Mirror mirror on the wall

Filippo De Grandi
DISI
University of Trento
Trento
filippo.degrandi@studenti.unitn.it

I. Setup

The vulnerable environment was built using a custom Docker image based on ubuntu:18.04. The image integrates NGINX 1.9.0 with OpenSSL 1.0.1f, a version known for containing several well-documented vulnerabilities such as Heartbleed (*CVE-2014-0160*) and weak RC4 cipher support.

The relevant configuration files are:

Dockerfile

- Compiles NGINX against OpenSSL 1.0.1f using the –with-openssl flag.
- Enables deprecated options (enable-ssl2, enable-des, enable-rc4, enable-weak-ssl-ciphers) to ensure weak cipher suites are available.
- Generates a self-signed certificate and key (512-bit RSA) with a very low security margin.
- The container exposes port 4444 for HTTPS.

nginx.conf

- Enables insecure SSL/TLS versions: SSLv2, SSLv3, TLSv1, and TLSv1.2.
- Sets weak cipher suites, explicitly including RC4, DES, and aNULL ciphers.
- Disables HSTS and certificate transparency.
- Uses 512-bit DH parameters, allowing weak ephemeral key exchanges.

These configurations were intentionally designed to make the server vulnerable to a wide range of TLS attacks.

II. Analysis with TLSAssistant

The container was executed and analyzed with:

```shell
docker run \
  --network host --rm \
  -v $(pwd)/results:/tlsassistant/results \
  -t odinmylord/tlsa_dev -s localhost:4444
```

Two HTML reports were generated:

- full.html: Complete analysis across all modules.
- mitzvah_nomore.html: Focused analysis of RC4-related vulnerabilities.

III. Results Overview

TLSAssistant identified the server as potentially vulnerable to a large number of attacks, including:

Category	Example Vulnerabilities	Root Cause
Protocol Weaknesses	SSLv2, SSLv3 support; BEAST; DROWN	Deprecated TLS versions enabled
Cipher Weaknesses	Bar Mitzvah, RC4 NOMORE, Sweet32	Use of RC4 and DES ciphers
Compression-related	CRIME, BREACH	TLS compression and gzip active
Session Issues	3SHAKE, Renegotiation attack	Missing `extended_master_secret`
HSTS / HTTPS Misconfigurations	HSTS not set / HTTPS not enforced	Missing security headers
Forward Secrecy	PFS module flagged	Weak DH key size (512-bit)

The Recap section in full.html shows most modules (e.g., BEAST, 3SHAKE, DROWN, BREACH) marked as Potentially Vulnerable. mitzvah_nomore.html confirms Bar Mitzvah (CVE-2015-2808) and RC4 NOMORE vulnerabilities caused by the enabled RC4 cipher.

References