# **CTF Challenge: SSL/TLS Assessment Using SSLTrust**

# **1. Introduction**

SSLTrust is a tool designed to inspect SSL/TLS certificates installed on websites and assess their security. This challenge will introduce you to using SSLTrust to evaluate the SSL/TLS configuration of a specific domain.

# **2. Tools and Requirements**

Access to the internet and search for SSLTrust

# **3. Scenario**

You are a cybersecurity analyst responsible for verifying the SSL/TLS configuration of a client's website. Your objective is to use SSLTrust to determine the status of the SSL/TLS certificates and identify one potential security vulnerability.

# **4. Process to Follow while Performing CTF**

1. Go to SSLTrust: [**https://www.ssltrust.com.au/ssl-tools/website-security-check**](https://www.ssltrust.com.au/ssl-tools/website-security-check)

2. Enter [**https://defendtheweb.net/?hackthis=**](https://defendtheweb.net/?hackthis=) in the field, start the SSL/TLS check.

3. After scanning go to the SSL/TLS check defendweb.net and click on the **view report** option again click on **Protocols** option.

3. Solve the CTF.

# **5. Let’s Begin the Challenge**

**Question**

**Flag 1: Mention one offered protocols of the website**

*Answer: TLS1\_1*

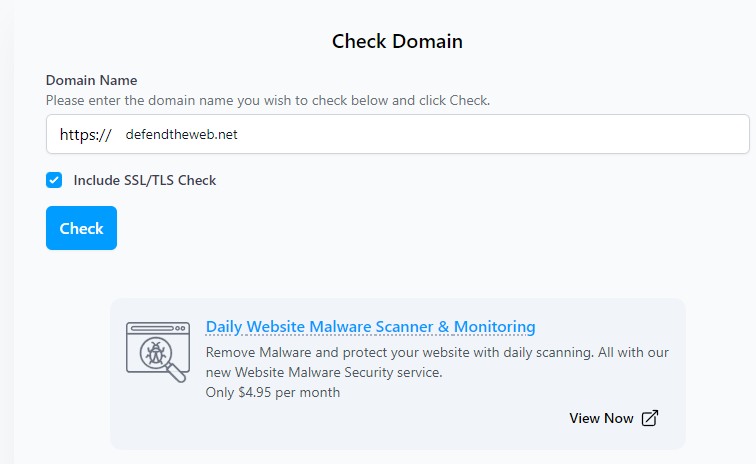
**Flag 2: Is SSLv2 & SSLv3 offered?**

*Answer: No*

**Flag 3: What is the IP address and port number of the websites?**

*Answer: 3.10.42.19 port 443*

Hint



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated