HTTP Server <= 2.2.4 413 Error HTTP Request Method Cross-Site Scripting Weakness 299. | [28424] Apache 2.x HTTP Server Arbitrary HTTP Request Headers Security Weakness 300. | [28365] Apache 2.2.2 CGI Script Source Code Information Disclosure Vulnerability 301. | [27915] Apache James 2.2 SMTP Denial of Service Vulnerability 302. | [27135] Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution 303. | [26710] Apache CXF prior to 2.5.10, 2.6.7 and 2.7.4 - Denial of Service 304. | [24590] Apache 2.0.x mod\_ssl Remote Denial of Service Vulnerability 305. | [23581] Apache 2.0.4x mod\_perl Module File Descriptor Leakage Vulnerability 306. | [23482] Apache 2.0.4x mod\_php Module File Descriptor Leakage Vulnerability (2) 307. | [23481] Apache 2.0.4x mod\_php Module File Descriptor Leakage Vulnerability (1) 308. | [23296] Red Hat Apache 2.0.40 Directory Index Default Configuration Error 309. | [23282] apache cocoon 2.14/2.2 - Directory Traversal vulnerability 310. | [22191] Apache Web Server 2.0.x MS-DOS Device Name Denial of Service Vulnerability 311. | [21854] Apache 2.0.39/40 Oversized STDERR Buffer Denial of Service Vulnerability 312. | [21719] Apache 2.0 Path Disclosure Vulnerability 313. | [21697] Apache 2.0 Encoded Backslash Directory Traversal Vulnerability 314. | [20272] Apache 1.2.5/1.3.1,UnityMail 2.0 MIME Header DoS Vulnerability 315. | [19828] Cobalt RaQ 2.0/3.0 Apache .htaccess Disclosure Vulnerability 316. | [18984] Apache Struts <= 2.2.1.1 - Remote Command Execution 317. | [18329] Apache Struts2 <= 2.3.1 - Multiple Vulnerabilities 318. | [17691] Apache Struts < 2.2.0 - Remote Command Execution 319. | [15319] Apache 2.2 (Windows) Local Denial of Service 320. | [14617] Apache JackRabbit 2.0.0 webapp XPath Injection 321. | [11650] Apache 2.2.14 mod\_isapi Dangling Pointer Remote SYSTEM Exploit 322. | [8458] Apache Geronimo <= 2.1.3 - Multiple Directory Traversal Vulnerabilities 323. | [5330] Apache 2.0 mod\_jk2 2.0.2 - Remote Buffer Overflow Exploit (win32) 324. | [3996] Apache 2.0.58 mod\_rewrite Remote Overflow Exploit (win2k3) 325. | [2237] Apache < 1.3.37, 2.0.59, 2.2.3 (mod\_rewrite) Remote Overflow PoC 326. | [1056] Apache <= 2.0.49 Arbitrary Long HTTP Headers Denial of Service 327. | [855] Apache <= 2.0.52 HTTP GET request Denial of Service Exploit 328. | [132] Apache 1.3.x - 2.0.48 - mod\_userdir Remote Users Disclosure Exploit 329. | [38] Apache <= 2.0.45 APR Remote Exploit -Apache-Knacker.pl 330. | [34] Webfroot Shoutbox < 2.32 (Apache) Remote Exploit 331. | [11] Apache <= 2.0.44 Linux Remote Denial of Service Exploit 332. | [9] Apache HTTP Server 2.x Memory Leak Exploit 333. | 334. | OpenVAS (Nessus) - http://www.openvas.org: 335. | [855524] Solaris Update for Apache 2 120544-14 336. | [855077] Solaris Update for Apache 2 120543-14 337. | [100858] Apache 'mod\_proxy\_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability 338. | [72626] Debian Security Advisory DSA 2579-1 (apache2) 339. | [71551] Gentoo Security Advisory GLSA 201206-25 (apache) 340. | [71550] Gentoo Security Advisory GLSA 201206-24 (apache tomcat) 341. | [71485] Debian Security Advisory DSA 2506-1 (libapache-mod-security) 342. | [71256] Debian Security Advisory DSA 2452-1 (apache2) 343. | [71238] Debian Security Advisory DSA 2436-1 (libapache2-mod-fcgid) 344. | [70724] Debian Security Advisory DSA 2405-1 (apache2) 345. | [70235] Debian Security Advisory DSA 2298-2 (apache2) 346. | [70233] Debian Security Advisory DSA 2298-1 (apache2) 347. | [69988] Debian Security Advisory DSA 2279-1 (libapache2-mod-authnz-external) 348. | [69338] Debian Security Advisory DSA 2202-1 (apache2) 349. | [65131] SLES9: Security update for Apache 2 oes/CORE 350. | [64426] Gentoo Security Advisory GLSA 200907-04 (apache) 351. | [61381] Gentoo Security Advisory GLSA 200807-06 (apache) 352. | [60582] Gentoo Security Advisory GLSA 200803-19 (apache) 353. | [58745] Gentoo Security Advisory GLSA 200711-06 (apache) 354. | [57851] Gentoo Security Advisory GLSA 200608-01 (apache) 355. | [56246] Gentoo Security Advisory GLSA 200602-03 (Apache) 356. | [55392] Gentoo Security Advisory GLSA 200509-12 (Apache) 357. | [55129] Gentoo Security Advisory GLSA 200508-15 (apache) 358. | [54739] Gentoo Security Advisory GLSA 200411-18 (apache) 359. | [54724] Gentoo Security Advisory GLSA 200411-03 (apache) 360. | [54712] Gentoo Security Advisory GLSA 200410-21 (apache) 361. | [54689] Gentoo Security Advisory GLSA 200409-33 (net=www/apache) 362. | [54677] Gentoo Security Advisory GLSA 200409-21 (apache) 363. | [54610] Gentoo Security Advisory GLSA 200407-03 (Apache) 364. | [54601] Gentoo Security Advisory GLSA 200406-16 (Apache) 365. | [54590] Gentoo Security Advisory GLSA 200406-05 (Apache) 366. | [54582] Gentoo Security Advisory GLSA 200405-22 (Apache) 367. | [54529] Gentoo Security Advisory GLSA 200403-04 (Apache) 368. | [54499] Gentoo Security Advisory GLSA 200310-04 (Apache) 369. | [54498] Gentoo Security Advisory GLSA 200310-03 (Apache) 370. | [11092] Apache 2.0.39 Win32 directory traversal 371. | [66081] SLES11: Security update for Apache 2 372. | [66074] SLES10: Security update for Apache 2 373. | [66070] SLES9: Security update for Apache 2 374. | [65893] SLES10: Security update for Apache 2 375. | [65888] SLES10: Security update for Apache 2 376. | [65510] SLES9: Security update for Apache 2 377. | [65249] SLES9: Security update for Apache 2 378. | [65230] SLES9: Security update for Apache 2 379. | [65228] SLES9: Security update for Apache 2 380. | [65207] SLES9: Security update for Apache 2 381. | [65136] SLES9: Security update for Apache 2 382. | [65017] SLES9: Security update for Apache 2 383. | 384. | SecurityTracker - https://www.securitytracker.com: 385. | [1008196] Apache 2.x on Windows May Return Unexpected Files For URLs Ending With Certain Characters 386. | [1007143] Apache 2.0 Web Server May Use a Weaker Encryption Implementation Than Specified in Some Cases 387. | [1006444] Apache 2.0 Web Server Line Feed Buffer Allocation Flaw Lets Remote Users Deny Service 388. | [1005963] Apache Web Server 2.x Windows Device Access Flaw Lets Remote Users Crash the Server or Possibly Execute Arbitrary Code 389. | [1004770] Apache 2.x Web Server ap\_log\_rerror() Function May Disclose Full Installation Path to Remote Users 390. | 391. | OSVDB - http://www.osvdb.org: 392. | [20897] PHP w/ Apache 2 SAPI virtual() Function Unspecified INI Setting Disclosure 393. |\_ 394. **|\_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2** 395. 3306/tcp open mysql? 396. | fingerprint-strings: 397. | NULL: 398. |\_ Host '192.168.56.3' is not allowed to connect to this MariaDB server 399. 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service : 400. SF-Port3306-TCP:V=7.92%I=7%D=6/15%Time=62A9D03C%P=x86\_64-pc-linux-gnu%r(NU 401. SF:LL,4B,"G\0\0\x01\xffj\x04Host\x20'192\.168\.56\.3'\x20is\x20not\x20allo 402. SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server"); 403. Service Info: Host: localhost   Resultados ZAP   1. (lista de vulnerabilidades de la página web)   Resultados Sqlmap   1. (lista de vulnerabilidades)   Resultados Apache Benchmarking   1. (cuantos clientes puede soportar el servidor) |

## Medidas específicas de corrección

|  |  |
| --- | --- |
| • De las vulnerabilidades descubiertas en el apartado anterior, cuales se corrigen y por qué. • Y cuales no y por qué  **• En la entrega que se haga YA deben estar corregidas**  **pfSense1 (#R1):**   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. 2. **CVE-2020-26147, CVE-2020-24588, CVE-2020-26144**, los tres se ven mitigados por el uso de encriptación de aplicación HTTPS y las encriptaciones a nivel de transporte como puede ser una VPN, y además nuestra versión ya está parcheada, por lo que no es necesario resolverlo 3. **CVE-2022-0778:** este bucle infinito generaría una denegación de servicio importante frente a alguien enviando un certificado erróneo a propósito, algo bastante fácil de hacer y muy común. Afortunadamente, nuestra versión descargada es de finales de Mayo y ya tiene el pache del 15 de Marzo que lo resuelve, por lo que no requiere actualización. 4. **CVE-2022-23084, CVE-2022-23085** no solo nuestra instalación es por defecto (que carece de esa configuración que permite al proceso vulnerar el nivel de privilegios), sino que el parche se sacó a comienzos de Abril, y nuestro Firewall es posterior a eso. 5. **CVE-2022-23088:** este firewall rara vez actuaría como cliente en una comunicación wireless, es mucho más probable que actúe como servidor, Además, se ve mitigado por el hecho de que en la red real nuestro router no estaría empleando Wi-fi sino se comunicaría por red cableada, y arreglado porque el parche ya se encuentra instalado (se publicó durante la primera semana de Abril de 2022). 6. **CVE-2022-23086** nuestro pfSense está actualizado a una versión donde se arregló esa vulnerabilidad, por lo que ya no se requiere parchearla. 7. **CVE-2021-29632** nuestro pfSense de la empresa ya está actualizado a una versión donde se arregló esa inestabilidad del sistema, por lo que ya no se requiere parchearla. 8. (lista de vulnerabilidades de los servicios, indicando si se corrige o no y por qué)   **pfSense2 (#R2)**:   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. 2. ***53/tcp open domain Unbound*** -> Nuestra empresa no necesita que se empleen servicios DNS de momento, pero este es el firewall de un cliente en edificio remoto que a lo mejor sí necesite el uso de DNS para la vida cotidiana. Además, en la red real es muy probable que acabásemos utilizando DNS de todas formas. 3. **CVE-2020-26147, CVE-2020-24588, CVE-2020-26144**, los tres se ven mitigados por el uso de encriptación HTTPS, y además nuestra versión ya está parcheada, por lo que no es prioritario resolverlo. 4. **CVE-2022-0778:** este bucle infinito genera una denegación de servicio importante frente a alguien enviando un certificado erróneo a propósito, algo bastante fácil de hacer y muy común. Esta versión de FreeBSD fue descargada meses antes de que se parcheara. -> Se requiere actualización 5. **CVE-2022-23084, CVE-2022-23085** nuestra instalación es por defecto, por lo que carece de esa configuración que permite al proceso de la jaula influenciar el entorno del huésped. 6. **CVE-2022-23088:** esto en sí no afectaría demasiado al firewall ya que normalmente no actuaría como cliente salvo en su parte WAN (que es posible que fuera alámbrica), pero sí es importante ya que en la red real al menos uno de los lados (la LAN) debe estar empleando Wireless 802.11 de acuerdo al enunciado del proyecto, lo que podría suponer una gran probabilidad de alguien infectando el firewall y provocando que reenviara paquetes a otro lugar, incluso de una VPN (aunque llegara encriptado al atacante). Lo que es más importante, esta versión del firewall no posee el parche que lo resuelve instalado, por lo que es imperativo actualizar. 7. **CVE-2022-23086** este pfSense no posee el parche por lo que frente a algún administrador corrupto introduciendo discos adicionales (o incluso algo como un Rubber Ducky pero para hacer creeer que es una unidad de disco), se recomienda actualizar a la versión 12.2 o 12.3 más reciente (o remover todos los periféricos que no sean usados para conexión alámbrica o inalámbrica y puedan usarse para introducir unidades de almacenamiento), aunque este evento sea poco probable. 8. **CVE-2021-29632** nuestro pfSense remoto ya está actualizado a una versión donde se arregló esa inestabilidad del sistema, por lo que ya no se requiere parchearla. De hecho, se parcheó mucho antes que la versión 13.0 STABLE. 9. (lista de vulnerabilidades de los servicios, indicando si se corrige o no y por qué)   **ClienteRemoto** **(#LANB1**):   1. ***Microsoft Windows RPC:*** las interfaces MSRPC pueden usarse por un atacante para recolectar información importante y comprometer servidores (p.ej. robar la contraseña de la VPN y colarse). Se deben cerrar los puertos **135,**  **49152,** **49153,** **49154,** **49155,** **49156,** **49157**. Hay que corregirlo 2. ***5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)*** -> 1º el cliente que sepamos no necesita esto. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. Hay que corregirlo 3. **139**/tcp open netbios-ssn Microsoft Windows netbios-ssn -> Servicio empleado por RPC, si es posible debería cerrarse el puerto. Hay que corregirlo 4. **445**/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) -> Nuestro cliente remoto se supone que no debe tener un “grupo de trabajo” fuera de acceder a nuestra VPN. Cerrar puerto si es posible. Hay que corregirlo 5. Hay muchas aplicaciones que Microsoft Windows 7 tiene instaladas por defecto y no permite desinstalar fácilmente, así que cualquier vulnerabilidad relacionada con dichas aplicaciones no puede corregirse mediante la eliminación de la aplicación. Además este es el ordenador de un cliente, no deberíamos realmente alterarlos demasiado ya que pueden ser usado para otros propósitos, a menos que la vulnerabilidad sea importante. 6. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **Servidor (#LANB2):**   1. **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) -> 1º es una versión más antigua de HTTP que la empleada para la versión actual de nuestro servidor, que solo debe hacer lo mínimo pedido. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. 3º No está en uso. Todas estas razones son más que suficientes para corregirlas 2. **mod\_sed: Read/write beyond bounds (**[**CVE-2022-23943**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943)**)** es una vulnerabilidad importante quepermite reescribir memoria heap con código del atacante, debe ser solucionado -> *La solución más fácil es actualizar Apache a su última versión.* Hay que corregirlo  HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier ([CVE-2022-22720](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720)) una vulnerabilidad importante por la que el Apache falla en cerrar conexiones entrantes frente a fallos, descarta el cuerpo y permite robar datos por http request. -> *La solución más fácil es actualizar Apache a su última versión.* Hay que corregirlomod\_proxy\_ajp: Possible request smuggling ([CVE-2022-26377](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26377)) una vulnerabilidad de nivel medio en el mod\_proxy\_ajp permite a un atacante robar requests del servidor AJP . Aunque nosotros no estamos empleando ningún proxy, así que en nuestro caso no tiene tanta importancia. Aún así por si acaso se recomienda actualizar el Apache a la última versión.  1. **Windows 10 permite extraer las contraseñas con hash de NTLM de todas las cuentas de un dispositivo debido a políticas demasiado permisivas (**[**CVE-2021-36934**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36934)**)** esto es grave porque permite a cualquier usuario que ejecuta código local o remotamente acceder a bases de datos y registros sin necesidad de permisos. Esta vulnerabilidad está presente a partir de la versión 1809 de Windows 10, pero afortunadamente se remedió/parcheó en Agosto del 2021, así que la solución sería actualizar a la última versión de Windows, y si no, vernos forzados a mitigarlo según las indicaciones de Microsoft y limitar el acceso a ese archivo (Microsoft, 2021). Hay que corregirlo  |  | | --- | | **Restrict access to the contents of %windir%\system32\config**  Command Prompt (Run as administrator): icacls %windir%\system32\config\\*.\* /inheritance:e  Windows PowerShell (Run as administrator): icacls $env:windir\system32\config\\*.\* /inheritance:e  **Delete Volume Shadow Copy Service (VSS) shadow copies**   * Delete any System Restore points and Shadow volumes that existed prior to restricting access to %windir%\system32\config. * Create a new System Restore point (if desired). |   *Un efecto secundario de la actualización es que también resuelve otra vulnerabilidad, y ahora se necesitará ser administrador para instalar controladores de “Point and Print”.*   1. **Windows 10 antes del 9-11-2021 permitía a Windows Installer subir de privilegios y poder borrar cualquier archivo - aunque no permitía al usuario verlos ni modificarlos (**[**CVE-2021-41379**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41379)**)** cualquiera que pudiera acceder a nuestro servidor directamente podría ejecutar esto y borrar elementos clave de nuestro servicio o del sistema, aunque no se permita acceso normalmente a nuestro servidor, mejor solucionarlo. Afortunadamente esto se puede resolver con una actualización. Hay que corregirlo 2. **AV1 Video Extension Remote Code Execution Vulnerability (**[**CVE-2022-30193**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30193)**)** esta vulnerabilidad provoca que se ejecute código arbitrario, pero solo afecta si se descarga código remoto de una página web y si se posee la extensión de vídeo AV1 no parcheada integrada como aplicación de Microsoft Store. Afortunadamente nuestro Windows 10 no posee dicha extensión, y de hecho habíamos borrado otras similares antes de comenzar a evaluar esta parte, y como al actualizar si se fuera a instalar, ya sería la versión parcheada, esta vulnerabilidad tiene baja o nula prioridad para nosotros. 3. **Windows SMB Denial of Service Vulnerability** ([CVE-2022-32230](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32230)) este ataque de denegación de servicio se basa en desestabilizar el Windows 10 para que crashee; se detectó en Junio de 2022 recientemente, aunque el equipo de Microsoft asegura que ya tienen el parche. Como esto supone un arreglo en la estabilidad del sistema, sería recomendable actualizar nuestro Windows 10. Hay que corregirlo 4. **Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability** ([CVE-2022-30190](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190)) cuando la herramienta de diagnóstico de Windows es llamada mediante una URL en una aplicación como Microsoft Word, se puede ejecutar código arbitrario y de ahí instalar, ver, modificar o borrar datos y aplicaciones con los permisos con los que se ejecutó la aplicación que tenía la URL. Aunque esto debería ser poco común ya que nuestro servidor no se supone que deba estarse yendo a URLs externas ni tampoco tiene Microsoft Word, sí podría explotarse desde la red local quizá mediante otros editores de texto pre-instalados. Una buena opción sería actualizar ya que esto ya se encuentra parchado en versiones de Windows desde Junio de 2022, aunque viendo todas las vulnerabilidades que están apareciendo, si tuviéramos más tiempo a lo mejor rentaría pasar a un Sistema Operativo con menos funcionalidades y fisuras. Hay que corregirlo 5. **Windows Hyper-V Remote Code Execution Vulnerability** ([CVE-2022-30163](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30163)) Si el atacante gana una condición de carrera en una máquina huésped, no importa que sea una máquina virtual sin privilegios, una aplicación específicamente diseñada puede hacer que la máquina huésped ejecute código desde la máquina virtual, saltándose el propósito por el cuál existen máquinas virtuales para hacer pruebas de seguridad. Afortunadamente para nosotros, aparentemente el esfuerzo necesario es alto, aún no se ha probado en la práctica (lo que no quiere decir que no haya algún agente con este código) y ya existe un posible parche, por lo que una actualización a la nueva versión parcheada es tremendamente recomendable. Pero aún así que este exploit fuera remotamente posible pone muchas banderas rojas y si se probase que se puede hacer recomendaríamos encarecidamente deshabilitar Hiper-V y recurrir a otros servicios de virtualización. Hay que corregirlo 6. Aunque el servidor rara vez use Firefox excepto para conectarse a la configuración del router si requiere, Firefox, como cualquier aplicación, es recomendable actualizarlo para asegurarse de mantener la máxima compatibilidad con nuevas funcionalidades, además de resolver cualquier nuevo fallo de seguridad detectado. Hay que corregirlo 7. **(CVE-2022-29376)** **Xampp para Windows v8.1.4** **y más antiguos permite ejecutar código malicioso ya que su directorio de instalación no está protegido adecuadamente**. En caso de éxito tiene muy gran alcance, podrían incluso suplantarnos el programa. Y en este caso tiene un fácil remedio que hará este intento de intrusión más difícil sin necesidad de actualizar: haciendo que todas las carpetas y subcarpetas del XAMPP con ejecutables y binarios sean de solo lectura excepto administradores. Hay que corregirlo 8. Hay muchas aplicaciones que Microsoft Windows 10 tiene instaladas por defecto y no permite desinstalar fácilmente, así que cualquier vulnerabilidad relacionada con dichas aplicaciones no puede corregirse mediante la eliminación de la aplicación, como mucho la actualización del sistema 9. La mayoría de vulnerabilidades detectadas por vulscan (menos las marcadas en negrita) ya han sido parcheadas oficialmente o las hemos comprobado manualmente nosotros y no suceden ya o no aplican. Por la tanto no requieren ser corregidas por nuestra parte. **La excepción es la denegación de servicio**, la cual esperamos sea mitigada mediante el uso de la VPN y la inhabilidad de acceder al servidor de la BBDD y página web desde el exterior sin la VPN 10. Las marcadas con negrita de la parte del nmap con vulscan se esperan resolver con actualización a la última versión de Apache 11. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   CORRECIONES POR HACER:  VER SI SE PUEDE BORAR EL USBPcap 1.5.4.0  ACTUALIZAR FIREFOX EN AMBAS MAQUINAS FINALES.  ACTUALIZAR EL APACHE/XAMPP  HACER QUE TODAS LAS CARPETAS DE BINARIOS DEL XAMPP SEAN DE SOLO LECTURA Y NO SE PUEDAN SOBREESCRIBIR.  ACTUALIZAR EL WINDOWS 10 A LA ÚLTIMA VERSIÓN. |

## Recomendaciones sobre implantación de medidas preventivas.

Entrenar a nuestros trabajadores en medidas de seguridad, entre ellas no dejar la contraseña de usuario por ahí ni dejarla grabada, tratar de mantener su SW y HW actualizado, no hablar de los clientes públicamente ni de nada relacionado con las seguridad (nada fuera del entorno laboral), y tener mucho cuidado con la instalación de SW de terceros, a ser posible no instalarlo (pues, por ejemplo, en servicios de mensajería y especialmente en servicios móviles, los mensajes enviados se suelen guardar en una base de datos local del dispositivo que, dependiendo del algoritmo de cifrado empleado, podría ser descifrado). Esta última medida debería ser notificada a nuestros clientes también para que tengan cuidado en las redes móviles.

En cuanto a los dispositivos móviles, recomendamos tanto a trabajadores como a nuestros clientes que se sigan algunos de los preceptos de seguridad en dispositivos móviles de mensajería instantánea (Centro Criptológico Nacional, 2021):

1. *Mantener el teléfono bloqueado. De esta forma, se reducirá el riesgo si el dispositivo cae en las manos equivocadas.*
2. *Sería recomendable eliminar las previsualizaciones de los mensajes y extremar las medidas cuando no se disponga del teléfono al alcance.*
3. *En la medida de lo posible, se recomienda la configuración de las aplicaciones para solo recibir mensajes de personas autorizadas.*
4. *Desactivar la conectividad adicional del teléfono cuando no se vaya a utilizar, como podría ser la conexión WiFi o Bluetooth, ya que además de reducir el consumo de batería, reduce la posible superficie de ataque sobre el dispositivo.*
5. *Utilizar aplicaciones de mensajería instantánea cuyo código fuente esté abierto a la comunidad y haya sido revisado. En ese sentido existen alternativas que, además, aseguran la confidencialidad en las comunicaciones, cifrando el tráfico extremo a extremo (e2e).*

Además, usaríamos la mejor encriptación wireless (WPA3 por el momento), y los dispositivos móviles deberían tener una doble verificación de sistema biométrico y contraseña, y no estar rooteados. De hecho para mayor seguridad los móviles corporativos deberían resetearse cada mes para asegurarse de que no están rooteados.

Dejar los sistemas cerrados bajo llave (contraseña electrónica y llave física) dentro de una habitación con sistema de refrigeración y medidas anti-incendios, y filtros de aire (más una cámara de presión positiva) para prevenir polvo e insectos dentro de la cámara, con una trampa de luz ultravioleta para eliminar cualquier posible insecto que se cuele. El servidor debería estar desplegado en el edificio de la empresa, para mayor seguridad. Y tener cámaras con reconocimiento facial y otros métodos de seguridad biométrica.

También deberíamos añadir redundancias como medida extra en caso de caída o fallo (p. ej. backup de la BBDD, múltiples switches, generadores de emergencia) pero no lo hemos implementado porque o bien no se podían simular en máquina virtual, o se podrían simular pero a riesgo de falta de memoria (p.ej: un ordenador teniendo que soportar la red básica más los backups).

El control de acceso debería ser distribuido, de tal forma que dar privilegios más altos a alguien requiera de la colaboración de todos los administradores, para complicar la corrupción permitiendo accesos maliciosos al sistema.

Además como protección extra frente a alguien logrando robar credenciales de la VPN y acceder, deberíamos añadir un segundo firewall detrás del primero para evitar que alguien empleara el servicio VPN para mandar paquetes a servicios previamente inaccesibles; pero no lo hemos resuelto porque nos han pedido no alterar la infraestructura.

Por último, y tras haber realizado los apartados anteriores de la auditoría, recomendaríamos pasar el servidor a un Sistema Operativo más sencillo, robusto, con menos vulnerabildiades y centrado solo en BBDD y mensajería, como alguna versión de Linux.

(Esta imagen de abajo es por referencia, no incluirla en la memoria final)Tabla

Descripción generada automáticamente)

# REFERENCIAS

FreeBSD. (15 de 7 de 2022). *www.freebsd.org*. Obtenido de www.freebsd.org: https://www.freebsd.org/security/advisories/FreeBSD-SA-22:02.wifi.asc

FreeBSD. (15 de 7 de 2022). *www.freebsd.org*. Obtenido de www.freebsd.org: https://www.freebsd.org/security/advisories/FreeBSD-SA-22:03.openssl.asc

FreeBSD. (15 de 7 de 2022). *www.freebsd.org*. Obtenido de www.freebsd.org: https://www.freebsd.org/security/advisories/FreeBSD-SA-22:04.netmap.asc

FreeBSD. (15 de 7 de 2022). *www.freebsd.org*. Obtenido de www.freebsd.org: https://www.freebsd.org/security/advisories/FreeBSD-SA-22:07.wifi\_meshid.asc

FreeBSD. (15 de 7 de 2022). *www.freebsd.org*. Obtenido de www.freebsd.org: https://www.freebsd.org/security/advisories/FreeBSD-SA-22:06.ioctl.asc

FreeBSD. (15 de 7 de 2022). *www.freebsd.org*. Obtenido de www.freebsd.org: https://www.freebsd.org/security/advisories/FreeBSD-SA-22:01.vt.asc

Microsoft. (9 de 10 de 2020). *docs.microsoft.com*. Obtenido de microsoft.com: https://docs.microsoft.com/en-us/lifecycle/announcements/windows-10-1903-end-of-servicing

Microsoft. (12 de 8 de 2021). *msrc.microsoft.com*. Obtenido de msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

Microsoft. (9 de 11 de 2021). *msrc.microsoft.com*. Obtenido de msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379

Microsoft. (14 de 6 de 2022). *msrc.microsoft.com*. Obtenido de msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30193

Microsoft. (14 de 6 de 2022). *msrc.microsoft.com*. Obtenido de msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-32230

Microsoft. (14 de 6 de 2022). *msrc.microsoft.com*. Obtenido de msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

Microsoft. (14 de 6 de 2022). *msrc.microsoft.com*. Obtenido de msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163

Mozilla Foundation Security Advisory 2022-20. (31 de 5 de 2022). *www.mozilla.org/en-US/security/*. Obtenido de www.mozilla.org/en-US/security/: https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/

Vulmon. (14 de 6 de 2022). *vulmon.com*. Obtenido de vulmon.com: https://vulmon.com/searchpage?q=xampp&sortby=bydate

Vulmon. (6 de 7 de 2022). *vulmon.com*. Obtenido de vulmon.com: https://vulmon.com/vulnerabilitydetails?qid=CVE-2022-29376&scoretype=cvssv3

Centro Criptológico Nacional. (1 de 3 de 2021). *https://www.ccn-cert.cni.es*. Obtenido de Centro Criptológico Nacional: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2473-ccn-cert-bp-01-principios-y-recomendaciones-basicas-en-ciberseguridad/file.html

Sánchez, B. B. (1 de 5 de 2022). *moodle.* Obtenido de Enunciado y propuesta Segundo Parcial: https://moodle.upm.es/titulaciones/oficiales/pluginfile.php/9386654/mod\_resource/content/3/Enunciado%20y%20propuesta%20Segundo%20parcial.pdf

WunderTech. (8 de 06 de 2022). *WunderTech*. Obtenido de WunderTech: https://www.youtube.com/watch?v=cxhIpmov4TY