

Vulnerability Report — BeeBox

Eric Grossermann

Target: 169.254.6.63

Introducción

Este informe resume los hallazgos obtenidos mediante un escaneo con **Nmap** (puertos **22, 80 y 443**) utilizando scripts **NSE** de detección de vulnerabilidades.

Se identificaron múltiples vulnerabilidades críticas y de alta severidad en los servicios web y de cifrado TLS.

A continuación se presentan las cinco detecciones representativas, con su evidencia, impacto y recomendaciones de mitigación:

Detenciones

#	Detection	Service / Version (Nmap)	CVE / ID	Brief Impact	Reference
1	SSL/TLS CCS Injection	Apache + OpenSSL 0.9.8g (443)	CVE-2014-0224	Man-in-the-middle (MITM) posible; compromiso de sesión TLS	<u>CVE-2014-0224</u>
2	SSL POODLE (SSLv3)	Apache + OpenSSL 0.9.8g (443)	CVE-2014-3566	Fuga de información por padding oracle; recuperación de texto plano	<u>CVE-2014-3566</u>
3	Logjam / Weak DH params	Apache + OpenSSL 0.9.8g (443)	CVE-2015-4000	Downgrade a cifrado débil de 512-bits; riesgo de descifrado pasivo	<u>CVE-2015-4000</u>
4	Slowloris DoS Susceptibility	Apache 2.2.8 (80)	CVE-2007-6750	Agotamiento de recursos HTTP (Denegación de Servicio)	<u>CVE-2007-6750</u>
5	Permissive crossdomain policy	HTTP (80) - /crossdomain.xml	N/A	Política de dominio cruzado excesivamente permisiva (CSRF / exfiltración)	<u>Adobe Cross-Domain Policy</u>

1. SSL/TLS CCS Injection

Service / Version: Apache + OpenSSL 0.9.8g (443)

Identifier: CVE-2014-0224

Evidence (excerpt):

ssl-ccs-injection: VULNERABLE: SSL/TLS MITM vulnerability (CCS Injection).

OpenSSL antes de 0.9.8za, 1.0.0m y 1.0.1h permite ataques de intermediario que comprometen la sesión TLS.

Impact:

Un atacante puede interceptar y manipular el tráfico cifrado, comprometiendo la confidencialidad de las comunicaciones.

Remediation:

Actualizar OpenSSL a una versión parcheada. Aplicar las actualizaciones del sistema y regenerar parámetros TLS seguros.

2. SSL POODLE (SSLv3)

Service / Version: Apache + OpenSSL 0.9.8g (443)

Identifier: CVE-2014-3566

Evidence (excerpt):

ssl-poodle: VULNERABLE: SSL POODLE information leak.

El protocolo SSLv3 utiliza un padding no determinista que permite extraer información en texto plano.

Impact:

Riesgo de exposición de datos sensibles mediante ataque de tipo padding-oracle.

Remediation:

Deshabilitar completamente SSLv3 y forzar el uso de TLS 1.2 o superior.

Actualizar OpenSSL y Apache.

3. Logjam / Weak DH Parameters

Service / Version: Apache + OpenSSL 0.9.8g (443)

Identifier: CVE-2015-4000

Evidence (excerpt):

ssl-dh-params: EXPORT-GRADE DH GROUP 1 and WEAK DH GROUP 1 (512 / 1024-bit detected).

Impact:

Permite que un atacante degrade la conexión a un cifrado débil y realice descifrado pasivo del tráfico.

Remediation:

Actualizar OpenSSL/mod_ssl a una versión moderna y usar parámetros Diffie-Hellman de al menos 2048 bits.

Deshabilitar grupos DHE_EXPORT y ciphers débiles.

4. Slowloris DoS Susceptibility

Service / Version: Apache 2.2.8 (80)

Identifier: CVE-2007-6750

Evidence (excerpt):

http-slowloris-check: VULNERABLE: Slowloris DOS attack likely vulnerable.

Impact:

Un atacante puede mantener múltiples conexiones parciales abiertas, saturando los recursos del servidor y causando denegación de servicio.

Remediation:

Configurar **mod_reqtimeout**, usar un proxy inverso, o aplicar limitaciones de conexión en firewall.

5. Permissive Cross-Domain Policy

Service / Version: HTTP (80) - /crossdomain.xml

Identifier: N/A

Evidence (excerpt):

```
<allow-access-from domain="*">
```

Archivo crossdomain.xml permite acceso desde cualquier dominio.

Impact:

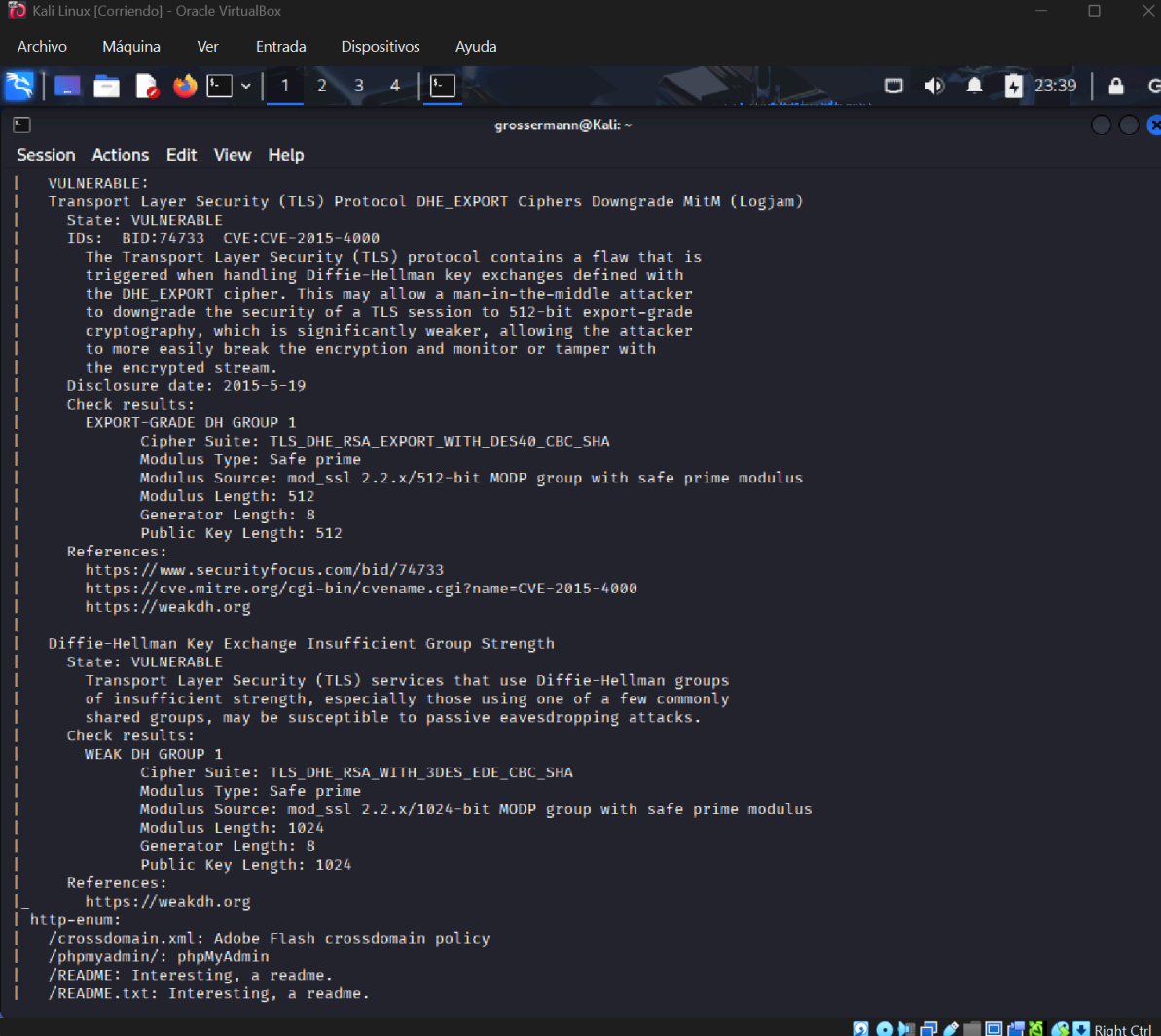
Exposición a ataques **CSRF** o robo de datos desde aplicaciones externas no autorizadas.

Remediation:

Restringir los dominios en el archivo `crossdomain.xml` o eliminarlo si no es necesario.

Notas finales

Este informe se basa en un escaneo **no destructivo** con scripts NSE de Nmap y encabezados de servidor.



```
Kali Linux [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
1 2 3 4
grossermann@Kali: ~
Session Actions Edit View Help
VULNERABLE:
Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
State: VULNERABLE
IDS: BID:74733 CVE:CVE-2015-4000
The Transport Layer Security (TLS) protocol contains a flaw that is
triggered when handling Diffie-Hellman key exchanges defined with
the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
to downgrade the security of a TLS session to 512-bit export-grade
cryptography, which is significantly weaker, allowing the attacker
to more easily break the encryption and monitor or tamper with
the encrypted stream.
Disclosure date: 2015-5-19
Check results:
EXPORT-GRADE DH GROUP 1
Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Modulus Type: Safe prime
Modulus Source: mod_ssl 2.2.x/512-bit MODP group with safe prime modulus
Modulus Length: 512
Generator Length: 8
Public Key Length: 512
References:
https://www.securityfocus.com/bid/74733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
https://weakdh.org
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Modulus Type: Safe prime
Modulus Source: mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
http-enum:
/crossdomain.xml: Adobe Flash crossdomain policy
/phpmyadmin/: phpMyAdmin
/README: Interesting, a readme.
/README.txt: Interesting, a readme.
```