Syracuse University

IST-623 Bonus Lab

Encrypting and Decrypting Web Traffic with HTTPS

ThulasiRam RuppaKrishnan

IST 623

Professor Joon Park

Contents

Lab Environment

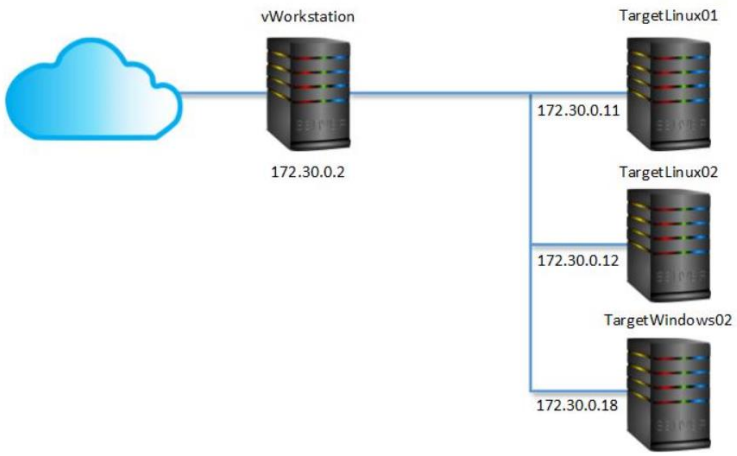
Encrypting and Decrypting Web Traffic with HTTPS

Access Control, Authentication, and Public Key Infrastructure - Lab 10

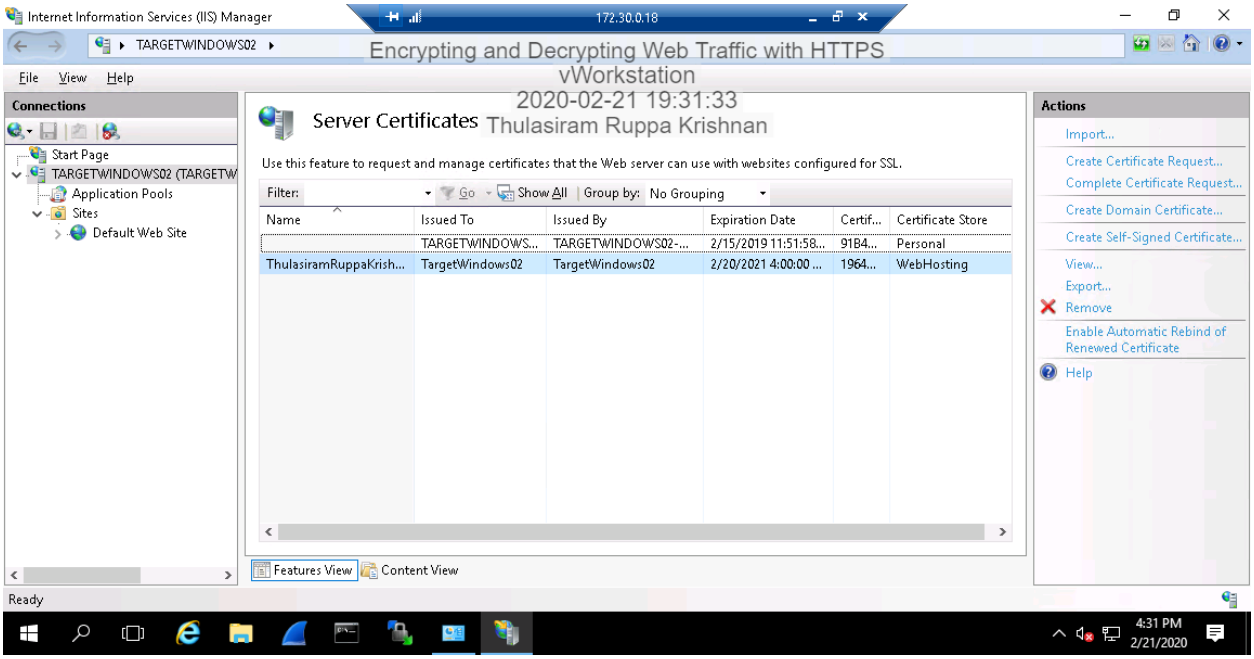
Current Step	Not Started
Progress	0%
StateSave Slot	New

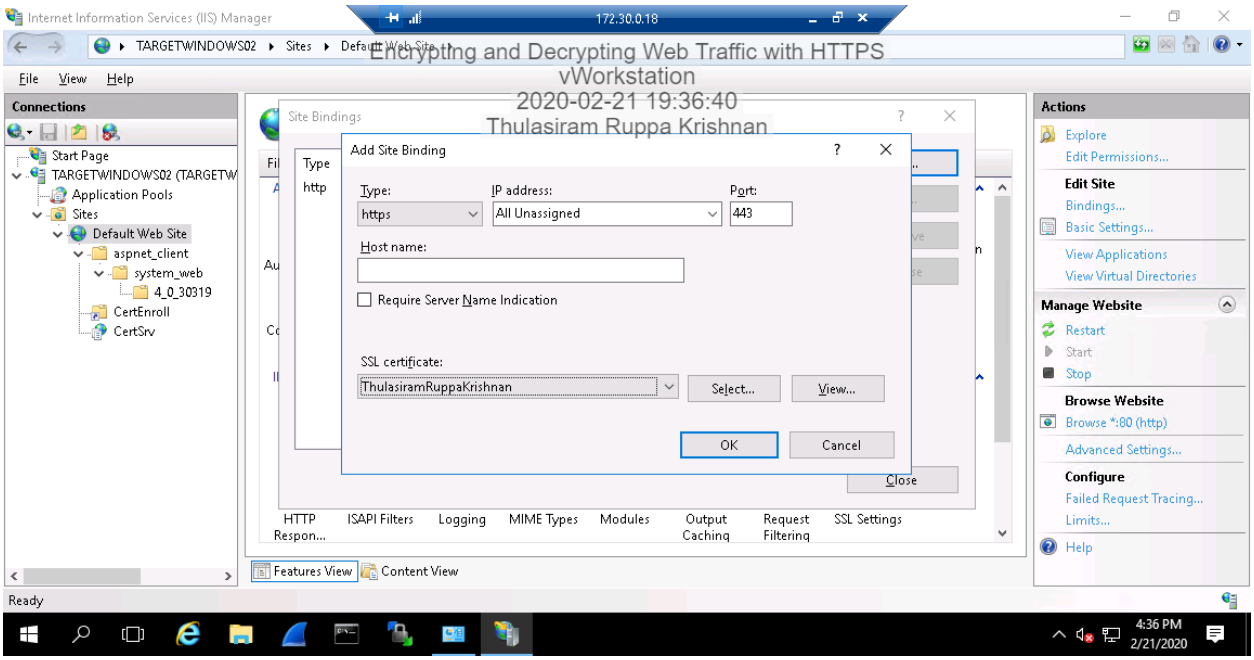
START LAB PREVIEW LAB GUIDE

Topology

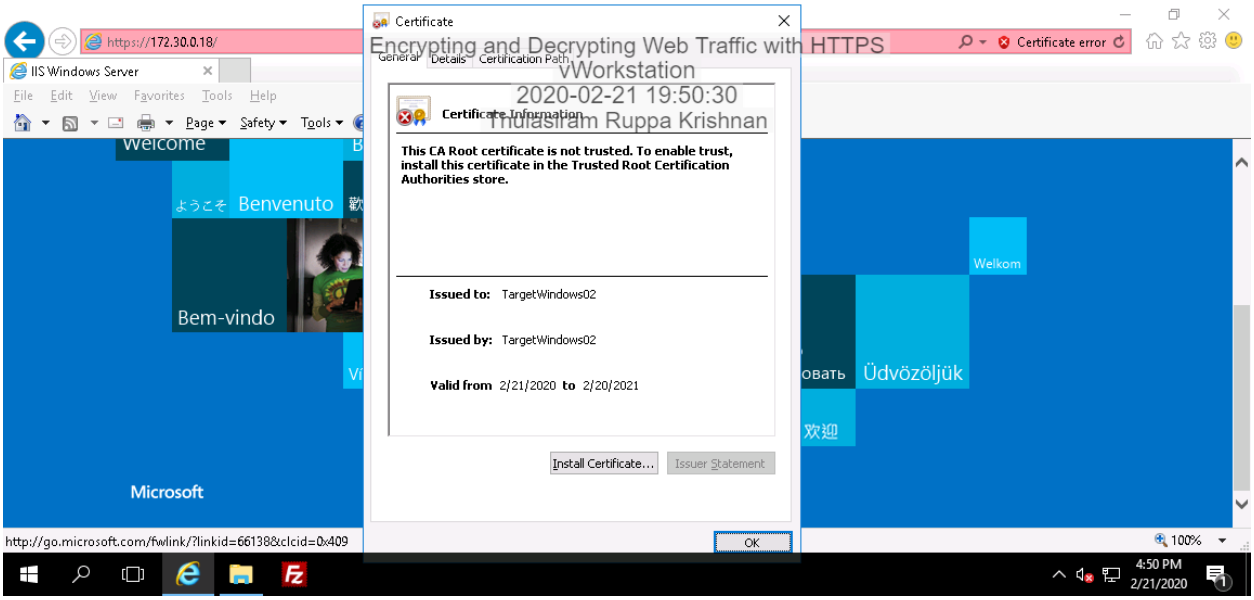


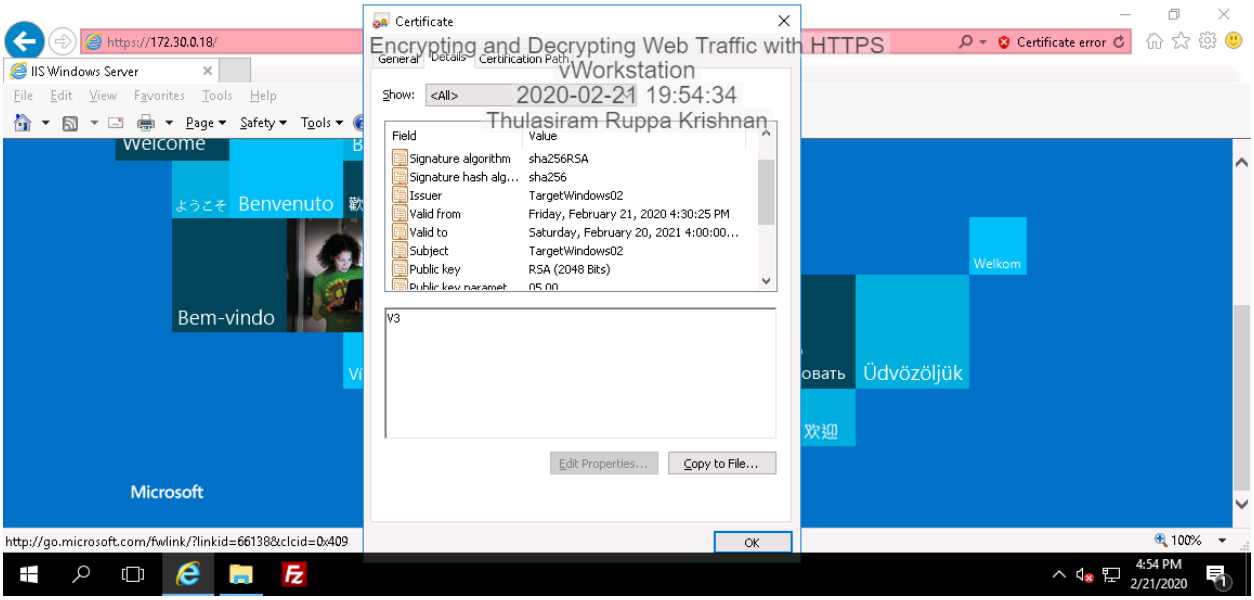
Part 1: Create an SSL Certificate





Part 2: View SSL Certificate





Part 3: Challenge Question

Discuss at least three security vulnerabilities/limitations in the current SSL protocol (70 words for each).

A Quick History of SSL/TLS

July 1994	SSLv1	Netscape Communications developed SSL (Secure Sockets Layer) to handle the encryption over a web browser/web server link. SSLv1 was in use internally within Netscape and reportedly cracked within the first 10 minutes of it being shown to MIT students. It was never released to the public.
Nov 1994	SSLv2	Version 2 of the SSL protocol suite released by and a proprietary product of Netscape. Significant flaws discovered a few months after release. SSLv2 was officially withdrawn less than a year later.
Oct 1995	PCT 1.0	Microsoft release a competing standard to SSL named PCT (Private Communications Technology). Supported in Microsoft products only and the source of significant exploits over the years. It has not been supported in any browser since IE5 but is still supported by current versions of IIS.
Nov 1995	SSLv3	Released to address significant exploited SSLv2 and PCT flaws.
Jan 1999	TLS 1.0	International standard specification of the SSL/PCT security protocols, named TLS (Transport Layer Security). TLS 1.0 and SSLv3 are largely identical.
Apr 2006	TLS 1.1	Update to address potential flaws determined by researchers in TLS 1.0. These flaws were exploited by a global and devastating cyberattack named BEAST in 2011 (6 years after TLS 1.0 was superseded).
Apr 2008	TLS 1.2	Update to address potential flaws determined by researchers in TLS 1.1. These flaws have not been observed to be exploited (yet).
May 2013	Edward Snowdon	Whistleblower reveals state of insecurity across the internet, and how it is being actively exploited by (at least) NSA
Aug 2013	TLS 1.3	Work begins on an update to TLS 1.2 addressing, amongst other issues, weaknesses revealed by Snowdon
Late 2013/early 2014		Chrome, Safari, IE and Firefox all add support for TLS 1.2.
Oct 2015		A cyberattack named POODLE exploits flaws in SSLv3. 10% of all internet servers found vulnerable, despite flaws identified and corrected 15 years previously

Mar 2016	A cyberattack named DROWN exploits flaws in SSLv2. 33% of all internet servers found vulnerable, despite flaws identified and corrected 21 years previously
Jul 2016	PCI Council releases edict that a requirement of PCI-DSS compliance is that any site that handles credit card data **must not support** TLS 1.0 or lower. Full compliance is required prior to **July 2018.**
Jul 2017	Paypal discontinues support for TLS 1.0 and TLS 1.1. All merchant connections can only use TLS 1.2. Consumer websites (eg www.paypal.com) will also be restricted to TLS 1.2 before end 2017.
August 2018	It has been over eight years since the last encryption protocol update, but the final version of **TLS 1.3 has now been published as of August 2018**. TLS 1.3 includes a lot of security and performance improvements. With the HTTP/2 protocol update in late 2015, and now TLS 1.3 in 2018, encrypted connections are now more secure and faster than ever.

SSL Endpoint Vulnerabilities

BEAST (Browser Exploit Against SSL/TLS)
Related Warning

"The server is vulnerable to the BEAST attack."

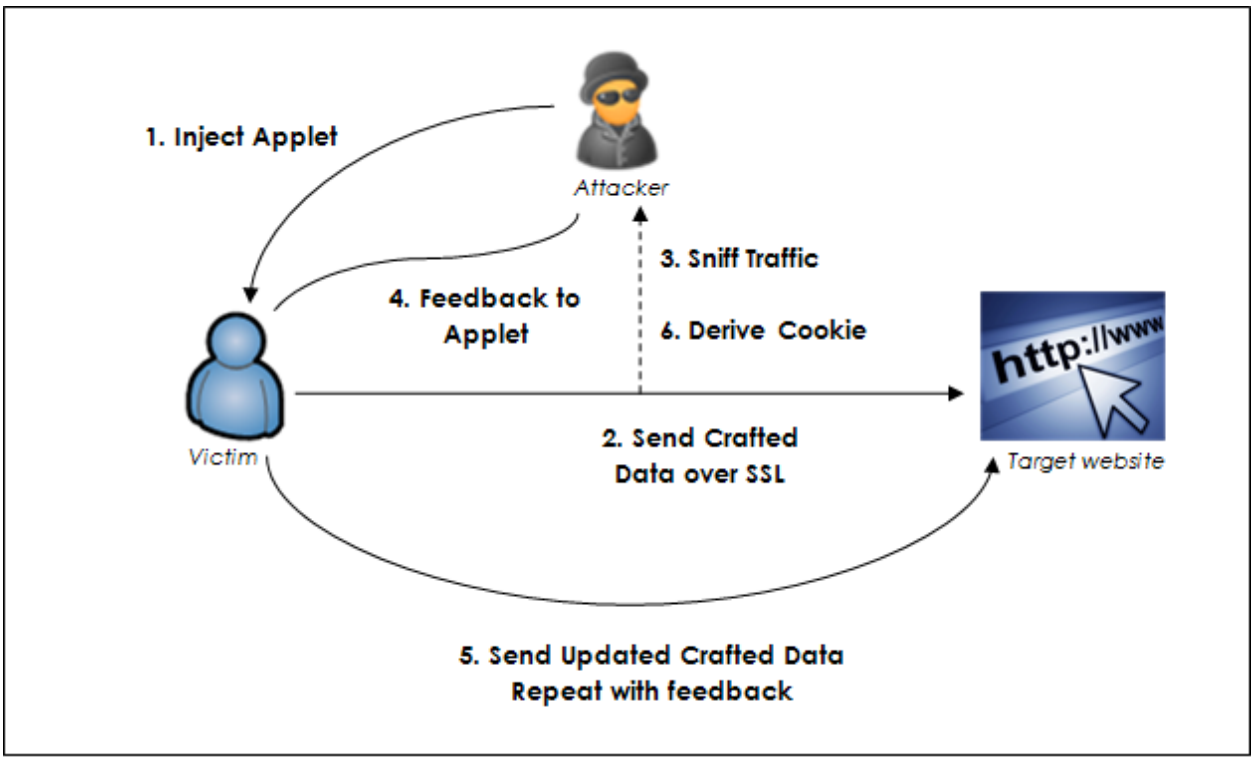
Background

Cipher suites are used to establish security settings for a network connection that uses the Transport Layer (TLS)/Secure Socket Layer (SSL) protocol.

Problem

Block-based cipher suites are vulnerable to the BEAST attack. Older versions of the TLS protocol (1.0) and the SSL protocol (2.0 and 3.0) are vulnerable to the BEAST attack.

Most browsers are vulnerable to the BEAST attack. In a BEAST attack, the attacker acts as a man-in-the-middle and uses specially crafted plaintext input to decrypt the contents of an SSL-encrypted or TLS-encrypted session between a Web browser and an e-commerce website. This type of attack allows the attacker to recover sensitive information (e.g. HTTP Authentication cookies).



If you are vulnerable to the BEAST attack, you receive a warning.

Solution

Enable TLS 1.1 and/or TLS 1.2 on servers that support TLS 1.1 and 1.2.

Enable TLS 1.1 and/or TLS 1.2 in Web browsers that support TLS 1.1 and 1.2.

Workaround

Disable all block-based cipher suites in your server's SSL configuration.

BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext)

Related Notice

"The server is vulnerable to the BREACH attack."

Background

Many Web pages are compressed to reduce bandwidth and latency issues before they are sent. The server uses the deflate algorithm to compress the body of an HTTP reply. The browser decompresses it and then, processes it as if it had never been compressed.

Problem

The BREACH attack manipulates the use of HTTP-level compression to pull out information from HTTPS-protected data, including email addresses, security tokens, and other plain text strings.

If you are vulnerable to the BREACH attack, you receive a notice.

Solutions/Workarounds

Web Server:

Turn off compression for pages that include PII (Personally Identifiable Information).

Web Browser:

Force browser not to invite HTTP compression use.

Web Applications:

Consider moving to Cipher AES128.

Remove compression support on dynamic content.

Reduce secrets in response buddies.

Use rate-limiting requests.

References : https://www.scu.edu/is/secure/resources-and-information/ssl-vulnerabilities-/