INFORME TÉCNICO

Análisis de Vulnerabilidades en Máquinas Virtuales

Cliente:	Propietario de las máquinas
Fecha:	10/09/2025
Preparado por:	Santiago Sabogal Millan, Esteban Fernando Forero Montejo, Laura Maria Franco Ulloa
Clasificación:	Confidencial
Versión:	1.0

Resumen Técnico

Hallazgos Principales

Se identificaron 136 vulnerabilidades en total, con 15 críticas, 8 altas, 91 medias y 22 bajas. El hallazgo más crítico es la detección repetida de SSL Versión 2 y 3 en BEE\#-BOX, lo que indica una exposición significativa en sistemas clave.

Riesgo Principal Identificado

El riesgo principal es la posible interrupción operacional y filtración de datos debido a las vulnerabilidades críticas de SSL, que podrían permitir ataques de intermediario y comprometer la confidencialidad, resultando en daños reputacionales y incumplimiento normativo como GDPR.

Recomendaciones Estratégicas

1. Implementar una política de gestión de vulnerabilidades proactiva que priorice la remediación de fallos críticos.
2. Fortalecer los controles de seguridad en la capa de transporte mediante la actualización a protocolos TLS modernos.
3. Realizar auditorías de seguridad regulares y capacitar al personal en concienciación sobre ciberseguridad.
4. Establecer un marco de respuesta a incidentes para mitigar rápidamente cualquier brecha detectada.

Resumen de Hallazgos por Host

Vulnerabilidades Críticas

Atención Inmediata Requerida

Las siguientes vulnerabilidades requieren acción inmediata debido a su alto riesgo de explotación y potencial impacto en la organización.

Máquina BEE-BOX

ID	Descripción	Severidad	Estado
VULN-B001	SSL Version 2 and 3 Protocol Detection	Crítica	Pendiente
VULN-B002	SSL Version 2 and 3 Protocol Detection	Crítica	Pendiente
VULN-B003	SSL Version 2 and 3 Protocol Detection	Crítica	Pendiente
VULN-B004	SSL Version 2 and 3 Protocol Detection	Crítica	Pendiente
VULN-B005	Samba 'AndX' Request Heap-Based Buffer Overflow	Crítica	Pendiente

Máquina METASPLOITABLE

ID	Descripción	Severidad	Estado
VULN-M001	Apache Tomcat SEoL (<= 5.5.x)	Crítica	Pendiente
VULN-M002	SSL Version 2 and 3 Protocol Detection	Crítica	Pendiente
VULN-M003	SSL Version 2 and 3 Protocol Detection	Crítica	Pendiente
VULN-M004	Canonical Ubuntu Linux SEoL (8.04.x)	Crítica	Pendiente
VULN-M005	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Crítica	Pendiente
VULN-M006	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Crítica	Pendiente
VULN-M007	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Crítica	Pendiente
VULN-M008	UnrealIRCd Backdoor Detection	Crítica	Pendiente
VULN-M009	Bind Shell Backdoor Detection	Crítica	Pendiente
VULN-M010	VNC Server 'password' Password	Crítica	Pendiente

Vulnerabilidades de Alta Prioridad

Máquina BEE-BOX

ID	Descripción	Severidad	Estado
VULN-B006	SNMP Agent Default Community Name (public)	Alta	Pendiente
VULN-B007	Drupal Database Abstraction API SQLi	Alta	Pendiente
VULN-B008	Drupal Database Abstraction API SQLi	Alta	Pendiente
VULN-B009	Drupal Database Abstraction API SQLi	Alta	Pendiente
VULN-B010	Drupal Database Abstraction API SQLi	Alta	Pendiente

Máquina METASPLOITABLE

ID	Descripción	Severidad	Estado
VULN-M011	rlogin Service Detection	Alta	Pendiente
VULN-M012	rsh Service Detection	Alta	Pendiente
VULN-M013	Apache Tomcat AJP Connector Request Injection (Ghost-cat)	Alta	Pendiente

Vulnerabilidades de Prioridad Media

Máquina BEE-BOX

ID	Descripción	Severidad	Estado
VULN-B011	TLS Version 1.0 Protocol Detection	Media	Pendiente
VULN-B012	TLS Version 1.0 Protocol Detection	Media	Pendiente
VULN-B013	TLS Version 1.0 Protocol Detection	Media	Pendiente
VULN-B014	TLS Version 1.0 Protocol Detection	Media	Pendiente
VULN-B015	Apache mod_status /server-status Information Disclosure	Media	Pendiente
VULN-B016	Apache mod_status /server-status Information Disclosure	Media	Pendiente
VULN-B017	HTTP TRACE / TRACK Methods Allowed	Media	Pendiente
VULN-B018	HTTP TRACE / TRACK Methods Allowed	Media	Pendiente
VULN-B019	nginx < 1.17.7 Information Disclosure	Media	Pendiente
VULN-B020	nginx < 1.17.7 Information Disclosure	Media	Pendiente

ID	Descripción	Severidad	Estado
VULN-B021	TLS Version 1.1 Deprecated Protocol	Media	Pendiente
VULN-B022	SSL Certificate Expiry	Media	Pendiente
VULN-B023	SSL Certificate Expiry	Media	Pendiente
VULN-B024	SSL Certificate Expiry	Media	Pendiente
VULN-B025	SSL Certificate Expiry	Media	Pendiente
VULN-B026	SSL Weak Cipher Suites Supported	Media	Pendiente
VULN-B027	SSL Weak Cipher Suites Supported	Media	Pendiente
VULN-B028	SSL Weak Cipher Suites Supported	Media	Pendiente
VULN-B029	SSL Certificate Signed Using Weak Hashing Algorithm	Media	Pendiente
VULN-B030	SSL Certificate Signed Using Weak Hashing Algorithm	Media	Pendiente
VULN-B031	SSL Certificate Signed Using Weak Hashing Algorithm	Media	Pendiente
VULN-B032	SSL Medium Strength Cipher Suites Supported (SWEET32)	Media	Pendiente
VULN-B033	SSL Medium Strength Cipher Suites Supported (SWEET32)	Media	Pendiente
VULN-B034	SSL Medium Strength Cipher Suites Supported (SWEET32)	Media	Pendiente
VULN-B035	SSL Medium Strength Cipher Suites Supported (SWEET32)	Media	Pendiente
VULN-B036	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS	Media	Pendiente
VULN-B037	SSL Certificate with Wrong Hostname	Media	Pendiente
VULN-B038	SSL Certificate with Wrong Hostname	Media	Pendiente
VULN-B039	SSL Certificate with Wrong Hostname	Media	Pendiente
VULN-B040	SSL Certificate with Wrong Hostname	Media	Pendiente
VULN-B041	SSL Certificate Cannot Be Trusted	Media	Pendiente
VULN-B042	SSL Certificate Cannot Be Trusted	Media	Pendiente
VULN-B043	SSL Certificate Cannot Be Trusted	Media	Pendiente
VULN-B044	SSL Certificate Cannot Be Trusted	Media	Pendiente
VULN-B045	SMTP Service STARTTLS Plaintext Command Injection	Media	Pendiente
VULN-B046	SSL Self-Signed Certificate	Media	Pendiente
VULN-B047	SSL Self-Signed Certificate	Media	Pendiente
VULN-B048	SSL Self-Signed Certificate	Media	Pendiente
VULN-B049	SSL Self-Signed Certificate	Media	Pendiente
VULN-B050	SMB Signing not required	Media	Pendiente
VULN-B051	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media	Pendiente
VULN-B052	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media	Pendiente

ID	Descripción	Severidad	Estado
VULN-B053	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media	Pendiente
VULN-B054	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS	Media	Pendiente
VULN-B055	OpenSSL Heartbeat Information Disclosure (Heartbleed)	Media	Pendiente
VULN-B056	SNMP 'GETBULK' Reflection DDoS	Media	Pendiente
VULN-B057	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	Media	Pendiente
VULN-B058	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	Pendiente
VULN-B059	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	Pendiente
VULN-B060	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	Pendiente
VULN-B061	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	Pendiente
VULN-B062	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Media	Pendiente
VULN-B063	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Media	Pendiente
VULN-B064	Apache Server ETag Header Information Disclosure	Media	Pendiente
VULN-B065	Apache Server ETag Header Information Disclosure	Media	Pendiente
VULN-B066	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Media	Pendiente
VULN-B067	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Media	Pendiente
VULN-B068	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Media	Pendiente
VULN-B069	SSH Weak Algorithms Supported	Media	Pendiente
VULN-B070	Samba Badlock Vulnerability	Media	Pendiente
VULN-B071	Network Time Protocol (NTP) Mode 6 Scanner	Media	Pendiente

Máquina METASPLOITABLE

ID	Descripción	Severidad	Estado
VULN-M014	TLS Version 1.0 Protocol Detection	Media	Pendiente
VULN-M015	TLS Version 1.0 Protocol Detection	Media	Pendiente
VULN-M016	HTTP TRACE / TRACK Methods Allowed	Media	Pendiente
VULN-M017	Apache Tomcat Default Files	Media	Pendiente
VULN-M018	ISC BIND Service Downgrade / Reflected DoS	Media	Pendiente

ID	Descripción	Severidad	Estado
VULN-M019	ISC BIND Denial of Service	Media	Pendiente
VULN-M020	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	Media	Pendiente
VULN-M021	SSL Certificate Expiry	Media	Pendiente
VULN-M022	SSL Certificate Expiry	Media	Pendiente
VULN-M023	SSL Weak Cipher Suites Supported	Media	Pendiente
VULN-M024	NFS Shares World Readable	Media	Pendiente
VULN-M025	Unencrypted Telnet Server	Media	Pendiente
VULN-M026	SSL Medium Strength Cipher Suites Supported (SWEET32)	Media	Pendiente
VULN-M027	SSL Medium Strength Cipher Suites Supported (SWEET32)	Media	Pendiente
VULN-M028	SSL Certificate with Wrong Hostname	Media	Pendiente
VULN-M029	SSL Certificate with Wrong Hostname	Media	Pendiente
VULN-M030	SSL Certificate Cannot Be Trusted	Media	Pendiente
VULN-M031	SSL Certificate Cannot Be Trusted	Media	Pendiente
VULN-M032	SMTP Service STARTTLS Plaintext Command Injection	Media	Pendiente
VULN-M033	SSL Self-Signed Certificate	Media	Pendiente
VULN-M034	SSL Self-Signed Certificate	Media	Pendiente
VULN-M035	SMB Signing not required	Media	Pendiente
VULN-M036	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media	Pendiente
VULN-M037	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Media	Pendiente
VULN-M038	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	Pendiente
VULN-M039	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Media	Pendiente
VULN-M040	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Media	Pendiente
VULN-M041	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Media	Pendiente
VULN-M042	SSH Weak Algorithms Supported	Media	Pendiente
VULN-M043	Samba Badlock Vulnerability	Media	Pendiente

Vulnerabilidades Bajas

Máquina BEE-BOX

ID	Descripción	Severidad	Estado
VULN-B072	ICMP Timestamp Request Remote Date Disclosure	Baja	Pendiente
VULN-B073	X Server Detection	Baja	Pendiente
VULN-B074	SSH Weak Key Exchange Algorithms Enabled	Baja	Pendiente
VULN-B075	SSL Anonymous Cipher Suites Supported	Baja	Pendiente
VULN-B076	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Baja	Pendiente
VULN-B077	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Baja	Pendiente
VULN-B078	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Baja	Pendiente
VULN-B079	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Baja	Pendiente
VULN-B080	SSH Server CBC Mode Ciphers Enabled	Baja	Pendiente
VULN-B081	SSH Weak MAC Algorithms Enabled	Baja	Pendiente
VULN-B082	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Baja	Pendiente
VULN-B083	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Baja	Pendiente
VULN-B084	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Baja	Pendiente
VULN-B085	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Baja	Pendiente

Máquina METASPLOITABLE

ID	Descripción	Severidad	Estado
VULN-M044	ICMP Timestamp Request Remote Date Disclosure	Baja	Pendiente
VULN-M045	X Server Detection	Baja	Pendiente
VULN-M046	SSH Weak Key Exchange Algorithms Enabled	Baja	Pendiente
VULN-M047	SSL Anonymous Cipher Suites Supported	Baja	Pendiente
VULN-M048	SSH Server CBC Mode Ciphers Enabled	Baja	Pendiente
VULN-M049	SSH Weak MAC Algorithms Enabled	Baja	Pendiente
VULN-M050	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Baja	Pendiente
VULN-M051	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Baja	Pendiente

Vulnerabilidades Críticas

VULN-B001: SSL Version 2 and 3 Protocol Detection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic tiene la vulnerabilidad SSL Version 2 and 3 Protocol Detection en el puerto tcp/25/smtp, que permite el uso de protocolos SSL obsoletos con debilidades criptográficas.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones, permitiendo a atacantes realizar ataques man-in-the-middle o descifrar datos sensibles, lo que podría resultar en pérdida de información, violaciones de cumplimiento como PCI DSS, y daño reputacional.

Urgencia: Crítica. La puntuación CVSS de 9.8 indica un alto riesgo de explotación remota sin autenticación, con impacto completo en confidencialidad, integridad y disponibilidad. Los protocolos SSL 2.0 y 3.0 son fácilmente explotables en ataques como POODLE, y su presencia en un servicio SMTP podría ser utilizada como punto de entrada para movimientos laterales en la red, exigiendo una acción inmediata para prevenir compromisos severos.

Acción: Deshabilitar SSL 2.0 y 3.0 en el servicio SMTP y configurar el uso exclusivo de TLS 1.2 o superior con suites de cifrado aprobadas.

Análisis Técnico

- **Nombre:** SSL Version 2 and 3 Protocol Detection
- **ID del Plugin:** 20007
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el puerto 25 acepta conexiones cifradas con SSLv2 y SSLv3, protocolos afectados por múltiples fallas criptográficas, como esquemas de padding inseguros en modo CBC y mecanismos de renegociación vulnerables. Según la salida del plugin, SSLv2 soporta cifrados débiles como EXP-RC2-CBC-MD5 (40-bit) y RC4-MD5 (128-bit), mientras que SSLv3 incluye suites de baja resistencia como EXP-DES-CBC-SHA (40-bit) y mediana como DES-CBC3-SHA (3DES), así como cifrados fuertes pero aún inseguros en el contexto de SSLv3. Esto permite a un atacante realizar downgrade attacks o explotar vulnerabilidades como POODLE para descifrar comunicaciones, comprometiendo la seguridad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical

- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el servidor de la red o implementar reglas de firewall para restringir el acceso al puerto 25 hasta que se aplique la corrección.
2. **Corrección:** Modificar la configuración del servidor SMTP para deshabilitar SSL 2.0 y 3.0, y habilitar solo TLS 1.2 o superior con suites de cifrado seguras (e.g., AES-GCM).
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que SSLv2 y SSLv3 están deshabilitados y que solo se usan protocolos y cifrados seguros.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos obsoletos, realizar auditorías periódicas de configuración, y mantener el sistema y software actualizados para prevenir regresiones.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

VULN-B002: SSL Version 2 and 3 Protocol Detection

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) tiene habilitados SSLv2 y SSLv3, lo que permite ataques de downgrade y man-in-the-middle debido a vulnerabilidades criptográficas conocidas.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones, pudiendo llevar a la exposición de datos sensibles y daños reputacionales si se explota.

Urgencia: Crítica. La puntuación CVSS de 9.8 indica un alto riesgo de explotación remota sin autenticación, permitiendo a un atacante descifrar comunicaciones o realizar ataques de intermediario fácilmente, lo que podría resultar en un compromiso completo del sistema y movimiento lateral en la red.

Acción: Deshabilitar SSLv2 y SSLv3 en el servicio configurando solo TLS 1.2 o superior con suites de cifrado aprobadas.

Análisis Técnico

- **Nombre:** SSL Version 2 and 3 Protocol Detection
- **ID del Plugin:** 20007
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto tcp/443 acepta conexiones SSLv2 y SSLv3, utilizando cifrados débiles como RC4 con claves de 40 bits y MD5 para MAC, que son susceptibles a ataques como POODLE, permitiendo a un atacante realizar downgrade de protocolo y descifrar tráfico mediante técnicas de man-in-the-middle, explotando esquemas de padding inseguros y renegociación de sesión.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red o implementar reglas de firewall para restringir el acceso al puerto 443 hasta la corrección.
2. **Corrección:** Configurar el servidor web para deshabilitar SSLv2 y SSLv3, y habilitar solo TLS 1.2 o superior con cifrados fuertes como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que SSLv2 y SSLv3 están deshabilitados y solo se usan protocolos seguros.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos SSL obsoletos y realizar auditorías periódicas de configuración de servicios.

Conclusión: La habilitación de SSLv2 y SSLv3 en BEE-BOX representa un riesgo crítico que exige una acción inmediata para prevenir el compromiso de comunicaciones y proteger los activos empresariales.

VULN-B003: SSL Version 2 and 3 Protocol Detection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Version 2 and 3 Protocol Detection, que permite el uso de protocolos SSL inseguros en el puerto tcp/8443.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones, permitiendo a atacantes descifrar datos sensibles o realizar ataques man-in-the-middle, lo que podría resultar en pérdida de datos, violaciones de cumplimiento normativo y daño reputacional.

Urgencia: Crítica. La puntuación CVSS de 9.8 indica un alto riesgo de explotación remota sin autenticación, facilitando ataques como POODLE que pueden degradar la seguridad de las comunicaciones y llevar a compromisos significativos del sistema; debe abordarse de inmediato para prevenir accesos no autorizados y proteger la infraestructura crítica.

Acción: Deshabilitar SSL 2.0 y 3.0 en el servicio y configurar TLS 1.2 o superior con suites de cifrado aprobadas.

Análisis Técnico

- **Nombre:** SSL Version 2 and 3 Protocol Detection
- **ID del Plugin:** 20007
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto 8443 acepta conexiones SSLv3, que utiliza cifrados como 3DES-CBC con esquemas de padding inseguros, permitiendo a un atacante realizar downgrade attacks para explotar vulnerabilidades como POODLE y descifrar comunicaciones; aunque se soportan cifrados fuertes como AES, la habilitación de SSLv3 crea un vector de ataque crítico que compromete la seguridad criptográfica.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red o implementar reglas de firewall para bloquear el tráfico no esencial al puerto 8443 hasta la corrección.
2. **Corrección:** Configurar el servicio web para deshabilitar SSL 2.0 y 3.0, y habilitar exclusivamente TLS 1.2 o superior con cifrados seguros como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que SSLv3 está deshabilitado y solo se usan protocolos seguros.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos obsoletos y realizar auditorías periódicas para asegurar el cumplimiento con estándares como PCI DSS.

Conclusión: La vulnerabilidad crítica en SSLv3 expone el sistema a compromisos inmediatos de datos y exige su deshabilitación urgente para salvaguardar la integridad de las comunicaciones y cumplir con los requisitos de seguridad.

VULN-B004: SSL Version 2 and 3 Protocol Detection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) tiene habilitados SSLv2 y SSLv3 en el puerto tcp/9443, lo que permite ataques de downgrade y descifrado de comunicaciones.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de los datos transmitidos, pudiendo llevar a filtraciones de información sensible y daños reputacionales debido a la facilidad de explotación en entornos de red.

Urgencia: Crítica. La puntuación CVSS de 9.8 indica un alto riesgo de explotación remota sin autenticación, permitiendo a un atacante realizar ataques man-in-the-middle y descifrar comunicaciones fácilmente, lo que podría servir como punto de entrada para compromisos más profundos en la red.

Acción: Deshabilitar SSLv2 y SSLv3 en el servicio afectado y configurar TLS 1.2 o superior con suites de cifrado aprobadas.

Análisis Técnico

- **Nombre:** SSL Version 2 and 3 Protocol Detection
- **ID del Plugin:** 20007
- **Severidad:** Crítica

- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto 9443 acepta conexiones SSLv2 y SSLv3, que utilizan esquemas criptográficos vulnerables como CBC con relleno inseguro y suites de cifrado débiles (e.g., RC4-MD5, DES-CBC-SHA), permitiendo ataques como POODLE para downgrade y descifrado. El plugin_output detalla múltiples cifrados de baja y media fuerza soportados, lo que facilita la explotación por parte de atacantes para interceptar y manipular tráfico encriptado sin necesidad de credenciales.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red o implementar reglas de firewall para bloquear el acceso no autorizado al puerto 9443.
2. **Corrección:** Configurar el servicio para deshabilitar SSLv2 y SSLv3, y habilitar solo TLS 1.2 o superior con cifrados fuertes como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los protocolos inseguros están deshabilitados y que las comunicaciones utilizan TLS seguro.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de SSL y cifrados débiles, y realizar auditorías periódicas para asegurar el cumplimiento con estándares como PCI DSS.

Conclusión: La habilitación de SSLv2 y SSLv3 en BEE-BOX representa un riesgo crítico de compromiso de datos y exige su deshabilitación inmediata para proteger la integridad y confidencialidad de las comunicaciones.

VULN-B005: Samba 'AndX' Request Heap-Based Buffer Overflow

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) ejecuta Samba en Linux Kernel 2.6.24-16-generic y es vulnerable a un desbordamiento de búfer en montón en la solicitud 'AndX' (CVE-2012-0870).

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de los datos compartidos a través de Samba, y afectar la disponibilidad del servicio, lo que podría resultar en pérdida de datos, interrupción operativa y daño reputacional.

Urgencia: Crítica. La vulnerabilidad tiene un CVSS2 de 10.0, indicando que es fácilmente explotable de forma remota sin autenticación, permitiendo la ejecución de código arbitrario y denegación de servicio, lo que podría conducir a un compromiso completo del sistema y facilitar movimientos laterales en la red.

Acción: Aplicar los parches proporcionados por el proveedor de Samba.

Análisis Técnico

- **Nombre:** Samba 'AndX' Request Heap-Based Buffer Overflow
- **ID del Plugin:** 58327
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/445/cifs)

La vulnerabilidad en Samba, específicamente en el manejo de solicitudes 'AndX', permite un desbordamiento de búfer en montón debido a una falta de validación adecuada de la entrada. Un atacante remoto puede enviar una solicitud especialmente manipulada al puerto 445/tcp (cifs), sobrescribiendo memoria en el montón y ejecutando código arbitrario con los privilegios del servicio Samba, o causar una denegación de servicio si el exploit falla. Esto explota una debilidad en la gestión de memoria durante el procesamiento de protocolos SMB/CIFS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))
- **VPR Score:** 5.9
- **EPSS Score:** 0.489

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red para prevenir explotaciones mientras se aplican correcciones.
2. Corrección: Actualizar Samba a una versión parcheada que aborde CVE-2012-0870, siguiendo las guías del proveedor.
3. Verificación: Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que el parche se aplicó correctamente y la vulnerabilidad está mitigada.
4. Prevención: Implementar monitoreo continuo de la red para detectar intentos de explotación y establecer procesos regulares de gestión de parches para todos los sistemas.

Conclusión: La vulnerabilidad crítica en Samba representa un riesgo inminente de compromiso total del sistema y exige la aplicación inmediata de parches para salvaguardar la infraestructura y prevenir accesos no autorizados.

VULN-M001: Apache Tomcat SEoL (<= 5.5.x)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) ejecuta una versión no soportada de Apache Tomcat SEoL (\<= 5.5.x), exponiéndolo a vulnerabilidades de seguridad.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad, integridad y disponibilidad de los datos y servicios, pudiendo resultar en acceso no autorizado, manipulación de información, y daño reputacional debido a la falta de soporte y parches de seguridad.

Urgencia: Crítica. La puntuación CVSS de 10.0 indica que es fácilmente explotable de forma remota sin autenticación, permitiendo a un atacante comprometer completamente el sistema, acceder a datos sensibles, y potencialmente usarlo como punto de entrada para movimientos laterales en la red, lo que exige una acción inmediata.

Acción: Actualizar Apache Tomcat a una versión soportada.

Análisis Técnico

- **Nombre:** Apache Tomcat SEoL (<= 5.5.x)
- **ID del Plugin:** 171340
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/8180/www)

Según la salida del plugin, el servidor en http://192.168.122.29:8180/ ejecuta Apache Tomcat versión 5.5, que alcanzó su fin de vida de seguridad el 30 de septiembre de 2012, hace más de 12 años. Al no estar mantenida, esta versión carece de parches para vulnerabilidades conocidas y desconocidas, lo que significa que cualquier exploit disponible podría ser utilizado para comprometer el servicio web, permitiendo a atacantes ejecutar código arbitrario, robar datos, o tomar control del sistema subyacente, con implicaciones técnicas graves debido a la alta criticidad del CVSS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 10.0 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red para prevenir explotaciones mientras se aplica la corrección.
2. Corrección: Actualizar Apache Tomcat a una versión actual y soportada, como la serie 10.x o superior, siguiendo las guías oficiales de Apache.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades post-actualización para confirmar que la versión vulnerable ha sido eliminada y no hay regresiones.
4. Prevención: Implementar un programa de gestión de parches regular para mantener todos los software actualizados y monitorear continuamente los endpoints en busca de versiones obsoletas.

Conclusión: La versión no soportada de Apache Tomcat representa un riesgo crítico de compromiso total del sistema y exige una actualización inmediata para mitigar amenazas de seguridad y proteger los activos empresariales.

VULN-M002: SSL Version 2 and 3 Protocol Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad SSL Version 2 and 3 Protocol Detection en el servicio SMTP (puerto 25), que permite el uso de protocolos SSL obsoletos con debilidades criptográficas.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones, permitiendo a atacantes realizar ataques man-in-the-middle o descifrar datos sensibles, lo que podría resultar en pérdida de información, violaciones de cumplimiento normativo y daño reputacional.

Urgencia: Crítica. La puntuación CVSS de 9.8 indica un alto riesgo de explotación remota sin autenticación, con impactos severos en confidencialidad, integridad y disponibilidad. Los protocolos SSL 2.0 y 3.0 son fácilmente explotables en ataques como POODLE, pudiendo servir como punto de entrada para compromisos más amplios en la red, por lo que requiere atención inmediata.

Acción: Deshabilitar SSL 2.0 y 3.0 en el servicio SMTP y configurar el uso exclusivo de TLS 1.2 o superior con suites de cifrado aprobadas.

Análisis Técnico

- **Nombre:** SSL Version 2 and 3 Protocol Detection
- **ID del Plugin:** 20007
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el host acepta conexiones cifradas con SSLv2 y SSLv3, protocolos afectados por múltiples fallos criptográficos, como esquemas de padding inseguros en modo CBC y mecanismos de renegociación vulnerables. El plugin_output detalla que se admiten cifrados débiles (e.g., EXP-RC4-MD5 con claves de 40 bits) y medios (e.g., DES-CBC-SHA), así como algunos fuertes (e.g., AES256-SHA), pero la presencia de SSLv2/3 permite a atacantes forzar downgrades para explotar debilidades, facilitando ataques man-in-the-middle que pueden descifrar comunicaciones o alterar datos en tránsito.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red o implementar reglas de firewall para bloquear el tráfico no esencial al puerto 25 hasta la corrección.
2. **Corrección:** Modificar la configuración del servidor SMTP (e.g., en Postfix o Sendmail) para deshabilitar SSLv2 y SSLv3, y habilitar solo TLS 1.2 o superior con cifrados seguros como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección usando herramientas como Nessus o OpenSSL s_client para confirmar que solo se aceptan protocolos TLS seguros.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos obsoletos y realizar auditorías periódicas de configuración para asegurar el cumplimiento con estándares como PCI DSS.

Conclusión: La detección de SSLv2/3 en SMTP representa un riesgo crítico que exige la deshabilitación inmediata de estos protocolos para prevenir compromisos de seguridad y proteger la integridad de las comunicaciones empresariales.

VULN-M003: SSL Version 2 and 3 Protocol Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con PostgreSQL en el puerto 5432 tiene habilitados los protocolos SSLv2 y SSLv3, lo que presenta la vulnerabilidad SSL Version 2 and 3 Protocol Detection.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de los datos al permitir ataques man-in-the-middle y descifrado de comunicaciones, lo que podría resultar en pérdida de información sensible, incumplimiento de normativas como PCI DSS, y daño reputacional.

Urgencia: Crítica. La puntuación CVSS de 9.8 indica un alto riesgo de explotación remota sin autenticación, facilitando ataques como POODLE que pueden degradar la seguridad criptográfica y llevar a compromisos completos del sistema; debe abordarse de inmediato para prevenir accesos no autorizados y movimientos laterales en la red.

Acción: Deshabilitar SSL 2.0 y 3.0 en el servicio PostgreSQL y configurar TLS 1.2 o superior con suites de cifrado aprobadas.

Análisis Técnico

- **Nombre:** SSL Version 2 and 3 Protocol Detection
- **ID del Plugin:** 20007
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El servicio PostgreSQL en el host acepta conexiones cifradas usando SSLv3, que incluye cifrados de fuerza media y alta como 3DES-CBC y AES-CBC, pero estos protocolos tienen debilidades inherentes como esquemas de padding inseguros y renegociación de sesión vulnerable, permitiendo a un atacante realizar downgrade attacks o descifrar tráfico mediante exploits como POODLE, comprometiendo la confidencialidad e integridad de las comunicaciones.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red o implementar reglas de firewall para restringir el acceso al puerto 5432 hasta la corrección.

2. **Corrección:** Modificar la configuración de PostgreSQL para deshabilitar SSLv2 y SSLv3, y habilitar solo TLS 1.2 o superior con cifrados fuertes como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los protocolos inseguros están deshabilitados y que el servicio solo acepta conexiones seguras.
4. **Prevención:** Establecer políticas de seguridad que exijan el uso exclusivo de TLS moderno y realizar auditorías periódicas para asegurar el cumplimiento con estándares como NIST y PCI DSS.

Conclusión: La vulnerabilidad crítica en SSLv3 expone el sistema a compromisos totales y exige una acción inmediata para proteger los datos y cumplir con los requisitos de seguridad.

VULN-M004: Canonical Ubuntu Linux SEoL (8.04.x)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) ejecuta una versión no soportada de Canonical Ubuntu Linux 8.04.x, lo que constituye la vulnerabilidad Canonical Ubuntu Linux SEoL (8.04.x).

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad, integridad y disponibilidad de los datos y sistemas, ya que la falta de parches de seguridad puede permitir accesos no autorizados y daños significativos, afectando la reputación de la organización debido a posibles brechas.

Urgencia: Crítica. La puntuación CVSS de 10.0 indica que es fácilmente explotable de forma remota sin autenticación, lo que podría llevar a un compromiso completo del sistema, permitiendo a un atacante obtener control total, exfiltrar datos sensibles y usar el host como punto de partida para ataques laterales en la red, exigiendo una acción inmediata para mitigar riesgos severos.

Acción: Actualizar el sistema operativo a una versión soportada de Canonical Ubuntu Linux.

Análisis Técnico

- **Nombre:** Canonical Ubuntu Linux SEoL (8.04.x)
- **ID del Plugin:** 201352
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/80/www)

La vulnerabilidad surge porque Ubuntu Linux 8.04.x alcanzó su fin de soporte de seguridad el 9 de mayo de 2013, hace más de 12 años, lo que significa que no recibe actualizaciones de seguridad del vendor. Esto deja el sistema expuesto a múltiples exploits conocidos y desconocidos, ya que cualquier vulnerabilidad en el kernel o software asociado permanece sin parchear, permitiendo a atacantes remotos ejecutar código arbitrario, comprometer servicios y acceder a recursos del sistema sin restricciones, tal como se indica en el plugin_output que confirma el estado de fin de vida.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 10.0 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. Contención: Aislar el host de la red inmediatamente para prevenir accesos no autorizados y limitar el movimiento lateral.
2. Corrección: Actualizar el sistema operativo a una versión soportada como Ubuntu 20.04 LTS o superior, siguiendo los procedimientos estándar de actualización.
3. Verificación: Realizar un escaneo de vulnerabilidades post-actualización usando herramientas como Nessus para confirmar que el sistema está parcheado y seguro.
4. Prevención: Implementar un programa de gestión de parches regular para asegurar que todos los sistemas se mantengan actualizados y dentro del ciclo de soporte, además de monitorear continuamente el estado de los endpoints.

Conclusión: La presencia de un sistema operativo no soportado representa un riesgo crítico de compromiso total y exige su actualización inmediata para proteger los activos empresariales y prevenir daños catastróficos.

VULN-M005: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad Debian OpenSSH/OpenSSL Package Random Number Generator Weakness, que genera claves SSH débiles debido a un error en el generador de números aleatorios de OpenSSL.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones SSH, permitiendo a atacantes descifrar sesiones o realizar ataques man-in-the-middle, lo que podría resultar en acceso no autorizado a datos sensibles y daño reputacional.

Urgencia: Crítica. La vulnerabilidad tiene un CVSS2 de 10.0, indicando que es fácilmente explotable de forma remota sin autenticación, lo que puede llevar a un compromiso completo del sistema y servir como punto de entrada para movimientos laterales en la red, exigiendo atención inmediata.

Acción: Regenerar todo el material criptográfico, incluyendo las claves SSH, SSL y OpenVPN, en el host afectado.

Análisis Técnico

- **Nombre:** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
- **ID del Plugin:** 32314
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/22/ssh)

La vulnerabilidad surge de un error en el paquete OpenSSL de Debian/Ubuntu, donde se eliminaron fuentes de entropía, resultando en claves SSH predecibles. Esto permite a un atacante adivinar la clave privada remota, facilitando el descifrado de sesiones SSH o la ejecución de ataques man-in-the-middle, comprometiendo la seguridad de las comunicaciones y exponiendo datos sensibles.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))
- **VPR Score:** 5.1
- **EPSS Score:** 0.0165

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red para prevenir explotaciones.
2. Corrección: Regenerar todas las claves criptográficas usando una versión corregida de OpenSSL y aplicar parches de seguridad.
3. Verificación: Validar la fortaleza de las nuevas claves mediante herramientas de análisis y escaneos de vulnerabilidades.
4. Prevención: Implementar monitoreo continuo y políticas de gestión de claves para evitar recurrencias.

Conclusión: La debilidad en el generador de números aleatorios representa un riesgo crítico que exige la regeneración inmediata de claves para proteger la integridad y confidencialidad de las comunicaciones del negocio.

VULN-M006: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad Debian OpenSSH/OpenSSL Package Random Number Generator Weakness, donde el certificado SSL utiliza una clave débil debido a un generador de números aleatorios defectuoso en OpenSSL.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones SSL, permitiendo a atacantes descifrar sesiones o realizar ataques man-in-the-middle, lo que podría resultar en acceso no autorizado a datos sensibles y daño reputacional.

Urgencia: Crítica. La vulnerabilidad es fácilmente explotable con herramientas como Core Impact, otorgando a atacantes la capacidad de comprometer completamente las comunicaciones SSL y potencialmente acceder a otros sistemas en la red, lo que exige una acción inmediata para prevenir un incidente de seguridad grave.

Acción: Regenerar todo el material criptográfico, incluyendo claves SSH, SSL y OpenVPN, en el host afectado.

Análisis Técnico

- **Nombre:** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
- **ID del Plugin:** 32321
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

La vulnerabilidad surge de un error en la versión de OpenSSL empaquetada para Debian y Ubuntu, donde se eliminaron fuentes de entropía en el generador de números aleatorios, resultando en claves criptográficas predecibles. Esto permite a un atacante adivinar la clave privada del certificado SSL, facilitando el descifrado de sesiones o la ejecución de ataques man-in-the-middle, comprometiendo la seguridad de las comunicaciones en el puerto tcp/25/smtp y otros servicios que utilicen SSL.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))
- **VPR Score:** 5.1
- **EPSS Score:** 0.0165

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red para prevenir explotaciones durante la remediación.
2. Corrección: Regenerar todas las claves criptográficas (SSH, SSL, OpenVPN) utilizando una versión corregida de OpenSSL y aplicar parches de seguridad.
3. Verificación: Validar la fortaleza de las nuevas claves mediante herramientas de análisis de certificados y escaneos de vulnerabilidades para asegurar que el problema esté resuelto.
4. Prevención: Implementar políticas de gestión de claves y auditorías regulares para detectar y corregir vulnerabilidades similares en el futuro.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

VULN-M007: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check), donde el certificado SSL utiliza una clave débil debido a un generador de números aleatorios defectuoso en OpenSSL.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones SSL, permitiendo a atacantes descifrar sesiones o realizar ataques man-in-the-middle, lo que podría resultar en acceso no autorizado a datos sensibles y daño reputacional.

Urgencia: Crítica. La vulnerabilidad tiene un CVSS2 de 10.0, indicando que es fácilmente explotable de forma remota sin autenticación, lo que puede llevar a un compromiso completo del sistema y servir como punto de entrada para movimientos laterales en la red, exigiendo atención inmediata.

Acción: Regenerar todo el material criptográfico, incluyendo claves SSH, SSL y OpenVPN, en el host afectado.

Análisis Técnico

- **Nombre:** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
- **ID del Plugin:** 32321
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

La vulnerabilidad surge de un error en la versión de OpenSSL en sistemas Debian y Ubuntu, donde se eliminaron fuentes de entropía en el generador de números aleatorios, haciendo que las claves criptográficas sean predecibles. Esto permite a un atacante adivinar la clave privada del certificado SSL, facilitando el descifrado de comunicaciones o la ejecución de ataques man-in-the-middle, comprometiendo la seguridad de las sesiones SSL en el puerto tcp/5432/postgresql.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))
- **VPR Score:** 5.1
- **EPSS Score:** 0.0165

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red para prevenir explotaciones mientras se aplica la corrección.
2. **Corrección:** Regenerar todas las claves criptográficas (SSH, SSL, OpenVPN) utilizando una versión corregida de OpenSSL y aplicar parches de seguridad.
3. **Verificación:** Validar que las nuevas claves sean seguras mediante herramientas de análisis de certificados y pruebas de penetración para asegurar que la vulnerabilidad ha sido mitigada.
4. **Prevención:** Implementar monitoreo continuo de vulnerabilidades, actualizar regularmente el software, y seguir mejores prácticas criptográficas para evitar recurrencias.

Conclusión: La debilidad en el generador de números aleatorios de OpenSSL representa un riesgo crítico que compromete la seguridad de las comunicaciones y exige la regeneración inmediata de las claves para proteger los activos empresariales.

VULN-M008: UnrealIRCd Backdoor Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) ejecuta UnrealIRCd con un backdoor que permite la ejecución remota de código arbitrario.

Riesgo para el Negocio: Este backdoor compromete la confidencialidad, integridad y disponibilidad del sistema, permitiendo a atacantes acceder y manipular datos sensibles, lo que podría resultar en pérdida de reputación y cumplimiento normativo.

Urgencia: Crítica. La vulnerabilidad es fácilmente explotable con herramientas como Metasploit, otorgando control total del sistema de inmediato, y puede servir como punto de entrada para ataques más amplios en la red, requiriendo acción urgente para prevenir un compromiso catastrófico.

Acción: Reinstalar UnrealIRCd descargando y verificando el software con las sumas de comprobación MD5/SHA1 publicadas.

Análisis Técnico

- **Nombre:** UnrealIRCd Backdoor Detection
- **ID del Plugin:** 46882
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/6667/irc)

El plugin_output indica que el servidor IRC se ejecuta con privilegios de root (uid=0, gid=0), lo que significa que cualquier explotación exitosa del backdoor en UnrealIRCd otorga a un atacante control completo sobre el sistema, permitiendo la ejecución de comandos arbitrarios, acceso a todos los datos, y potencial escalada de privilegios sin restricciones, exacerbando el riesgo debido a la naturaleza crítica del servicio en red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))
- **VPR Score:** 7.4
- **EPSS Score:** 0.868

Acciones Recomendadas

1. Contención: Aislar inmediatamente el host de la red para prevenir la explotación y propagación del backdoor.
2. Corrección: Desinstalar la versión vulnerable de UnrealIRCd, descargar una versión segura desde una fuente confiable, y verificar su integridad usando las sumas MD5/SHA1 proporcionadas antes de la reinstalación.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que el backdoor ha sido eliminado y no hay compromisos residuales.
4. Prevención: Implementar monitoreo continuo de logs y tráfico de red, aplicar parches de seguridad de manera proactiva, y educar al personal sobre las mejores prácticas para evitar instalaciones de software no verificadas.

Conclusión: El backdoor en UnrealIRCd representa una amenaza crítica que exige una acción inmediata de reinstalación para evitar el control no autorizado y proteger la infraestructura empresarial.

VULN-M009: Bind Shell Backdoor Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) tiene una vulnerabilidad de Bind Shell Backdoor Detection que permite acceso no autenticado a un shell.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad, integridad y disponibilidad de los datos y sistemas, pudiendo causar daños reputacionales significativos debido a un posible control total por atacantes.

Urgencia: Crítica. La facilidad de explotación, con un atacante capaz de obtener acceso root inmediato sin autenticación, representa un riesgo extremo de compromiso total del sistema y movimiento lateral en la red, exigiendo acción inmediata.

Acción: Verificar si el host ha sido comprometido y reinstalar el sistema si es necesario.

Análisis Técnico

- **Nombre:** Bind Shell Backdoor Detection
- **ID del Plugin:** 51988
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/1524/wild_shell)

Nessus detectó un shell escuchando en el puerto TCP 1524 sin autenticación, permitiendo la ejecución remota de comandos; la salida del comando 'id' confirmó acceso con privilegios de root (uid=0), indicando que un atacante puede tomar control completo del sistema Linux Ubuntu 8.04 con kernel 2.6, ejecutar código arbitrario y potencialmente escalar privilegios o propagarse en la red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. Contención: Aislar inmediatamente el host de la red para prevenir acceso no autorizado.
2. Corrección: Reinstalar el sistema operativo desde una fuente confiable y aplicar configuraciones seguras.
3. Verificación: Realizar un escaneo post-remediación con Nessus u otras herramientas para confirmar la eliminación del backdoor.
4. Prevención: Implementar monitoreo continuo de puertos y servicios, y reforzar las políticas de seguridad para evitar configuraciones inseguras.

Conclusión: La presencia de este backdoor otorga control total a atacantes y exige su eliminación inmediata para mitigar el riesgo crítico de compromiso del sistema y la red.

VULN-M010: VNC Server 'password' Password

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) tiene una vulnerabilidad crítica en el servicio VNC (tcp/5900) donde se utiliza una contraseña débil 'password', permitiendo acceso no autorizado.

Riesgo para el Negocio: Un atacante podría comprometer la confidencialidad, integridad y disponibilidad del sistema, lo que podría resultar en pérdida de datos, interrupción del servicio y daño reputacional para la organización.

Urgencia: Crítica. La vulnerabilidad es fácilmente explotable de forma remota sin autenticación, permitiendo a un atacante tomar control total del sistema inmediatamente, lo que podría servir como punto de entrada para movimientos laterales en la red y otros ataques más amplios.

Acción: Asegurar el servicio VNC con una contraseña fuerte y compleja.

Análisis Técnico

- **Nombre:** VNC Server 'password' Password
- **ID del Plugin:** 61708
- **Severidad:** Crítica
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5900/vnc)

La vulnerabilidad surge porque el servidor VNC está configurado con la contraseña predeterminada 'password', que es extremadamente débil y fácil de adivinar. Nessus pudo autenticarse exitosamente usando esta contraseña, demostrando que un atacante remoto podría establecer una conexión VNC, obtener acceso gráfico al sistema y ejecutar comandos arbitrarios, comprometiendo completamente la seguridad del host Linux.

Puntuación de Riesgo:
- **Factor de Riesgo:** Critical
- **Puntuación Base CVSS v2.0:** 10.0 ((CVSS2\#AV:N/AC:L/Au:N/C:C/I:C/A:C))

Acciones Recomendadas

1. Contención: Deshabilitar inmediatamente el servicio VNC si no es esencial o restringir el acceso a redes de confianza mediante firewalls.
2. Corrección: Cambiar la contraseña del servicio VNC a una contraseña fuerte y única que cumpla con las políticas de seguridad, utilizando al menos 12 caracteres con una mezcla de mayúsculas, minúsculas, números y símbolos.
3. Verificación: Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que la contraseña ha sido fortalecida y que el acceso no autorizado ya no es posible.
4. Prevención: Implementar políticas de gestión de contraseñas, realizar auditorías regulares de seguridad, y considerar el uso de autenticación multifactor o alternativas más seguras como SSH para acceso remoto.

Conclusión: La debilidad en la contraseña de VNC expone el sistema a un control total no autorizado, exigiendo una corrección inmediata para mitigar el riesgo crítico de compromiso empresarial.

Vulnerabilidades Altas

VULN-B006: SNMP Agent Default Community Name (public)

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic tiene la vulnerabilidad SNMP Agent Default Community Name (public) en el puerto udp/161/snmp.

Riesgo para el Negocio: Un atacante puede acceder a información confidencial o modificar configuraciones del sistema, comprometiendo la integridad y confidencialidad de los datos, lo que podría llevar a interrupciones operativas y daños reputacionales.

Urgencia: Alta. La vulnerabilidad es fácil de explotar con herramientas comunes y permite acceso no autorizado que podría usarse como punto de entrada para ataques más avanzados, aunque no otorga control inmediato total, su corrección es urgente para prevenir escaladas de privilegios y movimientos laterales en la red.

Acción: Cambiar la cadena de comunidad predeterminada de SNMP o deshabilitar el servicio si no es necesario.

Análisis Técnico

- **Nombre:** SNMP Agent Default Community Name (public)
- **ID del Plugin:** 41028
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (udp/161/snmp)

El servidor SNMP remoto responde a la cadena de comunidad predeterminada 'public', lo que permite a un atacante adivinar y utilizar esta credencial para consultar o modificar información del sistema a través del protocolo SNMP en el puerto UDP 161, exponiendo datos sensibles y permitiendo posibles cambios en la configuración si los permisos lo permiten.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 5.2
- **EPSS Score:** 0.9233

Acciones Recomendadas

1. Contención: Filtrar el tráfico UDP entrante al puerto 161 usando firewalls para restringir el acceso no autorizado inmediatamente.
2. Corrección: Deshabilitar el servicio SNMP en el host si no se utiliza, o cambiar la cadena de comunidad predeterminada a una más segura y compleja.
3. Verificación: Realizar un escaneo de vulnerabilidades después de los cambios para confirmar que el servicio ya no responde a cadenas predeterminadas y validar la configuración.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de cadenas de comunidad predeterminadas en SNMP y realizar auditorías regulares para detectar configuraciones inseguras.

Conclusión: La exposición de la cadena de comunidad predeterminada en SNMP representa un riesgo alto de compromiso de datos y requiere acción inmediata para mitigar posibles accesos no autorizados y proteger la integridad del sistema.

VULN-B007: Drupal Database Abstraction API SQLi

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) ejecuta Drupal con una vulnerabilidad de inyección SQL en la API de abstracción de base de datos, permitiendo ejecución arbitraria de SQL.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de los datos, pudiendo resultar en escalada de privilegios o ejecución remota de código, lo que podría dañar la reputación y la disponibilidad del servicio.

Urgencia: Alta. La vulnerabilidad es fácilmente explotable con herramientas como Metasploit, tiene un alto riesgo de compromiso directo del sistema y puede servir como punto de entrada para ataques más amplios en la red, requiriendo atención prioritaria.

Acción: Actualizar Drupal a la versión 7.32 o superior.

Análisis Técnico

- **Nombre:** Drupal Database Abstraction API SQLi
- **ID del Plugin:** 78515
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/80/www)

La vulnerabilidad surge de un fallo en la API de abstracción de base de datos de Drupal, donde solicitudes manipuladas, como la enviada en el plugin_output (por ejemplo, name[0;SELECT+@version;#]=0), permiten inyectar y ejecutar código SQL arbitrario. Esto se evidencia en los errores de conversión de tipos y advertencias mostradas, como 'Array to string conversion', que confirman la explotación exitosa y podrían llevar a la ejecución de comandos PHP o acceso no autorizado a la base de datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 7.4

- **EPSS Score:** 0.9432

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor afectado de la red para prevenir explotaciones adicionales.
2. Corrección: Aplicar la actualización a Drupal 7.32 o una versión posterior para parchear la vulnerabilidad.
3. Verificación: Realizar pruebas de penetración o escaneos post-parche para confirmar que la vulnerabilidad ha sido mitigada.
4. Prevención: Implementar controles de entrada de datos y WAFs para detectar y bloquear intentos de inyección SQL en el futuro.

Conclusión: La alta explotabilidad de esta vulnerabilidad en Drupal amenaza directamente la integridad del sistema y exige una actualización inmediata para evitar compromisos severos.

VULN-B008: Drupal Database Abstraction API SQLi

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) ejecuta Drupal con una vulnerabilidad de inyección SQL en la API de abstracción de base de datos, permitiendo ejecución arbitraria de SQL.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de los datos, permitiendo a atacantes acceder o modificar información sensible, y potencialmente causar daño reputacional debido a la exposición de datos.

Urgencia: Alta. La vulnerabilidad es fácilmente explotable con herramientas como Metasploit, tiene un alto riesgo de escalada de privilegios y ejecución remota de código, lo que podría conducir a un compromiso completo del sistema y servir como punto de entrada para ataques adicionales en la red.

Acción: Actualizar Drupal a la versión 7.32 o superior.

Análisis Técnico

- **Nombre:** Drupal Database Abstraction API SQLi
- **ID del Plugin:** 78515
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

La vulnerabilidad se debe a un fallo en la API de abstracción de base de datos de Drupal, donde solicitudes manipuladas, como la enviada por Nessus en el POST a /drupal/, inyectan código SQL malicioso. Esto se evidencia en el plugin_output, que muestra errores como 'mb_strlen() expects parameter 1 to be string, array given', indicando que el parámetro 'name' es tratado como un array en lugar de una cadena, permitiendo la ejecución de consultas SQL arbitrarias como 'SELECT @version', lo que puede resultar en acceso no autorizado a la base de datos y potencial ejecución de código PHP remoto.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 7.4
- **EPSS Score:** 0.9432

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor afectado de la red para prevenir explotaciones adicionales.
2. Corrección: Aplicar la actualización a Drupal 7.32 o una versión posterior para parchear la vulnerabilidad.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que la actualización ha mitigado el riesgo.
4. Prevención: Implementar controles de entrada de datos, como sanitización y uso de consultas preparadas, y establecer un programa de gestión de parches regular para evitar vulnerabilidades similares en el futuro.

Conclusión: La vulnerabilidad de inyección SQL en Drupal representa un alto riesgo de compromiso del sistema y debe ser corregida inmediatamente para proteger la integridad de los datos y prevenir accesos no autorizados.

VULN-B009: Drupal Database Abstraction API SQLi

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) ejecuta Drupal con una vulnerabilidad de inyección SQL en la API de abstracción de base de datos, permitiendo ejecución arbitraria de SQL.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de los datos, permitiendo a atacantes acceder o modificar información sensible, y potencialmente escalar privilegios para ejecutar código remoto, lo que podría dañar la reputación de la organización.

Urgencia: Alta. La vulnerabilidad es fácilmente explotable con herramientas como Metasploit y tiene un alto riesgo de compromiso directo del sistema, incluyendo ejecución remota de código, lo que la convierte en una prioridad inmediata para mitigar y prevenir movimientos laterales en la red.

Acción: Actualizar Drupal a la versión 7.32 o superior.

Análisis Técnico

- **Nombre:** Drupal Database Abstraction API SQLi
- **ID del Plugin:** 78515
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9080/www)

La vulnerabilidad se debe a una falla en la API de abstracción de base de datos de Drupal, que no sanitiza adecuadamente las entradas del usuario, permitiendo inyecciones SQL a través de solicitudes POST manipuladas, como se demostró con la explotación de Nessus que inyectó código SQL para recuperar la versión de la base de datos, resultando en errores de conversión de tipos y ejecución arbitraria de consultas que pueden llevar a la exposición de datos o ejecución de código PHP.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 7.4
- **EPSS Score:** 0.9432

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor afectado de la red para prevenir explotaciones adicionales.
2. Corrección: Aplicar la actualización a Drupal 7.32 o una versión posterior para parchear la vulnerabilidad.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que la actualización fue exitosa y no hay residuos de explotación.
4. Prevención: Implementar controles de entrada de datos, como validación y sanitización, y establecer procesos regulares de parcheo para mantener el software actualizado.

Conclusión: La vulnerabilidad de inyección SQL en Drupal representa un alto riesgo de compromiso del sistema y exige una actualización inmediata para proteger los datos y prevenir accesos no autorizados.

VULN-B010: Drupal Database Abstraction API SQLi

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) ejecuta Drupal con una vulnerabilidad de inyección SQL en la API de abstracción de base de datos, permitiendo ejecución arbitraria de SQL.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de los datos, permitiendo a atacantes acceder o modificar información sensible, y potencialmente causar daño reputacional si se explota.

Urgencia: Alta. La vulnerabilidad es fácilmente explotable con herramientas como Metasploit y puede conducir a ejecución remota de código o escalada de privilegios, representando un riesgo inmediato de compromiso del sistema y movimiento lateral en la red.

Acción: Actualizar Drupal a la versión 7.32 o superior.

Análisis Técnico

- **Nombre:** Drupal Database Abstraction API SQLi
- **ID del Plugin:** 78515
- **Severidad:** Alta

- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

La vulnerabilidad se debe a un fallo en la API de abstracción de base de datos de Drupal, donde las solicitudes manipuladas, como la enviada en el plugin_output, inyectan código SQL malicioso a través de parámetros no sanitizados, lo que resulta en errores como conversiones de tipo y ejecución de consultas arbitrarias, evidenciado por la salida que incluye advertencias de funciones como mb_strlen y escapeLike, confirmando la explotación exitosa y el potencial para acceso no autorizado a la base de datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 7.4
- **EPSS Score:** 0.9432

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor afectado de la red para prevenir explotaciones adicionales.
2. Corrección: Aplicar la actualización a Drupal 7.32 o una versión posterior para parchear la vulnerabilidad.
3. Verificación: Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que la actualización ha mitigado el riesgo.
4. Prevención: Implementar prácticas de desarrollo seguro, como la validación de entradas y el uso de consultas parametrizadas, para evitar futuras inyecciones SQL.

Conclusión: La alta explotabilidad de esta vulnerabilidad de inyección SQL en Drupal amenaza directamente la integridad del sistema y exige una actualización inmediata para evitar compromisos severos.

VULN-M011: rlogin Service Detection

Resumen Ejecutivo

Problema: El servicio rlogin está ejecutándose en el host 192.168.122.29 (METASPLOITABLE), lo que representa la vulnerabilidad rlogin Service Detection debido a la transmisión de datos en texto claro.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al permitir el robo de credenciales y la integridad al facilitar accesos no autenticados, lo que podría resultar en pérdida de datos y daño reputacional.

Urgencia: Alta. La facilidad de explotación mediante herramientas como Metasploit y el potencial para un compromiso directo del sistema, incluyendo la posibilidad de movimientos laterales en la red, justifican una acción prioritaria para mitigar riesgos inmediatos.

Acción: Deshabilitar el servicio rlogin y reemplazarlo con SSH para asegurar las comunicaciones.

Análisis Técnico

- **Nombre:** rlogin Service Detection
- **ID del Plugin:** 10205
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/513/rlogin)

El servicio rlogin opera en el puerto TCP/513 y transmite datos, incluyendo credenciales de inicio de sesión, en texto claro, lo que permite a un atacante realizar ataques man-in-the-middle para interceptar información sensible. Adicionalmente, la vulnerabilidad puede ser explotada mediante adivinación de números de secuencia TCP o suplantación de IP, facilitando el bypass de autenticación y el acceso no autorizado a través de archivos como .rhosts, lo que convierte privilegios limitados en control completo del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 6.7
- **EPSS Score:** 0.5006

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red para prevenir explotaciones activas.
2. Corrección: Comentar la línea 'login' en /etc/inetd.conf y reiniciar el proceso inetd, o deshabilitar completamente el servicio rlogin.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que el servicio está deshabilitado y no hay tráfico no cifrado.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de servicios no cifrados como rlogin, y promover el uso exclusivo de SSH con autenticación fuerte y monitoreo continuo.

Conclusión: La vulnerabilidad rlogin en METASPLOITABLE presenta un alto riesgo de compromiso del sistema y exige su corrección inmediata para proteger la confidencialidad e integridad de los datos.

VULN-M012: rsh Service Detection

Resumen Ejecutivo

Problema: El servicio rsh está ejecutándose en el host 192.168.122.29 (METASPLOITABLE), lo que representa la vulnerabilidad rsh Service Detection debido a la transmisión de datos en texto claro.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al permitir que atacantes intercepten credenciales, y la integridad al facilitar accesos no autenticados, lo que podría llevar a pérdida de datos y daño reputacional.

Urgencia: Alta. La facilidad de explotación con herramientas como Metasploit y el alto riesgo de compromiso directo del sistema, incluyendo la posibilidad de movimiento lateral en la red, justifican una acción prioritaria para mitigar amenazas inmediatas.

Acción: Deshabilitar el servicio rsh comentando la línea correspondiente en /etc/inetd.conf y reiniciando el proceso inetd.

Análisis Técnico

- **Nombre:** rsh Service Detection
- **ID del Plugin:** 10245
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/514/rsh)

El servicio rsh opera sobre el puerto TCP/514 y transmite toda la información, incluidas las credenciales de inicio de sesión, en texto claro, lo que permite a un atacante man-in-the-middle capturar datos sensibles. Además, la autenticación débil basada en archivos .rhosts o rhosts.equiv puede ser explotada para obtener acceso no autorizado sin contraseña, y si el host es vulnerable a la suposición de números de secuencia TCP o spoofing IP, se puede eludir por completo la autenticación, facilitando compromisos completos del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 6.7
- **EPSS Score:** 0.5006

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red para prevenir explotaciones activas.
2. Corrección: Deshabilitar el servicio rsh editando /etc/inetd.conf y reiniciando inetd, o eliminarlo completamente del sistema.
3. Verificación: Realizar un escaneo de puertos para confirmar que el servicio rsh ya no está activo y probar el acceso seguro mediante SSH.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de servicios no cifrados como rsh, y promover el uso exclusivo de SSH con autenticación fuerte y cifrado.

Conclusión: La ejecución del servicio rsh en METASPLOITABLE plantea un alto riesgo de compromiso del sistema y exige su deshabilitación inmediata para proteger la confidencialidad e integridad de los datos.

VULN-M013: Apache Tomcat AJP Connector Request Injection (Ghostcat)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) ejecuta Apache Tomcat con una vulnerabilidad de inyección de solicitudes en el conector AJP (Ghostcat), permitiendo la lectura de archivos y posible ejecución remota de código.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al exponer archivos sensibles del servidor web y amenaza la integridad y disponibilidad si se logra la ejecución remota de código, lo que podría resultar en pérdida de datos, interrupción del servicio y daño reputacional.

Urgencia: Crítica. La vulnerabilidad tiene un CVSS de 9.8, es fácilmente explotable de forma remota sin autenticación y puede conducir a un compromiso completo del sistema, incluyendo la posibilidad de movimiento lateral en la red, lo que exige una acción inmediata para mitigar riesgos significativos.

Acción: Actualizar el servidor Tomcat a la versión 7.0.100, 8.5.51, 9.0.31 o superior y configurar el conector AJP para requerir autorización.

Análisis Técnico

- **Nombre:** Apache Tomcat AJP Connector Request Injection (Ghostcat)
- **ID del Plugin:** 134862
- **Severidad:** Alta
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/8009/ajp13)

La vulnerabilidad en el conector AJP de Apache Tomcat permite a un atacante remoto inyectar solicitudes maliciosas para leer archivos arbitrarios, como se demuestra en la salida del plugin donde se accede a /WEB-INF/web.xml, lo que podría escalar a la inclusión de archivos y ejecución de código JSP si se permite la carga de archivos, explotando debilidades en el manejo de solicitudes AJP que no validan adecuadamente las entradas.

Puntuación de Riesgo:
- **Factor de Riesgo:** High
- **Puntuación Base CVSS v3.0:** 9.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 7.5 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:P))
- **VPR Score:** 8.9
- **EPSS Score:** 0.9446

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor afectado de la red para prevenir explotaciones adicionales.
2. Corrección: Aplicar las actualizaciones de Tomcat a las versiones seguras especificadas y modificar la configuración del AJP para incluir autenticación.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que la vulnerabilidad ha sido mitigada y no hay residuos de explotación.
4. Prevención: Implementar monitoreo continuo de la red, revisar y endurecer las configuraciones de seguridad de todos los servidores Tomcat, y capacitar al personal en prácticas de seguridad para evitar futuras vulnerabilidades.

Conclusión: La vulnerabilidad Ghostcat en Tomcat representa un riesgo crítico que podría llevar a un compromiso total del sistema y debe ser abordada de inmediato mediante actualización y configuración segura para proteger los activos empresariales.

Vulnerabilidades Medias

VULN-B011: TLS Version 1.0 Protocol Detection

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) presenta la vulnerabilidad TLS Version 1.0 Protocol Detection en el servicio SMTP (puerto 25), que utiliza una versión obsoleta de TLS con deficiencias criptográficas.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de las comunicaciones de correo electrónico, permitiendo a atacantes interceptar datos sensibles, lo que podría resultar en pérdida de información y daño reputacional para la organización.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, el uso de TLS 1.0 viola estándares de cumplimiento como PCI DSS y aumenta el riesgo de fugas de datos, justificando una corrección prioritaria en el corto plazo para evitar posibles incidentes de seguridad.

Acción: Habilitar soporte para TLS 1.2 y 1.3, y deshabilitar TLS 1.0 en el servicio SMTP.

Análisis Técnico

- **Nombre:** TLS Version 1.0 Protocol Detection
- **ID del Plugin:** 104743
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el host BEE-BOX con sistema operativo Linux Kernel 2.6.24-16-generic acepta conexiones cifradas utilizando TLSv1, como se indica en la salida del plugin 'TLSv1 is enabled and the server supports at least one cipher'. TLS 1.0 contiene fallos de diseño criptográfico conocidos, como vulnerabilidades a ataques BEAST y POODLE, que podrían permitir a un atacante descifrar tráfico en condiciones específicas de red, comprometiendo la integridad y confidencialidad de las comunicaciones de correo.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red de producción si es posible, o implementar reglas de firewall para restringir el acceso al puerto 25 solo a direcciones IP autorizadas.
2. Corrección: Configurar el servicio SMTP para deshabilitar TLS 1.0 y habilitar exclusivamente TLS 1.2 o superior, utilizando cifrados fuertes como AES-GCM.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que TLS 1.0 está deshabilitado y que solo se admiten versiones seguras de TLS.
4. Prevención: Establecer políticas de seguridad que exijan el uso de TLS 1.2 o superior en todos los servicios, realizar auditorías periódicas de configuración, y capacitar al personal en mejores prácticas criptográficas.

Conclusión: El uso de TLS 1.0 en el servicio SMTP representa un riesgo medio que amenaza la confidencialidad de los datos y el cumplimiento normativo, requiriendo su corrección inmediata para proteger las comunicaciones de la organización.

VULN-B012: TLS Version 1.0 Protocol Detection

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) presenta la vulnerabilidad TLS Version 1.0 Protocol Detection, que permite el uso de una versión obsoleta de TLS.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de los datos transmitidos, permitiendo a atacantes interceptar información sensible, y dañar la reputación de la organización al incumplir estándares de seguridad como PCI DSS.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle y no conduce a un compromiso directo inmediato, el riesgo de fuga de datos y el incumplimiento normativo justifican una corrección prioritaria en el corto plazo para evitar posibles brechas de seguridad.

Acción: Habilitar el soporte para TLS 1.2 y 1.3, y deshabilitar TLS 1.0 en el servicio afectado.

Análisis Técnico

- **Nombre:** TLS Version 1.0 Protocol Detection
- **ID del Plugin:** 104743
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto tcp/443 del host BEE-BOX, que ejecuta Linux Kernel 2.6.24-16-generic, acepta conexiones cifradas con TLSv1.0, una versión con deficiencias criptográficas conocidas, como vulnerabilidades a ataques como BEAST o POODLE, que podrían permitir a un atacante descifrar tráfico o realizar downgrade attacks, comprometiendo la integridad y confidencialidad de las comunicaciones, aunque las implementaciones modernas mitigan parcialmente estos problemas.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el tráfico hacia el puerto 443 si es crítico y monitorear actividades sospechosas.
2. Corrección: Configurar el servidor web para deshabilitar TLS 1.0 y habilitar solo TLS 1.2 y 1.3, utilizando cifrados fuertes como AES-GCM.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que TLS 1.0 está deshabilitado y validar la configuración con herramientas como sslyze.
4. Prevención: Implementar políticas de seguridad que exijan el uso de versiones TLS actualizadas y realizar auditorías periódicas para asegurar el cumplimiento continuo.

Conclusión: El soporte de TLS 1.0 en BEE-BOX representa un riesgo medio que debe abordarse prontamente para proteger la confidencialidad de los datos y cumplir con los requisitos normativos, mediante la actualización inmediata de la configuración TLS.

VULN-B013: TLS Version 1.0 Protocol Detection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad TLS Version 1.0 Protocol Detection en el puerto tcp/8443, utilizando una versión obsoleta de TLS.

Riesgo para el Negocio: Esto puede comprometer la confidencialidad de los datos transmitidos, permitiendo a atacantes interceptar información sensible, y dañar la reputación de la organización al no cumplir con estándares de seguridad como PCI DSS.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo inmediato, la debilidad criptográfica aumenta el riesgo de fugas de datos y podría servir como punto de entrada para ataques más avanzados, justificando una corrección prioritaria en el corto plazo.

Acción: Habilitar soporte para TLS 1.2 y 1.3, y deshabilitar TLS 1.0 en el servicio afectado.

Análisis Técnico

- **Nombre:** TLS Version 1.0 Protocol Detection
- **ID del Plugin:** 104743
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto 8443 acepta conexiones cifradas con TLSv1, que contiene fallos criptográficos conocidos, como vulnerabilidades a ataques BEAST o POODLE, lo que podría permitir a un atacante descifrar tráfico bajo condiciones específicas, aunque las implementaciones modernas mitigan parcialmente estos problemas; sin embargo, el uso continuado expone a riesgos de interceptación y no cumple con los estándares actuales de seguridad.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium

- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el tráfico al puerto 8443 si es crítico y monitorear actividades sospechosas.
2. Corrección: Configurar el servidor para deshabilitar TLS 1.0 y habilitar únicamente TLS 1.2 o superior, utilizando cifrados fuertes.
3. Verificación: Realizar pruebas de penetración y escaneos post-corrección para confirmar que TLS 1.0 está deshabilitado y no hay regresiones.
4. Prevención: Implementar políticas de seguridad que exijan el uso de versiones TLS actualizadas y realizar auditorías periódicas para detectar configuraciones obsoletas.

Conclusión: La presencia de TLS 1.0 en BEE-BOX representa un riesgo medio que debe abordarse prontamente para proteger la confidencialidad de los datos y cumplir con los requisitos regulatorios, evitando posibles brechas de seguridad.

VULN-B014: TLS Version 1.0 Protocol Detection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad TLS Version 1.0 Protocol Detection, que permite conexiones cifradas con una versión obsoleta de TLS.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de los datos transmitidos, permitiendo a atacantes interceptar información sensible, y dañar la reputación de la organización al no cumplir con estándares de seguridad como PCI DSS.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, el uso de TLS 1.0 viola regulaciones de cumplimiento y podría facilitar ataques de descifrado, por lo que debe abordarse en el corto plazo para mitigar riesgos de fuga de datos y evitar sanciones.

Acción: Habilitar soporte para TLS 1.2 y 1.3, y deshabilitar TLS 1.0 en el servicio afectado.

Análisis Técnico

- **Nombre:** TLS Version 1.0 Protocol Detection
- **ID del Plugin:** 104743
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto tcp/9443 acepta conexiones cifradas con TLSv1, lo que indica que utiliza protocolos criptográficos antiguos con vulnerabilidades conocidas, como BEAST o POODLE, que pueden ser explotados en ataques de intermediario para descifrar tráfico; aunque las implementaciones modernas

mitigan algunos problemas, la falta de soporte para versiones más seguras como TLS 1.2 o 1.3 aumenta el riesgo de interceptación no autorizada y compromiso de la integridad de los datos en tránsito.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red de producción si es crítico y monitorear el tráfico para detectar actividades sospechosas.
2. **Corrección:** Configurar el servidor web para deshabilitar TLS 1.0 y habilitar exclusivamente TLS 1.2 o superior, utilizando cifrados fuertes como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que TLS 1.0 está deshabilitado y validar el cumplimiento con herramientas como OpenSSL o Nmap.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de protocolos TLS actualizados en todos los servicios y realizar auditorías periódicas para asegurar el cumplimiento continuo.

Conclusión: El soporte de TLS 1.0 en BEE-BOX representa un riesgo medio que debe corregirse prontamente para proteger la confidencialidad de los datos y evitar incumplimientos regulatorios.

VULN-B015: Apache mod_status /server-status Information Disclosure

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Apache en Linux Kernel 2.6.24-16-generic tiene la vulnerabilidad Apache mod_status /server-status Information Disclosure que permite la divulgación de información del servidor.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al exponer datos sensibles del servidor, lo que podría facilitar ataques dirigidos y dañar la reputación de la organización si se explota.

Urgencia: Media. La explotación es sencilla y remota sin autenticación, pero solo resulta en una fuga de información limitada que no compromete directamente la integridad o disponibilidad; sin embargo, puede ser un paso inicial para ataques más graves y debe abordarse prontamente para mitigar riesgos.

Acción: Actualizar la configuración de Apache para deshabilitar mod_status o restringir el acceso a hosts específicos.

Análisis Técnico

- **Nombre:** Apache mod_status /server-status Information Disclosure
- **ID del Plugin:** 10677
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro

- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/80/www)

Nessus explotó la vulnerabilidad enviando una solicitud HTTP a http://192.168.122.187/server-status, lo que permitió recuperar información detallada como hosts actuales, solicitudes en proceso, número de trabajadores y utilización de CPU, exponiendo datos internos del servidor sin necesidad de autenticación, lo que facilita el reconocimiento por parte de atacantes.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Restringir inmediatamente el acceso a /server-status mediante reglas de firewall o listas de control de acceso.
2. **Corrección:** Modificar el archivo de configuración de Apache (e.g., httpd.conf) para deshabilitar mod_status o limitar el acceso con directivas como 'Require ip'.
3. **Verificación:** Realizar pruebas de penetración o escaneos con herramientas como Nessus para confirmar que el acceso a /server-status está bloqueado.
4. **Prevención:** Implementar revisiones periódicas de configuración y monitoreo continuo para detectar y prevenir exposiciones similares en el futuro.

Conclusión: La divulgación de información a través de mod_status representa un riesgo de confidencialidad que debe mitigarse rápidamente para proteger los datos del servidor y prevenir explotaciones adicionales.

VULN-B016: Apache mod_status /server-status Information Disclosure

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Apache en Linux Kernel 2.6.24-16-generic tiene la vulnerabilidad Apache mod_status /server-status Information Disclosure que permite la divulgación de información del servidor.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al exponer datos sensibles del servidor, lo que podría ser utilizado por atacantes para planificar ataques más avanzados y dañar la reputación de la organización.

Urgencia: Media. La explotación es sencilla y no requiere autenticación, permitiendo a atacantes remotos acceder a información crítica del servidor, aunque no conduce directamente a un compromiso total, sí facilita la recopilación de inteligencia para ataques posteriores, por lo que debe abordarse prontamente para mitigar riesgos de escalada.

Acción: Actualizar la configuración de Apache para deshabilitar mod_status o restringir el acceso a hosts específicos.

Análisis Técnico

- **Nombre:** Apache mod_status /server-status Information Disclosure
- **ID del Plugin:** 10677
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

La vulnerabilidad se explota mediante una solicitud HTTP no autenticada a la URL '/server-status', como se demostró con la petición a https://192.168.122.187/server-status, lo que revela detalles operativos del servidor Apache, incluyendo hosts activos, solicitudes en proceso, estadísticas de workers y utilización de CPU, lo que proporciona a atacantes información valiosa para evaluar y potencialmente explotar otras debilidades en el sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Bloquear el acceso a '/server-status' en el firewall o mediante reglas de Apache de forma inmediata para prevenir divulgaciones adicionales.
2. **Corrección:** Modificar el archivo de configuración de Apache (e.g., httpd.conf) para deshabilitar el módulo mod_status o configurar directivas como 'Location' para limitar el acceso solo a direcciones IP autorizadas.
3. **Verificación:** Realizar un escaneo de vulnerabilidades con herramientas como Nessus para confirmar que el acceso a '/server-status' ya no es posible y revisar los logs del servidor en busca de intentos de acceso no autorizados.
4. **Prevención:** Implementar revisiones periódicas de configuración y políticas de seguridad para asegurar que módulos similares estén adecuadamente restringidos, y capacitar al personal sobre mejores prácticas de hardening de servidores web.

Conclusión: La divulgación de información a través de mod_status en Apache representa un riesgo de confidencialidad que debe mitigarse rápidamente para proteger los datos del servidor y prevenir su uso en ataques más severos.

VULN-B017: HTTP TRACE / TRACK Methods Allowed

Resumen Ejecutivo

Problema: El servidor web en 192.168.122.187 (BEE-BOX) permite los métodos HTTP TRACE y TRACK, lo que constituye la vulnerabilidad HTTP TRACE / TRACK Methods Allowed.

Riesgo para el Negocio: Esta vulnerabilidad puede conducir a la divulgación de información confidencial, como encabezados HTTP, lo que podría ser explotado en ataques de cross-site tracing (XST) para comprometer la confidencialidad de los datos y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad tiene un riesgo medio debido a su facilidad de explotación remota sin autenticación, pero su impacto principal es la fuga de información en lugar de un compromiso directo del sistema; sin embargo, podría servir como un paso inicial para ataques más avanzados y debe abordarse prontamente para mitigar riesgos de seguridad.

Acción: Deshabilitar los métodos HTTP TRACE y TRACK en la configuración del servidor web.

Análisis Técnico

- **Nombre:** HTTP TRACE / TRACK Methods Allowed
- **ID del Plugin:** 11213
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/80/www)

El servidor Apache en 192.168.122.187 responde a solicitudes TRACE devolviendo un eco de la solicitud original, como se evidencia en la salida del plugin donde una solicitud TRACE resultó en una respuesta 200 OK que reflejaba los encabezados HTTP; esto permite a atacantes potenciales obtener información sensible, como cookies o tokens, a través de técnicas como XST, explotando que estos métodos están destinados solo para depuración y no deberían estar habilitados en entornos de producción.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 4.0
- **EPSS Score:** 0.524

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para bloquear solicitudes TRACE y TRACK en la red perimetral.
2. **Corrección:** Modificar el archivo de configuración de Apache (e.g., httpd.conf o archivos de virtualhost) añadiendo 'TraceEnable off' o usando reglas de reescritura como 'RewriteEngine on', 'RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)', 'RewriteRule . - [F]'.
3. **Verificación:** Realizar pruebas de penetración o escaneos con herramientas como Nessus para confirmar que los métodos están deshabilitados y no responden.
4. **Prevención:** Establecer políticas de seguridad que deshabiliten métodos HTTP innecesarios por defecto en todos los servidores web y realizar auditorías regulares.

Conclusión: La habilitación de métodos HTTP de depuración representa un riesgo medio para la confidencialidad y debe corregirse de inmediato para prevenir la exposición de información sensible y fortalecer la postura de seguridad general.

VULN-B018: HTTP TRACE / TRACK Methods Allowed

Resumen Ejecutivo

Problema: El servidor web en 192.168.122.187 (BEE-BOX) permite los métodos HTTP TRACE y TRACK, lo que constituye la vulnerabilidad HTTP TRACE / TRACK Methods Allowed.

Riesgo para el Negocio: Esta vulnerabilidad puede permitir a atacantes realizar ataques de cross-site tracing (XST) para robar información confidencial, como cookies de autenticación, comprometiendo la confidencialidad de los datos y potencialmente dañando la reputación de la organización.

Urgencia: Media. La explotación de esta vulnerabilidad es relativamente sencilla y puede conducir a la divulgación de información sensible, aunque no permite una toma de control directa del sistema; sin embargo, su corrección es importante para prevenir posibles ataques de escalada y cumplir con estándares de seguridad.

Acción: Deshabilitar los métodos HTTP TRACE y TRACK en la configuración del servidor web.

Análisis Técnico

- **Nombre:** HTTP TRACE / TRACK Methods Allowed
- **ID del Plugin:** 11213
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servidor web Apache en la dirección IP 192.168.122.187 responde a solicitudes TRACE y TRACK, como se evidencia en la salida del plugin, donde una solicitud TRACE devuelve un eco completo de la solicitud original, incluyendo encabezados HTTP. Esto puede ser explotado en combinación con vulnerabilidades de cross-site scripting (XSS) para realizar ataques de XST, permitiendo a atacantes acceder a información confidencial como cookies, lo que podría facilitar el robo de sesiones o otros ataques.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 4.0
- **EPSS Score:** 0.524

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para bloquear solicitudes TRACE y TRACK en la red perimetral.
2. Corrección: Modificar la configuración de Apache añadiendo 'TraceEnable off' o usando reglas de reescritura como 'RewriteEngine on', 'RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)', 'RewriteRule . - [F]' en el archivo de configuración.
3. Verificación: Realizar un escaneo de vulnerabilidades después de los cambios para confirmar que los métodos están deshabilitados.
4. Prevención: Establecer políticas de seguridad que prohíban métodos HTTP innecesarios y realizar auditorías regulares de configuración.

Conclusión: La habilitación de métodos HTTP de depuración como TRACE y TRACK representa un riesgo de fuga de información que debe ser corregido para proteger la confidencialidad de los datos y mantener la integridad del servidor web.

VULN-B019: nginx < 1.17.7 Information Disclosure

Resumen Ejecutivo

Problema: El servidor web en 192.168.122.187 ejecuta nginx versión 1.4.0, afectado por la vulnerabilidad de divulgación de información nginx < 1.17.7.

Riesgo para el Negocio: Esta vulnerabilidad puede conducir a la exposición de información confidencial, comprometiendo la confidencialidad y potencialmente dañando la reputación de la organización si se explota.

Urgencia: Media. La vulnerabilidad tiene un riesgo moderado con un CVSS de 5.3, es fácilmente explotable a través de la red sin autenticación, pero solo resulta en divulgación de información limitada sin comprometer la integridad o disponibilidad; sin embargo, podría ser utilizada como un paso inicial para ataques más avanzados, por lo que debe abordarse en el corto plazo.

Acción: Actualizar nginx a la versión 1.17.7 o superior.

Análisis Técnico

- **Nombre:** nginx < 1.17.7 Information Disclosure
- **ID del Plugin:** 134220
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8080/www)

Según la salida del plugin, el servidor en http://192.168.122.187:8080/ está ejecutando nginx versión 1.4.0, que es anterior a la versión corregida 1.17.7. Esta vulnerabilidad permite a un atacante remoto acceder a información sensible a través del encabezado del servidor u otros vectores, lo que podría revelar detalles internos del sistema sin necesidad de autenticación, aunque no permite la ejecución de código o alteración de datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 2.2
- **EPSS Score:** 0.7147

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para restringir el acceso al puerto 8080 solo a direcciones IP autorizadas y monitorear el tráfico en busca de actividades sospechosas.
2. **Corrección:** Actualizar el software nginx a la versión 1.17.7 o posterior siguiendo los procedimientos estándar de actualización del sistema.
3. **Verificación:** Realizar un escaneo de vulnerabilidades después de la actualización para confirmar que la versión ha sido corregida y que no hay exposiciones residuales.

4. **Prevención:** Establecer políticas de gestión de parches regulares para mantener todo el software actualizado y realizar auditorías de seguridad periódicas para identificar y mitigar vulnerabilidades similares.

Conclusión: La vulnerabilidad de divulgación de información en nginx representa un riesgo moderado para la confidencialidad y debe corregirse prontamente para prevenir posibles filtraciones de datos y fortalecer la postura de seguridad general.

VULN-B020: nginx < 1.17.7 Information Disclosure

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) ejecuta nginx versión 1.4.0 en el puerto 8443, afectado por la vulnerabilidad de divulgación de información nginx < 1.17.7.

Riesgo para el Negocio: Esta vulnerabilidad puede conducir a la exposición de información confidencial, comprometiendo la confidencialidad y potencialmente dañando la reputación de la organización si los datos sensibles son accedidos por actores maliciosos.

Urgencia: Media. La vulnerabilidad tiene un CVSS v3 de 5.3, indicando un riesgo moderado con impacto en la confidencialidad, pero no afecta la integridad o disponibilidad. Es fácilmente explotable a través de la red sin requerir autenticación, lo que podría permitir a atacantes obtener información sensible, aunque no conduce directamente a un compromiso total del sistema; sin embargo, debe abordarse prontamente para prevenir posibles escaladas de privilegios o ataques adicionales.

Acción: Actualizar nginx a la versión 1.17.7 o superior.

Análisis Técnico

- **Nombre:** nginx < 1.17.7 Information Disclosure
- **ID del Plugin:** 134220
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

Según la salida del plugin, el servidor web en https://192.168.122.187:8443/ está ejecutando nginx versión 1.4.0, que es anterior a la versión corregida 1.17.7. Esta vulnerabilidad, identificada como CVE-2019-20372, permite la divulgación de información a través de respuestas del servidor, lo que podría exponer detalles internos del sistema o configuración a actores remotos sin necesidad de autenticación, facilitando la recolección de inteligencia para ataques posteriores.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 2.2
- **EPSS Score:** 0.7147

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y considerar restringir el acceso al puerto 8443 si es posible.
2. Corrección: Actualizar nginx a la versión 1.17.7 o posterior siguiendo los procedimientos estándar de parcheo.
3. Verificación: Validar que la actualización se haya aplicado correctamente verificando la versión del servidor y realizando pruebas para asegurar que la vulnerabilidad esté mitigada.
4. Prevención: Implementar un programa de gestión de vulnerabilidades para mantener el software actualizado y realizar escaneos regulares de seguridad.

Conclusión: La vulnerabilidad de divulgación de información en nginx representa un riesgo moderado para la confidencialidad y exige una actualización inmediata para proteger los datos sensibles y prevenir posibles explotaciones.

VULN-B021: TLS Version 1.1 Deprecated Protocol

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con sistema operativo Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad TLS Version 1.1 Deprecated Protocol en el puerto tcp/8443.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de los datos transmitidos, permitiendo a atacantes interceptar información sensible, y dañar la reputación de la organización al no cumplir con estándares de seguridad modernos.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero el uso de TLS 1.1 expone a riesgos de interceptación de datos y no es compatible con navegadores principales, lo que podría afectar la disponibilidad del servicio y facilitar ataques de escalada si se combina con otras vulnerabilidades.

Acción: Habilitar soporte para TLS 1.2 y/o 1.3 y deshabilitar TLS 1.1 en el servicio afectado.

Análisis Técnico

- **Nombre:** TLS Version 1.1 Deprecated Protocol
- **ID del Plugin:** 157288
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto 8443 acepta conexiones cifradas con TLSv1.1, un protocolo obsoleto que carece de soporte para suites de cifrado modernas y seguras, como aquellas que utilizan modos de cifrado autenticado (GCM). Esto permite que un atacante, en un escenario de man-in-the-middle, pueda forzar el uso de cifrados débiles o explotar vulnerabilidades conocidas en TLS 1.1 para descifrar el tráfico, comprometiendo la confidencialidad e integridad de los datos transmitidos. La salida del plugin confirma que TLSv1.1 está habilitado y al menos un cifrado es soportado, indicando una exposición directa a estos riesgos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de explotación y aislar temporalmente el host si se identifica actividad sospechosa.
2. **Corrección:** Configurar el servicio para deshabilitar TLS 1.1 y habilitar exclusivamente TLS 1.2 o superior, utilizando suites de cifrado fuertes como AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que TLS 1.1 está deshabilitado y que el servicio opera correctamente con protocolos seguros.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de TLS 1.2 o superior en todos los servicios, y realizar auditorías periódicas para asegurar el cumplimiento.

Conclusión: El soporte de TLS 1.1 en BEE-BOX representa un riesgo medio para la confidencialidad de los datos y debe corregirse prontamente para evitar interceptaciones no autorizadas y cumplir con los estándares de seguridad actuales.

VULN-B022: SSL Certificate Expiry

Resumen Ejecutivo

Problema: El servidor en 192.168.122.187 (BEE-BOX) tiene un certificado SSL expirado en el servicio SMTP, identificado como la vulnerabilidad SSL Certificate Expiry.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían dañar la reputación de la organización y exponer datos sensibles.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle, lo que podría llevar a la interceptación de correos electrónicos y otros datos, aunque no compromete directamente la confidencialidad o disponibilidad, sí representa un riesgo significativo que debe abordarse pronto para prevenir posibles escaladas.

Acción: Comprar o generar un nuevo certificado SSL y reemplazar el existente en el servidor.

Análisis Técnico

- **Nombre:** SSL Certificate Expiry
- **ID del Plugin:** 15901
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El certificado SSL para el servicio SMTP en el puerto 25 ha expirado, con fechas de validez del 28 de marzo de 2013 al 27 de abril de 2013, emitido por y para el sujeto con detalles como C=XX y CN=ubuntu.

Esto significa que las conexiones SSL/TLS ya no son consideradas seguras, ya que los clientes y servidores pueden rechazar o advertir sobre la conexión, permitiendo a atacantes realizar ataques man-in-the-middle para espiar o manipular el tráfico de correo sin ser detectados, aprovechando la falta de autenticación válida.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas y notificar a los usuarios sobre posibles riesgos en las comunicaciones.
2. Corrección: Adquirir un certificado SSL válido de una autoridad de certificación confiable e instalarlo en el servidor, asegurando que esté correctamente configurado.
3. Verificación: Realizar pruebas de conexión SSL/TLS usando herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado es válido y no expirado.
4. Prevención: Implementar procesos automatizados para monitorear y renovar certificados antes de su expiración, y educar al personal sobre las mejores prácticas de gestión de certificados.

Conclusión: El certificado SSL expirado en SMTP representa un riesgo medio que debe corregirse rápidamente para proteger la integridad de las comunicaciones y evitar posibles explotaciones.

VULN-B023: SSL Certificate Expiry

Resumen Ejecutivo

Problema: El servidor en 192.168.122.187 (BEE-BOX) tiene un certificado SSL expirado para el servicio tcp/443/www, identificado como SSL Certificate Expiry.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían alterar datos o dañar la reputación de la organización al mostrar advertencias de seguridad a los usuarios.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce directamente a un compromiso del sistema, pero aumenta el riesgo de interceptación de datos sensibles y afecta la confianza del usuario, por lo que debe abordarse en el corto plazo para mitigar posibles impactos operativos.

Acción: Comprar o generar un nuevo certificado SSL y reemplazar el existente en el servidor.

Análisis Técnico

- **Nombre:** SSL Certificate Expiry
- **ID del Plugin:** 15901
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic

- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El certificado SSL para el servicio en el puerto 443 ha expirado, con fechas de validez desde el 14 de abril de 2013 hasta el 13 de abril de 2018, lo que significa que ya no es considerado válido por los navegadores y clientes. Esto puede resultar en advertencias de seguridad para los usuarios, interrupciones en las conexiones HTTPS, y una mayor susceptibilidad a ataques como el downgrade de cifrado o la interceptación de tráfico, aunque no compromete directamente la confidencialidad o disponibilidad sin un ataque adicional.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y notificar a los usuarios sobre posibles problemas de conexión.
2. Corrección: Adquirir un certificado SSL válido de una autoridad de certificación confiable e instalarlo en el servidor, asegurando que las fechas de validez sean actuales.
3. Verificación: Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado esté correctamente implementado y no expire pronto.
4. Prevención: Establecer procesos automatizados para el monitoreo y renovación de certificados, y educar al personal sobre las mejores prácticas de gestión de certificados SSL.

Conclusión: El certificado SSL expirado en BEE-BOX representa un riesgo medio que debe corregirse prontamente para mantener la integridad de las comunicaciones y evitar daños a la reputación empresarial.

VULN-B024: SSL Certificate Expiry

Resumen Ejecutivo

Problema: El servidor en 192.168.122.187 (BEE-BOX) tiene un certificado SSL expirado en el puerto tcp/8443, identificado como SSL Certificate Expiry.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían alterar datos o dañar la reputación de la organización al mostrar advertencias de seguridad a los usuarios.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle activo, pero no conduce directamente a un compromiso del sistema; sin embargo, su corrección es urgente para prevenir posibles filtraciones de datos y mantener la confianza del usuario en los servicios SSL.

Acción: Comprar o generar un nuevo certificado SSL y reemplazar el existente en el servidor.

Análisis Técnico

- **Nombre:** SSL Certificate Expiry
- **ID del Plugin:** 15901

- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El certificado SSL del servidor en bee-box.bwapp.local expiró el 13 de abril de 2018, lo que significa que las conexiones SSL/TLS al puerto 8443 ya no son consideradas seguras por los navegadores y clientes; esto permite a atacantes realizar ataques man-in-the-middle para interceptar o manipular el tráfico cifrado, aunque no compromete directamente la confidencialidad o disponibilidad, sí debilita la integridad de las comunicaciones y puede resultar en advertencias que disuaden a los usuarios.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas en el puerto 8443 y considerar la desactivación temporal del servicio si es crítico.
2. Corrección: Adquirir un certificado SSL válido de una autoridad de certificación confiable e implementarlo en el servidor, asegurando que las fechas de validez sean actuales.
3. Verificación: Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado está correctamente instalado y no ha expirado.
4. Prevención: Establecer procesos automatizados para monitorear y renovar certificados SSL antes de su expiración, y educar al personal sobre las mejores prácticas de gestión de certificados.

Conclusión: El certificado SSL expirado en BEE-BOX representa un riesgo medio que debe abordarse prontamente para proteger la integridad de las comunicaciones y evitar daños reputacionales.

VULN-B025: SSL Certificate Expiry

Resumen Ejecutivo

Problema: El servidor en 192.168.122.187 (BEE-BOX) tiene un certificado SSL expirado para el servicio tcp/9443/www, identificado como SSL Certificate Expiry.

Riesgo para el Negocio: Un certificado SSL expirado puede permitir ataques man-in-the-middle, comprometiendo la integridad de los datos y dañando la reputación de la organización al mostrar advertencias de seguridad a los usuarios.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce directamente a un compromiso del sistema, pero podría facilitar la interceptación de datos sensibles. Debe abordarse en el corto plazo para mitigar riesgos de seguridad y mantener la confianza del usuario.

Acción: Comprar o generar un nuevo certificado SSL y reemplazar el existente en el servidor.

Análisis Técnico

- **Nombre:** SSL Certificate Expiry
- **ID del Plugin:** 15901
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El certificado SSL para el servicio en el puerto 9443 ha expirado, como se indica en los campos 'Not valid after: Apr 13 18:11:32 2018 GMT'. Esto significa que las conexiones SSL/TLS ya no son consideradas seguras por los navegadores y clientes, lo que puede resultar en advertencias de certificado inválido para los usuarios. Técnicamente, un certificado expirado no cifra las comunicaciones de manera fiable, permitiendo potencialmente a atacantes realizar ataques man-in-the-middle para espiar o manipular el tráfico, aunque no compromete directamente la confidencialidad o disponibilidad del servidor.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas y notificar a los usuarios sobre el certificado expirado hasta su corrección.
2. Corrección: Adquirir un nuevo certificado SSL de una autoridad de certificación confiable e instalarlo en el servidor, asegurando que esté configurado correctamente para el dominio bee-box.bwapp.local.
3. Verificación: Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado es válido y no expira pronto.
4. Prevención: Implementar un proceso automatizado de renovación de certificados y monitoreo proactivo para evitar futuras expiraciones, siguiendo las mejores prácticas de gestión de certificados.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

VULN-B026: SSL Weak Cipher Suites Supported

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Weak Cipher Suites Supported en el puerto tcp/25/smtp, que permite el uso de cifrados SSL débiles.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones al permitir que atacantes descifren datos transmitidos, lo que podría resultar en la exposición de información sensible y daño reputacional si se explota.

Urgencia: Media. La explotación requiere que el atacante esté en la misma red física y es más fácil en ese contexto, pero no conduce a un compromiso directo del sistema; sin embargo, la fuga de información confidencial justifica una corrección prioritaria en el corto plazo para mitigar riesgos de interceptación.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados débiles.

Análisis Técnico

- **Nombre:** SSL Weak Cipher Suites Supported
- **ID del Plugin:** 26928
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el puerto 25 soporta múltiples suites de cifrado SSL débiles, como EXP-RC2-CBC-MD5 y DES-CBC-SHA, que utilizan claves de cifrado de baja fuerza (<= 64 bits) y algoritmos obsoletos como RC4 y DES. Esto permite a un atacante realizar ataques de descifrado, especialmente en redes locales, comprometiendo la confidencialidad de los datos transmitidos al reducir la entropía criptográfica y facilitar la interceptación no autorizada.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de redes no confiables o implementar reglas de firewall para restringir el acceso al puerto 25 solo a direcciones IP autorizadas.
2. **Corrección:** Actualizar la configuración del servicio SMTP para deshabilitar los cifrados débiles listados, utilizando herramientas como OpenSSL para forzar el uso de suites modernas como TLS 1.2 o superiores con cifrados fuertes (e.g., AES-GCM).
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección con Nessus o herramientas similares para confirmar que los cifrados débiles ya no están soportados y validar la integridad de las comunicaciones.
4. **Prevención:** Establecer políticas de seguridad que exijan revisiones periódicas de configuraciones criptográficas y la adopción de mejores prácticas, como seguir las guías de NIST o CIS, para prevenir regresiones.

Conclusión: El soporte de cifrados SSL débiles en BEE-BOX representa un riesgo moderado de fuga de datos que debe abordarse prontamente para proteger la confidencialidad de las comunicaciones y mantener el cumplimiento normativo.

VULN-B027: SSL Weak Cipher Suites Supported

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Weak Cipher Suites Supported, que permite el uso de cifrados SSL débiles en el puerto tcp/443.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que un atacante podría descifrar comunicaciones sensibles, lo que podría llevar a la exposición de información privada y dañar la reputación de la organización.

Urgencia: Media. La explotación es más fácil si el atacante está en la misma red física, pero requiere un ataque man-in-the-middle activo; aunque no permite un compromiso directo del sistema, puede ser un paso inicial para ataques más avanzados y debe abordarse prontamente para mitigar riesgos de fuga de datos.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados SSL débiles.

Análisis Técnico

- **Nombre:** SSL Weak Cipher Suites Supported
- **ID del Plugin:** 26928
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto 443 soporta múltiples cifrados SSL débiles, como EXP-RC2-CBC-MD5 y DES-CBC-SHA, que utilizan claves de cifrado de baja fuerza (<= 64 bits) y algoritmos obsoletos como RC4 y DES, lo que facilita a un atacante realizar ataques de descifrado mediante fuerza bruta o man-in-the-middle, comprometiendo la confidencialidad de las comunicaciones sin afectar la integridad o disponibilidad del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de explotación y aislar temporalmente el host si es necesario.
2. **Corrección:** Reconfigurar el servidor web o aplicación para deshabilitar los cifrados débiles listados, utilizando solo suites modernas como TLS 1.2 o superiores con AES-GCM.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los cifrados débiles ya no están soportados.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados fuertes y realizar auditorías periódicas de configuración SSL/TLS.

Conclusión: Aunque el riesgo es medio, la presencia de cifrados SSL débiles en BEE-BOX debe corregirse rápidamente para proteger la confidencialidad de los datos y prevenir posibles explotaciones que podrían escalar a compromisos mayores.

VULN-B028: SSL Weak Cipher Suites Supported

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Weak Cipher Suites Supported, que permite el uso de cifrados SSL débiles en el puerto tcp/9443.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, permitiendo a atacantes descifrar comunicaciones sensibles, lo que podría resultar en fugas de información y daños reputacionales.

Urgencia: Media. La explotación es factible, especialmente en redes locales, con un impacto moderado en la confidencialidad, pero no permite compromisos directos del sistema o movimientos laterales; sin embargo, debe abordarse prontamente para mitigar riesgos de interceptación de datos.

Acción: Reconfigurar la aplicación afectada para deshabilitar el uso de cifrados SSL débiles.

Análisis Técnico

- **Nombre:** SSL Weak Cipher Suites Supported
- **ID del Plugin:** 26928
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto tcp/9443 soporta cifrados SSL débiles como EXP-RC2-CBC-MD5, EXP-RC4-MD5 y DES-CBC-SHA, que utilizan claves de cifrado de baja fuerza (<= 64 bits) y algoritmos obsoletos como RC2, RC4 y DES, lo que facilita a atacantes realizar ataques de fuerza bruta o man-in-the-middle para descifrar el tráfico SSL/TLS, comprometiendo la confidencialidad de las comunicaciones sin afectar la integridad o disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de redes no confiables para reducir el riesgo de explotación.
2. **Corrección:** Reconfigurar el servidor SSL/TLS para eliminar los cifrados débiles listados, utilizando solo suites modernas como TLS_AES_128_GCM_SHA256.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los cifrados débiles ya no están soportados.
4. **Prevención:** Implementar políticas de configuración de seguridad que prohíban el uso de cifrados obsoletos y realizar auditorías regulares de configuración SSL/TLS.

Conclusión: El soporte de cifrados SSL débiles en BEE-BOX representa un riesgo moderado para la confidencialidad de los datos y debe corregirse prontamente para prevenir posibles interceptaciones no autorizadas.

VULN-B029: SSL Certificate Signed Using Weak Hashing Algorithm

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Signed Using Weak Hashing Algorithm' en el puerto tcp/443, donde un certificado SSL utiliza el algoritmo de hash SHA-1, que es criptográficamente débil.

Riesgo para el Negocio: Esta vulnerabilidad compromete la integridad de las comunicaciones SSL/TLS, permitiendo a un atacante suplantar el servicio y realizar ataques de intermediario, lo que podría dañar la reputación de la organización y exponer datos sensibles.

Urgencia: Media. La explotación requiere un ataque de colisión activo y no conduce a un compromiso directo del sistema, pero facilita ataques de suplantación que podrían ser utilizados como paso inicial para compromisos más graves; debe abordarse en el corto plazo para mitigar riesgos de seguridad.

Acción: Contactar a la Autoridad de Certificación para reemitir el certificado SSL con un algoritmo de hash seguro como SHA-256 o superior.

Análisis Técnico

- **Nombre:** SSL Certificate Signed Using Weak Hashing Algorithm
- **ID del Plugin:** 35291
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto 443 de BEE-BOX emplea un certificado SSL firmado con SHA-1, un algoritmo vulnerable a ataques de colisión donde un atacante puede generar un certificado fraudulento con la misma firma digital. Esto permite la suplantación del servicio, comprometiendo la autenticidad y confidencialidad de las conexiones TLS. Aunque la explotación no es trivial y requiere condiciones específicas, como un ataque man-in-the-middle, el uso de SHA-1 viola las mejores prácticas criptográficas actuales, especialmente para certificados que expiran después de 2017, aumentando el riesgo de interceptación no autorizada.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.2
- **EPSS Score:** 0.0815

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas o intentos de suplantación.

2. Corrección: Reemplazar el certificado SSL actual con uno firmado con un algoritmo seguro (e.g., SHA-256) y actualizar la cadena de certificados.
3. Verificación: Utilizar herramientas como Nessus o OpenSSL para validar que el nuevo certificado cumple con los estándares criptográficos y no contiene hashes débiles.
4. Prevención: Implementar políticas que exijan el uso de algoritmos criptográficos fuertes en todos los certificados y realizar auditorías periódicas de seguridad SSL/TLS.

Conclusión: Aunque el riesgo es medio, la corrección de este certificado débil es esencial para proteger la integridad de las comunicaciones y prevenir posibles ataques de suplantación que podrían escalar a compromisos mayores.

VULN-B030: SSL Certificate Signed Using Weak Hashing Algorithm

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Signed Using Weak Hashing Algorithm' en el puerto tcp/8443, donde un certificado SSL utiliza el algoritmo de hash SHA-1, que es criptográficamente débil.

Riesgo para el Negocio: Esta vulnerabilidad compromete la integridad de las comunicaciones SSL/TLS, permitiendo a un atacante suplantar el servicio y realizar ataques de intermediario, lo que podría dañar la confianza del usuario y la reputación de la organización.

Urgencia: Media. La explotación requiere un ataque de colisión activo, como man-in-the-middle, y no conduce a un compromiso directo del sistema, pero podría ser utilizada como un paso inicial para ataques más severos si no se mitiga, justificando una corrección prioritaria en el corto plazo.

Acción: Contactar a la Autoridad de Certificación para reemitir el certificado SSL con un algoritmo de hash seguro, como SHA-256 o superior.

Análisis Técnico

- **Nombre:** SSL Certificate Signed Using Weak Hashing Algorithm
- **ID del Plugin:** 35291
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto 8443 del host BEE-BOX envía un certificado SSL firmado con SHA-1, un algoritmo vulnerable a ataques de colisión donde un atacante puede generar un certificado fraudulento con la misma firma digital, permitiendo la suplantación del servicio y el interceptación de comunicaciones encriptadas, aunque la explotación práctica depende de capacidades criptográficas avanzadas y un entorno de ataque activo.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))

- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.2
- **EPSS Score:** 0.0815

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas relacionadas con certificados SSL.
2. Corrección: Reemplazar el certificado actual con uno firmado con un algoritmo de hash fuerte, como SHA-256, y asegurar que toda la cadena de certificados cumpla con los estándares actuales.
3. Verificación: Utilizar herramientas como Nessus o OpenSSL para validar que el nuevo certificado no utiliza algoritmos débiles y realizar pruebas de penetración para confirmar la mitigación.
4. Prevención: Implementar políticas de gestión de certificados que exijan el uso de algoritmos criptográficos seguros y realizar auditorías periódicas para evitar recurrencias.

Conclusión: Aunque el riesgo es medio, la corrección de este certificado SSL débil es esencial para proteger la integridad de las comunicaciones y mantener la confianza en los servicios en línea.

VULN-B031: SSL Certificate Signed Using Weak Hashing Algorithm

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Signed Using Weak Hashing Algorithm' en el puerto tcp/9443, donde un certificado SSL utiliza el algoritmo de hash SHA-1, que es criptográficamente débil.

Riesgo para el Negocio: Esta vulnerabilidad compromete la integridad de las comunicaciones SSL/TLS, permitiendo a un atacante suplantar el servicio y realizar ataques de intermediario, lo que podría dañar la confianza del usuario y la reputación de la organización.

Urgencia: Media. Aunque la explotación requiere un ataque de intermediario activo y no conduce directamente a un compromiso del sistema, el uso de SHA-1 está obsoleto y puede facilitar ataques de colisión, aumentando el riesgo de suplantación en entornos sensibles; se recomienda abordarlo en el corto plazo para mitigar posibles vectores de ataque y cumplir con estándares de seguridad modernos.

Acción: Contactar a la Autoridad de Certificación para reemitir el certificado SSL utilizando un algoritmo de hash seguro como SHA-256 o superior.

Análisis Técnico

- **Nombre:** SSL Certificate Signed Using Weak Hashing Algorithm
- **ID del Plugin:** 35291
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto 9443 del host BEE-BOX emplea un certificado SSL firmado con SHA-1, un algoritmo vulnerable a ataques de colisión donde un atacante puede generar un certificado fraudulento con la misma firma digital. Esto permite la suplantación del servicio en un ataque man-in-the-middle, comprometiendo la autenticidad y confidencialidad de las comunicaciones. El certificado, válido hasta 2018, ya ha expirado, pero su presencia indica una configuración insegura que debe ser corregida para prevenir exploits potenciales.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.2
- **EPSS Score:** 0.0815

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar posibles ataques de intermediario y aislar temporalmente el servicio si se identifica actividad sospechosa.
2. Corrección: Reemplazar el certificado SSL actual con uno firmado con un algoritmo seguro como SHA-256, coordinando con la Autoridad de Certificación para su emisión e instalación.
3. Verificación: Utilizar herramientas como Nessus o OpenSSL para validar que el nuevo certificado no utiliza algoritmos débiles y realizar pruebas de penetración para asegurar la integridad de las comunicaciones.
4. Prevención: Implementar políticas de gestión de certificados que exijan el uso de algoritmos criptográficos fuertes, realizar auditorías periódicas de certificados SSL/TLS, y capacitar al personal en mejores prácticas de seguridad.

Conclusión: La debilidad del hash SHA-1 en el certificado SSL representa un riesgo moderado de suplantación que debe abordarse prontamente para proteger la integridad de las comunicaciones y mantener la confianza en los servicios de la organización.

VULN-B032: SSL Medium Strength Cipher Suites Supported (SWEET32)

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32) en el servicio SMTP en el puerto tcp/25.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones al permitir que atacantes descifren datos sensibles, lo que podría resultar en fugas de información y daño reputacional si se explota.

Urgencia: Media. La explotación requiere que el atacante esté en la misma red física y es más factible en entornos locales, pero el impacto potencial en la confidencialidad justifica una corrección prioritaria en el corto plazo para mitigar riesgos de interceptación de datos.

Acción: Reconfigurar la aplicación afectada para evitar el uso de suites de cifrado de fuerza media.

Análisis Técnico

- **Nombre:** SSL Medium Strength Cipher Suites Supported (SWEET32)
- **ID del Plugin:** 42873
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el host soporta suites de cifrado SSL de fuerza media, como DES-CBC3-MD5 y EDH-RSA-DES-CBC3-SHA, que utilizan claves de 64 a menos de 112 bits o el algoritmo 3DES. Esto facilita ataques de descifrado, especialmente en redes locales, donde un atacante podría realizar un ataque de birthday bound para romper el cifrado en un tiempo razonable, comprometiendo la integridad y confidencialidad de las comunicaciones de correo electrónico.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.2879

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de explotación y aislar el host si es necesario.
2. **Corrección:** Actualizar la configuración del servicio SMTP para deshabilitar las suites de cifrado de fuerza media y permitir solo cifrados fuertes como AES con claves de al menos 128 bits.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que las suites de cifrado débiles ya no están soportadas.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas de configuración SSL/TLS.

Conclusión: La vulnerabilidad SWEET32 en BEE-BOX amenaza la confidencialidad de las comunicaciones y debe ser corregida prontamente para prevenir posibles interceptaciones de datos sensibles.

VULN-B033: SSL Medium Strength Cipher Suites Supported (SWEET32)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) con sistema operativo Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32), que permite el uso de cifrados SSL de fuerza media.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que los cifrados débiles pueden ser descifrados por atacantes, lo que podría resultar en la exposición de información sensible y daños reputacionales.

Urgencia: Media. La explotación de esta vulnerabilidad requiere que el atacante esté en la misma red física y es más fácil de eludir en comparación con cifrados fuertes, pero aún representa un riesgo significativo de fuga de información si se aprovecha, justificando una corrección prioritaria en el corto plazo para mitigar posibles brechas de seguridad.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados de fuerza media.

Análisis Técnico

- **Nombre:** SSL Medium Strength Cipher Suites Supported (SWEET32)
- **ID del Plugin:** 42873
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

La vulnerabilidad surge porque el servicio en el puerto tcp/443 soporta suites de cifrado SSL de fuerza media, como DES-CBC3-MD5, EDH-RSA-DES-CBC3-SHA y DES-CBC3-SHA, que utilizan claves de 64 a menos de 112 bits o el algoritmo 3DES, lo que facilita a un atacante en la misma red física realizar ataques de fuerza bruta o de birthday para descifrar las comunicaciones, comprometiendo la confidencialidad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.2879

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y aislar temporalmente el host si es necesario.
2. Corrección: Reconfigurar el servicio SSL/TLS para deshabilitar los cifrados de fuerza media y permitir solo suites fuertes, como aquellas con AES y claves de al menos 128 bits.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección usando Nessus o herramientas similares para confirmar que los cifrados débiles ya no están soportados.
4. Prevención: Implementar políticas de seguridad que exijan el uso de cifrados fuertes en todos los servicios y realizar auditorías periódicas para asegurar el cumplimiento.

Conclusión: El soporte de cifrados de fuerza media en SSL representa un riesgo moderado de fuga de datos y debe corregirse prontamente para proteger la confidencialidad de la información y mantener la integridad de la infraestructura de seguridad.

VULN-B034: SSL Medium Strength Cipher Suites Supported (SWEET32)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) con sistema operativo Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32), que permite el uso de cifrados SSL de fuerza media.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que un atacante podría descifrar información sensible, lo que podría resultar en pérdida de datos y daño reputacional para la organización.

Urgencia: Media. La explotación requiere que el atacante esté en la misma red física y no conduce a un compromiso directo del sistema, pero la facilidad relativa de descifrado y el potencial de fuga de información justifican una corrección prioritaria en el corto plazo para mitigar riesgos de seguridad.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados de fuerza media.

Análisis Técnico

- **Nombre:** SSL Medium Strength Cipher Suites Supported (SWEET32)
- **ID del Plugin:** 42873
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto tcp/8443/www soporta suites de cifrado SSL de fuerza media, incluyendo EDH-RSA-DES-CBC3-SHA, ECDHE-RSA-DES-CBC3-SHA y DES-CBC3-SHA, que utilizan claves de 64 a menos de 112 bits o el algoritmo 3DES-CBC con 168 bits. Estos cifrados son vulnerables a ataques como SWEET32, que explotan la pequeña longitud de bloque en 3DES para realizar ataques de birthday bound, permitiendo a un atacante descifrar datos cifrados si pueden interceptar tráfico suficiente, lo que compromete la confidencialidad de las comunicaciones sin autenticación adicional requerida.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.2879

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y aislar el host si es necesario.
2. Corrección: Reconfigurar el servicio para deshabilitar los cifrados de fuerza media y habilitar solo suites fuertes como AES con claves de al menos 128 bits.
3. Verificación: Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que los cifrados vulnerables han sido eliminados.
4. Prevención: Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas de configuración SSL/TLS.

Conclusión: El soporte de cifrados de fuerza media en BEE-BOX representa un riesgo moderado para la confidencialidad de los datos y debe corregirse prontamente para prevenir posibles fugas de información y cumplir con estándares de seguridad robustos.

VULN-B035: SSL Medium Strength Cipher Suites Supported (SWEET32)

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32) en el puerto tcp/9443/www.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que cifrados de fuerza media pueden ser descifrados por atacantes en la misma red, lo que podría llevar a la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad tiene un CVSS3 de 7.5, indicando un alto impacto en la confidencialidad, pero su explotación requiere que el atacante esté en la misma red física, lo que limita la facilidad de explotación. Aunque no es inmediatamente explotable de forma remota, debe abordarse prontamente para prevenir posibles filtraciones de datos y evitar que sirva como punto de entrada para ataques más avanzados.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados de fuerza media.

Análisis Técnico

- **Nombre:** SSL Medium Strength Cipher Suites Supported (SWEET32)
- **ID del Plugin:** 42873
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto tcp/9443/www soporta suites de cifrado SSL de fuerza media, como DES-CBC3-MD5 y DES-CBC3-SHA, que utilizan claves de 64 a menos de 112 bits o el algoritmo 3DES. Estos cifrados son vulnerables a ataques como SWEET32, que explotan la debilidad en el tamaño de bloque de 64 bits para realizar ataques de birthday bound, permitiendo a un atacante en la misma red descifrar datos cifrados tras capturar una cantidad suficiente de tráfico, comprometiendo la confidencialidad de las comunicaciones sin autenticación requerida.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.2879

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar actividades sospechosas y considerar el aislamiento temporal del host si es necesario.
2. **Corrección:** Reconfigurar el servidor o aplicación para deshabilitar los cifrados de fuerza media, utilizando solo suites fuertes como AES con claves de al menos 128 bits.

3. **Verificación:** Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que los cifrados vulnerables han sido eliminados.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas para asegurar el cumplimiento con estándares criptográficos actualizados.

Conclusión: La vulnerabilidad SWEET32 en BEE-BOX representa un riesgo moderado para la confidencialidad de los datos y debe ser corregida prontamente para prevenir posibles filtraciones y fortalecer la postura de seguridad de la red.

VULN-B036: NTP ntpd Mode 7 Error Response Packet Loop Remote DoS

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) ejecuta una versión vulnerable de ntpd en Linux Kernel 2.6.24-16-generic, susceptible a NTP ntpd Mode 7 Error Response Packet Loop Remote DoS.

Riesgo para el Negocio: Esta vulnerabilidad puede causar una denegación de servicio, afectando la disponibilidad del servicio de tiempo y potencialmente interrumpiendo operaciones críticas que dependen de la sincronización horaria, lo que podría dañar la reputación si no se mitiga.

Urgencia: Media. La explotación es relativamente sencilla y puede consumir recursos de CPU de manera indefinida, pero no compromete directamente la confidencialidad o integridad de los datos; sin embargo, su corrección es prioritaria para prevenir interrupciones en servicios dependientes y evitar que sea utilizada como punto de entrada para ataques más avanzados.

Acción: Actualizar ntpd a la versión 4.2.4p8, 4.2.6 o superior.

Análisis Técnico

- **Nombre:** NTP ntpd Mode 7 Error Response Packet Loop Remote DoS
- **ID del Plugin:** 43156
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (udp/123/ntp)

La vulnerabilidad en ntpd permite que un atacante remoto envíe paquetes de error modo 7 con direcciones IP de origen y destino falsificadas para que coincidan con la IP del objetivo, lo que provoca que el servicio responda a sí mismo en un bucle infinito, consumiendo recursos excesivos de CPU y resultando en una denegación de servicio sin requerir autenticación.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:P))
- **VPR Score:** 3.6
- **EPSS Score:** 0.8693

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red o implementar reglas de firewall para bloquear tráfico UDP no esencial en el puerto 123.
2. Corrección: Actualizar el software ntpd a una versión parcheada como 4.2.4p8 o posterior siguiendo los procedimientos de gestión de cambios.
3. Verificación: Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que la actualización ha mitigado el problema y que el servicio funciona correctamente.
4. Prevención: Establecer monitoreo continuo de tráfico de red para detectar intentos de explotación y aplicar parches de seguridad de manera proactiva en todos los sistemas similares.

Conclusión: La vulnerabilidad en ntpd representa un riesgo medio que amenaza la disponibilidad del servicio y debe ser corregida urgentemente mediante actualización para prevenir interrupciones operativas y fortalecer la postura de seguridad general.

VULN-B037: SSL Certificate with Wrong Hostname

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.168.122.187) presenta un certificado SSL con un nombre de host incorrecto en el servicio SMTP, identificado como 'SSL Certificate with Wrong Hostname'.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques de intermediario que podrían dañar la reputación de la organización al exponer datos sensibles en tránsito.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle, pero no conduce a un compromiso directo del sistema; sin embargo, su corrección es importante para prevenir posibles filtraciones de información y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido para el servicio SMTP en el host BEE-BOX.

Análisis Técnico

- **Nombre:** SSL Certificate with Wrong Hostname
- **ID del Plugin:** 45411
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El plugin de Nessus detectó que el certificado SSL presentado para el servicio SMTP en el puerto tcp/25 tiene un 'commonName' (CN) configurado como 'ubuntu', que no coincide con las identidades conocidas del host (192.168.122.187 o BEE-BOX). Esto indica un error de configuración que permite a un atacante realizar ataques de intermediario, interceptando y posiblemente modificando las comunicaciones cifradas sin ser detectado, ya que los clientes pueden recibir advertencias de certificado no válido pero podrían ignorarlas, comprometiendo la confidencialidad e integridad de los datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas y considerar la desactivación temporal del servicio si es crítico hasta la corrección.
2. Corrección: Obtener e instalar un certificado SSL válido que incluya el nombre correcto del host (BEE-BOX o la dirección IP) utilizando una autoridad de certificación confiable o herramientas como OpenSSL para generarlo internamente.
3. Verificación: Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que el certificado ahora es válido y no presenta discrepancias.
4. Prevención: Implementar políticas de gestión de certificados que incluyan revisiones periódicas y automatizadas para asegurar que todos los servicios usen certificados correctos y actualizados.

Conclusión: Aunque el riesgo es medio, la corrección del certificado SSL es esencial para proteger las comunicaciones SMTP y prevenir posibles brechas de seguridad que podrían afectar la integridad de los datos y la reputación empresarial.

VULN-B038: SSL Certificate with Wrong Hostname

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Certificate with Wrong Hostname, donde el certificado SSL tiene un nombre común incorrecto.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques de suplantación de identidad que dañen la reputación de la organización y expongan datos sensibles a interceptación.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle, pero no permite acceso directo al sistema; sin embargo, su corrección es importante para prevenir posibles escaladas de ataque y cumplir con estándares de seguridad.

Acción: Generar o adquirir un certificado SSL válido para el servicio en el puerto tcp/443.

Análisis Técnico

- **Nombre:** SSL Certificate with Wrong Hostname
- **ID del Plugin:** 45411
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El plugin de Nessus detectó que el certificado SSL presentado por el servicio en 192.168.122.187 tiene un Common Name (CN) de 'bee-box.bwapp.local', que no coincide con las identidades conocidas del host (192.168.122.187). Esto indica que el certificado fue emitido para un nombre de host diferente, lo que puede permitir a un atacante realizar ataques de suplantación si puede redirigir el tráfico, comprometiendo la autenticidad y confidencialidad de las conexiones SSL/TLS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium

- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de suplantación o ataques man-in-the-middle.
2. **Corrección:** Reemplazar el certificado SSL actual con uno válido que coincida con el nombre del host o dirección IP del servicio.
3. **Verificación:** Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado es correcto y está correctamente instalado.
4. **Prevención:** Implementar políticas de gestión de certificados que aseguren la renovación y validación periódica de certificados SSL para todos los servicios.

Conclusión: Aunque el riesgo es medio, la corrección del certificado SSL incorrecto es esencial para proteger la integridad de las comunicaciones y prevenir posibles ataques de suplantación.

VULN-B039: SSL Certificate with Wrong Hostname

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) presenta la vulnerabilidad SSL Certificate with Wrong Hostname, donde el certificado SSL tiene un nombre común incorrecto.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques de suplantación de identidad que podrían dañar la reputación de la organización y exponer datos sensibles a interceptación.

Urgencia: Media. La vulnerabilidad tiene un CVSS de 5.3, indicando un riesgo moderado debido a que es fácilmente explotable en ataques man-in-the-middle, pero no conduce a un compromiso directo del sistema; sin embargo, podría ser utilizada como un paso inicial para ataques más severos si no se mitiga.

Acción: Generar o adquirir un certificado SSL válido para el host 192.168.122.187.

Análisis Técnico

- **Nombre:** SSL Certificate with Wrong Hostname
- **ID del Plugin:** 45411
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto tcp/8443 presenta un certificado SSL cuyo commonName es bee-box.bwapp.local, mientras que el host real es 192.168.122.187 o BEE-BOX, lo que indica una discrepancia en la identidad del servidor; esto puede ser explotado mediante ataques de suplantación para interceptar o manipular comunicaciones SSL/TLS, comprometiendo la confidencialidad e integridad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de explotación y considerar la desactivación temporal del servicio si es crítico.
2. **Corrección:** Generar un nuevo certificado SSL con el commonName correcto que coincida con el hostname o dirección IP del servidor y reinstalarlo en el servicio.
3. **Verificación:** Utilizar herramientas como OpenSSL o Nessus para validar que el certificado ahora presenta la identidad correcta y no genera advertencias.
4. **Prevención:** Implementar políticas de gestión de certificados que aseguren la renovación y validación periódica de los certificados SSL para evitar discrepancias futuras.

Conclusión: Aunque el riesgo es moderado, la discrepancia en el certificado SSL debe corregirse prontamente para prevenir posibles ataques de suplantación y proteger la integridad de las comunicaciones del negocio.

VULN-B040: SSL Certificate with Wrong Hostname

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Certificate with Wrong Hostname, donde el certificado SSL tiene un nombre común incorrecto.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques de suplantación de identidad que podrían dañar la reputación de la organización y exponer datos sensibles a interceptación.

Urgencia: Media. La vulnerabilidad es de riesgo medio según CVSS, con un vector que indica facilidad de explotación en red, pero solo afecta la integridad sin comprometer la confidencialidad o disponibilidad; sin embargo, podría ser explotada en combinación con otros ataques para escalar privilegios o realizar movimientos laterales, por lo que debe abordarse en un plazo razonable para mitigar riesgos potenciales.

Acción: Adquirir o generar un certificado SSL válido para el servicio en el puerto tcp/9443.

Análisis Técnico

- **Nombre:** SSL Certificate with Wrong Hostname
- **ID del Plugin:** 45411
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

La vulnerabilidad surge porque el servicio en el puerto tcp/9443 presenta un certificado SSL cuyo atributo commonName (CN) es 'bee-box.bwapp.local', mientras que el host real es identificado como 192.168.122.187 o BEE-BOX; esta discrepancia permite que atacantes realicen ataques de man-in-the-middle para interceptar o manipular comunicaciones, ya que los clientes podrían aceptar el certificado incorrecto si no validan adecuadamente el nombre del host, comprometiendo la integridad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall temporales para restringir el acceso al puerto 9443 si es crítico, y notificar a los usuarios sobre el riesgo potencial de conexiones no seguras.
2. **Corrección:** Obtener un certificado SSL válido que coincida con el nombre de host correcto (por ejemplo, BEE-BOX o 192.168.122.187) e instalarlo en el servicio afectado.
3. **Verificación:** Utilizar herramientas como Nessus o OpenSSL para confirmar que el nuevo certificado se presenta correctamente y no tiene discrepancias en el commonName.
4. **Prevención:** Establecer procesos automatizados para la gestión y renovación de certificados, y capacitar al personal en prácticas de validación de certificados para evitar recurrencias.

Conclusión: Aunque el riesgo es medio, la discrepancia en el certificado SSL debe corregirse prontamente para proteger la integridad de las comunicaciones y prevenir posibles explotaciones que afecten la seguridad de la red.

VULN-B041: SSL Certificate Cannot Be Trusted

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Certificate Cannot Be Trusted en el servicio SMTP, donde el certificado SSL no es confiable debido a una cadena de confianza rota.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de las comunicaciones, facilitando ataques man-in-the-middle que podrían exponer datos sensibles y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad tiene un CVSS de 6.5, indicando un riesgo moderado con impacto en confidencialidad e integridad, pero no en disponibilidad; aunque requiere un ataque man-in-the-middle activo para explotarse, su corrección es prioritaria para prevenir posibles filtraciones de información y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido y confiable para el servicio SMTP.

Análisis Técnico

- **Nombre:** SSL Certificate Cannot Be Trusted

- **ID del Plugin:** 51192
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El análisis técnico revela que el certificado X.509 del servidor tiene problemas de confianza: un certificado ha expirado (con fecha de caducidad el 27 de abril de 2013) y el certificado raíz es autofirmado por una autoridad desconocida, lo que rompe la cadena de confianza. Esto impide la verificación adecuada de la autenticidad del servidor, permitiendo que un atacante intercepte y manipule las comunicaciones SMTP mediante ataques man-in-the-middle, aunque la explotación depende de condiciones de red específicas.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar actividades sospechosas y considerar el uso temporal de conexiones alternativas seguras.
2. **Corrección:** Obtener un certificado SSL de una autoridad de certificación pública reconocida y configurarlo correctamente en el servidor.
3. **Verificación:** Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que el certificado es válido y la cadena de confianza está intacta.
4. **Prevención:** Implementar políticas de gestión de certificados que incluyan renovaciones automáticas y auditorías regulares para evitar futuros incidentes.

Conclusión: La vulnerabilidad en el certificado SSL de BEE-BOX representa un riesgo moderado para la seguridad de las comunicaciones, exigiendo su corrección pronta para mitigar posibles ataques y proteger la integridad de los datos.

VULN-B042: SSL Certificate Cannot Be Trusted

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Cannot Be Trusted' debido a un certificado SSL no confiable en el puerto tcp/443.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, facilitando ataques man-in-the-middle que podrían dañar la reputación de la organización y exponer información sensible.

Urgencia: Media. La vulnerabilidad tiene un CVSS de 6.5, indicando un riesgo moderado con impacto en confidencialidad e integridad, pero no en disponibilidad; aunque no es explotable directamente, puede ser aprovechada en combinación con otros ataques para comprometer la seguridad, por lo que debe abordarse en el corto plazo para mitigar riesgos potenciales.

Acción: Adquirir o generar un certificado SSL válido y confiable para el servicio.

Análisis Técnico

- **Nombre:** SSL Certificate Cannot Be Trusted
- **ID del Plugin:** 51192
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El análisis técnico revela que el certificado X.509 del servidor ha expirado (con fecha 'Not After: Apr 13 18:11:32 2018 GMT') y está firmado por una autoridad de certificación desconocida, lo que rompe la cadena de confianza; esto impide la verificación de la autenticidad del servidor, permitiendo posibles ataques man-in-the-middle donde un atacante podría interceptar y manipular comunicaciones cifradas sin ser detectado, aunque la explotación requiere condiciones específicas como la presencia de un atacante activo en la red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas y considerar el uso temporal de conexiones alternativas seguras.
2. Corrección: Obtener e instalar un certificado SSL válido de una autoridad de certificación pública reconocida, asegurando que no esté expirado y tenga una cadena de confianza intacta.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado es confiable y no presenta errores.
4. Prevención: Implementar políticas de gestión de certificados que incluyan renovaciones automáticas y auditorías regulares para evitar futuros incidentes similares.

Conclusión: La vulnerabilidad en el certificado SSL de BEE-BOX representa un riesgo moderado para la seguridad que debe corregirse prontamente para proteger la integridad de las comunicaciones y prevenir posibles explotaciones.

VULN-B043: SSL Certificate Cannot Be Trusted

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Certificate Cannot Be Trusted, donde el certificado SSL no es confiable debido a una cadena de certificados rota.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, facilitando ataques man-in-the-middle que podrían dañar la reputación de la organización y exponer información sensible.

Urgencia: Media. La vulnerabilidad tiene un CVSS de 6.5, indicando un riesgo moderado que podría ser explotado fácilmente en entornos de red no seguros, pero no permite un compromiso directo

del sistema; sin embargo, su corrección es importante para prevenir posibles ataques y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido y confiable para el servicio en el puerto tcp/8443.

Análisis Técnico

- **Nombre:** SSL Certificate Cannot Be Trusted
- **ID del Plugin:** 51192
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El análisis técnico revela que el certificado X.509 del servidor ha expirado (Not After: Apr 13 18:11:32 2018 GMT) y está firmado por una autoridad de certificación desconocida, lo que rompe la cadena de confianza; esto impide la verificación de la autenticidad del servidor, facilitando ataques man-in-the-middle donde un atacante podría interceptar y manipular comunicaciones SSL/TLS sin ser detectado.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall temporales para restringir el acceso al puerto 8443 hasta que se resuelva la vulnerabilidad.
2. **Corrección:** Obtener un certificado SSL de una autoridad de certificación pública reconocida y configurarlo correctamente en el servidor.
3. **Verificación:** Utilizar herramientas como OpenSSL o Nessus para validar que la nueva cadena de certificados es confiable y no contiene errores.
4. **Prevención:** Establecer procesos de monitoreo y renovación automática de certificados para evitar expiraciones futuras y asegurar el cumplimiento de las mejores prácticas de seguridad.

Conclusión: La vulnerabilidad en el certificado SSL de BEE-BOX representa un riesgo moderado para la seguridad de la red y debe corregirse prontamente para proteger la integridad de las comunicaciones y prevenir posibles ataques.

VULN-B044: SSL Certificate Cannot Be Trusted

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Cannot Be Trusted' debido a un certificado SSL no confiable en el puerto tcp/9443.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, facilitando ataques man-in-the-middle que podrían dañar la reputación de la organización y exponer información sensible.

Urgencia: Media. La vulnerabilidad es explotable de forma remota sin autenticación, pero requiere un ataque man-in-the-middle activo para causar impacto directo; sin embargo, su corrección es prioritaria para prevenir posibles filtraciones de datos y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido y confiable para el servicio en el puerto tcp/9443.

Análisis Técnico

- **Nombre:** SSL Certificate Cannot Be Trusted
- **ID del Plugin:** 51192
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El análisis técnico revela que el certificado X.509 del servidor ha expirado (con fecha 'Not After: Apr 13 18:11:32 2018 GMT') y está autofirmado por una autoridad desconocida, lo que rompe la cadena de confianza; esto impide la verificación de la autenticidad del servidor, permitiendo que un atacante intercepte y manipule las comunicaciones SSL/TLS mediante técnicas de man-in-the-middle, aunque no compromete directamente la disponibilidad del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall temporales para restringir el acceso al puerto 9443 solo a redes confiables hasta la corrección.
2. **Corrección:** Obtener un certificado SSL de una autoridad certificadora (CA) pública reconocida, instalarlo en el servidor y configurar el servicio para usar solo certificados válidos y actualizados.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado es confiable y no presenta errores de cadena o expiración.
4. **Prevención:** Establecer un proceso de gestión de certificados que incluya monitoreo automático de fechas de expiración y renovación proactiva para evitar recurrencias.

Conclusión: La vulnerabilidad en el certificado SSL de BEE-BOX representa un riesgo medio que debe abordarse prontamente para proteger la integridad de las comunicaciones y prevenir posibles ataques de intermediario.

VULN-B045: SMTP Service STARTTLS Plaintext Command Injection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SMTP Service STARTTLS Plaintext Command Injection, permitiendo inyección de comandos durante la fase de texto plano.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al permitir el robo de credenciales SASL y correos electrónicos, y dañar la integridad al ejecutar comandos no autorizados, afectando la reputación del servicio de correo.

Urgencia: Media. La explotación requiere un ataque específico y no es trivial, pero el riesgo de compromiso de credenciales y datos sensibles es significativo si se aprovecha, pudiendo servir como punto de entrada para ataques más amplios; debe abordarse en un plazo razonable para mitigar riesgos potenciales.

Acción: Contactar al proveedor para verificar si hay una actualización disponible.

Análisis Técnico

- **Nombre:** SMTP Service STARTTLS Plaintext Command Injection
- **ID del Plugin:** 52611
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

La vulnerabilidad surge de una falla en la implementación de STARTTLS del servicio SMTP, donde comandos inyectados durante la fase de texto plano, como se observa en el plugin_output de Nessus con 'STARTTLS\r\nRSET\r\n' en un solo paquete, son ejecutados durante la fase de cifrado, permitiendo a un atacante remoto no autenticado manipular la sesión y potencialmente robar credenciales o datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.0 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:P/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.6945

Acciones Recomendadas

1. Contención: Aislar temporalmente el servicio SMTP o implementar reglas de firewall para restringir el acceso no autorizado.
2. Corrección: Aplicar parches o actualizaciones del proveedor para corregir la implementación de STARTTLS.
3. Verificación: Realizar pruebas de penetración o escaneos post-corrección para confirmar que la vulnerabilidad ha sido mitigada.
4. Prevención: Implementar monitoreo continuo de tráfico SMTP y reforzar las configuraciones de seguridad para prevenir inyecciones similares en el futuro.

Conclusión: La vulnerabilidad en el servicio SMTP representa un riesgo medio para la confidencialidad e integridad de los datos, exigiendo una corrección oportuna para proteger las credenciales y prevenir explotaciones.

VULN-B046: SSL Self-Signed Certificate

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta una vulnerabilidad SSL Self-Signed Certificate en el servicio SMTP (puerto 25), donde el certificado no está firmado por una autoridad reconocida.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían exponer datos sensibles y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle activo, lo que podría llevar a la interceptación de comunicaciones y potencialmente servir como punto de entrada para ataques más avanzados, pero no compromete directamente la disponibilidad del sistema.

Acción: Adquirir o generar un certificado SSL válido firmado por una autoridad de certificación reconocida para el servicio SMTP.

Análisis Técnico

- **Nombre:** SSL Self-Signed Certificate
- **ID del Plugin:** 57582
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el host utiliza un certificado X.509 autofirmado con detalles como Subject: C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu/E=root@ubuntu, que no está incluido en la lista de autoridades de certificación conocidas, lo que anula la protección SSL al permitir que un atacante suplante la identidad del servidor y realice ataques man-in-the-middle sin detección.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para restringir el acceso al puerto 25 solo a redes de confianza y monitorear las conexiones en busca de anomalías.
2. Corrección: Reemplazar el certificado autofirmado con uno emitido por una autoridad de certificación confiable y configurar el servicio para usar solo certificados válidos.
3. Verificación: Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado es reconocido y no genera advertencias.
4. Prevención: Establecer políticas de gestión de certificados que incluyan renovaciones automáticas y auditorías periódicas para evitar certificados no autorizados en todos los servicios.

Conclusión: La presencia de un certificado SSL autofirmado en SMTP representa un riesgo medio que debe corregirse para proteger las comunicaciones y prevenir posibles brechas de seguridad.

VULN-B047: SSL Self-Signed Certificate

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta una vulnerabilidad de **SSL Self-Signed Certificate** en el puerto tcp/443, donde la cadena de certificados termina en un certificado autofirmado no reconocido.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, permitiendo ataques man-in-the-middle que podrían llevar a la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en entornos de red no seguros, ya que no requiere autenticación y puede ser utilizada para interceptar comunicaciones, aunque no conduce directamente a un compromiso total del sistema; sin embargo, su corrección es prioritaria para proteger datos en tránsito y prevenir escaladas de ataque.

Acción: Adquirir o generar un certificado SSL válido firmado por una autoridad de certificación reconocida para el servicio.

Análisis Técnico

- **Nombre:** SSL Self-Signed Certificate
- **ID del Plugin:** 57582
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto tcp/443 utiliza un certificado X.509 autofirmado con Subject: C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com, que no está firmado por una autoridad de certificación confiable. Esto anula la autenticidad del SSL, permitiendo que un atacante realice un ataque man-in-the-middle al presentar un certificado falso, comprometiendo la confidencialidad e integridad de las comunicaciones cifradas sin ser detectado por los clientes que no verifican adecuadamente los certificados.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para restringir el acceso al puerto 443 solo a redes confiables y monitorear el tráfico en busca de actividades sospechosas.

2. Corrección: Reemplazar el certificado autofirmado con uno emitido por una autoridad de certificación reconocida y configurar el servicio para usar el nuevo certificado.
3. Verificación: Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que el certificado es válido y no se detectan issues relacionados.
4. Prevención: Establecer políticas para el uso exclusivo de certificados de confianza, realizar auditorías periódicas de certificados, y capacitar al personal sobre mejores prácticas de seguridad SSL/TLS.

Conclusión: La vulnerabilidad de certificado SSL autofirmado en BEE-BOX representa un riesgo medio que debe abordarse prontamente para salvaguardar la integridad de las comunicaciones y prevenir posibles brechas de seguridad.

VULN-B048: SSL Self-Signed Certificate

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta una vulnerabilidad SSL Self-Signed Certificate en el puerto tcp/8443, donde el certificado no está firmado por una autoridad reconocida.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, permitiendo ataques man-in-the-middle que podrían llevar a la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en entornos de red no seguros, ya que no requiere autenticación y puede ser utilizada para interceptar comunicaciones, aunque no conduce directamente a un compromiso total del sistema; sin embargo, su corrección es prioritaria para prevenir posibles filtraciones de datos y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido firmado por una autoridad de certificación reconocida para el servicio en el puerto 8443.

Análisis Técnico

- **Nombre:** SSL Self-Signed Certificate
- **ID del Plugin:** 57582
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto tcp/8443 utiliza un certificado X.509 autofirmado con Subject C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com, que no está incluido en la lista de autoridades de certificación confiables; esto anula la protección SSL, permitiendo que un atacante realice un ataque man-in-the-middle para espiar o modificar el tráfico cifrado entre el cliente y el servidor, aunque no compromete directamente la disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para restringir el acceso al puerto 8443 solo a redes confiables y monitorear el tráfico en busca de actividades sospechosas.
2. Corrección: Reemplazar el certificado autofirmado con uno emitido por una autoridad de certificación reconocida y configurar el servicio para usar solo certificados válidos.
3. Verificación: Realizar pruebas de penetración y usar herramientas como OpenSSL para validar que la cadena de certificados esté correctamente firmada y no genere advertencias en los clientes.
4. Prevención: Establecer políticas de gestión de certificados que incluyan renovaciones automáticas y auditorías regulares para evitar el uso de certificados autofirmados en entornos de producción.

Conclusión: La presencia de un certificado SSL autofirmado en BEE-BOX representa un riesgo medio que debe abordarse de inmediato para proteger la confidencialidad de los datos y prevenir posibles interceptaciones no autorizadas.

VULN-B049: SSL Self-Signed Certificate

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta una vulnerabilidad de **SSL Self-Signed Certificate** en el puerto tcp/9443, donde el certificado SSL no está firmado por una autoridad reconocida.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, permitiendo ataques man-in-the-middle que podrían llevar a la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en entornos de red no seguros, ya que no requiere autenticación y puede ser utilizada para interceptar comunicaciones, aunque no conduce directamente a un compromiso total del sistema; sin embargo, su corrección es prioritaria para prevenir posibles escaladas de ataque y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido firmado por una autoridad de certificación reconocida para el servicio en el puerto tcp/9443.

Análisis Técnico

- **Nombre:** SSL Self-Signed Certificate
- **ID del Plugin:** 57582
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El análisis técnico revela que el certificado X.509 en la cadena enviada por el host remoto es autofirmado, con detalles como Subject: C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com, y no está incluido en la lista de autoridades de certificación conocidas; esto anula la efectividad de SSL al permitir que un atacante realice un ataque man-in-the-middle, interceptando y posiblemente modificando las comunicaciones cifradas sin ser detectado, lo que compromete la confidencialidad e integridad de los datos en tránsito.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de redes públicas o implementar reglas de firewall para restringir el acceso al puerto afectado.
2. Corrección: Reemplazar el certificado autofirmado con uno emitido por una autoridad de certificación confiable y configurar el servicio para usar el nuevo certificado.
3. Verificación: Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que el certificado ahora es válido y no se detectan issues relacionados.
4. Prevención: Establecer políticas de gestión de certificados que incluyan renovaciones automáticas y monitoreo continuo para evitar el uso de certificados autofirmados en el futuro.

Conclusión: La presencia de un certificado SSL autofirmado en BEE-BOX representa un riesgo medio que debe abordarse prontamente para proteger la integridad de las comunicaciones y prevenir posibles brechas de seguridad.

VULN-B050: SMB Signing not required

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) con SMB no requiere firma de mensajes, permitiendo ataques man-in-the-middle.

Riesgo para el Negocio: Esta vulnerabilidad compromete la integridad de las comunicaciones SMB, lo que podría permitir a atacantes manipular datos o interceptar información sensible, afectando la confidencialidad y reputación de la organización.

Urgencia: Media. La explotación es relativamente sencilla en entornos de red comprometidos, pero requiere un ataque man-in-the-middle activo, lo que limita su impacto inmediato; sin embargo, podría ser utilizada como un paso inicial para ataques más severos, por lo que se recomienda abordarla en el corto plazo para mitigar riesgos de escalada.

Acción: Forzar la firma de mensajes SMB en la configuración del servidor, utilizando las opciones apropiadas en Windows o Samba.

Análisis Técnico

- **Nombre:** SMB Signing not required
- **ID del Plugin:** 57608
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/445/cifs)

La vulnerabilidad SMB Signing not required en el puerto tcp/445/cifs del host Linux Kernel 2.6.24-16-generic permite que un atacante no autenticado realice ataques man-in-the-middle al no verificar la autenticidad de los mensajes SMB, lo que puede llevar a la manipulación o interceptación de datos en tránsito, explotando la falta de requisitos de firma digital en las comunicaciones.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red si es posible para prevenir explotaciones durante la remediación.
2. Corrección: Configurar el servidor SMB para requerir firma de mensajes; en Windows, habilitar 'Microsoft network server\: Digitally sign communications (always)' mediante políticas de grupo, y en Samba, establecer 'server signing = mandatory' en smb.conf.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que la firma SMB está habilitada y funcionando correctamente.
4. Prevención: Implementar monitoreo continuo de configuraciones SMB y realizar auditorías regulares de seguridad para asegurar el cumplimiento de las mejores prácticas.

Conclusión: Aunque el riesgo es medio, la falta de firma SMB en BEE-BOX debe corregirse prontamente para proteger la integridad de las comunicaciones y prevenir posibles ataques de intermediario que podrían escalar a compromisos mayores.

VULN-B051: SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) con sistema operativo Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL RC4 Cipher Suites Supported (Bar Mitzvah) en el servicio tcp/25/smtp, que permite el uso de cifrados RC4 inseguros.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de datos sensibles transmitidos, como cookies HTTP, lo que podría llevar a la exposición de información privada y dañar la reputación de la organización si se explota.

Urgencia: Media. La explotación requiere la obtención de millones de textos cifrados y condiciones específicas, lo que limita su facilidad inmediata, pero el alto puntaje EPSS (0.9267) indica una probabilidad significativa de explotación en el entorno actual, y podría ser utilizada como un paso inicial en ataques más avanzados si no se mitiga.

Acción: Reconfigurar la aplicación afectada para deshabilitar los cifrados RC4 y priorizar el uso de TLS 1.2 con suites AES-GCM.

Análisis Técnico

- **Nombre:** SSL RC4 Cipher Suites Supported (Bar Mitzvah)

- **ID del Plugin:** 65821
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el puerto 25 soporta múltiples suites de cifrado RC4, incluyendo EXP-RC4-MD5, RC4-MD5, ADH-RC4-MD5 y RC4-SHA, como se detalla en el plugin_output. RC4 genera un flujo pseudoaleatorio con sesgos que reducen la aleatoriedad, permitiendo a un atacante, tras capturar una gran cantidad de textos cifrados (por ejemplo, decenas de millones), derivar el texto plano mediante análisis estadístico. Esto afecta la confidencialidad de las comunicaciones, especialmente en datos repetitivos como cookies, y se ve agravado por el uso de cifrados de baja fuerza (ej., RC4(40)) y autenticación débil en algunas suites.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.9267

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y aislar temporalmente el host si es necesario.
2. Corrección: Deshabilitar todos los cifrados RC4 en la configuración del servidor SMTP y aplicar parches o actualizaciones para soportar sólo suites seguras como AES-GCM con TLS 1.2 o superior.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar la eliminación de los cifrados RC4 y validar la configuración mediante herramientas como Nessus.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de cifrados obsoletos, realizar auditorías regulares de configuración, y educar al personal sobre mejores prácticas criptográficas.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

VULN-B052: SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) con sistema operativo Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL RC4 Cipher Suites Supported (Bar Mitzvah), que permite el uso de cifrados RC4 inseguros en el puerto tcp/443.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de datos sensibles, como cookies HTTP, lo que podría llevar a la exposición de información privada y dañar la reputación de la organización si se explota.

Urgencia: Media. Aunque la explotación requiere condiciones específicas, como la obtención de millones de cifrados, el alto EPSS score de 0.9267 indica una probabilidad significativa de ataque en el mundo real, y la fuga de información confidencial podría ser utilizada en ataques más avanzados.

Acción: Reconfigurar la aplicación afectada para deshabilitar los cifrados RC4 y priorizar el uso de TLS 1.2 con suites AES-GCM.

Análisis Técnico

- **Nombre:** SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- **ID del Plugin:** 65821
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto 443 soporta múltiples suites de cifrado RC4, incluyendo EXP-RC4-MD5, RC4-MD5 y RC4-SHA, que utilizan claves de 40 a 128 bits. RC4 genera un flujo pseudoaleatorio con sesgos que, tras millones de cifrados, permiten a un atacante derivar texto plano, como se detalla en las referencias CVE-2013-2566 y CVE-2015-2808. Esto debilita la seguridad de las comunicaciones SSL/TLS, exponiendo datos sensibles a interceptaciones.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.9267

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de redes públicas si es crítico y monitorear el tráfico para detectar intentos de explotación.
2. **Corrección:** Deshabilitar todos los cifrados RC4 en la configuración del servidor web y aplicar parches o actualizaciones para usar sólo suites seguras como AES-GCM con TLS 1.2 o superior.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar la eliminación de RC4 y validar la configuración con herramientas como SSL labs.
4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de cifrados obsoletos, realizar auditorías regulares de configuración, y educar al personal sobre mejores prácticas criptográficas.

Conclusión: El soporte de cifrados RC4 en BEE-BOX representa un riesgo medio para la confidencialidad de datos y debe corregirse prontamente para prevenir posibles fugas de información y cumplir con los estándares de seguridad modernos.

VULN-B053: SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic soporta suites de cifrado SSL RC4, lo que constituye la vulnerabilidad SSL RC4 Cipher Suites Supported (Bar Mitzvah).

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de datos sensibles, como cookies HTTP, lo que podría llevar a accesos no autorizados y dañar la reputación de la organización debido a posibles filtraciones de información.

Urgencia: Media. La explotación requiere la obtención de millones de cifrados y condiciones específicas, lo que dificulta un ataque inmediato, pero el riesgo de fuga de información confidencial justifica una corrección prioritaria en el corto plazo para prevenir posibles brechas de seguridad.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados RC4.

Análisis Técnico

- **Nombre:** SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- **ID del Plugin:** 65821
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto tcp/9443 soporta múltiples suites de cifrado RC4, incluyendo EXP-RC4-MD5, RC4-MD5 y RC4-SHA, que utilizan claves de 40 a 128 bits. RC4 genera un flujo pseudoaleatorio con sesgos que, tras millones de cifrados, permiten a un atacante derivar texto plano, comprometiendo la confidencialidad en comunicaciones como las de HTTP.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.9267

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y aplicar reglas de firewall para limitar accesos no esenciales.
2. Corrección: Deshabilitar los cifrados RC4 en la configuración del servidor web y priorizar el uso de TLS 1.2 con suites AES-GCM.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar la eliminación de los cifrados RC4 y validar la configuración segura.
4. Prevención: Implementar políticas de seguridad que exijan el uso de cifrados fuertes y realizar auditorías periódicas para asegurar el cumplimiento con estándares criptográficos actualizados.

Conclusión: El soporte de cifrados RC4 en BEE-BOX representa un riesgo medio para la confidencialidad de datos, exigiendo su corrección inmediata para mitigar potenciales accesos no autorizados y proteger la integridad de la información.

VULN-B054: Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic tiene habilitado el comando monlist en ntpd, lo que permite una vulnerabilidad de denegación de servicio.

Riesgo para el Negocio: Esta vulnerabilidad puede causar interrupciones en la disponibilidad del servicio NTP, afectando la sincronización de tiempo en la red y potencialmente facilitando ataques DDoS que dañen la reputación y operaciones.

Urgencia: Media. La explotación es relativamente sencilla y no requiere autenticación, con un impacto alto en disponibilidad, pero no compromete directamente la confidencialidad o integridad; sin embargo, podría ser utilizada como vector para ataques más amplios, por lo que debe abordarse prontamente.

Acción: Agregar 'disable monitor' al archivo ntp.conf y reiniciar el servicio, o actualizar a NTP versión 4.2.7-p26 o superior.

Análisis Técnico

- **Nombre:** Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS
- **ID del Plugin:** 71783
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (udp/123/ntp)

El demonio ntpd en el puerto UDP/123 tiene el comando monlist habilitado, que devuelve una lista de hosts recientes, como se observa en la salida del plugin que incluye 192.168.122.1; esto permite a un atacante enviar solicitudes forjadas REQ_MON_GETLIST para saturar el tráfico de red hacia una dirección IP específica, explotando una vulnerabilidad en ntp_request.c que puede resultar en denegación de servicio o ser utilizada para reconocimiento y ataques DDoS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:N/A:P))
- **VPR Score:** 6.7
- **EPSS Score:** 0.9173

Acciones Recomendadas

1. **Contención:** Restringir el acceso al servicio NTP solo a hosts de confianza mediante firewalls o listas de control de acceso.
2. **Corrección:** Actualizar ntpd a la versión 4.2.7-p26 o posterior, o modificar la configuración en ntp.conf añadiendo la directiva 'disable monitor' y reiniciando el servicio.
3. **Verificación:** Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que el comando monlist está deshabilitado y no se pueden recuperar listas de hosts.
4. **Prevención:** Implementar monitoreo continuo de servicios NTP, aplicar parches de seguridad de manera proactiva, y revisar regularmente las configuraciones para evitar la reaparición de vulnerabilidades similares.

Conclusión: La vulnerabilidad en ntpd representa un riesgo significativo para la disponibilidad y debe corregirse de inmediato para prevenir posibles ataques de denegación de servicio y proteger la integridad operativa de la red.

VULN-B055: OpenSSL Heartbeat Information Disclosure (Heartbleed)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) ejecuta una versión vulnerable de OpenSSL en el puerto tcp/8443, permitiendo la divulgación de información sensible a través de la vulnerabilidad Heartbleed.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al exponer datos sensibles como contraseñas y claves privadas, lo que podría llevar a accesos no autorizados y daños reputacionales significativos.

Urgencia: Media. La vulnerabilidad es fácilmente explotable con herramientas como Metasploit y Core Impact, permitiendo a atacantes remotos leer hasta 64KB de memoria del servidor sin autenticación, lo que podría facilitar compromisos adicionales o el robo de información crítica, pero no afecta directamente la integridad o disponibilidad del sistema.

Acción: Actualizar OpenSSL a la versión 1.0.1g o posterior, o recompilarlo con el flag '-DOPENSSL_NO_HEARTBEATS' para deshabilitar la funcionalidad vulnerable.

Análisis Técnico

- **Nombre:** OpenSSL Heartbeat Information Disclosure (Heartbleed)
- **ID del Plugin:** 73412
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

La vulnerabilidad Heartbleed (CVE-2014-0160) es un fallo de lectura fuera de límites en la implementación de OpenSSL del protocolo TLS Heartbeat (RFC 6520), donde un mensaje manipulado puede hacer que el servidor devuelva hasta 64KB de memoria adyacente no inicializada, como se evidencia en el plugin_output de Nessus que muestra datos en hexadecimal, incluyendo fragmentos de cadenas XML y referencias a objetos internos de Java, lo que indica la exposición potencial de información sensible almacenada en memoria durante las operaciones del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.9444

Acciones Recomendadas

1. Contención: Aislar temporalmente el sistema de la red para prevenir explotaciones mientras se aplica la corrección.
2. Corrección: Actualizar OpenSSL a la versión 1.0.1g o superior, o aplicar el parche correspondiente y reiniciar los servicios afectados.
3. Verificación: Realizar pruebas de penetración o usar herramientas como Nessus para confirmar que la vulnerabilidad ha sido mitigada y que no se puede extraer más memoria.
4. Prevención: Implementar monitoreo continuo de vulnerabilidades, mantener el software actualizado, y revisar regularmente las configuraciones de seguridad para evitar recurrencias.

Conclusión: La vulnerabilidad Heartbleed representa un riesgo significativo para la confidencialidad de los datos y requiere una acción inmediata de actualización para proteger la información sensible del servidor.

VULN-B056: SNMP 'GETBULK' Reflection DDoS

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic tiene una vulnerabilidad en el servicio SNMP udp/161 que permite un ataque de denegación de servicio distribuido reflejado mediante solicitudes GETBULK.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la disponibilidad de servicios al permitir ataques DDoS reflejados, lo que podría resultar en interrupciones operativas y daños reputacionales si se explota.

Urgencia: Media. La vulnerabilidad tiene un riesgo medio debido a que su explotación requiere que un atacante utilice el servicio SNMP para reflejar tráfico hacia otros objetivos, no compromete directamente la confidencialidad o integridad, pero puede ser explotada con relativa facilidad para causar interrupciones de servicio, aunque no sirve como escalón para otros ataques más graves.

Acción: Deshabilitar el servicio SNMP en el host remoto si no se utiliza, o restringir y monitorear el acceso.

Análisis Técnico

- **Nombre:** SNMP 'GETBULK' Reflection DDoS
- **ID del Plugin:** 76474
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (udp/161/snmp)

El demonio SNMP remoto responde con una cantidad excesiva de datos a solicitudes GETBULK que especifican un valor anormalmente alto para 'max-repetitions', como se evidencia en el plugin_output de Nessus, donde una solicitud de 42 bytes genera una respuesta de 2251 bytes, permitiendo a un atacante amplificar el tráfico y dirigirlo hacia un objetivo para saturar sus recursos en un ataque DDoS reflejado.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium

- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:N/A:P))
- **VPR Score:** 4.4
- **EPSS Score:** 0.0787

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red o implementar reglas de firewall para bloquear el tráfico SNMP no autorizado.
2. Corrección: Deshabilitar el servicio SNMP si no es necesario, o aplicar configuraciones seguras como cambiar la cadena comunitaria predeterminada y limitar los valores de 'max-repetitions'.
3. Verificación: Realizar pruebas de penetración o escaneos post-corrección para confirmar que el servicio ya no es vulnerable a ataques de reflexión.
4. Prevención: Implementar monitoreo continuo del tráfico SNMP, educar al personal sobre las mejores prácticas de seguridad, y mantener el software actualizado para prevenir vulnerabilidades similares.

Conclusión: La vulnerabilidad de SNMP en BEE-BOX presenta un riesgo medio que amenaza la disponibilidad y debe abordarse mediante la deshabilitación o aseguramiento del servicio para mitigar posibles ataques DDoS.

VULN-B057: OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic está afectado por la vulnerabilidad OpenSSL 'ChangeCipherSpec' MiTM, que permite la descifrado de datos sensibles.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de los datos transmitidos, pudiendo llevar a la exposición de información sensible y daño reputacional si es explotada.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y tiene un impacto moderado en la confidencialidad e integridad, pero su alta puntuación EPSS (0.929) y la posibilidad de ser un vector para otros ataques justifican una corrección prioritaria en el corto plazo.

Acción: Actualizar OpenSSL a la versión 0.9.8za, 1.0.0m o 1.0.1h según corresponda.

Análisis Técnico

- **Nombre:** OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
- **ID del Plugin:** 77200
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio OpenSSL en el puerto tcp/8443 acepta mensajes ChangeCipherSpec prematuras durante el handshake SSL/TLS, lo que deriva claves de cifrado y MAC a partir de información pública, permitiendo a un atacante MiTM descifrar o falsificar comunicaciones; esto se evidencia en la finalización del handshake con claves débiles, como se observa en la salida del plugin.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.6 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L))
- **Puntuación Base CVSS v2.0:** 6.8 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:P/A:P))
- **VPR Score:** 7.7
- **EPSS Score:** 0.929

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red o implementar reglas de firewall para restringir el acceso al puerto 8443.
2. Corrección: Aplicar el parche de OpenSSL actualizando a la versión 0.9.8za, 1.0.0m o 1.0.1h, y reiniciar el servicio para activar los cambios.
3. Verificación: Realizar un escaneo de vulnerabilidades post-parche para confirmar que la vulnerabilidad ha sido mitigada y probar la funcionalidad del servicio.
4. Prevención: Establecer políticas de gestión de parches regulares, deshabilitar protocolos obsoletos como SSLv3, y monitorear continuamente las comunicaciones en busca de actividades sospechosas.

Conclusión: La vulnerabilidad OpenSSL 'ChangeCipherSpec' MiTM en BEE-BOX representa un riesgo moderado para la seguridad de los datos y debe ser corregida urgentemente para prevenir posibles brechas de confidencialidad e integridad.

VULN-B058: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE), que permite la divulgación de información sensible a través de servicios SSL/TLS.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, lo que podría resultar en la exposición de información sensible y dañar la reputación de la organización si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y múltiples intentos, pero la posibilidad de divulgación de información sensible justifica una corrección prioritaria en el corto plazo para mitigar riesgos de seguridad.

Acción: Deshabilitar SSLv3 en el servidor afectado.

Análisis Técnico

- **Nombre:** SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- **ID del Plugin:** 78479
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic

- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servidor en 192.168.122.187 soporta SSLv3 con suites de cifrado CBC, lo que permite a un atacante realizar un ataque de oráculo de padding para descifrar bytes seleccionados del texto cifrado en aproximadamente 256 intentos por byte, aprovechando la falta de soporte para el mecanismo TLS Fallback SCSV que prevendría el rollback de versión a SSLv3.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 3.4 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.1
- **EPSS Score:** 0.9377

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aislar temporalmente el servidor si es necesario.
2. Corrección: Deshabilitar SSLv3 en la configuración del servicio SMTP y otros servicios afectados; si no es posible deshabilitarlo inmediatamente, habilitar el mecanismo TLS Fallback SCSV.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que SSLv3 está deshabilitado y que no se permiten conexiones con versiones inseguras.
4. Prevención: Implementar políticas de seguridad que deshabiliten protocolos obsoletos como SSLv3 en todos los sistemas, y realizar auditorías regulares para asegurar el cumplimiento con las mejores prácticas criptográficas.

Conclusión: Aunque la explotación requiere condiciones específicas, la vulnerabilidad POODLE amenaza la confidencialidad de los datos y debe ser corregida prontamente para proteger la información sensible y mantener la integridad de la seguridad de la red.

VULN-B059: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE), que permite la divulgación de información sensible a través de servicios SSL/TLS.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de datos transmitidos, lo que podría resultar en la exposición de información sensible y daños reputacionales si es explotada.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y múltiples intentos, pero la facilidad de downgrade a SSLv3 y la falta de mecanismos de protección como Fallback SCSV aumentan el riesgo de divulgación de datos en entornos no seguros, aunque no conduce a un compromiso directo del sistema.

Acción: Deshabilitar SSLv3 en el servidor afectado.

Análisis Técnico

- **Nombre:** SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- **ID del Plugin:** 78479
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

La vulnerabilidad POODLE explota el manejo de bytes de relleno en SSL 3.0 con cifrados CBC, permitiendo a un atacante MitM descifrar bytes seleccionados del texto cifrado mediante la forzadura de conexiones SSLv3 repetidas; el servidor en 192.168.122.187 soporta SSLv3 con suites CBC y carece del mecanismo Fallback SCSV, facilitando el rollback de versiones y aumentando la superficie de ataque a pesar del soporte para TLS más reciente.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 3.4 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.1
- **EPSS Score:** 0.9377

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de downgrade o ataques MitM.
2. Corrección: Deshabilitar SSLv3 en la configuración del servidor web y habilitar TLS Fallback SCSV si es necesario temporalmente.
3. Verificación: Realizar escaneos post-corrección para confirmar que SSLv3 está deshabilitado y solo se usan protocolos seguros como TLS 1.2 o superior.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de protocolos obsoletos y realizar auditorías regulares de configuración SSL/TLS.

Conclusión: Aunque el riesgo es medio, la vulnerabilidad POODLE amenaza la confidencialidad de los datos y debe mitigarse deshabilitando SSLv3 para proteger la información sensible y mantener la integridad del servicio.

VULN-B060: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE), que permite la divulgación de información sensible a través de servicios SSL/TLS.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, lo que podría resultar en la exposición de información sensible y dañar la reputación de la organización si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y múltiples intentos, pero la posibilidad de divulgación de información sensible justifica una corrección prioritaria en el corto plazo para mitigar riesgos de seguridad.

Acción: Deshabilitar SSLv3 en el servidor afectado.

Análisis Técnico

- **Nombre:** SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- **ID del Plugin:** 78479
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servidor en 192.168.122.187 soporta SSLv3 con suites de cifrado CBC, lo que permite a un atacante man-in-the-middle forzar una degradación a SSLv3 y explotar la vulnerabilidad POODLE para descifrar bytes seleccionados del texto cifrado mediante un oráculo de padding, con un éxito en aproximadamente 256 intentos por byte, comprometiendo la confidencialidad de las comunicaciones.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 3.4 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.1
- **EPSS Score:** 0.9377

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para restringir el acceso al puerto 8443 y monitorear el tráfico en busca de actividades sospechosas.
2. **Corrección:** Deshabilitar SSLv3 en la configuración del servidor web y, si es necesario temporalmente, habilitar el mecanismo TLS Fallback SCSV para prevenir la degradación de versiones.
3. **Verificación:** Utilizar herramientas como Nessus o OpenSSL para confirmar que SSLv3 está deshabilitado y que solo se utilizan protocolos TLS seguros.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos obsoletos como SSLv3 y realizar auditorías periódicas para asegurar el cumplimiento.

Conclusión: La vulnerabilidad POODLE en BEE-BOX representa un riesgo moderado para la confidencialidad de los datos, exigiendo la deshabilitación inmediata de SSLv3 para proteger la información sensible.

VULN-B061: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE), que permite la divulgación de información sensible a través de servicios SSL/TLS.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de datos transmitidos, lo que podría resultar en la exposición de información sensible y dañar la reputación de la organización si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y múltiples intentos, pero la facilidad de downgrade a SSLv3 y la falta de mecanismos de protección como Fallback SCSV aumentan el riesgo de divulgación de datos en entornos no seguros, aunque no conduce a un compromiso directo del sistema.

Acción: Deshabilitar SSLv3 en el servidor afectado.

Análisis Técnico

- **Nombre:** SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- **ID del Plugin:** 78479
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

La vulnerabilidad POODLE explota el manejo de bytes de relleno en SSL 3.0 con cifrados CBC, permitiendo a un atacante MitM descifrar bytes seleccionados del texto cifrado mediante la forzadura de conexiones SSLv3 repetidas; Nessus confirmó que el servidor soporta SSLv3 con suites CBC y carece de Fallback SCSV, facilitando el rollback de versiones a pesar del soporte para TLS más reciente.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 3.4 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.1
- **EPSS Score:** 0.9377

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para bloquear tráfico no autorizado y monitorear conexiones SSL/TLS en busca de actividades sospechosas.
2. **Corrección:** Deshabilitar SSLv3 en la configuración del servidor web y habilitar TLS Fallback SCSV si es necesario temporalmente.
3. **Verificación:** Realizar escaneos post-corrección con herramientas como Nessus para confirmar que SSLv3 está deshabilitado y solo se usan protocolos seguros.
4. **Prevención:** Adoptar políticas de seguridad que exijan el uso exclusivo de TLS 1.2 o superior y realizar auditorías periódicas de configuraciones criptográficas.

Conclusión: Aunque el riesgo es medio, la vulnerabilidad POODLE amenaza la confidencialidad de los datos y debe mitigarse deshabilitando SSLv3 para proteger la información sensible y mantener la integridad de las comunicaciones.

VULN-B062: SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) soporta suites de cifrado EXPORT_RSA débiles de hasta 512 bits, conocido como la vulnerabilidad SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK).

Riesgo para el Negocio: Esta vulnerabilidad puede permitir a un atacante realizar un ataque de downgrade para comprometer la integridad de las comunicaciones, lo que podría llevar a la interceptación de datos sensibles y dañar la reputación de la organización debido a fallos de seguridad.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero facilita la interceptación de datos. Debe abordarse en el corto plazo para mitigar riesgos de fuga de información y cumplir con estándares de seguridad.

Acción: Reconfigurar el servicio para eliminar el soporte de suites de cifrado EXPORT_RSA.

Análisis Técnico

- **Nombre:** SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
- **ID del Plugin:** 81606
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El host remoto, ejecutando Linux Kernel 2.6.24-16-generic en el puerto tcp/25/smtp, admite suites de cifrado EXPORT_RSA como EXP-DES-CBC-SHA, EXP-RC2-CBC-MD5 y EXP-RC4-MD5, que utilizan claves de hasta 512 bits. Estas claves son vulnerables a factorización rápida, permitiendo a un atacante en una posición man-in-the-middle forzar el uso de estos cifrados débiles mediante un ataque de downgrade, como se detalla en CVE-2015-0204, comprometiendo la confidencialidad e integridad de las comunicaciones SSL/TLS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:N/I:P/A:N))
- **VPR Score:** 1.4
- **EPSS Score:** 0.9191

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red si es crítico hasta la corrección.
2. **Corrección:** Reconfigurar el servicio SMTP para deshabilitar específicamente las suites de cifrado EXPORT_RSA y usar solo cifrados fuertes como AES con claves de al menos 2048 bits.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar la eliminación de los cifrados débiles y validar la configuración.

4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de cifrados obsoletos y realizar auditorías regulares de configuración en todos los servicios.

Conclusión: Aunque el riesgo es medio, la presencia de cifrados débiles en FREAK debe corregirse prontamente para proteger la integridad de las comunicaciones y evitar posibles interceptaciones de datos.

VULN-B063: SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) soporta suites de cifrado EXPORT_RSA débiles de hasta 512 bits, identificado como SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK).

Riesgo para el Negocio: Esto puede permitir a un atacante realizar un ataque de downgrade para comprometer la confidencialidad de las comunicaciones, lo que podría resultar en la exposición de datos sensibles y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad tiene un riesgo de explotación moderado que requiere un ataque man-in-the-middle activo, pero si se explota, podría conducir a la interceptación de datos cifrados. Debe abordarse prontamente para prevenir posibles filtraciones de información, aunque no es crítico debido a la necesidad de condiciones específicas de ataque.

Acción: Reconfigurar el servicio para eliminar el soporte de suites de cifrado EXPORT_RSA.

Análisis Técnico

- **Nombre:** SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
- **ID del Plugin:** 81606
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El host remoto soporta múltiples suites de cifrado EXPORT_RSA con claves de hasta 512 bits, como EXP-DES-CBC-SHA (0x00, 0x08), EXP-RC2-CBC-MD5 (0x00, 0x06), y EXP-RC4-MD5 (0x00, 0x03), que utilizan algoritmos de cifrado débiles (por ejemplo, DES-CBC con clave de 40 bits) y autenticación RSA. Un atacante puede explotar esto mediante un ataque de downgrade para forzar el uso de estos cifrados exportables, permitiendo factorizar la clave RSA de 512 bits en poco tiempo y descifrar las comunicaciones, comprometiendo la seguridad de la sesión TLS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:N/I:P/A:N))
- **VPR Score:** 1.4
- **EPSS Score:** 0.9191

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aplicar reglas de firewall para restringir accesos no autorizados.
2. **Corrección:** Reconfigurar el servicio web en el puerto tcp/443 para deshabilitar específicamente las suites de cifrado EXPORT_RSA y otros cifrados débiles, utilizando herramientas como OpenSSL o ajustes de configuración del servidor.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que las suites EXPORT_RSA ya no están soportadas y validar que solo se usen cifrados fuertes.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso exclusivo de cifrados modernos y realizar auditorías periódicas para asegurar el cumplimiento de las mejores prácticas criptográficas.

Conclusión: El soporte de cifrados débiles EXPORT_RSA en BEE-BOX presenta un riesgo moderado de interceptación de datos que debe corregirse para proteger la confidencialidad de las comunicaciones y mantener la integridad de la infraestructura.

VULN-B064: Apache Server ETag Header Information Disclosure

Resumen Ejecutivo

Problema: El servidor web Apache en el host BEE-BOX (192.168.122.187) tiene una vulnerabilidad de divulgación de información en el encabezado ETag.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al exponer información sensible como números de inodo, lo que podría facilitar ataques dirigidos y dañar la reputación de la organización si se explota.

Urgencia: Media. La vulnerabilidad tiene un riesgo moderado debido a su facilidad de explotación a través de solicitudes HTTP normales, pero solo resulta en una fuga de información limitada que no permite un compromiso directo del sistema; sin embargo, podría ser utilizada como un paso inicial para ataques más avanzados, por lo que debe abordarse en el próximo ciclo de parches.

Acción: Modificar el encabezado ETag del servidor Apache para excluir los números de inodo en su cálculo.

Análisis Técnico

- **Nombre:** Apache Server ETag Header Information Disclosure
- **ID del Plugin:** 88098
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/80/www)

La vulnerabilidad surge porque el servidor Apache incluye el número de inodo de los archivos en el encabezado ETag, como se evidencia en la salida del plugin de Nessus que muestra 'ETag: "ccb16-24c-506e4489b4a00"' con un número de inodo de 838422; esto permite a un atacante remoto obtener información sensible sobre la estructura del sistema de archivos mediante simples solicitudes HTTP, lo que podría ayudar en la enumeración de archivos o en la planificación de ataques posteriores, aunque no compromete directamente la integridad o disponibilidad del servidor.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.9
- **EPSS Score:** 0.0032

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall o WAF para bloquear solicitudes maliciosas que intenten explotar esta vulnerabilidad, reduciendo el riesgo inmediato de divulgación.
2. **Corrección:** Aplicar la configuración recomendada en la documentación de Apache para modificar el encabezado ETag y eliminar la inclusión de inodos, asegurando que solo se utilicen atributos menos sensibles como el tamaño del archivo.
3. **Verificación:** Realizar pruebas de penetración o escaneos con herramientas como Nessus para confirmar que el encabezado ETag ya no divulga información sensible después de la corrección.
4. **Prevención:** Establecer políticas de configuración de servidores web que eviten el uso de ETags con datos sensibles y realizar auditorías regulares de seguridad para detectar configuraciones similares en otros sistemas.

Conclusión: Esta vulnerabilidad de divulgación de información en Apache representa un riesgo moderado para la confidencialidad y debe corregirse prontamente para prevenir su explotación y fortalecer la postura de seguridad general.

VULN-B065: Apache Server ETag Header Information Disclosure

Resumen Ejecutivo

Problema: El servidor web Apache en el host BEE-BOX (192.168.122.187) tiene la vulnerabilidad Apache Server ETag Header Information Disclosure, que permite la divulgación de información sensible a través del encabezado ETag.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al exponer detalles internos del sistema, como números de inodo, lo que podría facilitar ataques dirigidos y dañar la reputación de la organización si se explota.

Urgencia: Media. La vulnerabilidad tiene un riesgo moderado debido a su facilidad de explotación a través de solicitudes HTTP normales, pero solo resulta en una fuga de información limitada sin comprometer directamente la integridad o disponibilidad; sin embargo, podría ser utilizada como un paso inicial para ataques más avanzados, por lo que se recomienda abordarla en un plazo razonable.

Acción: Modificar el encabezado ETag del servidor Apache para excluir los números de inodo en su cálculo.

Análisis Técnico

- **Nombre:** Apache Server ETag Header Information Disclosure

- **ID del Plugin:** 88098
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

Nessus detectó que el servidor Apache en el puerto 443 divulga información sensible en el encabezado ETag, específicamente el número de inodo (838422), el tamaño del archivo (588 bytes) y la hora de modificación (Nov. 2, 2014) para archivos solicitados; esto ocurre porque Apache incluye por defecto el inodo en la generación del ETag, permitiendo a un atacante remoto recopilar datos que podrían ayudar en la enumeración de archivos o en la planificación de ataques más sofisticados, aunque no conduce a una ejecución de código directa.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.9
- **EPSS Score:** 0.0032

Acciones Recomendadas

1. Contención: Implementar reglas de firewall o WAF para bloquear solicitudes maliciosas que intenten explotar esta vulnerabilidad temporalmente.
2. Corrección: Aplicar la configuración recomendada en Apache para modificar el ETag, eliminando el inode mediante la directiva FileETag en el archivo de configuración.
3. Verificación: Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que el ETag ya no divulga información sensible.
4. Prevención: Establecer políticas de hardening para servidores web, incluyendo revisiones periódicas de configuraciones y la aplicación de parches de seguridad.

Conclusión: Aunque el riesgo es medio, la divulgación de información a través del ETag debe corregirse para proteger la confidencialidad y prevenir posibles escaladas de ataques en el servidor.

VULN-B066: SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSL DROWN Attack, que permite a un atacante descifrar tráfico TLS capturado debido al soporte de SSLv2.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones, pudiendo exponer datos sensibles y dañar la reputación de la organización si se produce una filtración.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle activo y condiciones específicas, el impacto potencial en la confidencialidad es significativo, y podría ser utilizado como un paso intermedio para ataques más avanzados, justificando una corrección prioritaria en el corto plazo.

Acción: Deshabilitar SSLv2 y las suites de cifrado de grado de exportación en el servidor.

Análisis Técnico

- **Nombre:** SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
- **ID del Plugin:** 89058
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

La vulnerabilidad se debe a que el host soporta SSLv2 y cifrados débiles, como EXP-RC2-CBC-MD5 y EXP-RC4-MD5, que utilizan claves de 40 bits y algoritmos obsoletos, permitiendo a un atacante realizar un ataque de oráculo de padding Bleichenbacher para descifrar conexiones TLS capturadas previamente, explotando la reutilización de claves privadas en servidores que admiten SSLv2.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 3.6
- **EPSS Score:** 0.9015

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aislar temporalmente el host si es necesario.
2. Corrección: Deshabilitar SSLv2 y todas las suites de cifrado de exportación en la configuración del servicio SMTP (puerto 25) y verificar que las claves privadas no se usen en servidores con soporte SSLv2.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que SSLv2 está deshabilitado y solo se usan cifrados seguros.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de protocolos y cifrados obsoletos, y realizar auditorías regulares de configuración.

Conclusión: La vulnerabilidad SSL DROWN representa un riesgo medio para la confidencialidad de los datos, exigiendo la deshabilitación inmediata de SSLv2 para proteger las comunicaciones y prevenir posibles filtraciones.

VULN-B067: SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSL DROWN Attack, que permite a un atacante descifrar tráfico TLS debido al soporte de SSLv2.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones cifradas, lo que podría resultar en la exposición de datos sensibles y daños reputacionales si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y condiciones específicas, como captura previa de tráfico, lo que limita su facilidad de explotación, pero el impacto en la confidencialidad es significativo si se logra, pudiendo servir como punto de entrada para ataques más avanzados.

Acción: Deshabilitar SSLv2 y las suites de cifrado de grado de exportación en el servidor.

Análisis Técnico

- **Nombre:** SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
- **ID del Plugin:** 89058
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

La vulnerabilidad se debe a que el host soporta SSLv2 y cifrados débiles como EXP-RC2-CBC-MD5 y EXP-RC4-MD5, que utilizan claves de 40 bits, permitiendo un ataque de oráculo de padding Bleichenbacher que puede descifrar conexiones TLS capturadas al explotar servidores con la misma clave privada.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 3.6
- **EPSS Score:** 0.9015

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aislar temporalmente el host si es necesario.
2. Corrección: Deshabilitar SSLv2 y todas las suites de cifrado de exportación en la configuración del servidor web, y asegurar que las claves privadas no se usen en servidores que soporten SSLv2.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que SSLv2 está deshabilitado y solo se usan cifrados seguros.
4. Prevención: Implementar políticas de seguridad que prohíban el uso de protocolos obsoletos y realizar auditorías regulares de configuración criptográfica.

Conclusión: Aunque la urgencia es media, corregir esta vulnerabilidad es crucial para proteger la confidencialidad de las comunicaciones y prevenir posibles filtraciones de datos.

VULN-B068: SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) está afectado por la vulnerabilidad SSL DROWN Attack, que permite a un atacante descifrar tráfico TLS capturado debido al soporte de SSLv2.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones, lo que podría resultar en la exposición de datos sensibles y daños reputacionales si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y condiciones específicas, como el uso de claves privadas compartidas con servidores SSLv2, lo que limita su facilidad de explotación, pero el impacto potencial en la confidencialidad justifica una corrección prioritaria en el corto plazo para prevenir filtraciones de información.

Acción: Deshabilitar SSLv2 y las suites de cifrado de grado de exportación en el servidor afectado.

Análisis Técnico

- **Nombre:** SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
- **ID del Plugin:** 89058
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

La vulnerabilidad DROWN explota una debilidad en SSLv2 mediante un ataque de oráculo de padding de Bleichenbacher, permitiendo descifrar conexiones TLS si el mismo par de claves se utiliza en un servidor que soporta SSLv2. El plugin_output muestra que el host soporta suites de cifrado vulnerables, incluyendo EXP-RC2-CBC-MD5 y EXP-RC4-MD5 con claves débiles de 40 bits, así como RC4-MD5 con clave de 128 bits, lo que facilita a un atacante realizar conexiones especialmente diseñadas para recuperar la clave de sesión y descifrar tráfico previamente capturado.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 3.6
- **EPSS Score:** 0.9015

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red pública para reducir el riesgo de interceptación de tráfico.
2. **Corrección:** Deshabilitar SSLv2 y todas las suites de cifrado de exportación en la configuración del servidor web, y asegurar que las claves privadas no se compartan con servicios que soporten SSLv2.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-correción para confirmar que SSLv2 está deshabilitado y no se detectan cifrados débiles.
4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de protocolos obsoletos como SSLv2 y realizar auditorías regulares de configuración criptográfica.

Conclusión: La vulnerabilidad DROWN en BEE-BOX representa un riesgo moderado para la confidencialidad, exigiendo la deshabilitación inmediata de SSLv2 para proteger las comunicaciones y prevenir posibles filtraciones de datos.

VULN-B069: SSH Weak Algorithms Supported

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSH Weak Algorithms Supported, que permite el uso de algoritmos de cifrado débiles en el servicio SSH.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones SSH, permitiendo a atacantes potencialmente descifrar datos sensibles, lo que podría resultar en fugas de información y daño reputacional.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero facilita la interceptación de datos; debe abordarse en el corto plazo para mitigar riesgos de espionaje y prevenir su uso como punto de entrada para ataques más avanzados.

Acción: Eliminar los algoritmos de cifrado débiles (arcfour, arcfour128, arcfour256) de la configuración del servidor SSH.

Análisis Técnico

- **Nombre:** SSH Weak Algorithms Supported
- **ID del Plugin:** 90317
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/22/ssh)

Nessus detectó que el servidor SSH en el puerto 22 soporta algoritmos de cifrado débiles como arcfour, arcfour128 y arcfour256 tanto para comunicaciones servidor-a-cliente como cliente-a-servidor, lo que viola las recomendaciones del RFC 4253 debido a problemas con claves débiles que pueden ser explotados en ataques para descifrar el tráfico, comprometiendo la confidencialidad sin afectar directamente la integridad o disponibilidad.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico SSH en busca de actividades sospechosas y considerar el aislamiento temporal si se detecta un ataque.
2. **Corrección:** Modificar el archivo de configuración SSH (e.g., /etc/ssh/sshd_config) para deshabilitar los cifrados débiles especificando 'Ciphers' con algoritmos seguros como aes256-ctr.

3. **Verificación:** Ejecutar nuevamente el escaneo de Nessus o usar herramientas como ssh-audit para confirmar que los algoritmos débiles han sido eliminados.
4. **Prevención:** Implementar políticas de configuración segura para SSH en todos los servidores y realizar auditorías periódicas para asegurar el cumplimiento con estándares criptográficos.

Conclusión: Aunque el riesgo es medio, la corrección de los algoritmos débiles en SSH es esencial para proteger la confidencialidad de las comunicaciones y debe realizarse prontamente para evitar posibles interceptaciones de datos.

VULN-B070: Samba Badlock Vulnerability

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Samba está afectado por la vulnerabilidad Badlock, que permite a un atacante man-in-the-middle forzar una degradación de la autenticación.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de datos sensibles en bases de datos de Active Directory, lo que podría resultar en acceso no autorizado a información crítica y daño reputacional.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y condiciones específicas, lo que limita su facilidad, pero el impacto potencial es alto al permitir la ejecución de llamadas de red arbitrarias y modificación de datos de seguridad. Debe abordarse en el corto plazo para prevenir posibles compromisos en entornos vulnerables.

Acción: Actualizar Samba a la versión 4.2.11, 4.3.8, 4.4.2 o superior.

Análisis Técnico

- **Nombre:** Samba Badlock Vulnerability
- **ID del Plugin:** 90509
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/445/cifs)

Nessus detectó que el parche para Badlock no ha sido aplicado en el servidor Samba que ejecuta en el puerto tcp/445/cifs. Esta vulnerabilidad, identificada como CVE-2016-2118, surge de una negociación inadecuada del nivel de autenticación en los protocolos SAM y LSAD sobre canales RPC, permitiendo a un atacante interceptar el tráfico y degradar la autenticación para ejecutar operaciones Samba arbitrarias en el contexto del usuario interceptado, lo que podría llevar a la visualización o alteración de datos en bases de datos de seguridad.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 6.8 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:P/A:P))
- **VPR Score:** 5.9
- **EPSS Score:** 0.7865

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red o implementar reglas de firewall para restringir el acceso al puerto 445 si es posible.
2. Corrección: Aplicar la actualización de Samba a la versión 4.2.11, 4.3.8, 4.4.2 o posterior siguiendo las guías oficiales de Samba.
3. Verificación: Realizar un escaneo posterior con Nessus u otras herramientas para confirmar que la vulnerabilidad ha sido mitigada y que el servicio funciona correctamente.
4. Prevención: Establecer políticas de gestión de parches regulares, monitorear el tráfico de red para detectar actividades sospechosas de man-in-the-middle, y educar a los usuarios sobre los riesgos asociados con conexiones no seguras.

Conclusión: La vulnerabilidad Badlock en Samba presenta un riesgo medio que requiere actualización prioritaria para proteger la integridad de los datos sensibles y prevenir posibles explotaciones en la red.

VULN-B071: Network Time Protocol (NTP) Mode 6 Scanner

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic tiene la vulnerabilidad Network Time Protocol (NTP) Mode 6 Scanner que responde a consultas modo 6.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la disponibilidad del servicio al permitir ataques de denegación de servicio reflejados, lo que podría afectar la operatividad del negocio y dañar la reputación si se explota.

Urgencia: Media. La vulnerabilidad tiene un riesgo medio debido a su facilidad de explotación remota sin autenticación, pero el impacto se limita principalmente a la disponibilidad sin comprometer la confidencialidad o integridad; sin embargo, podría ser utilizada como un vector inicial para ataques más amplios si no se mitiga.

Acción: Restringir las consultas modo 6 en el servidor NTP.

Análisis Técnico

- **Nombre:** Network Time Protocol (NTP) Mode 6 Scanner
- **ID del Plugin:** 97861
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (udp/123/ntp)

El servidor NTP en el host remoto responde a consultas modo 6, como se evidencia en la salida del plugin que muestra detalles como la versión 'ntpd 4.2.4p4' y información del sistema. Esto permite a un atacante no autenticado enviar consultas especialmente diseñadas para explotar la vulnerabilidad, potencialmente causando una amplificación de tráfico en ataques de denegación de servicio reflejados, lo que podría saturar recursos de red y afectar el servicio sin comprometer directamente los datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium

- **Puntuación Base CVSS v3.0:** 5.8 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:N/A:P))

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor NTP de la red pública o implementar reglas de firewall para bloquear consultas modo 6 entrantes.
2. Corrección: Configurar el demonio NTP para deshabilitar o restringir el acceso a consultas modo 6, por ejemplo, usando opciones como 'restrict default nomodify notrap noquery' en ntp.conf.
3. Verificación: Realizar pruebas de penetración o escaneos posteriores para confirmar que las consultas modo 6 ya no son respondidas y que el servidor funciona correctamente.
4. Prevención: Implementar monitoreo continuo de tráfico NTP, actualizar regularmente el software NTP a versiones seguras, y educar al personal sobre mejores prácticas de configuración para prevenir vulnerabilidades similares.

Conclusión: La vulnerabilidad en NTP mode 6 representa un riesgo medio para la disponibilidad del servicio y debe ser mitigada rápidamente para prevenir posibles ataques de denegación de servicio y proteger la infraestructura de red.

VULN-M014: TLS Version 1.0 Protocol Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad TLS Version 1.0 Protocol Detection en el servicio SMTP (puerto 25), que utiliza una versión obsoleta de TLS con deficiencias criptográficas.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de las comunicaciones de correo electrónico, permitiendo a atacantes interceptar información sensible, lo que podría resultar en daños reputacionales y violaciones de cumplimiento normativo como PCI DSS.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, la presencia de TLS 1.0 aumenta el riesgo de interceptación de datos y no cumple con los estándares de seguridad modernos, justificando su corrección en el corto plazo para mitigar riesgos de fuga de información y evitar sanciones por incumplimiento.

Acción: Habilitar el soporte para TLS 1.2 y 1.3, y deshabilitar el soporte para TLS 1.0 en el servicio SMTP.

Análisis Técnico

- **Nombre:** TLS Version 1.0 Protocol Detection
- **ID del Plugin:** 104743
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el host METASPLOITABLE acepta conexiones cifradas con TLSv1, lo que indica que utiliza protocolos criptográficos obsoletos con vulnerabilidades conocidas, como BEAST o POODLE, que pueden ser explotadas en ataques man-in-the-middle para descifrar tráfico. Aunque las implementaciones modernas mitigan algunos problemas, TLS 1.0 carece de las mejoras de seguridad de versiones posteriores, exponiendo las comunicaciones a riesgos de interceptación y violación de la integridad de los datos, especialmente en entornos donde el tráfico no está adecuadamente protegido.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el servicio SMTP de redes no confiables o implementar reglas de firewall para restringir el acceso mientras se aplica la corrección.
2. **Corrección:** Configurar el servidor SMTP para deshabilitar TLS 1.0 y habilitar exclusivamente TLS 1.2 y 1.3, utilizando cifrados fuertes como AES-GCM.
3. **Verificación:** Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que TLS 1.0 está deshabilitado y que las conexiones utilizan solo versiones seguras de TLS.
4. **Prevención:** Establecer políticas de seguridad que exijan la auditoría regular de configuraciones criptográficas y la actualización continua de protocolos para cumplir con estándares como PCI DSS y evitar la reintroducción de versiones obsoletas.

Conclusión: El uso de TLS 1.0 en el servicio SMTP representa un riesgo moderado para la confidencialidad de los datos y el cumplimiento normativo, exigiendo su corrección pronta para proteger las comunicaciones y evitar posibles brechas de seguridad.

VULN-M015: TLS Version 1.0 Protocol Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) tiene la vulnerabilidad TLS Version 1.0 Protocol Detection en el servicio PostgreSQL en el puerto tcp/5432.

Riesgo para el Negocio: El uso de TLS 1.0 puede comprometer la confidencialidad de los datos transmitidos, permitiendo a atacantes interceptar información sensible, lo que podría resultar en daños reputacionales y violaciones de cumplimiento como PCI DSS.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle y no conduce a un compromiso directo inmediato, la debilidad criptográfica aumenta el riesgo de fugas de datos y no cumple con los estándares modernos de seguridad, por lo que debe abordarse en el próximo ciclo de parches para mitigar riesgos potenciales.

Acción: Habilitar el soporte para TLS 1.2 y 1.3, y deshabilitar el soporte para TLS 1.0 en el servicio PostgreSQL.

Análisis Técnico

- **Nombre:** TLS Version 1.0 Protocol Detection
- **ID del Plugin:** 104743
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El servicio PostgreSQL en el puerto 5432 acepta conexiones cifradas utilizando TLSv1, que tiene fallos criptográficos conocidos, como vulnerabilidades a ataques como BEAST o POODLE, lo que podría permitir a un atacante descifrar el tráfico en condiciones específicas de red, comprometiendo la confidencialidad de los datos en tránsito.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.1 ((CVSS2\#AV:N/AC:H/Au:N/C:C/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor de redes no confiables si es posible para reducir la exposición.
2. Corrección: Configurar el servicio PostgreSQL para deshabilitar TLS 1.0 y habilitar solo TLS 1.2 o superior, utilizando cifrados fuertes.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que TLS 1.0 está deshabilitado y que las conexiones utilizan versiones seguras de TLS.
4. Prevención: Implementar políticas de seguridad que exijan el uso de protocolos criptográficos modernos y realizar auditorías regulares para garantizar el cumplimiento.

Conclusión: Aunque el riesgo es medio, la corrección de TLS 1.0 es esencial para proteger la confidencialidad de los datos y cumplir con los estándares de seguridad, requiriendo su implementación prioritaria.

VULN-M016: HTTP TRACE / TRACK Methods Allowed

Resumen Ejecutivo

Problema: El servidor web en METASPLOITABLE (192.168.122.29) permite los métodos HTTP TRACE y TRACK, lo que constituye la vulnerabilidad HTTP TRACE / TRACK Methods Allowed.

Riesgo para el Negocio: Esta vulnerabilidad puede conducir a la divulgación de información confidencial, como cookies de sesión, a través de ataques de tipo cross-site tracing, comprometiendo la confidencialidad y potencialmente dañando la reputación de la organización.

Urgencia: Media. La explotación de esta vulnerabilidad es relativamente sencilla y no requiere autenticación, pero su impacto principal es la fuga de información en lugar de un compromiso directo del sistema. Debe abordarse en el corto plazo para mitigar riesgos de espionaje y cumplir con estándares de seguridad, aunque no es tan urgente como vulnerabilidades que permiten ejecución remota de código.

Acción: Deshabilitar los métodos HTTP TRACE y TRACK en la configuración del servidor web Apache.

Análisis Técnico

- **Nombre:** HTTP TRACE / TRACK Methods Allowed
- **ID del Plugin:** 11213
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/80/www)

La vulnerabilidad surge porque el servidor Apache en la IP 192.168.122.29 responde a solicitudes TRACE y TRACK, métodos HTTP diseñados para depuración que reflejan la solicitud recibida de vuelta al cliente. En el output del plugin, se observa que una solicitud TRACE enviada por Nessus fue respondida con un código 200 OK, devolviendo exactamente los encabezados de la solicitud, lo que demuestra que estos métodos están habilitados. Técnicamente, esto puede ser explotado en combinación con técnicas como cross-site scripting (XSS) para robar cookies de autenticación u otra información sensible, ya que un atacante podría usar TRACE para obtener datos reflejados en las respuestas, aunque no permite directamente la ejecución de código o modificación de datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 4.0
- **EPSS Score:** 0.524

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para bloquear solicitudes HTTP que utilicen los métodos TRACE y TRACK en la red perimetral.
2. **Corrección:** Modificar el archivo de configuración de Apache (e.g., httpd.conf o archivos de virtual host) añadiendo 'TraceEnable off' para versiones compatibles, o usar reglas de rewrite como 'RewriteEngine on', 'RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)', 'RewriteRule . - [F]' para deshabilitar estos métodos y devolver un error 403.
3. **Verificación:** Realizar un escaneo de vulnerabilidades con herramientas como Nessus o ejecutar pruebas manuales enviando solicitudes TRACE/TACK para confirmar que ya no son respondidas con éxito.
4. **Prevención:** Establecer políticas de seguridad que deshabiliten métodos HTTP innecesarios por defecto en todos los servidores web, y realizar auditorías periódicas para asegurar el cumplimiento.

Conclusión: La habilitación de métodos HTTP TRACE y TRACK en METASPLOITABLE presenta un riesgo medio de fuga de información confidencial, exigiendo su deshabilitación inmediata para proteger la integridad de los datos y mantener la confidencialidad del sistema.

VULN-M017: Apache Tomcat Default Files

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad Apache Tomcat Default Files, que expone archivos predeterminados en el servidor web.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al permitir que atacantes obtengan información sensible sobre la configuración del servidor, lo que podría facilitar ataques más avanzados y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad es fácilmente explotable a través de solicitudes HTTP estándar sin autenticación, lo que podría llevar a la divulgación de información que sirva como punto de entrada para otros ataques, pero no permite un compromiso directo del sistema o interrupción del servicio.

Acción: Eliminar los archivos predeterminados, como la página de índice y los ejemplos de JSP y servlets, y configurar una página de error personalizada en el servidor Apache Tomcat.

Análisis Técnico

- **Nombre:** Apache Tomcat Default Files
- **ID del Plugin:** 12085
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/8180/www)

La vulnerabilidad se manifiesta a través del puerto TCP 8180, donde el servidor Apache Tomcat en Linux Ubuntu 8.04 expone archivos predeterminados, como tomcat-docs/index.html, y no devuelve una página personalizada para recursos no existentes, lo que puede revelar detalles de la instalación y facilitar a los atacantes el mapeo del entorno y la planificación de exploits adicionales basados en la información obtenida.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Restringir el acceso al puerto 8180 mediante firewalls o listas de control de acceso para limitar la exposición temporalmente.
2. **Corrección:** Eliminar todos los archivos predeterminados no esenciales, incluyendo las páginas de índice y ejemplos, y seguir las guías de OWASP para configurar páginas de error personalizadas que no divulguen información.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los archivos predeterminados han sido removidos y que las páginas de error no filtran datos sensibles.
4. **Prevención:** Implementar políticas de hardening para servidores Tomcat, como deshabilitar servicios innecesarios y realizar auditorías regulares de seguridad para evitar la reinstalación de archivos predeterminados en futuras actualizaciones o despliegues.

Conclusión: La exposición de archivos predeterminados en Apache Tomcat representa un riesgo de divulgación de información que debe abordarse prontamente para proteger la confidencialidad y prevenir posibles escaladas de ataques.

VULN-M018: ISC BIND Service Downgrade / Reflected DoS

Resumen Ejecutivo

Problema: El servidor DNS en 192.168.122.29 (METASPLOITABLE) ejecuta ISC BIND 9.4.2 y es vulnerable a ISC BIND Service Downgrade / Reflected DoS, permitiendo ataques de denegación de servicio.

Riesgo para el Negocio: Esta vulnerabilidad puede degradar la disponibilidad del servicio DNS, afectando la resolución de nombres y la conectividad de red, lo que podría dañar la reputación y la operatividad del negocio.

Urgencia: Media. La vulnerabilidad tiene un CVSS3 de 8.6, indicando un alto impacto en la disponibilidad, pero su explotación requiere un atacante remoto no autenticado y no conduce a compromisos directos del sistema; sin embargo, puede ser utilizada en ataques de reflexión, por lo que debe abordarse en el corto plazo para mitigar riesgos operativos.

Acción: Actualizar ISC BIND a la versión 9.11.19 o superior.

Análisis Técnico

- **Nombre:** ISC BIND Service Downgrade / Reflected DoS
- **ID del Plugin:** 136769
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (udp/53/dns)

La vulnerabilidad en ISC BIND 9.4.2 se debe a que no limita adecuadamente el número de consultas durante el procesamiento de respuestas de referencia, lo que permite a un atacante remoto enviar solicitudes maliciosas para degradar el rendimiento del servidor recursivo o utilizarlo en ataques de denegación de servicio reflejados, aumentando la carga y potencialmente interrumpiendo el servicio DNS sin comprometer la confidencialidad o integridad de los datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 8.6 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:N/A:P))
- **VPR Score:** 5.2
- **EPSS Score:** 0.0334

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para limitar el tráfico UDP/53 desde fuentes no confiables y monitorear el tráfico DNS en busca de anomalías.
2. Corrección: Actualizar el software ISC BIND a la versión 9.11.19 o superior siguiendo las instrucciones del proveedor.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que la actualización ha mitigado el problema y que el servicio DNS funciona correctamente.

4. Prevención: Establecer políticas de gestión de parches regulares, configurar BIND para limitar las consultas recursivas y educar al personal sobre las mejores prácticas de seguridad DNS.

Conclusión: La vulnerabilidad en ISC BIND amenaza la disponibilidad del servicio DNS y requiere una actualización prioritaria para proteger la infraestructura de red y mantener la continuidad del negocio.

VULN-M019: ISC BIND Denial of Service

Resumen Ejecutivo

Problema: El servidor METASPLOITABLE (192.168.122.29) ejecuta una versión vulnerable de ISC BIND en el puerto UDP/53, susceptible a una denegación de servicio debido a una falla de aserción.

Riesgo para el Negocio: Esta vulnerabilidad puede causar interrupciones en la disponibilidad del servicio DNS, afectando la resolución de nombres y potencialmente impactando operaciones críticas que dependen de la conectividad de red, lo que podría dañar la reputación si los servicios se vuelven inaccesibles.

Urgencia: Media. La explotación requiere un atacante remoto no autenticado que envíe mensajes especialmente manipulados, pero la probabilidad es moderada debido a la necesidad de condiciones específicas y la puntuación EPSS alta de 0.9228 indica un riesgo significativo de explotación en el entorno. Aunque no compromete la confidencialidad o integridad, la denegación de servicio podría ser utilizada como un paso inicial para ataques más amplios, por lo que se recomienda abordarla en un plazo corto para mitigar impactos operativos.

Acción: Actualizar ISC BIND a la versión 9.11.19 o superior para parchear la vulnerabilidad.

Análisis Técnico

- **Nombre:** ISC BIND Denial of Service
- **ID del Plugin:** 136808
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (udp/53/dns)

La vulnerabilidad CVE-2020-8617 en ISC BIND versión 9.4.2, como se indica en el plugin_output, implica una falla de aserción que puede ser explotada mediante mensajes DNS manipulados para provocar que el servicio se detenga, resultando en una denegación de servicio. Esto afecta la disponibilidad del servidor DNS sin comprometer datos, pero interrumpe la funcionalidad crítica de resolución de nombres en la red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:N/I:N/A:P))
- **VPR Score:** 4.4
- **EPSS Score:** 0.9228

Acciones Recomendadas

1. Contención: Monitorear el tráfico DNS en busca de actividades sospechosas y aplicar reglas de firewall para bloquear intentos de explotación.
2. Corrección: Actualizar el software BIND a la versión 9.11.19 o una versión parcheada compatible, siguiendo las guías de ISC.
3. Verificación: Realizar pruebas de funcionalidad después de la actualización para asegurar que el servicio DNS opera correctamente y escanear nuevamente con Nessus para confirmar la remediación.
4. Prevención: Implementar parches de seguridad de manera proactiva, revisar y endurecer las configuraciones de BIND, y establecer monitoreo continuo para detectar vulnerabilidades similares.

Conclusión: La vulnerabilidad en ISC BIND plantea un riesgo medio de denegación de servicio que debe abordarse prontamente mediante la actualización para mantener la disponibilidad operativa y prevenir interrupciones en la infraestructura de red.

VULN-M020: ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Resumen Ejecutivo

Problema: El servidor DNS en 192.168.122.29 (METASPLOITABLE) ejecuta ISC BIND 9.4.2, afectado por la vulnerabilidad de denegación de servicio ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS.

Riesgo para el Negocio: Esta vulnerabilidad puede causar la caída del servidor DNS, interrumpiendo la resolución de nombres y afectando la disponibilidad de servicios críticos, lo que podría dañar la reputación y operaciones empresariales.

Urgencia: Media. La explotación requiere autenticación y acceso remoto, pero si se aprovecha, provoca una denegación de servicio inmediata al hacer que el servidor se cierre, lo que podría ser utilizado como un paso inicial para ataques más amplios en la red, aunque no conduce a compromisos de confidencialidad o integridad directamente.

Acción: Actualizar ISC BIND a la versión 9.11.22, 9.16.6, 9.17.4 o superior.

Análisis Técnico

- **Nombre:** ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
- **ID del Plugin:** 139915
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (udp/53/dns)

La vulnerabilidad en ISC BIND versión 9.4.2 surge de un error de aserción al verificar una respuesta truncada a una solicitud firmada con TSIG, lo que permite a un atacante autenticado enviar dicha respuesta para provocar la salida abrupta del servidor, resultando en una denegación de servicio sin comprometer datos, como se indica en la salida del plugin que muestra la versión instalada y fija.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H))
- **Puntuación Base CVSS v2.0:** 4.0 ((CVSS2\#AV:N/AC:L/Au:S/C:N/I:N/A:P))
- **VPR Score:** 4.4
- **EPSS Score:** 0.0045

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor de la red si es posible para prevenir explotaciones.
2. Corrección: Aplicar la actualización de BIND a una versión segura como 9.11.22 o posterior.
3. Verificación: Realizar pruebas post-actualización para confirmar que la vulnerabilidad está mitigada y el servicio DNS funciona correctamente.
4. Prevención: Implementar monitoreo continuo y políticas de parcheo proactivas para evitar vulnerabilidades similares en el futuro.

Conclusión: Aunque el riesgo es medio, la vulnerabilidad en BIND amenaza la disponibilidad del DNS y debe corregirse prontamente para mantener la continuidad operativa y prevenir interrupciones en la red.

VULN-M021: SSL Certificate Expiry

Resumen Ejecutivo

Problema: El servidor METASPLOITABLE (192.168.122.29) tiene un certificado SSL expirado en el servicio SMTP, identificado como SSL Certificate Expiry.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían dañar la reputación de la organización y exponer datos sensibles.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un contexto de red, ya que un certificado expirado facilita ataques de interceptación sin autenticación adicional, pero no conduce directamente a un compromiso total del sistema; sin embargo, podría ser un paso inicial para ataques más graves si no se corrige.

Acción: Comprar o generar un nuevo certificado SSL y reemplazar el existente.

Análisis Técnico

- **Nombre:** SSL Certificate Expiry
- **ID del Plugin:** 15901
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El certificado SSL para el servicio SMTP en el puerto tcp/25 ha expirado desde el 16 de abril de 2010, como se indica en los campos 'Not valid after'. Esto significa que las conexiones SSL/TLS no pueden es-

tablecer un canal seguro de forma confiable, ya que los clientes y servidores pueden rechazar o advertir sobre el certificado inválido, permitiendo potencialmente a atacantes realizar ataques man-in-the-middle para interceptar, modificar o leer comunicaciones sin ser detectados, aunque no compromete directamente la confidencialidad o disponibilidad de manera severa según las puntuaciones CVSS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el servidor de redes públicas si es crítico y monitorear el tráfico SMTP para detectar actividades sospechosas.
2. **Corrección:** Adquirir un certificado SSL válido de una autoridad de certificación confiable e implementarlo en el servicio SMTP, asegurando que esté correctamente configurado.
3. **Verificación:** Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado esté instalado y no haya expirado, y realizar pruebas de conectividad.
4. **Prevención:** Establecer un proceso de gestión de ciclos de vida de certificados con alertas automáticas para renovaciones antes de la expiración, y auditar regularmente todos los servicios SSL/TLS en la infraestructura.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

VULN-M022: SSL Certificate Expiry

Resumen Ejecutivo

Problema: El servidor METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad SSL Certificate Expiry, donde el certificado SSL ha caducado.

Riesgo para el Negocio: Esto puede comprometer la integridad de las comunicaciones, permitiendo ataques man-in-the-middle que alteren datos, y dañar la reputación al mostrar descuido en la gestión de seguridad.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle, lo que podría llevar a la interceptación o modificación de datos sensibles, aunque no compromete directamente la confidencialidad o disponibilidad; sin embargo, su corrección es prioritaria para prevenir escaladas de ataque y mantener la confianza del usuario.

Acción: Comprar o generar un nuevo certificado SSL y reemplazar el existente.

Análisis Técnico

- **Nombre:** SSL Certificate Expiry
- **ID del Plugin:** 15901
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El certificado SSL del servicio PostgreSQL en el puerto tcp/5432 ha caducado, con fechas de validez del 17 de marzo de 2010 al 16 de abril de 2010, lo que significa que ya no es válido según los estándares de seguridad; esto permite que atacantes realicen ataques man-in-the-middle para espiar o manipular las comunicaciones cifradas, explotando la falta de autenticación adecuada y potencialmente accediendo a datos en tránsito sin detección.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar actividades sospechosas y considerar la implementación temporal de reglas de firewall para restringir el acceso no autorizado.
2. Corrección: Adquirir un certificado SSL válido de una autoridad de certificación confiable o generar uno interno, y configurarlo en el servicio PostgreSQL para reemplazar el certificado caducado.
3. Verificación: Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado está instalado correctamente y es válido, verificando las fechas de expiración y la cadena de confianza.
4. Prevención: Establecer un proceso automatizado de gestión de certificados que incluya alertas tempranas para renovaciones, realizar auditorías periódicas de certificados SSL en todos los servicios, y capacitar al personal en mejores prácticas de seguridad criptográfica.

Conclusión: La caducidad del certificado SSL en PostgreSQL representa un riesgo medio que exige una acción inmediata para prevenir posibles manipulaciones de datos y proteger la integridad de las comunicaciones.

VULN-M023: SSL Weak Cipher Suites Supported

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 en Ubuntu 8.04 presenta la vulnerabilidad SSL Weak Cipher Suites Supported en el servicio SMTP (puerto tcp/25), que permite el uso de cifrados SSL débiles.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones al permitir que atacantes descifren datos transmitidos, lo que podría resultar en la exposición de información sensible y daño reputacional si se explota.

Urgencia: Media. La explotación de esta vulnerabilidad es factible, especialmente en redes locales, pero requiere un ataque man-in-the-middle activo para interceptar y descifrar el tráfico; aunque no conduce a un compromiso directo del sistema, facilita la fuga de información y podría ser un paso inicial para ataques más avanzados, por lo que debe abordarse en el corto plazo para mitigar riesgos de seguridad.

Acción: Reconfigurar la aplicación afectada para deshabilitar el uso de cifrados SSL débiles.

Análisis Técnico

- **Nombre:** SSL Weak Cipher Suites Supported
- **ID del Plugin:** 26928
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el host remoto soporta múltiples suites de cifrado SSL débiles, incluyendo cifrados de exportación con claves de 40 bits o menos (como EXP-RC2-CBC-MD5 y EXP-RC4-MD5), así como cifrados no autenticados (como ADH-DES-CBC-SHA). Estos cifrados utilizan algoritmos obsoletos y de baja entropía (por ejemplo, RC4, DES, RC2), lo que los hace susceptibles a ataques de fuerza bruta o criptoanálisis. En un escenario de ataque, un adversario en la misma red podría realizar un ataque man-in-the-middle para downgrade la conexión SSL a un cifrado débil, interceptar el tráfico SMTP y descifrar mensajes de correo electrónico, comprometiendo la confidencialidad sin alterar la integridad o disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red pública o implementar reglas de firewall para restringir el acceso al puerto 25 solo a hosts confiables.
2. **Corrección:** Reconfigurar el servidor SMTP (por ejemplo, en Postfix o Sendmail) para deshabilitar los cifrados débiles listados en el plugin_output, utilizando herramientas como openssl ciphers para especificar suites seguras (por ejemplo, TLS_AES_256_GCM_SHA384).
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección usando Nessus o OpenVAS para confirmar que los cifrados débiles ya no están soportados y validar la configuración SSL con herramientas como sslyze.
4. **Prevención:** Establecer políticas de seguridad que exijan el uso exclusivo de cifrados fuertes (por ejemplo, TLS 1.2 o superior con AES-GCM) y realizar auditorías periódicas de configuración SSL en todos los servicios de red.

Conclusión: El soporte de cifrados SSL débiles en el servicio SMTP representa un riesgo moderado para la confidencialidad de los datos y debe corregirse prontamente para prevenir posibles intercepta-ciones y cumplir con estándares de seguridad criptográfica.

VULN-M024: NFS Shares World Readable

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 en Ubuntu 8.04 tiene la vulnerabilidad NFS Shares World Readable, donde el servidor NFS exporta recursos compartidos sin restricciones de acceso.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad al permitir que actores no autorizados accedan y lean datos sensibles almacenados en los recursos compartidos, lo que podría resultar en fugas de información y daños reputacionales.

Urgencia: Media. La vulnerabilidad es fácilmente explotable a través de la red sin autenticación, lo que permite a atacantes remotos leer información confidencial, aunque no compromete la integridad o disponibilidad directamente; sin embargo, puede servir como punto de entrada para ataques posteriores y debe abordarse prontamente para mitigar riesgos de exposición de datos.

Acción: Implementar restricciones de acceso apropiadas en todos los recursos compartidos de NFS basadas en hostname, IP o rango de IP.

Análisis Técnico

- **Nombre:** NFS Shares World Readable
- **ID del Plugin:** 42256
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/2049/rpc-nfs)

La vulnerabilidad surge porque el servidor NFS en el puerto tcp/2049 está exportando recursos compartidos, específicamente el directorio raíz '/', sin aplicar restricciones de acceso, lo que significa que cualquier cliente en la red puede montar y leer estos recursos sin autenticación; esto viola los principios de seguridad de NFS y expone potencialmente todos los datos en los recursos compartidos a accesos no autorizados, facilitando la recolección de información sensible y aumentando la superficie de ataque.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el servidor NFS de la red o implementar reglas de firewall para restringir el acceso al puerto 2049 solo a hosts autorizados.
2. Corrección: Modificar el archivo /etc/exports para agregar restricciones de acceso, como 'ro,sync,no_subtree_check 192.168.1.0/24' para limitar a una subred específica, y reiniciar el servicio NFS.
3. Verificación: Utilizar herramientas como showmount o escaneos NFS para confirmar que los recursos compartidos ya no son accesibles mundialmente y realizar pruebas de acceso desde hosts no autorizados.
4. Prevención: Establecer políticas de seguridad para NFS que incluyan revisiones periódicas de configuraciones, uso de NFSv4 con Kerberos para autenticación, y monitoreo continuo de accesos no autorizados.

Conclusión: La exposición de recursos NFS sin restricciones en METASPLOITABLE representa un riesgo significativo de fuga de datos y debe corregirse de inmediato para proteger la confidencialidad de la información y prevenir accesos no autorizados.

VULN-M025: Unencrypted Telnet Server

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) ejecuta un servidor Telnet no cifrado, permitiendo la transmisión de datos en texto claro.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de los datos, ya que las credenciales y comandos pueden ser interceptados, lo que podría llevar a accesos no autorizados y daños reputacionales.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo, pero es relativamente fácil de ejecutar en redes no confiables, pudiendo servir como punto de entrada para ataques más avanzados; debe abordarse prontamente para mitigar riesgos de fuga de información.

Acción: Deshabilitar el servicio Telnet y utilizar SSH en su lugar.

Análisis Técnico

- **Nombre:** Unencrypted Telnet Server
- **ID del Plugin:** 42263
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/23/telnet)

El servidor Telnet en el puerto tcp/23 transmite todo el tráfico, incluyendo inicios de sesión y comandos, en texto claro sin cifrado, como se evidencia en el banner recogido por Nessus que muestra un prompt de login; esto permite a un atacante en la misma red interceptar y manipular las comunicaciones, exponiendo credenciales como 'msfadmin/msfadmin' y facilitando el espionaje o modificación de datos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.8 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de redes no confiables para prevenir interceptaciones.
2. **Corrección:** Desinstalar o detener el servicio Telnet y configurar SSH con autenticación segura.
3. **Verificación:** Realizar pruebas de penetración para confirmar que Telnet está deshabilitado y SSH funciona correctamente.
4. **Prevención:** Implementar políticas que prohíban el uso de protocolos no cifrados y realizar auditorías regulares de servicios de red.

Conclusión: El servidor Telnet no cifrado en METASPLOITABLE representa un riesgo medio que debe corregirse rápidamente para proteger la confidencialidad de los datos y prevenir accesos no autorizados.

VULN-M026: SSL Medium Strength Cipher Suites Supported (SWEET32)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 en Ubuntu 8.04 presenta la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32) en el servicio SMTP en el puerto tcp/25.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones al permitir que atacantes descifren datos transmitidos, lo que podría resultar en la exposición de información sensible y daño reputacional si se explota.

Urgencia: Media. La vulnerabilidad tiene un CVSS3 de 7.5, indicando un alto impacto en la confidencialidad, pero su explotación requiere que el atacante esté en la misma red física, lo que limita la facilidad de ataque. Aunque no es inmediatamente explotable de forma remota, debe abordarse prontamente para prevenir posibles filtraciones de datos y evitar que sirva como punto de entrada para ataques más avanzados.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados de fuerza media.

Análisis Técnico

- **Nombre:** SSL Medium Strength Cipher Suites Supported (SWEET32)
- **ID del Plugin:** 42873
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el host soporta suites de cifrado SSL de fuerza media, incluyendo cifrados como DES-CBC3-MD5 y EDH-RSA-DES-CBC3-SHA, que utilizan longitudes de clave entre 64 y 112 bits o el algoritmo 3DES. Estos cifrados son vulnerables a ataques como SWEET32 (CVE-2016-2183), que explotan colisiones en bloques de cifrado para descifrar datos en tránsito después de capturar un volumen suficiente de tráfico, comprometiendo la confidencialidad de las comunicaciones sin autenticación y con un vector de ataque de red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.2879

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de redes no confiables para reducir el riesgo de explotación.

2. **Corrección:** Reconfigurar el servicio SMTP para deshabilitar los cifrados de fuerza media y habilitar solo suites fuertes, como AES con claves de al menos 128 bits.
3. **Verificación:** Realizar un escaneo posterior con Nessus o herramientas similares para confirmar que los cifrados vulnerables han sido eliminados.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas para detectar configuraciones inseguras.

Conclusión: La vulnerabilidad SWEET32 en METASPLOITABLE representa un riesgo medio para la confidencialidad y debe corregirse prontamente mediante la reconfiguración del servicio para prevenir la posible interceptación de comunicaciones sensibles.

VULN-M027: SSL Medium Strength Cipher Suites Supported (SWEET32)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad SSL Medium Strength Cipher Suites Supported (SWEET32) en el servicio PostgreSQL en el puerto tcp/5432, que permite el uso de cifrados SSL de fuerza media.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que un atacante podría descifrar información sensible, lo que podría resultar en pérdida de datos y daño reputacional si se explota.

Urgencia: Media. La vulnerabilidad tiene un CVSS3 de 7.5, indicando un alto impacto en la confidencialidad, pero su explotación requiere que el atacante esté en la misma red física, lo que limita la facilidad de explotación en entornos no locales; sin embargo, debe abordarse prontamente para prevenir posibles filtraciones de datos y evitar que sirva como punto de entrada para ataques más avanzados.

Acción: Reconfigurar la aplicación PostgreSQL para deshabilitar el uso de cifrados de fuerza media.

Análisis Técnico

- **Nombre:** SSL Medium Strength Cipher Suites Supported (SWEET32)
- **ID del Plugin:** 42873
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El servicio PostgreSQL en el host soporta cifrados SSL de fuerza media, específicamente EDH-RSA-DES-CBC3-SHA y DES-CBC3-SHA, que utilizan 3DES-CBC con claves de 168 bits, considerados inseguros según los estándares actuales debido a vulnerabilidades como SWEET32 (CVE-2016-2183), que permiten ataques de birthday bound para reducir la seguridad efectiva a aproximadamente 112 bits, facilitando el descifrado de datos en tránsito si un atacante intercepta el tráfico en la misma red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium

- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 6.1
- **EPSS Score:** 0.2879

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de redes no confiables o implementar reglas de firewall para restringir el acceso al puerto 5432.
2. Corrección: Modificar la configuración de PostgreSQL para eliminar los cifrados de fuerza media, utilizando solo suites fuertes como AES-GCM.
3. Verificación: Ejecutar un escaneo de vulnerabilidades con Nessus o herramientas similares para confirmar que los cifrados inseguros han sido deshabilitados.
4. Prevención: Establecer políticas de seguridad que exijan el uso exclusivo de cifrados fuertes en todos los servicios y realizar auditorías periódicas.

Conclusión: La vulnerabilidad SWEET32 en PostgreSQL amenaza la confidencialidad de los datos y debe corregirse rápidamente para mitigar riesgos de interceptación y cumplir con las mejores prácticas de seguridad.

VULN-M028: SSL Certificate with Wrong Hostname

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad SSL Certificate with Wrong Hostname en el servicio SMTP.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la integridad de las comunicaciones al permitir ataques de suplantación de identidad, lo que podría dañar la reputación de la organización y exponer datos sensibles a interceptación.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en un ataque man-in-the-middle, pero no conduce directamente a un compromiso del sistema; sin embargo, su corrección es importante para prevenir posibles escaladas de ataque y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido para el servicio SMTP con el nombre de host correcto.

Análisis Técnico

- **Nombre:** SSL Certificate with Wrong Hostname
- **ID del Plugin:** 45411
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el puerto 25 utiliza un certificado SSL cuyo atributo commonName (CN) es ‘ubuntu804-base.localdomain’, que no coincide con las identidades conocidas del host (192.168.122.29

o METASPLOITABLE). Esto indica una mala configuración que puede ser explotada mediante ataques de intermediario para interceptar o manipular comunicaciones, aunque no compromete directamente la confidencialidad o disponibilidad, sí afecta la integridad al permitir la suplantación del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle en el servicio SMTP.
2. **Corrección:** Reemplazar el certificado SSL actual con uno válido que incluya el nombre de host correcto (por ejemplo, METASPLOITABLE o la dirección IP) y configurar el servicio para usar solo certificados confiables.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado se presenta correctamente y no hay discrepancias.
4. **Prevención:** Implementar políticas de gestión de certificados que aseguren la renovación y validación periódica de certificados SSL para todos los servicios, y capacitar al personal en mejores prácticas de seguridad criptográfica.

Conclusión: La discrepancia en el certificado SSL del servicio SMTP representa un riesgo de integridad que debe corregirse para prevenir ataques de suplantación y proteger la confianza en las comunicaciones de la organización.

VULN-M029: SSL Certificate with Wrong Hostname

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad 'SSL Certificate with Wrong Hostname' en el servicio PostgreSQL en el puerto 5432.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían llevar a la exposición de datos sensibles y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad tiene un CVSS de 5.3, indicando un riesgo moderado debido a que no compromete directamente la confidencialidad o disponibilidad, pero facilita ataques de suplantación que podrían ser explotados en combinación con otras debilidades para escalar privilegios o acceder a información, aunque requiere un atacante en la red para su explotación efectiva.

Acción: Adquirir o generar un certificado SSL válido para el servicio PostgreSQL en este host.

Análisis Técnico

- **Nombre:** SSL Certificate with Wrong Hostname
- **ID del Plugin:** 45411
- **Severidad:** Media

- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El servicio PostgreSQL en el puerto tcp/5432 presenta un certificado SSL cuyo atributo 'commonName' (CN) es 'ubuntu804-base.localdomain', que no coincide con las identidades conocidas del host (192.168.122.29). Esto indica un error de configuración que rompe la validación de certificados, permitiendo que un atacante realice ataques man-in-the-middle para interceptar o manipular comunicaciones cifradas, aunque no compromete directamente la confidencialidad de los datos en tránsito sin una explotación activa.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red de producción si es crítico, o implementar reglas de firewall para restringir el acceso al puerto 5432 hasta la corrección.
2. **Corrección:** Generar un nuevo certificado SSL con el commonName correcto que coincida con el nombre del host o dirección IP, utilizando herramientas como OpenSSL, y configurarlo en el servicio PostgreSQL.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado es válido y no presenta discrepancias, utilizando Nessus o herramientas similares.
4. **Prevención:** Establecer procesos de gestión de certificados que incluyan revisiones periódicas y automatizadas para asegurar que todos los certificados SSL estén actualizados y correctamente configurados en todos los servicios.

Conclusión: Aunque el riesgo es moderado, la discrepancia en el certificado SSL debe corregirse prontamente para prevenir posibles ataques de suplantación y mantener la integridad de las comunicaciones en la red.

VULN-M030: SSL Certificate Cannot Be Trusted

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad 'SSL Certificate Cannot Be Trusted' en el servicio SMTP (puerto 25), donde el certificado SSL no es confiable debido a una cadena de certificados rota.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de las comunicaciones, facilitando ataques man-in-the-middle que podrían exponer datos sensibles y dañar la reputación de la organización.

Urgencia: Media. La vulnerabilidad tiene un CVSS de 6.5, indicando un riesgo moderado, pero su explotación requiere un ataque man-in-the-middle activo, lo que limita la facilidad de explotación inmediata. Sin embargo, si no se corrige, podría ser utilizada como un punto de entrada para ataques más avanzados en la red.

Acción: Adquirir o generar un certificado SSL válido y confiable para el servicio SMTP.

Análisis Técnico

- **Nombre:** SSL Certificate Cannot Be Trusted
- **ID del Plugin:** 51192
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El análisis técnico revela que el certificado X.509 del servidor tiene problemas de confianza: uno de los certificados en la cadena ha expirado (con fecha de caducidad el 16 de abril de 2010) y el certificado raíz es autofirmado por una autoridad desconocida (OCOSA), lo que rompe la cadena de confianza. Esto impide la verificación adecuada de la autenticidad del servidor, permitiendo potencialmente ataques man-in-the-middle donde un atacante podría interceptar y manipular las comunicaciones SMTP sin ser detectado, comprometiendo la seguridad de los datos en tránsito.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar actividades sospechosas en el puerto 25 y considerar el uso temporal de conexiones cifradas alternativas si es posible.
2. **Corrección:** Obtener un certificado SSL de una autoridad de certificación pública reconocida y configurarlo correctamente en el servidor, asegurando que toda la cadena de certificados esté presente y sea válida.
3. **Verificación:** Realizar un escaneo de seguridad post-implementación para confirmar que el certificado es ahora confiable y no genera advertencias, utilizando herramientas como Nessus o OpenSSL.
4. **Prevención:** Establecer procesos regulares de revisión y renovación de certificados para evitar caducidades, y implementar políticas de seguridad que exijan el uso de certificados de confianza en todos los servicios.

Conclusión: Aunque el riesgo no es crítico, la vulnerabilidad en el certificado SSL de METASPLOITABLE debe corregirse prontamente para proteger las comunicaciones y prevenir posibles explotaciones que comprometan la seguridad de la red.

VULN-M031: SSL Certificate Cannot Be Trusted

Resumen Ejecutivo

Problema: El servidor PostgreSQL en 192.168.122.29 (METASPLOITABLE) presenta la vulnerabilidad 'SSL Certificate Cannot Be Trusted' debido a un certificado SSL no confiable.

Riesgo para el Negocio: Esto compromete la confidencialidad e integridad de los datos transmitidos, facilitando ataques man-in-the-middle y potencialmente dañando la reputación de la organización si se explota.

Urgencia: Media. La vulnerabilidad tiene un riesgo medio según CVSS, con un vector que indica acceso de red sin autenticación, pero requiere un ataque man-in-the-middle activo para la explotación. No es críticamente urgente ya que no permite un compromiso directo del sistema, pero debe abordarse para prevenir posibles filtraciones de datos y cumplir con estándares de seguridad.

Acción: Adquirir o generar un certificado SSL válido y confiable para el servicio PostgreSQL.

Análisis Técnico

- **Nombre:** SSL Certificate Cannot Be Trusted
- **ID del Plugin:** 51192
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El análisis técnico revela que el certificado SSL del servidor PostgreSQL ha expirado (con fecha de caducidad en 2010) y está firmado por una autoridad de certificación desconocida y autofirmada, lo que rompe la cadena de confianza. Esto impide la verificación adecuada de la autenticidad del servidor, permitiendo que un atacante realice ataques man-in-the-middle para interceptar o manipular comunicaciones cifradas, aunque no compromete directamente la disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para restringir el acceso al puerto 5432 solo a hosts confiables y monitorear el tráfico en busca de actividades sospechosas.
2. **Corrección:** Obtener un certificado SSL de una autoridad de certificación pública reconocida, instalarlo en el servidor PostgreSQL y configurar el servicio para usar solo conexiones SSL válidas.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado es válido y la cadena de confianza está intacta, utilizando herramientas como Nessus.
4. **Prevención:** Establecer políticas para la gestión regular de certificados, incluyendo renovaciones automáticas antes de la expiración, y educar al personal sobre mejores prácticas de seguridad en comunicaciones cifradas.

Conclusión: Aunque el riesgo no es crítico, la vulnerabilidad en el certificado SSL debe corregirse prontamente para proteger la integridad de los datos y prevenir posibles ataques man-in-the-middle en el entorno.

VULN-M032: SMTP Service STARTTLS Plaintext Command Injection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con servicio SMTP en tcp/25 presenta la vulnerabilidad SMTP Service STARTTLS Plaintext Command Injection, permitiendo inyección de comandos durante la fase de texto plano.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al permitir el robo de credenciales SASL y correos electrónicos, y dañar la integridad al ejecutar comandos no autorizados, lo que podría afectar la reputación del negocio.

Urgencia: Media. La explotación requiere un atacante remoto no autenticado y puede ser aprovechada para robar información sensible, pero no conduce a un compromiso inmediato del sistema; sin embargo, su puntuación VPR de 7.3 indica un riesgo significativo que justifica una corrección prioritaria en el corto plazo para prevenir accesos no autorizados y posibles ataques posteriores.

Acción: Contactar al proveedor para verificar y aplicar actualizaciones disponibles que corrijan la implementación de STARTTLS.

Análisis Técnico

- **Nombre:** SMTP Service STARTTLS Plaintext Command Injection
- **ID del Plugin:** 52611
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

La vulnerabilidad surge de un defecto en la implementación de STARTTLS del servicio SMTP, donde comandos inyectados durante la fase de texto plano, como se observa en el plugin_output de Nessus que envió 'STARTTLS\r\nRSET\r\n' en un solo paquete y recibió respuestas confirmatorias, son ejecutados durante la fase cifrada, permitiendo a un atacante manipular el protocolo para obtener credenciales o datos sensibles sin autenticación.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.0 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:P/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.6945

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host afectado de la red para prevenir explotaciones mientras se aplica la corrección.
2. **Corrección:** Actualizar el software SMTP a una versión que parchee las CVE asociadas, como CVE-2011-0411 y otras listadas.
3. **Verificación:** Realizar pruebas de penetración o escaneos post-corrección usando herramientas como Nessus para confirmar que la vulnerabilidad ha sido mitigada.
4. **Prevención:** Implementar monitoreo continuo de tráfico SMTP y aplicar parches de seguridad de manera proactiva en todos los servicios similares.

Conclusión: Esta vulnerabilidad de inyección de comandos en SMTP representa un riesgo medio que amenaza la confidencialidad de datos y exige una acción inmediata de actualización para proteger la infraestructura de correo electrónico.

VULN-M033: SSL Self-Signed Certificate

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta un certificado SSL autofirmado en el servicio SMTP, vulnerabilidad identificada como SSL Self-Signed Certificate.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de las comunicaciones, permitiendo ataques man-in-the-middle que podrían exponer datos sensibles y dañar la reputación de la organización.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo, pero es relativamente fácil de ejecutar en redes no seguras, lo que podría llevar a la interceptación de comunicaciones y servir como punto de entrada para ataques más avanzados; debe abordarse en el corto plazo para mitigar riesgos.

Acción: Adquirir o generar un certificado SSL válido de una autoridad de certificación reconocida para el servicio SMTP.

Análisis Técnico

- **Nombre:** SSL Self-Signed Certificate
- **ID del Plugin:** 57582
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el puerto TCP/25 utiliza un certificado X.509 autofirmado emitido para 'ubuntu804-base.localdomain', que no está firmado por una autoridad de certificación reconocida. Esto anula la confianza en SSL/TLS, ya que un atacante podría realizar un ataque man-in-the-middle al presentar su propio certificado autofirmado, interceptando y posiblemente modificando las comunicaciones sin que el cliente detecte la anomalía, comprometiendo la confidencialidad e integridad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para restringir el acceso al servicio SMTP solo a redes de confianza y monitorear el tráfico en busca de actividades sospechosas.

2. Corrección: Reemplazar el certificado autofirmado con uno emitido por una autoridad de certificación confiable y configurar el servicio para usar solo certificados válidos.
3. Verificación: Realizar pruebas de penetración y usar herramientas como OpenSSL para validar que el nuevo certificado esté correctamente instalado y la cadena de certificados sea confiable.
4. Prevención: Establecer políticas de gestión de certificados que incluyan renovaciones automáticas, auditorías regulares y capacitación en mejores prácticas de seguridad para evitar certificados autofirmados en entornos de producción.

Conclusión: El certificado SSL autofirmado en SMTP representa un riesgo medio que debe corregirse prontamente para proteger las comunicaciones y prevenir posibles brechas de seguridad.

VULN-M034: SSL Self-Signed Certificate

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta una vulnerabilidad SSL Self-Signed Certificate en el servicio PostgreSQL en el puerto tcp/5432.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad e integridad de los datos transmitidos, permitiendo ataques man-in-the-middle que podrían resultar en acceso no autorizado a información sensible y daño reputacional.

Urgencia: Media. La vulnerabilidad es fácilmente explotable en entornos de red no confiables, ya que no requiere autenticación y puede ser utilizada para interceptar comunicaciones, aunque no conduce directamente a un compromiso total del sistema; debe abordarse en el corto plazo para mitigar riesgos de fuga de datos.

Acción: Adquirir o generar un certificado SSL válido firmado por una autoridad de certificación reconocida para el servicio PostgreSQL.

Análisis Técnico

- **Nombre:** SSL Self-Signed Certificate
- **ID del Plugin:** 57582
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El servicio PostgreSQL utiliza un certificado X.509 autofirmado, como se indica en el plugin_output, con detalles del sujeto que incluyen C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain. Esto significa que la cadena de certificados no está respaldada por una autoridad de confianza, lo que anula la autenticación SSL/TLS y permite a un atacante realizar ataques man-in-the-middle para espiar o modificar el tráfico de datos entre el cliente y el servidor, comprometiendo la seguridad de las comunicaciones.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 6.5 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N))

- **Puntuación Base CVSS v2.0:** 6.4 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:P/A:N))

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para restringir el acceso al puerto 5432 solo a hosts confiables y monitorear el tráfico en busca de actividades sospechosas.
2. Corrección: Reemplazar el certificado autofirmado con uno emitido por una autoridad de certificación reconocida y configurar el servicio PostgreSQL para usar solo conexiones SSL válidas.
3. Verificación: Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que el nuevo certificado es válido y que no se presentan errores de cadena de certificados.
4. Prevención: Establecer políticas para el uso exclusivo de certificados de confianza en todos los servicios, realizar auditorías periódicas de certificados SSL/TLS, y capacitar al personal en mejores prácticas de criptografía.

Conclusión: La presencia de un certificado SSL autofirmado en PostgreSQL representa un riesgo medio que debe corregirse prontamente para proteger la confidencialidad de los datos y prevenir posibles interceptaciones no autorizadas.

VULN-M035: SMB Signing not required

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con SMB en el puerto 445 tiene la vulnerabilidad SMB Signing not required, lo que permite ataques man-in-the-middle.

Riesgo para el Negocio: Esta vulnerabilidad compromete la integridad de las comunicaciones SMB, permitiendo a atacantes manipular datos en tránsito, lo que podría llevar a fraudes o pérdida de confianza en los sistemas afectados.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce a una compromiso directo del sistema, pero facilita ataques posteriores; debe abordarse en el próximo ciclo de parches para mitigar riesgos de escalada.

Acción: Habilitar la firma de mensajes SMB en la configuración del servidor.

Análisis Técnico

- **Nombre:** SMB Signing not required
- **ID del Plugin:** 57608
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/445/cifs)

La vulnerabilidad SMB Signing not required en el servicio CIFS/SMB del puerto 445 permite que un atacante no autenticado realice ataques man-in-the-middle al interceptar y modificar comunicaciones entre el cliente y el servidor, ya que el servidor no exige la firma digital de los mensajes, lo que debilita la autenticidad e integridad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.3 ((CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:N/I:P/A:N))

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de redes no confiables si es posible.
2. Corrección: Configurar el servidor SMB para requerir firma de mensajes; en Samba, establecer 'server signing = mandatory' en smb.conf.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que la firma está habilitada.
4. Prevención: Implementar políticas de seguridad que exijan firmas SMB en todos los servidores y realizar auditorías regulares.

Conclusión: Aunque el riesgo es medio, la falta de firma SMB debe corregirse para proteger la integridad de las comunicaciones y prevenir posibles ataques de manipulación de datos.

VULN-M036: SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 en Ubuntu 8.04 soporta suites de cifrado RC4 en el servicio SMTP en el puerto 25, lo que constituye la vulnerabilidad SSL RC4 Cipher Suites Supported (Bar Mitzvah).

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de datos sensibles, como cookies HTTP, si un atacante intercepta múltiples cifrados, lo que podría llevar a filtraciones de información y daños reputacionales.

Urgencia: Media. Aunque la explotación requiere la obtención de millones de cifrados y condiciones específicas, el riesgo de fuga de información confidencial es significativo si se explota, y podría ser utilizado como un paso inicial en ataques más avanzados, pero no permite un compromiso inmediato del sistema.

Acción: Reconfigurar la aplicación afectada para evitar el uso de cifrados RC4 y preferir suites como TLS 1.2 con AES-GCM.

Análisis Técnico

- **Nombre:** SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- **ID del Plugin:** 65821
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el host remoto admite múltiples suites de cifrado RC4, incluyendo EXP-RC4-MD5, EXP-ADH-RC4-MD5, RC4-MD5, ADH-RC4-MD5 y RC4-SHA, que utilizan cifrado RC4 con longitudes

de clave de 40 o 128 bits. RC4 genera un flujo pseudoaleatorio con sesgos conocidos, lo que permite a un atacante, tras capturar una gran cantidad de textos cifrados (por ejemplo, decenas de millones), derivar el texto plano mediante análisis estadístico, comprometiendo la confidencialidad de los datos transmitidos, aunque esto no afecta la integridad o disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.9267

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de explotación y considerar el bloqueo temporal de conexiones no esenciales si se identifica actividad sospechosa.
2. **Corrección:** Reconfigurar el servidor SMTP para deshabilitar todas las suites de cifrado RC4, implementando en su lugar cifrados más seguros como AES-GCM con TLS 1.2 o superior.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los cifrados RC4 ya no están soportados y validar la configuración de seguridad.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de cifrados obsoletos y realizar auditorías periódicas para asegurar el cumplimiento con las mejores prácticas criptográficas.

Conclusión: El soporte de cifrados RC4 en SMTP representa un riesgo medio para la confidencialidad de los datos y debe corregirse prontamente para prevenir posibles filtraciones de información y fortalecer la postura de seguridad general.

VULN-M037: SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con PostgreSQL en el puerto 5432 presenta la vulnerabilidad SSL RC4 Cipher Suites Supported (Bar Mitzvah), que permite el uso de cifrados RC4 inseguros.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de datos sensibles, como cookies o información de autenticación, lo que podría llevar a accesos no autorizados y daños reputacionales si se explota.

Urgencia: Media. La explotación requiere la obtención de millones de cifrados y condiciones específicas, lo que dificulta un ataque inmediato, pero el alto puntaje EPSS (0.9267) indica una probabilidad significativa de explotación en entornos reales, justificando una corrección prioritaria para prevenir filtraciones de información.

Acción: Reconfigurar la aplicación PostgreSQL para deshabilitar los cifrados RC4 y utilizar suites más seguras como TLS 1.2 con AES-GCM.

Análisis Técnico

- **Nombre:** SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- **ID del Plugin:** 65821
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

El servidor PostgreSQL en el puerto 5432 soporta el cifrado RC4-SHA (código 0x00, 0x05), que utiliza RC4 con una clave de 128 bits y autenticación SHA1. RC4 genera un flujo pseudoaleatorio con sesgos conocidos, permitiendo a un atacante, tras recolectar millones de cifrados, derivar el texto plano en ataques repetidos, como en el robo de cookies HTTP, aunque esto requiere un esfuerzo computacional sustancial y no compromete directamente la integridad o disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 5.0 ((CVSS2\#AV:N/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 7.3
- **EPSS Score:** 0.9267

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el servidor de redes públicas si es crítico y monitorear el tráfico para detectar intentos de explotación.
2. **Corrección:** Modificar la configuración de PostgreSQL para eliminar los cifrados RC4, preferiblemente actualizando a versiones que soporten solo suites seguras como TLS 1.2 con AES-GCM.
3. **Verificación:** Realizar un escaneo posterior con herramientas como Nessus para confirmar que los cifrados RC4 ya no están soportados y validar la configuración.
4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de cifrados débiles y realizar auditorías periódicas para asegurar el cumplimiento con estándares criptográficos actuales.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

VULN-M038: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Resumen Ejecutivo

Problema: El host 192.168.122.29 (METASPLOITABLE) está afectado por la vulnerabilidad SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE), que permite la divulgación de información sensible a través de servicios SSL/TLS.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, lo que podría resultar en la exposición de información sensible y daños reputacionales si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y múltiples intentos, pero la facilidad de downgrade a SSLv3 y la falta de soporte para Fallback SCSV aumentan el riesgo de divulgación de datos en entornos no seguros, aunque no conduce a un compromiso directo del sistema.

Acción: Deshabilitar SSLv3 en el servidor afectado.

Análisis Técnico

- **Nombre:** SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- **ID del Plugin:** 78479
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

La vulnerabilidad POODLE explota un fallo en el protocolo SSL 3.0 al manipular bytes de relleno en cifrados CBC, permitiendo a un atacante MitM descifrar bytes seleccionados del texto cifrado mediante la repetición de conexiones SSLv3 forzadas; el servidor en cuestión soporta SSLv3 con suites CBC y carece del mecanismo TLS Fallback SCSV, facilitando el rollback de versiones y la explotación potencial.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 3.4 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.1
- **EPSS Score:** 0.9377

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para restringir el acceso al puerto 25/smtp y monitorear el tráfico en busca de actividades sospechosas de MitM.
2. **Corrección:** Deshabilitar SSLv3 en la configuración del servicio smtp y habilitar solo protocolos TLS 1.2 o superiores para cifrado seguro.
3. **Verificación:** Realizar pruebas de escaneo post-corrección usando herramientas como Nessus para confirmar que SSLv3 está deshabilitado y no hay vulnerabilidades residuales.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos obsoletos como SSLv3 y realizar auditorías periódicas para asegurar el cumplimiento con estándares criptográficos actuales.

Conclusión: Aunque el riesgo es medio, la vulnerabilidad POODLE en el servidor smtp debe corregirse prontamente para proteger la confidencialidad de los datos y prevenir posibles filtraciones de información sensible.

VULN-M039: SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con PostgreSQL en el puerto 5432 está afectado por la vulnerabilidad POODLE (CVE-2014-3566), que permite la divulgación de información sensible a través de ataques man-in-the-middle.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, lo que podría resultar en la exposición de información sensible y daños reputacionales si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y múltiples intentos, pero el riesgo de divulgación de información es significativo y podría ser utilizado como un paso inicial para ataques más avanzados, justificando una corrección prioritaria.

Acción: Deshabilitar SSLv3 en el servidor PostgreSQL.

Análisis Técnico

- **Nombre:** SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- **ID del Plugin:** 78479
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/5432/postgresql)

La vulnerabilidad POODLE explota un fallo en el protocolo SSLv3 al manejar bytes de relleno en cifrados CBC, permitiendo a un atacante MitM descifrar bytes seleccionados del texto cifrado mediante la forzación de reconexiones SSLv3 repetidas; el servidor soporta SSLv3 con suites CBC y carece del mecanismo TLS Fallback SCSV, facilitando el rollback de versiones y aumentando la superficie de ataque.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 3.4 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 5.1
- **EPSS Score:** 0.9377

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para restringir el acceso no autorizado al puerto 5432 y monitorear el tráfico en busca de actividades sospechosas.
2. **Corrección:** Deshabilitar SSLv3 en la configuración de PostgreSQL y habilitar solo protocolos TLS seguros como TLSv1.2 o superior.
3. **Verificación:** Utilizar herramientas como Nessus o OpenSSL para confirmar que SSLv3 está deshabilitado y que el servidor ya no es vulnerable a POODLE.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos obsoletos y realizar auditorías regulares para asegurar el cumplimiento con las mejores prácticas criptográficas.

Conclusión: La vulnerabilidad POODLE en PostgreSQL representa un riesgo moderado de divulgación de información y debe ser mitigada deshabilitando SSLv3 para proteger la confidencialidad de los datos.

VULN-M040: SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 on Ubuntu 8.04 (hardy) presenta la vulnerabilidad SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) en el puerto tcp/25/smtp, que permite el uso de suites de cifrado débiles.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de las comunicaciones, permitiendo a un atacante realizar ataques de downgrade y descifrar datos sensibles, lo que podría dañar la reputación de la organización y exponer información crítica.

Urgencia: Media. Aunque la explotación requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, el soporte de cifrados débiles facilita la interceptación de comunicaciones y podría ser utilizado como un paso inicial para ataques más avanzados; se recomienda abordarla en el próximo ciclo de parches para mitigar riesgos potenciales.

Acción: Reconfigurar el servicio para eliminar el soporte de suites de cifrado EXPORT_RSA.

Análisis Técnico

- **Nombre:** SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
- **ID del Plugin:** 81606
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El host soporta suites de cifrado EXPORT_RSA con claves de hasta 512 bits, como EXP-DES-CBC-SHA, EXP-RC2-CBC-MD5 y EXP-RC4-MD5, que utilizan algoritmos de cifrado simétrico de baja fuerza (por ejemplo, DES-CBC con clave de 40 bits) y autenticación RSA. Un atacante en una posición man-in-the-middle puede forzar una degradación de la conexión TLS/SSL para usar estas suites débiles, aprovechando vulnerabilidades como CVE-2015-0204, y luego factorizar la clave RSA de 512 bits en un tiempo corto para descifrar las comunicaciones, comprometiendo la confidencialidad e integridad de los datos transmitidos a través del servicio SMTP.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:N/I:P/A:N))
- **VPR Score:** 1.4
- **EPSS Score:** 0.9191

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de la red si es posible para prevenir ataques durante la remediación.
2. **Corrección:** Reconfigurar el servicio SMTP para deshabilitar las suites de cifrado EXPORT_RSA, utilizando herramientas como OpenSSL para modificar la configuración de cifrados permitidos.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-remediación para confirmar que las suites débiles ya no están soportadas y validar la integridad de las comunicaciones.
4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de cifrados débiles en todos los servicios, realizar auditorías periódicas de configuración, y mantener el software actualizado para evitar vulnerabilidades similares.

Conclusión: El soporte de cifrados débiles en el servicio SMTP representa un riesgo moderado para la seguridad de las comunicaciones y debe corregirse prontamente para proteger la confidencialidad de los datos y cumplir con las mejores prácticas criptográficas.

VULN-M041: SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) está afectado por la vulnerabilidad SSL DROWN Attack, que permite a un atacante descifrar tráfico TLS capturado debido al soporte de SSLv2.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones, lo que podría resultar en la exposición de datos sensibles y dañar la reputación de la organización si se explota.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y condiciones específicas, como tráfico capturado previamente, lo que limita su facilidad de explotación. Sin embargo, el impacto potencial en la confidencialidad de los datos justifica una corrección prioritaria para prevenir riesgos de fuga de información.

Acción: Deshabilitar SSLv2 y las suites de cifrado de grado de exportación en el servidor.

Análisis Técnico

- **Nombre:** SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
- **ID del Plugin:** 89058
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

La vulnerabilidad DROWN aprovecha una debilidad en SSLv2, permitiendo un ataque de oráculo de relleno Bleichenbacher que puede descifrar conexiones TLS mediante el uso de claves privadas compartidas y cifrados débiles. El plugin_output muestra que el host soporta suites de cifrado vulnerables como EXP-RC2-CBC-MD5 y RC4-MD5, lo que facilita a un atacante realizar conexiones especialmente diseñadas para explotar esta falla y comprometer la confidencialidad del tráfico de red.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))
- **VPR Score:** 3.6
- **EPSS Score:** 0.9015

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el servidor de redes no confiables para reducir el riesgo de interceptación.
2. **Corrección:** Deshabilitar SSLv2 y todas las suites de cifrado de exportación en la configuración del servicio SMTP.
3. **Verificación:** Utilizar herramientas como OpenSSL o escáneres de vulnerabilidades para confirmar que SSLv2 está deshabilitado y solo se usan cifrados seguros.
4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de protocolos obsoletos y realicen auditorías regulares de configuración criptográfica.

Conclusión: Aunque la explotación no es trivial, la vulnerabilidad DROWN amenaza la confidencialidad de las comunicaciones y debe corregirse prontamente para proteger los datos sensibles y mantener la integridad de la infraestructura.

VULN-M042: SSH Weak Algorithms Supported

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad SSH Weak Algorithms Supported, que permite el uso de algoritmos de cifrado débiles en el servicio SSH.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de las comunicaciones SSH, permitiendo a atacantes descifrar datos sensibles, lo que podría resultar en fugas de información y daño reputacional.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y no conduce directamente a un compromiso total del sistema, pero facilita el acceso a información confidencial y podría ser utilizada como un paso inicial para ataques más avanzados; debe abordarse en el corto plazo para mitigar riesgos de interceptación.

Acción: Eliminar los algoritmos de cifrado débiles (arcfour, arcfour128, arcfour256) de la configuración del servidor SSH.

Análisis Técnico

- **Nombre:** SSH Weak Algorithms Supported
- **ID del Plugin:** 90317
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/22/ssh)

Nessus detectó que el servidor SSH en el puerto 22 soporta algoritmos de cifrado débiles como arcfour, arcfour128 y arcfour256 tanto para comunicaciones servidor-a-cliente como cliente-a-servidor, lo que viola las recomendaciones del RFC 4253 debido a problemas con claves débiles que pueden ser explotados mediante ataques de fuerza bruta o man-in-the-middle para descifrar el tráfico SSH, comprometiendo la confidencialidad de los datos transmitidos.

Puntuación de Riesgo:
- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v2.0:** 4.3 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico SSH en busca de actividades sospechosas y restringir el acceso temporalmente si es necesario.
2. Corrección: Modificar el archivo de configuración SSH (e.g., /etc/ssh/sshd_config) para deshabilitar los cifrados débiles especificados y reiniciar el servicio.
3. Verificación: Ejecutar un escaneo de vulnerabilidades post-corrección para confirmar que los algoritmos débiles ya no están soportados.
4. Prevención: Implementar políticas de seguridad que exijan el uso solo de algoritmos criptográficos fuertes y realizar auditorías regulares de configuración.

Conclusión: El soporte de cifrados débiles en SSH expone a riesgos de interceptación de datos, requiriendo su corrección pronta para proteger la confidencialidad y alinear con las mejores prácticas de seguridad.

VULN-M043: Samba Badlock Vulnerability

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) ejecuta Samba con la vulnerabilidad Badlock, permitiendo a un atacante man-in-the-middle forzar una degradación de autenticación.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad e integridad de datos sensibles en bases de datos SAM y AD, y potencialmente interrumpir servicios críticos, afectando la reputación de la organización.

Urgencia: Media. La explotación requiere un ataque man-in-the-middle activo y condiciones específicas, pero si se aprovecha, podría permitir el acceso no autorizado a información crítica y facilitar movimientos laterales en la red. Debe abordarse en un plazo razonable para mitigar riesgos significativos.

Acción: Actualizar Samba a la versión 4.2.11, 4.3.8, 4.4.2 o superior.

Análisis Técnico

- **Nombre:** Samba Badlock Vulnerability
- **ID del Plugin:** 90509
- **Severidad:** Media
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/445/cifs)

Nessus detectó que el parche para Badlock no se ha aplicado en el servidor Samba que opera en el puerto tcp/445. Esta vulnerabilidad, identificada como CVE-2016-2118, surge de una negociación inadecuada de niveles de autenticación en los protocolos SAM y LSAD a través de canales RPC, lo que permite a un atacante interceptar tráfico entre cliente y servidor para degradar la autenticación y ejecutar llamadas de red arbitrarias en el contexto del usuario interceptado, pudiendo acceder o modificar datos de seguridad y deshabilitar servicios.

Puntuación de Riesgo:

- **Factor de Riesgo:** Medium
- **Puntuación Base CVSS v3.0:** 7.5 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H))
- **Puntuación Base CVSS v2.0:** 6.8 ((CVSS2\#AV:N/AC:M/Au:N/C:P/I:P/A:P))
- **VPR Score:** 5.9
- **EPSS Score:** 0.7865

Acciones Recomendadas

1. Contención: Aislar temporalmente el host de la red o implementar reglas de firewall para restringir el acceso al puerto 445 si es posible.
2. Corrección: Aplicar la actualización de Samba a la versión 4.2.11, 4.3.8, 4.4.2 o posterior siguiendo las guías oficiales de Samba.
3. Verificación: Realizar un escaneo de vulnerabilidades post-parche con Nessus u otras herramientas para confirmar que la vulnerabilidad ha sido mitigada.
4. Prevención: Establecer políticas de gestión de parches regulares, monitorear el tráfico de red para detectar actividades sospechosas de man-in-the-middle, y educar a los usuarios sobre riesgos de seguridad en redes no confiables.

Conclusión: Se requiere la corrección de esta vulnerabilidad.

Vulnerabilidades Bajas

VULN-B072: ICMP Timestamp Request Remote Date Disclosure

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) con sistema operativo Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad ICMP Timestamp Request Remote Date Disclosure, permitiendo la divulgación de la hora exacta del sistema remoto.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al exponer información temporal, lo que podría facilitar ataques contra protocolos de autenticación basados en tiempo, aunque el impacto directo en la integridad o disponibilidad es limitado.

Urgencia: Baja. La explotación de esta vulnerabilidad es sencilla pero solo revela información de tiempo, sin permitir acceso no autorizado o compromiso directo del sistema; no sirve como escalón para otros ataques y su corrección puede programarse en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad.

Acción: Filtrar las solicitudes ICMP timestamp (13) y las respuestas ICMP timestamp (14) en el host afectado.

Análisis Técnico

- **Nombre:** ICMP Timestamp Request Remote Date Disclosure
- **ID del Plugin:** 10114
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (icmp/0)

La vulnerabilidad surge porque el host remoto responde a solicitudes ICMP timestamp, lo que permite a un atacante determinar la hora exacta configurada en la máquina. Según el plugin_output, la diferencia entre los relojes local y remoto es de 1 segundo, indicando una divulgación precisa de datos temporales. Esto puede ser utilizado para debilitar protocolos de autenticación que dependen de marcas de tiempo, aunque en sistemas como Windows las respuestas pueden ser inexactas, en este caso Linux proporciona información veraz, aumentando levemente el riesgo de ataques de sincronización o ingeniería social basados en tiempo.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v2.0:** 2.1 ((CVSS2\#AV:L/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 2.2
- **EPSS Score:** 0.0037

Acciones Recomendadas

1. Contención: Implementar reglas de firewall para bloquear el tráfico ICMP timestamp entrante y saliente en la red.
2. Corrección: Configurar el sistema para deshabilitar o filtrar las respuestas ICMP timestamp mediante ajustes en el kernel o herramientas de seguridad.
3. Verificación: Realizar pruebas de penetración o escaneos para confirmar que las solicitudes y respuestas ICMP timestamp ya no son respondidas por el host.
4. Prevención: Establecer políticas de seguridad que prohíban el uso de ICMP timestamp en todos los sistemas y realizar auditorías periódicas para detectar configuraciones similares.

Conclusión: Aunque el riesgo es bajo, la divulgación de la hora exacta en ICMP Timestamp Request debe corregirse para proteger la confidencialidad y prevenir posibles exploits en autenticaciones basadas en tiempo.

VULN-B073: X Server Detection

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) tiene un servidor X11 escuchando en el puerto tcp/6001, lo que representa la vulnerabilidad X Server Detection.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al permitir a atacantes espiar conexiones gráficas no cifradas, lo que podría exponer información sensible y dañar la reputación de la organización.

Urgencia: Baja. El riesgo de explotación es bajo ya que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero debe abordarse en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad y prevenir posibles fugas de información.

Acción: Restringir el acceso al puerto tcp/6001 o deshabilitar el soporte TCP en X11 usando la opción -nolisten tcp.

Análisis Técnico

- **Nombre:** X Server Detection
- **ID del Plugin:** 10407
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/6001/x11)

El servidor X11 versión 11.0 está ejecutándose en el host remoto, utilizando el protocolo no cifrado X11 que transmite datos gráficos en texto plano, lo que permite a atacantes en la misma red interceptar y observar las sesiones gráficas, aunque no comprometa directamente la integridad o disponibilidad del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. Contención: Bloquear el acceso no autorizado al puerto 6001 mediante reglas de firewall.
2. Corrección: Deshabilitar el soporte TCP para X11 ejecutando el servidor con la opción -nolisten tcp o restringiendo los permisos de red.
3. Verificación: Realizar un escaneo de puertos para confirmar que el servicio X11 ya no está accesible remotamente.
4. Prevención: Implementar políticas de seguridad que desalienten el uso de protocolos no cifrados y promover el uso de alternativas seguras como SSH con tunneling X11.

Conclusión: Aunque el riesgo es bajo, la presencia del servidor X11 expone la confidencialidad y debe corregirse para alinearse con las mejores prácticas de seguridad y prevenir posibles interceptaciones de datos.

VULN-B074: SSH Weak Key Exchange Algorithms Enabled

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con sistema operativo Linux Kernel 2.6.24-16-generic tiene habilitados algoritmos de intercambio de claves débiles en SSH, identificado como SSH Weak Key Exchange Algorithms Enabled.

Riesgo para el Negocio: Esta vulnerabilidad podría comprometer la confidencialidad de las comunicaciones SSH, permitiendo a atacantes realizar ataques de intermediario para interceptar datos sensibles, lo que podría dañar la reputación de la organización si se explota.

Urgencia: Baja. El riesgo de explotación es bajo debido a que requiere un ataque de intermediario activo y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos, sin necesidad de acción inmediata.

Acción: Deshabilitar los algoritmos de intercambio de claves débiles en la configuración del servidor SSH.

Análisis Técnico

- **Nombre:** SSH Weak Key Exchange Algorithms Enabled
- **ID del Plugin:** 153953
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/22/ssh)

El servidor SSH en el puerto tcp/22 está configurado para permitir algoritmos de intercambio de claves considerados débiles, como diffie-hellman-group-exchange-sha1 y diffie-hellman-group1-sha1, según se indica en el plugin_output. Estos algoritmos, basados en SHA-1 y grupos Diffie-Hellman pequeños, son vulnerables a ataques criptográficos como el descifrado mediante fuerza bruta o ataques de intermediario, lo que podría permitir a un atacante interceptar y posiblemente descifrar las comunicaciones

SSH, comprometiendo la confidencialidad de los datos transmitidos, aunque no afecta directamente la integridad o disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico SSH en busca de actividades sospechosas y considerar el uso de VPNs para comunicaciones sensibles hasta la corrección.
2. **Corrección:** Modificar el archivo de configuración del servidor SSH (generalmente /etc/ssh/sshd_config) para eliminar o comentar las líneas que habilitan los algoritmos débiles, como KexAlgorithms, y reiniciar el servicio SSH.
3. **Verificación:** Ejecutar un escaneo de vulnerabilidades después de los cambios para confirmar que los algoritmos débiles están deshabilitados y verificar la conectividad SSH.
4. **Prevención:** Implementar políticas de configuración segura para SSH que sigan las recomendaciones de RFC9142, realizar auditorías periódicas de configuración, y mantener el software actualizado para prevenir vulnerabilidades similares.

Conclusión: Aunque el riesgo es bajo, la presencia de algoritmos de intercambio de claves débiles en SSH debe corregirse para proteger la confidencialidad de las comunicaciones y alinearse con las mejores prácticas de seguridad criptográfica.

VULN-B075: SSL Anonymous Cipher Suites Supported

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic soporta suites de cifrado SSL anónimas, lo que permite ataques man-in-the-middle.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que un atacante podría interceptar y descifrar comunicaciones, lo que podría llevar a la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Baja. La explotación requiere un ataque man-in-the-middle activo y proximidad en la red, con un impacto limitado a la confidencialidad sin compromiso directo del sistema. Debe abordarse en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Reconfigurar la aplicación afectada para deshabilitar el uso de cifrados SSL anónimos y débiles.

Análisis Técnico

- **Nombre:** SSL Anonymous Cipher Suites Supported
- **ID del Plugin:** 31705
- **Severidad:** Baja

- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el puerto TCP/25 del host soporta múltiples suites de cifrado SSL anónimas, como ADH-AES128-SHA y EXP-ADH-DES-CBC-SHA, que utilizan intercambio de claves Diffie-Hellman sin autenticación. Esto permite que un atacante en la misma red realice un ataque man-in-the-middle para interceptar y potencialmente descifrar el tráfico, aunque no comprometa la integridad o disponibilidad del servicio. Los cifrados incluyen opciones de baja, media y alta resistencia, pero la falta de autenticación los hace inherentemente inseguros contra la suplantación de identidad.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))
- **VPR Score:** 4.4
- **EPSS Score:** 0.027

Acciones Recomendadas

1. **Contención:** Aislar temporalmente el host de redes no confiables para reducir el riesgo de explotación.
2. **Corrección:** Reconfigurar el servicio SMTP para eliminar los cifrados anónimos y débiles, utilizando solo suites seguras con autenticación certificada.
3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los cifrados anónimos ya no están soportados.
4. **Prevención:** Implementar políticas de configuración de cifrado en todos los servicios y realizar auditorías periódicas para asegurar el cumplimiento con las mejores prácticas de seguridad.

Conclusión: Aunque el riesgo es bajo, la corrección de los cifrados SSL anónimos en BEE-BOX es esencial para proteger la confidencialidad de las comunicaciones y mantener una postura de seguridad robusta.

VULN-B076: SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Certificate Chain Contains RSA Keys Less Than 2048 bits en el servicio SMTP.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de las comunicaciones al permitir ataques de descifrado, lo que podría dañar la reputación de la organización si se explota.

Urgencia: Baja. El riesgo de explotación es limitado, ya que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema; sin embargo, su corrección es recomendada para cumplir con estándares criptográficos y mejorar la higiene de seguridad.

Acción: Reemplazar el certificado con clave RSA de menos de 2048 bits y reemitir cualquier certificado firmado por el antiguo.

Análisis Técnico

- **Nombre:** SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- **ID del Plugin:** 69551
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El servicio SMTP en el puerto 25 utiliza un certificado X.509 con una clave RSA de 1024 bits, que es inferior al estándar mínimo de 2048 bits establecido por el CA/B Forum, lo que debilita la seguridad TLS al hacer que las comunicaciones sean más susceptibles a ataques de fuerza bruta o descifrado, aunque no se reporta explotación directa en este contexto.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle.
2. Corrección: Obtener e instalar un nuevo certificado con clave RSA de al menos 2048 bits desde una autoridad de certificación confiable.
3. Verificación: Validar la cadena de certificados usando herramientas como OpenSSL para asegurar que todas las claves cumplan con los estándares.
4. Prevención: Implementar políticas de gestión de certificados que exijan claves de longitud adecuada y realizar auditorías periódicas.

Conclusión: Aunque el riesgo es bajo, corregir esta vulnerabilidad es esencial para mantener la integridad criptográfica y proteger las comunicaciones del servicio SMTP.

VULN-B077: SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Chain Contains RSA Keys Less Than 2048 bits' en el puerto tcp/443.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de las comunicaciones SSL/TLS, permitiendo a atacantes descifrar datos sensibles, y dañar la reputación de la organización al no cumplir con estándares de seguridad.

Urgencia: Baja. El riesgo de explotación es bajo, ya que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero debe corregirse en el próximo ciclo de

mantenimiento para alinearse con las mejores prácticas criptográficas y evitar posibles problemas de compatibilidad con navegadores.

Acción: Reemplazar el certificado con clave RSA de 1024 bits por uno con al menos 2048 bits y reemitir cualquier certificado firmado por el antiguo.

Análisis Técnico

- **Nombre:** SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- **ID del Plugin:** 69551
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El servicio en el puerto tcp/443 utiliza un certificado X.509 con una clave RSA de solo 1024 bits, lo que viola los estándares del CA/B Forum que exigen claves de al menos 2048 bits desde 2014. Esto debilita la seguridad criptográfica, haciendo que las comunicaciones SSL/TLS sean susceptibles a ataques de fuerza bruta o de factorización, aunque no compromete directamente el sistema sin un ataque man-in-the-middle activo.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar posibles ataques man-in-the-middle hasta que se implemente la corrección.
2. Corrección: Generar y desplegar un nuevo certificado con una clave RSA de al menos 2048 bits, y reconfigurar el servicio para usarlo.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado cumple con los estándares y no hay claves débiles presentes.
4. Prevención: Establecer políticas de gestión de certificados que exijan claves de al menos 2048 bits y realizar auditorías periódicas para evitar regresiones.

Conclusión: Aunque el riesgo es bajo, la presencia de claves RSA débiles en el certificado SSL debe corregirse para fortalecer la seguridad de las comunicaciones y cumplir con los estándares criptográficos establecidos.

VULN-B078: SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad 'SSL Certificate Chain Contains RSA Keys Less Than 2048 bits' en el puerto tcp/8443.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de las comunicaciones SSL/TLS, permitiendo a atacantes descifrar datos sensibles, y dañar la reputación de la organización al no cumplir con estándares de seguridad.

Urgencia: Baja. El riesgo de explotación es bajo, ya que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema; sin embargo, su corrección es recomendada para mejorar la higiene de seguridad y cumplir con las mejores prácticas criptográficas.

Acción: Reemplazar el certificado con clave RSA de menos de 2048 bits y reemitir cualquier certificado firmado por el antiguo.

Análisis Técnico

- **Nombre:** SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- **ID del Plugin:** 69551
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/8443/www)

El servicio en el puerto tcp/8443 utiliza un certificado X.509 con una clave RSA de solo 1024 bits, lo que viola los estándares del CA/B Forum que exigen claves de al menos 2048 bits desde 2014. Esto debilita la criptografía SSL/TLS, haciendo que las comunicaciones sean susceptibles a ataques de fuerza bruta o de descifrado, aunque no compromete directamente la integridad o disponibilidad del sistema sin un ataque activo intermediario.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar posibles ataques man-in-the-middle.
2. Corrección: Generar y desplegar un nuevo certificado con una clave RSA de al menos 2048 bits, y reconfigurar el servicio para usarlo.
3. Verificación: Utilizar herramientas como Nessus o OpenSSL para confirmar que la nueva cadena de certificados cumple con los estándares de longitud de clave.
4. Prevención: Implementar políticas de gestión de certificados que exijan revisiones periódicas y el uso de claves criptográficas robustas en todos los servicios.

Conclusión: Aunque el riesgo es bajo, la presencia de claves RSA débiles en el certificado SSL debe corregirse para fortalecer la seguridad de las comunicaciones y alinearse con las mejores prácticas de la industria.

VULN-B079: SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) presenta la vulnerabilidad SSL Certificate Chain Contains RSA Keys Less Than 2048 bits, con un certificado de 1024 bits en uso.

Riesgo para el Negocio: Esto podría comprometer la confidencialidad de las comunicaciones SSL/TLS, permitiendo a atacantes descifrar datos sensibles, y dañar la reputación al no cumplir con estándares de seguridad.

Urgencia: Baja. El riesgo de explotación es bajo, ya que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con las mejores prácticas.

Acción: Reemplazar el certificado con clave RSA de menos de 2048 bits por uno más largo y reemitir cualquier certificado firmado por el antiguo.

Análisis Técnico

- **Nombre:** SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- **ID del Plugin:** 69551
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/9443/www)

El servicio en el puerto tcp/9443 utiliza un certificado X.509 con una clave RSA de solo 1024 bits, lo que viola los estándares del CA/B Forum que exigen claves de al menos 2048 bits desde 2014. Esto debilita la criptografía, haciendo que las comunicaciones SSL/TLS sean susceptibles a ataques de fuerza bruta o de factorización, potencialmente permitiendo a atacantes interceptar y descifrar datos transmitidos, aunque no compromete directamente la integridad o disponibilidad del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aislar temporalmente el servicio si es necesario.
2. Corrección: Generar y desplegar un nuevo certificado con una clave RSA de al menos 2048 bits, y reconfigurar el servicio para usarlo.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que el certificado cumple con los estándares y no hay claves débiles presentes.
4. Prevención: Implementar políticas de gestión de certificados que exijan claves de al menos 2048 bits y realizar auditorías periódicas para evitar regresiones.

Conclusión: Aunque el riesgo es bajo, la presencia de claves RSA débiles en el certificado debe corregirse para fortalecer la seguridad de las comunicaciones y alinearse con las mejores prácticas criptográficas.

VULN-B080: SSH Server CBC Mode Ciphers Enabled

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) tiene la vulnerabilidad SSH Server CBC Mode Ciphers Enabled, que permite el uso de cifrados CBC inseguros en SSH.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de los datos transmitidos, permitiendo a un atacante recuperar información sensible, lo que podría resultar en daños reputacionales y violaciones de cumplimiento.

Urgencia: Baja. El riesgo de explotación es bajo debido a que requiere un ataque man-in-the-middle activo y condiciones específicas, y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Deshabilitar los modos de cifrado CBC en el servidor SSH y habilitar cifrados más seguros como CTR o GCM.

Análisis Técnico

- **Nombre:** SSH Server CBC Mode Ciphers Enabled
- **ID del Plugin:** 70658
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/22/ssh)

El servidor SSH en el host está configurado para soportar algoritmos de Cipher Block Chaining (CBC) tanto para cliente-a-servidor como servidor-a-cliente, incluyendo 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, blowfish-cbc, cast128-cbc y rijndael-cbc@lysator.liu.se. Estos cifrados son vulnerables a ataques como el padding oracle, que pueden permitir a un atacante recuperar texto plano del texto cifrado si se intercepta la comunicación, aunque esto no implica una vulnerabilidad en la versión del software sino en la configuración.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))
- **VPR Score:** 1.4
- **EPSS Score:** 0.0307

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de explotación y aislar el host si es necesario.
2. Corrección: Modificar la configuración del servidor SSH para deshabilitar todos los cifrados CBC y habilitar solo modos seguros como CTR o GCM.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los cifrados CBC ya no están habilitados.
4. Prevención: Implementar políticas de configuración segura para SSH en todos los sistemas y realizar auditorías periódicas.

Conclusión: Aunque el riesgo es bajo, la corrección de esta vulnerabilidad es esencial para proteger la confidencialidad de los datos y mantener una postura de seguridad robusta.

VULN-B081: SSH Weak MAC Algorithms Enabled

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) tiene la vulnerabilidad SSH Weak MAC Algorithms Enabled, que permite algoritmos MAC débiles en el servicio SSH.

Riesgo para el Negocio: Esto podría comprometer la confidencialidad de los datos transmitidos, permitiendo a atacantes descifrar comunicaciones en un ataque man-in-the-middle, lo que podría llevar a la exposición de información sensible y daño reputacional.

Urgencia: Baja. El riesgo de explotación es bajo ya que requiere un ataque man-in-the-middle activo y no conduce directamente a un compromiso del sistema, pero debe corregirse en el próximo ciclo de mantenimiento para alinearse con las mejores prácticas de seguridad y reducir la superficie de ataque.

Acción: Deshabilitar los algoritmos MAC MD5 y de 96 bits en la configuración del servidor SSH.

Análisis Técnico

- **Nombre:** SSH Weak MAC Algorithms Enabled
- **ID del Plugin:** 71049
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/22/ssh)

El servidor SSH en el host BEE-BOX está configurado para soportar algoritmos MAC débiles como hmac-md5, hmac-md5-96 y hmac-sha1-96, tanto para cliente-a-servidor como servidor-a-cliente. Estos algoritmos son criptográficamente inseguros y pueden ser vulnerables a ataques de colisión o fuerza bruta, lo que podría permitir a un atacante manipular o descifrar el tráfico SSH en una sesión comprometida, aunque la explotación requiere condiciones de red específicas y no indica una versión de software vulnerable.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar actividades sospechosas relacionadas con SSH.
2. **Corrección:** Modificar el archivo de configuración SSH (e.g., /etc/ssh/sshd_config) para eliminar o comentar las líneas que habilitan hmac-md5, hmac-md5-96 y hmac-sha1-96, y reiniciar el servicio SSH.
3. **Verificación:** Ejecutar un escaneo de vulnerabilidades o usar herramientas como ssh-audit para confirmar que los algoritmos débiles están deshabilitados.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso solo de algoritmos MAC fuertes (e.g., hmac-sha2-256) y realizar auditorías regulares de configuración.

Conclusión: Aunque el riesgo es bajo, la presencia de algoritmos MAC débiles en SSH debe corregirse para proteger la confidencialidad de las comunicaciones y cumplir con las normas de seguridad criptográfica.

VULN-B082: SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) presenta la vulnerabilidad SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam), que permite el uso de suites de cifrado débiles en el servicio SMTP en el puerto tcp/25.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la integridad de las comunicaciones al permitir a un atacante realizar ataques de downgrade y descifrar datos, lo que podría dañar la reputación de la organización si se explota.

Urgencia: Baja. El riesgo de explotación es bajo debido a que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Reconfigurar el servicio para eliminar el soporte de las suites de cifrado EXPORT_DHE.

Análisis Técnico

- **Nombre:** SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
- **ID del Plugin:** 83738
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

El host soporta suites de cifrado EXPORT_DHE con claves de hasta 512 bits, como EXP-EDH-RSA-DES-CBC-SHA (código 0x00, 0x14), que utilizan intercambio de claves Diffie-Hellman débil y cifrado simétrico de baja entropía (e.g., DES-CBC con clave de 40 bits), permitiendo a un atacante realizar criptoanálisis para derivar la clave compartida en un tiempo corto y potencialmente descifrar las comunicaciones TLS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.5
- **EPSS Score:** 0.9391

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de downgrade de cifrado en tiempo real.
2. Corrección: Reconfigurar el servicio SMTP para deshabilitar todas las suites de cifrado EXPORT_DHE y usar solo cifrados fuertes como AES con claves de al menos 128 bits.
3. Verificación: Realizar un escaneo de vulnerabilidades post-corrección para confirmar que las suites débiles ya no están soportadas.
4. Prevención: Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas de configuración TLS.

Conclusión: Aunque el riesgo es bajo, la corrección de esta vulnerabilidad es esencial para proteger la integridad de las comunicaciones y alinearse con las mejores prácticas de seguridad criptográfica.

VULN-B083: SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) presenta la vulnerabilidad SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam), que permite el uso de cifrados débiles en el puerto tcp/443.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de las comunicaciones al permitir a un atacante descifrar datos, lo que podría resultar en la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Baja. El riesgo de explotación es limitado, ya que requiere un ataque man-in-the-middle activo y condiciones específicas, y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Reconfigurar el servicio para eliminar el soporte de suites de cifrado EXPORT_DHE.

Análisis Técnico

- **Nombre:** SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
- **ID del Plugin:** 83738
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

El host soporta suites de cifrado EXPORT_DHE con claves de hasta 512 bits, como EXP-EDH-RSA-DES-CBC-SHA (código 0x00, 0x14), que utilizan intercambio de claves Diffie-Hellman de 512 bits, autenticación RSA, cifrado DES-CBC de 40 bits y MAC SHA1. Esto permite a un atacante realizar criptoanálisis para descubrir el secreto compartido en poco tiempo, facilitando ataques de downgrade para forzar el uso de estos cifrados débiles y comprometer la confidencialidad de las comunicaciones SSL/TLS.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low

- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.5
- **EPSS Score:** 0.9391

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red en busca de actividades sospechosas que puedan indicar intentos de ataque man-in-the-middle.
2. **Corrección:** Reconfigurar el servicio web en el puerto 443 para deshabilitar todas las suites de cifrado EXPORT_DHE y utilizar solo cifrados fuertes, como aquellos con claves de al menos 2048 bits.
3. **Verificación:** Realizar un escaneo de vulnerabilidades después de la reconfiguración para confirmar que los cifrados débiles ya no están soportados.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas para asegurar el cumplimiento con las mejores prácticas criptográficas.

Conclusión: Aunque el riesgo es bajo, la presencia de cifrados débiles en Logjam debe abordarse para proteger la confidencialidad de las comunicaciones y mantener una postura de seguridad robusta.

VULN-B084: SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Resumen Ejecutivo

Problema: El host 192.168.122.187 (BEE-BOX) presenta la vulnerabilidad SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) en el servicio SMTP, permitiendo conexiones con moduli débiles de 512 bits.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la integridad de las comunicaciones, permitiendo a atacantes descifrar datos sensibles y dañar la reputación de la organización al exponer información confidencial.

Urgencia: Baja. La explotación requiere un ataque man-in-the-middle activo y recursos criptográficos significativos, aunque es técnicamente posible por individuos; sin embargo, el impacto directo es limitado y no conduce a un compromiso inmediato del sistema, por lo que la corrección puede programarse en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad.

Acción: Reconfigurar el servicio para usar moduli Diffie-Hellman únicos de 2048 bits o mayores.

Análisis Técnico

- **Nombre:** SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
- **ID del Plugin:** 83875
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/25/smtp)

La vulnerabilidad se manifiesta en conexiones SSL/TLS que utilizan suites de cifrado como TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA con moduli Diffie-Hellman de solo 512 bits en versiones SSLv3 y TLSv1.0, lo que facilita ataques Logjam donde un atacante puede calcular el secreto compartido mediante criptoanálisis, comprometiendo la confidencialidad e integridad de los datos transmitidos, aunque requiere proximidad de red y capacidad computacional.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.5
- **EPSS Score:** 0.9391

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aplicar reglas de firewall para restringir accesos no autorizados.
2. Corrección: Actualizar la configuración del servicio SMTP para deshabilitar suites de cifrado débiles y configurar moduli Diffie-Hellman de al menos 2048 bits.
3. Verificación: Realizar pruebas de penetración y escaneos de vulnerabilidades para confirmar que los moduli débiles han sido eliminados y las conexiones son seguras.
4. Prevención: Implementar políticas de seguridad que exijan el uso de cifrados modernos como TLS 1.2 o superior y realizar auditorías periódicas para mantener el cumplimiento con estándares criptográficos.

Conclusión: Aunque el riesgo es bajo, la vulnerabilidad Logjam debe abordarse para proteger la integridad de las comunicaciones y alinearse con las mejores prácticas de seguridad criptográfica.

VULN-B085: SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Resumen Ejecutivo

Problema: El host BEE-BOX (192.168.122.187) con Linux Kernel 2.6.24-16-generic presenta la vulnerabilidad SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) en el puerto tcp/443.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la integridad de las conexiones SSL/TLS, permitiendo a atacantes descifrar comunicaciones y potencialmente causar daños reputacionales si se explota.

Urgencia: Baja. El riesgo de explotación requiere un ataque man-in-the-middle activo y recursos criptográficos significativos, pero no conduce a un compromiso directo del sistema. Su corrección es recomendada en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Reconfigurar el servicio para utilizar un módulo Diffie-Hellman único de 2048 bits o mayor.

Análisis Técnico

- **Nombre:** SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
- **ID del Plugin:** 83875
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6.24-16-generic
- **Host y Puertos Afectados:** 192.168.122.187 (tcp/443/www)

La vulnerabilidad permite conexiones SSL/TLS con módulos Diffie-Hellman de solo 512 bits en suites de cifrado como TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA para SSLv3 y TLSv1.0, lo que facilita a atacantes realizar criptoanálisis para recuperar el secreto compartido en un tiempo corto, comprometiendo la confidencialidad e integridad de las comunicaciones mediante ataques como Logjam.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.5
- **EPSS Score:** 0.9391

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aplicar reglas de firewall para restringir accesos no autorizados.
2. **Corrección:** Reconfigurar el servicio SSL/TLS en el host para usar módulos Diffie-Hellman de al menos 2048 bits y deshabilitar suites de cifrado débiles como las que utilizan DES40_CBC_SHA.
3. **Verificación:** Realizar pruebas de penetración o escaneos de vulnerabilidades para confirmar que los módulos Diffie-Hellman han sido actualizados y no se permiten conexiones con moduli pequeños.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados fuertes y realizar auditorías regulares para asegurar el cumplimiento con estándares como NIST o best practices criptográficas.

Conclusión: Aunque el riesgo es bajo, la vulnerabilidad Logjam debe corregirse para proteger la integridad de las comunicaciones y mantener una postura de seguridad robusta en el entorno.

VULN-M044: ICMP Timestamp Request Remote Date Disclosure

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 on Ubuntu 8.04 (hardy) presenta la vulnerabilidad ICMP Timestamp Request Remote Date Disclosure, permitiendo la divulgación de la hora del sistema remoto.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al exponer información de tiempo, lo que podría facilitar ataques contra protocolos de autenticación basados en tiempo, aunque el impacto directo en la integridad o disponibilidad es limitado.

Urgencia: Baja. La explotación de esta vulnerabilidad requiere acceso a la red y solo revela información de tiempo, sin permitir acceso no autorizado o compromiso directo del sistema; no es un vector para ataques más graves y su corrección puede programarse en ciclos de mantenimiento regulares.

Acción: Filtrar las solicitudes ICMP timestamp (13) y las respuestas ICMP timestamp (14) en el host afectado.

Análisis Técnico

- **Nombre:** ICMP Timestamp Request Remote Date Disclosure
- **ID del Plugin:** 10114
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (icmp/0)

La vulnerabilidad surge porque el host remoto responde a solicitudes ICMP timestamp, lo que permite a un atacante determinar la hora exacta configurada en la máquina; según el plugin_output, la diferencia de reloj es de 1 segundo, lo que indica una divulgación precisa pero de bajo riesgo técnico, ya que no conduce a una explotación directa más allá de la recopilación de información.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v2.0:** 2.1 ((CVSS2\#AV:L/AC:L/Au:N/C:P/I:N/A:N))
- **VPR Score:** 2.2
- **EPSS Score:** 0.0037

Acciones Recomendadas

1. **Contención:** Implementar reglas de firewall para bloquear el tráfico ICMP timestamp entrante y saliente en la red.
2. **Corrección:** Configurar el sistema para deshabilitar las respuestas a solicitudes ICMP timestamp, siguiendo las mejores prácticas de seguridad.
3. **Verificación:** Realizar pruebas de penetración para confirmar que las solicitudes ICMP timestamp ya no son respondidas y monitorear el tráfico de red.
4. **Prevención:** Establecer políticas de seguridad que prohíban el uso de protocolos innecesarios y realizar auditorías periódicas de configuración.

Conclusión: Aunque el riesgo es bajo, la divulgación de la hora del sistema debe corregirse filtrando las solicitudes ICMP timestamp para proteger la confidencialidad y prevenir posibles ataques de ingeniería social.

VULN-M045: X Server Detection

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) tiene un servidor X11 escuchando en el puerto tcp/6000, lo que representa la vulnerabilidad X Server Detection.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad al permitir a atacantes espiar sesiones gráficas no cifradas, lo que podría exponer información sensible y dañar la reputación de la organización.

Urgencia: Baja. El riesgo de explotación es bajo ya que requiere un ataque man-in-the-middle activo y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y prevenir posibles fugas de información en entornos de alto riesgo.

Acción: Restringir el acceso al puerto tcp/6000 o deshabilitar el soporte TCP en X11 usando la opción -nolisten tcp.

Análisis Técnico

- **Nombre:** X Server Detection
- **ID del Plugin:** 10407
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/6000/x11)

El servidor X11 versión 11.0 está ejecutándose en el puerto tcp/6000, lo que permite conexiones remotas no cifradas; esto facilita que un atacante intercepte y monitoree el tráfico gráfico, potencialmente capturando entradas de teclado, datos visuales u otra información sensible transmitida durante las sesiones, aunque no compromete directamente la integridad o disponibilidad del sistema.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. **Contención:** Bloquear el acceso al puerto tcp/6000 mediante reglas de firewall para limitar la exposición inmediata.
2. **Corrección:** Deshabilitar el soporte TCP para X11 ejecutando el servidor con la opción -nolisten tcp o modificando la configuración del sistema.
3. **Verificación:** Realizar un escaneo de puertos después de los cambios para confirmar que el servicio ya no está accesible remotamente.
4. **Prevención:** Implementar políticas de seguridad que desalienten el uso de protocolos no cifrados y promover el uso de alternativas seguras como SSH con tunneling X11 para conexiones gráficas remotas.

Conclusión: Aunque el riesgo es bajo, la presencia del servidor X11 no cifrado debe corregirse para proteger la confidencialidad de los datos y alinearse con las mejores prácticas de seguridad.

VULN-M046: SSH Weak Key Exchange Algorithms Enabled

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) tiene la vulnerabilidad SSH Weak Key Exchange Algorithms Enabled, que permite algoritmos de intercambio de claves débiles en el servicio SSH.

Riesgo para el Negocio: Esta vulnerabilidad podría comprometer la confidencialidad de las comunicaciones SSH, permitiendo a atacantes interceptar datos sensibles, lo que podría resultar en daños reputacionales y violaciones de cumplimiento.

Urgencia: Baja. El riesgo de explotación es bajo debido a que requiere un ataque man-in-the-middle activo y no conduce directamente a compromisos del sistema, pero debe corregirse en el próximo ciclo de mantenimiento para alinearse con las mejores prácticas de seguridad y mitigar riesgos potenciales a largo plazo.

Acción: Deshabilitar los algoritmos de intercambio de claves débiles en la configuración del servidor SSH.

Análisis Técnico

- **Nombre:** SSH Weak Key Exchange Algorithms Enabled
- **ID del Plugin:** 153953
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/22/ssh)

El servidor SSH en el puerto 22 está configurado para permitir algoritmos de intercambio de claves débiles como diffie-hellman-group-exchange-sha1 y diffie-hellman-group1-sha1, que son considerados inseguros según el RFC9142. Esto podría permitir a un atacante realizar ataques de downgrade o man-in-the-middle para debilitar la seguridad de la conexión, aunque no explota directamente vulnerabilidades de software y depende de condiciones de red específicas para ser efectivo.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle relacionados con SSH.
2. Corrección: Modificar el archivo de configuración SSH (e.g., sshd_config) para deshabilitar los algoritmos débiles listados, como diffie-hellman-group-exchange-sha1 y diffie-hellman-group1-sha1.
3. Verificación: Realizar un escaneo de vulnerabilidades después de los cambios para confirmar que los algoritmos débiles ya no están habilitados.
4. Prevención: Implementar políticas de configuración segura para SSH y realizar auditorías periódicas para asegurar el cumplimiento con estándares criptográficos actualizados.

Conclusión: Aunque el riesgo es bajo, corregir esta vulnerabilidad es esencial para proteger la confidencialidad de las comunicaciones y mantener una postura de seguridad robusta.

VULN-M047: SSL Anonymous Cipher Suites Supported

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 on Ubuntu 8.04 (hardy) presenta la vulnerabilidad SSL Anonymous Cipher Suites Supported en el puerto tcp/25/smtp, que permite el uso de cifrados SSL anónimos sin verificación de identidad.

Riesgo para el Negocio: Esta vulnerabilidad compromete la confidencialidad de los datos transmitidos, ya que un atacante podría interceptar comunicaciones mediante un ataque man-in-the-middle, lo que podría llevar a la exposición de información sensible y dañar la reputación de la organización.

Urgencia: Baja. La explotación requiere que un atacante esté en la misma red física y realice un ataque man-in-the-middle activo, lo que limita su facilidad de explotación; aunque el impacto potencial en la confidencialidad es moderado (CVSS3 5.9), no permite compromisos directos del sistema ni movimiento lateral, por lo que la corrección puede planificarse en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad.

Acción: Reconfigurar la aplicación afectada para deshabilitar el uso de cifrados SSL anónimos y débiles.

Análisis Técnico

- **Nombre:** SSL Anonymous Cipher Suites Supported
- **ID del Plugin:** 31705
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el puerto 25 soporta múltiples suites de cifrado SSL anónimas, incluyendo EXP-ADH-DES-CBC-SHA, ADH-AES256-SHA y otras, que utilizan intercambio de claves Diffie-Hellman (DH) sin autenticación, lo que significa que no se verifica la identidad del servidor; esto permite a un atacante realizar un ataque man-in-the-middle para descifrar el tráfico, comprometiendo la confidencialidad de los datos, aunque la explotación es más difícil en redes no locales y no afecta la integridad o disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 5.9 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))
- **VPR Score:** 4.4
- **EPSS Score:** 0.027

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar actividades sospechosas y aislar temporalmente el host si es necesario en entornos de alto riesgo.
2. **Corrección:** Reconfigurar el servicio SMTP para eliminar los cifrados anónimos y débiles, utilizando solo suites fuertes con autenticación adecuada, como TLS con certificados válidos.

3. **Verificación:** Realizar un escaneo de vulnerabilidades post-corrección para confirmar que los cifrados anónimos ya no están soportados y validar la configuración.
4. **Prevención:** Implementar políticas de seguridad que exijan el uso de cifrados modernos y realizar auditorías periódicas para evitar regresiones en la configuración.

Conclusión: Aunque el riesgo es bajo, la presencia de cifrados SSL anónimos en el servicio SMTP debe corregirse para proteger la confidencialidad de los datos y alinearse con las mejores prácticas de seguridad criptográfica.

VULN-M048: SSH Server CBC Mode Ciphers Enabled

Resumen Ejecutivo

Problema: El servidor SSH en METASPLOITABLE (192.168.122.29) tiene habilitados cifrados en modo CBC, lo que constituye la vulnerabilidad SSH Server CBC Mode Ciphers Enabled.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la confidencialidad de los datos transmitidos, permitiendo a un atacante recuperar información sensible, lo que podría resultar en daños reputacionales y violaciones de cumplimiento.

Urgencia: Baja. El riesgo de explotación es bajo debido a que requiere un ataque man-in-the-middle activo y condiciones específicas, y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos modernos.

Acción: Deshabilitar los cifrados en modo CBC en la configuración del servidor SSH y habilitar modos más seguros como CTR o GCM.

Análisis Técnico

- **Nombre:** SSH Server CBC Mode Ciphers Enabled
- **ID del Plugin:** 70658
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/22/ssh)

El servidor SSH soporta algoritmos de cifrado en modo Cipher Block Chaining (CBC) tanto para cliente-a-servidor como servidor-a-cliente, incluyendo 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, blowfish-cbc, cast128-cbc y rijndael-cbc@lysator.liu.se. Esto puede permitir a un atacante realizar ataques de padding oracle o similares para recuperar texto plano del cifrado, aunque la explotación es compleja y depende de factores como la versión del software y la presencia de un ataque activo.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))
- **VPR Score:** 1.4
- **EPSS Score:** 0.0307

Acciones Recomendadas

1. Contención: Monitorear el tráfico SSH para detectar actividades sospechosas y considerar el aislamiento temporal si es necesario en entornos de alto riesgo.
2. Corrección: Modificar el archivo de configuración SSH (e.g., /etc/ssh/sshd_config) para eliminar las entradas de cifrados CBC y añadir 'Ciphers aes256-ctr,aes192-ctr,aes128-ctr' o equivalentes en GCM.
3. Verificación: Reiniciar el servicio SSH y usar herramientas como ssh-audit o nmap para confirmar que los cifrados CBC están deshabilitados y solo los modos seguros están activos.
4. Prevención: Implementar políticas de configuración segura para SSH en todos los servidores, realizar auditorías regulares, y mantener el software actualizado para prevenir vulnerabilidades similares.

Conclusión: Aunque el riesgo es bajo, la presencia de cifrados CBC en SSH debe corregirse para proteger la confidencialidad de los datos y alinearse con las mejores prácticas de seguridad criptográfica.

VULN-M049: SSH Weak MAC Algorithms Enabled

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) tiene habilitados algoritmos MAC débiles en SSH, específicamente hmac-md5 y hmac-md5-96, lo que constituye la vulnerabilidad SSH Weak MAC Algorithms Enabled.

Riesgo para el Negocio: Esta configuración podría permitir a un atacante realizar ataques de manipulación de datos o comprometer la integridad de las comunicaciones SSH, lo que podría llevar a la exposición de información sensible o daños reputacionales si se explota en un entorno de alto riesgo.

Urgencia: Baja. El riesgo de explotación es bajo ya que requiere un ataque man-in-the-middle activo y condiciones de red específicas, y no conduce directamente a un compromiso del sistema; sin embargo, su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Deshabilitar los algoritmos MAC MD5 y de 96 bits en la configuración del servidor SSH.

Análisis Técnico

- **Nombre:** SSH Weak MAC Algorithms Enabled
- **ID del Plugin:** 71049
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/22/ssh)

El servidor SSH en el host permite algoritmos MAC débiles como hmac-md5, hmac-md5-96 y hmac-sha1-96 tanto para cliente-a-servidor como servidor-a-cliente, lo que debilita la autenticidad de los mensajes; estos algoritmos son susceptibles a colisiones y ataques criptográficos, pudiendo permitir a un atacante modificar o falsificar datos durante la transmisión si se intercepta la comunicación, aunque no compromete directamente la confidencialidad o disponibilidad.

Puntuación de Riesgo:

- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:P/I:N/A:N))

Acciones Recomendadas

1. Contención: Monitorear el tráfico SSH en busca de actividades sospechosas y considerar el uso de VPNs para comunicaciones sensibles.
2. Corrección: Modificar el archivo de configuración SSH (e.g., /etc/ssh/sshd_config) para eliminar o comentar las líneas que habilitan hmac-md5, hmac-md5-96 y hmac-sha1-96, y reiniciar el servicio SSH.
3. Verificación: Ejecutar un escaneo de vulnerabilidades post-corrección para confirmar que los algoritmos débiles están deshabilitados y verificar la configuración con herramientas como ssh-audit.
4. Prevención: Implementar políticas de seguridad que exijan el uso de algoritmos MAC fuertes (e.g., hmac-sha2-256) y realizar auditorías regulares de configuración SSH.

Conclusión: Aunque el riesgo es bajo, la presencia de algoritmos MAC débiles en SSH debe corregirse para proteger la integridad de las comunicaciones y alinearse con las mejores prácticas de seguridad criptográfica.

VULN-M050: SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) con sistema operativo Linux Kernel 2.6 en Ubuntu 8.04 soporta suites de cifrado EXPORT_DHE débiles de 512 bits o menos en el servicio SMTP (puerto 25), conocido como Logjam.

Riesgo para el Negocio: Esta vulnerabilidad podría permitir a un atacante realizar un ataque de downgrade para comprometer la integridad de las comunicaciones, lo que podría llevar a la interceptación de datos sensibles y dañar la reputación de la organización si se explota.

Urgencia: Baja. El riesgo de explotación es bajo debido a que requiere un ataque man-in-the-middle activo y condiciones específicas, y no conduce a un compromiso directo del sistema, pero su corrección es recomendada para mejorar la higiene de seguridad y cumplir con estándares criptográficos.

Acción: Reconfigurar el servicio para eliminar el soporte de suites de cifrado EXPORT_DHE.

Análisis Técnico

- **Nombre:** SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
- **ID del Plugin:** 83738
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

El servicio SMTP en el host soporta suites de cifrado EXPORT_DHE con intercambio de claves Diffie-Hellman de 512 bits, como EXP-EDH-RSA-DES-CBC-SHA (código 0x00, 0x14), que utilizan cifrados débiles como DES-CBC(40) y RC4(40). Esto permite a un atacante realizar criptoanálisis para descubrir el secreto compartido en poco tiempo, facilitando un ataque de downgrade que compromete la confidencialidad e integridad de las comunicaciones, aunque no afecta directamente la disponibilidad del servicio.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.5
- **EPSS Score:** 0.9391

Acciones Recomendadas

1. **Contención:** Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aplicar reglas de firewall para restringir accesos no autorizados.
2. **Corrección:** Reconfigurar el servicio SMTP para deshabilitar las suites de cifrado EXPORT_DHE y utilizar solo cifrados fuertes, como aquellos con claves de al menos 2048 bits.
3. **Verificación:** Realizar un escaneo de vulnerabilidades después de la reconfiguración para confirmar que las suites débiles ya no están soportadas y validar la configuración mediante herramientas como OpenSSL.
4. **Prevención:** Implementar políticas de seguridad que prohíban el uso de cifrados débiles en todos los servicios, realizar auditorías periódicas, y mantener el software actualizado para prevenir vulnerabilidades similares.

Conclusión: Aunque el riesgo es bajo, la presencia de cifrados débiles en Logjam debe corregirse para fortalecer la postura de seguridad y seguir las mejores prácticas criptográficas, mitigando posibles ataques de interceptación.

VULN-M051: SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Resumen Ejecutivo

Problema: El host METASPLOITABLE (192.168.122.29) presenta la vulnerabilidad SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) en el servicio SMTP en el puerto 25, permitiendo conexiones con módulos Diffie-Hellman débiles.

Riesgo para el Negocio: Esta vulnerabilidad puede comprometer la integridad de las comunicaciones, permitiendo a atacantes descifrar o manipular datos, lo que podría dañar la confidencialidad y reputación de la organización si se explota.

Urgencia: Baja. La explotación requiere un ataque man-in-the-middle activo y recursos criptográficos significativos, aunque es técnicamente factible; sin embargo, el impacto directo es limitado y no conduce a un compromiso inmediato del sistema, por lo que la corrección puede programarse en el próximo ciclo de mantenimiento para mejorar la higiene de seguridad.

Acción: Reconfigurar el servicio para utilizar módulos Diffie-Hellman únicos de 2048 bits o mayores.

Análisis Técnico

- **Nombre:** SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
- **ID del Plugin:** 83875
- **Severidad:** Baja
- **Tipo:** Configuración / Protocolo Inseguro
- **SO Detectado:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- **Host y Puertos Afectados:** 192.168.122.29 (tcp/25/smtp)

La vulnerabilidad se manifiesta en conexiones SSL/TLS, específicamente con las versiones SSLv3 y TLSv1.0, utilizando el cipher suite TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA y módulos Diffie-Hellman de 512 bits, lo que facilita ataques Logjam donde un atacante puede calcular la clave compartida en un tiempo reducido, comprometiendo la confidencialidad e integridad de los datos transmitidos, aunque requiere proximidad de red y capacidad de interceptación.

Puntuación de Riesgo:
- **Factor de Riesgo:** Low
- **Puntuación Base CVSS v3.0:** 3.7 ((CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N))
- **Puntuación Base CVSS v2.0:** 2.6 ((CVSS2\#AV:N/AC:H/Au:N/C:N/I:P/A:N))
- **VPR Score:** 4.5
- **EPSS Score:** 0.9391

Acciones Recomendadas

1. Contención: Monitorear el tráfico de red para detectar intentos de ataque man-in-the-middle y aplicar reglas de firewall para restringir accesos no autorizados.
2. Corrección: Reconfigurar el servicio SMTP para deshabilitar cipher suites débiles y utilizar módulos Diffie-Hellman de al menos 2048 bits, siguiendo las mejores prácticas criptográficas.
3. Verificación: Realizar escaneos de vulnerabilidades post-corrección para confirmar que los módulos Diffie-Hellman cumplen con el tamaño mínimo requerido y que las conexiones son seguras.
4. Prevención: Implementar políticas de seguridad que exijan el uso de TLS 1.2 o superior y cipher suites fuertes, además de realizar auditorías periódicas de configuración criptográfica.

Conclusión: Aunque el riesgo es bajo, la vulnerabilidad Logjam en el servicio SMTP debe abordarse para proteger la integridad de las comunicaciones y alinearse con los estándares de seguridad modernos.