28 de abril de 2021
Ficha N° 1 Test SSL
CSIRT DE GOBIERNO

Comando de la semana "Test SSL"

I. Contexto

Este documento, denominado "comando de la semana", tiene como objetivo ilustrar sobre herramientas que pueden ser de utilidad para el lector, a objeto de ir potenciando las capacidades locales de autochequeo, detección simple de vulnerabilidades que están expuestas a internet en nuestros activos de información y, a su vez, la obtención de una verificación de la subsanación de aquellas que se les han reportado, facilitando la interacción con el CSIRT de Gobierno. El objetivo no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo rápido para temas específicos.

II. Introducción

¿Qué hacer si desde el CSIRT nos llega un ticket señalando que hay problemas con nuestro certificado SSL? ¿Cómo verificamos una vez que hemos aplicado alguna mitigación y queremos probar si ha tenido efecto, antes de reportar como solucionado el problema al CSIRT a nuestros auditores internos?

Para este caso existe un comando Linux que nos ayuda a detectar diversos problemas, vulnerabilidades y anomalías en los certificados que tenemos instalados en nuestros sitios y sistemas web. Por ejemplo, detecta las siguientes vulnerabilidades:

Heartbleed (CVE-2014-0160), CCS (CVE-2014-0224), Ticketbleed (CVE-2016-9244), ROBOT, Secure Renegotiation (RFC 5746), Secure Client-Initiated Renegotiation, CRIME TLS (CVE-2012-4929), BREACH (CVE-2013-3587), POODLE, SSL (CVE-2014-3566), TLS_FALLBACK_SCSV (RFC 7507), SWEET32 (CVE-2016-2183, CVE-2016-6329), FREAK (CVE-2015-0204), DROWN (CVE-2016-0800, CVE-2016-0703), LOGJAM (CVE-2015-4000), BEAST (CVE-2011-3389), LUCKY13 (CVE-2013-0169), RC4 (CVE-2013-2566, CVE-2015-2808) entre otros problemas.

El protocolo SSL es un estándar de seguridad global que permite la transferencia de datos cifrados entre un navegador y un servidor web, encripta tu información y se encarga de que la misma viaje de manera íntegra y segura hasta llegar al lugar de destino; de este modo, no podrá ser descifrada.

Para establecer esta conexión segura, se instala en un servidor web un certificado SSL (también llamado "certificado digital") que cumple dos funciones:

- Autenticar la identidad del sitio web, garantizando a los visitantes que no están en un sitio falso.
- Cifrar la información transmitida.

III. Paso a Paso

PASO 1: Un entorno adecuado para trabajar.

Primero debe contar con una distribución de Kali[1] Linux funcionando ya sea en una máquina física o en una máquina virtual[2][3].

PASO 2: Instalar el comando.

Una vez que se cuenta con este sistema operativo de manera funcional podemos instalar el comando testssl si no está presente en la distribución utilizada:

```
sudo apt-get install testssl.sh
```

PASO3: Verificar su instalación.

Una vez que se instalado podemos explorar las múltiples opciones que ofrece para su ejecución:

```
testssl --help

"testssl [options] <URI>"    or    "testssl <options>"
```

[1] https://www.kali.org/downloads/

[2] https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0

[3] https://www.virtualbox.org/wiki/Downloads

```
"testssl <options>", where <options> is:

    --help                  what you're looking at
    -b, --banner            displays banner + version of testssl
    -v, --version           same as previous
    -V, --local             pretty print all local ciphers
    -V, --local <pattern>       which local ciphers with <pattern> are available? If pattern is not a
number: word match

 <pattern> is always an ignore case word pattern of cipher hexcode or any other string in the name,
kx or bits

"testssl <URI>", where <URI> is:
 <URI>:  host|host:port|URL|URL:port   port 443 is default, URL can only contain HTTPS protocol)

"testssl [options] <URI>", where [options] is: …
```

Este comando nos permite detectar los siguientes problemas, debilidades o vulnerabilidades de nuestra implementación del certificado SSL en nuestro sitio o sistema web, de una manera no invasiva y rápida:

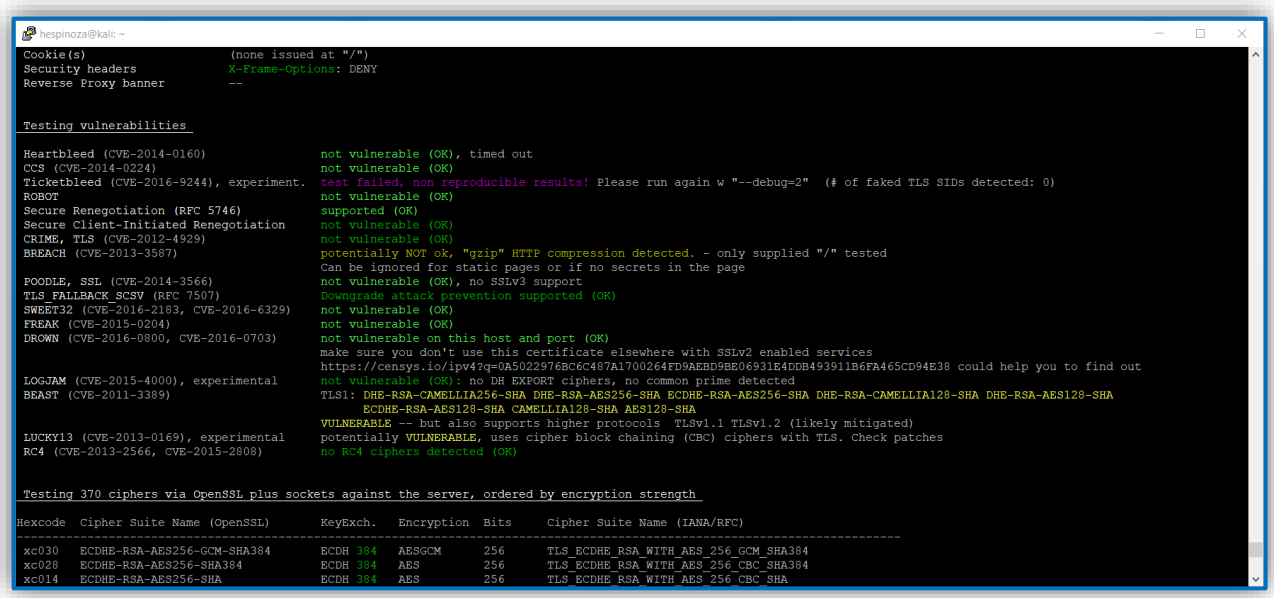
- Testing protocols via sockets except NPN+ALPN
- Testing cipher categories
- Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
- Testing server preferences
- Testing server defaults (Server Hello)
- Testing HTTP header response @ "/"
- Testing vulnerabilities
- Testing 370 ciphers via OpenSSL plus sockets against the server, ordered by encryption strength
- Running client simulations (HTTP) via sockets

Paso 4: Ponerlo en marcha para verificar nuestra infraestructura.

Como se ve un fragmento de reporte en una consola KALI después de la ejecución más simple:

```
testssl www.interior.gob.cl
```

Vista Parcial:



El resultado de este comando puede ser usado como evidencia de verificación para indicar que se han subsanado los problemas reportados por CSIRT.

Estudie las múltiples opciones que tiene el comando para obtener resultados específicos o redirigir la salida de este hacia otros formatos de archivo como json, html u otros.

En caso de cualquier inquietud no dudes en consultarnos a soc-csirt@interior.gob.cl.