**Advanced Executive Program in Cybersecurity**

Virtual Internship Project Problem Statement



**Network Security Consultant**

**Problem Statement:**

You are working as a network security consultant for El Banco Bank. Your primary responsibility is to secure the bank's assets by designing, integrating, and implementing complex network architecture solutions after reviewing the network security.

You should be able to troubleshoot very complex network issues spanning various types of technologies.

**Background of the problem statement:**

El Banco Bank is one of the fastest-growing banks in Europe with more than 1200 branches across the country and manages €200 billion in assets.

Handling millions of dollars of banking transactions per day, its customers hugely depend upon the security of their banking data. The recent surge in cyber-attacks and data breaches has become a significant issue for every organization.

**Expected Deliverables:**

**TASK 1:**

As a network security consultant, you have to review tickets raised by users due to digital certificate issues. To help them resolve these issues, you need to understand the organization's certificate information. Identify the likely issue and the possible solution for the following tickets:

**Ticket 1:**

Date: 10/11/2021

Submitted by: Bob Wood (Pen tester)

I am trying to browse this website using an IP address, but my browser displays a certificate error. What should I do?

Graphical user interface, text, application, email

Description automatically generated

**ANS :** NET::ERR\_CERT\_AUTHORITY\_INVALID is a security-related error that browsers display when they can’t verify a website’s SSL certificate. This error suggests the website might have received its SSL certificate from an untrustworthy Certificate Authority (CA), risking visitors’ data security if they continue.

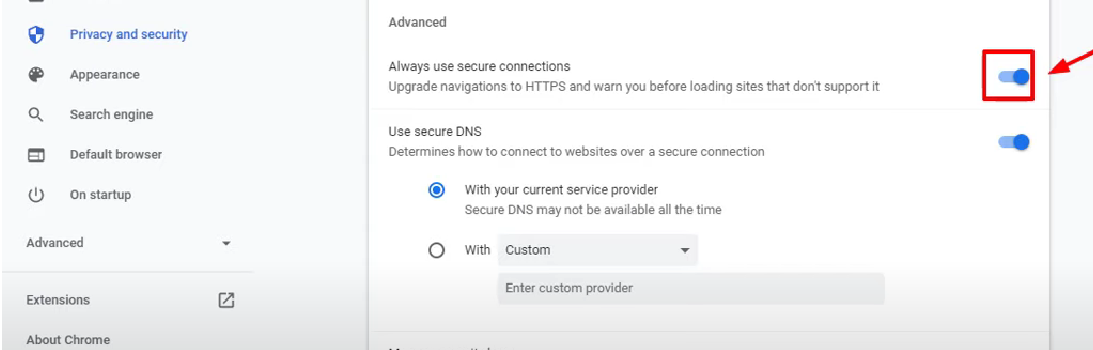
**What Causes the NET::ERR\_CERT\_AUTHORITY\_INVALID Error**

The NET::ERR\_CERT\_AUTHORITY\_INVALID error can result from SSL and browser-related issues, such as:

* **Expired SSL certificates** ‒ a browser usually marks an expired certificate invalid as it can’t ensure data encryption until renewed.
* **Self-signed certificates** ‒ this type of SSL certificate isn’t issued by a Certificate Authority (CA), lacking the third-party verification browsers need for trust.
* **Incorrect date and time** ‒ an outdated operating system can result in incorrect date and time settings, leading it to flag a valid certificate as expired.
* **Untrusted Certificate Authority** ‒ your website’s SSL certificate is issued by an unfamiliar CA that’s not listed on browsers’ trusted certification authorities.
* **Outdated browser cache or SSL state** ‒ browsers keep cached certificates for faster connections, but an old or corrupt cache can lead to a mismatch with the actual certificate.
* **VPN and security software interference** ‒ virtual private networks and certain security software like firewalls and antivirus can interfere with the SSL handshake process, resulting in browser warnings.
* **Conflicting browser extensions** ‒ an extension might incorrectly change or block the certificate information that the browser tries to verify.

## **How to Fix the NET::ERR\_CERT\_AUTHORITY\_INVALID Error**

* Clear your web browser’s cache and cookies
* Sync your computer’s time and date settings
* Temporarily disable browser extensions
* Update your web browser
* Clear cached certificate
* Keep your VPN temporarily disabled
* Deactivate your firewall or antivirus software
* Run an SSL test
* Get a new SSL certificate from a trusted Certificate Authority
* Renew the SSL certificate

Or else, 

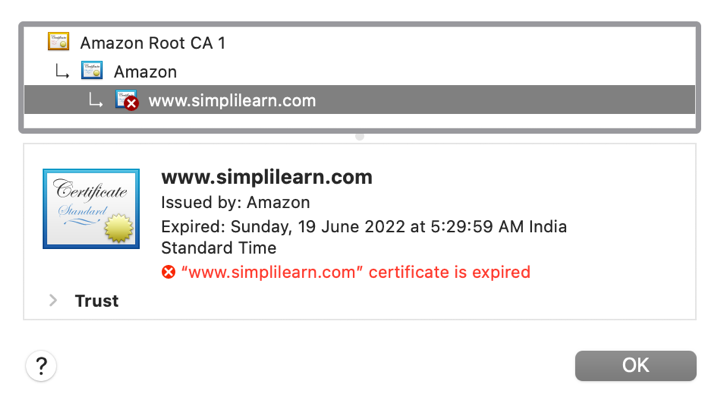
Disable it. So those websites who are not having ssl certificate means unsecure websites can easily be accessible.

**Ticket 2:**

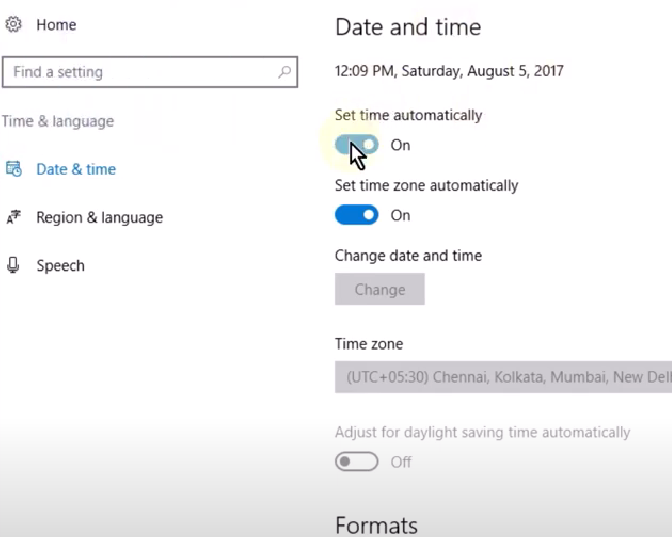
Date: 1/10/2021

Submitted By: Sheila Shaz (System Administrator)

I am trying to browse this website, but my browser displays an error that the certificate is expired. We have just renewed the certificate, and I am certain that the certificate will only expire in June 2022. What could be the reason for this error?

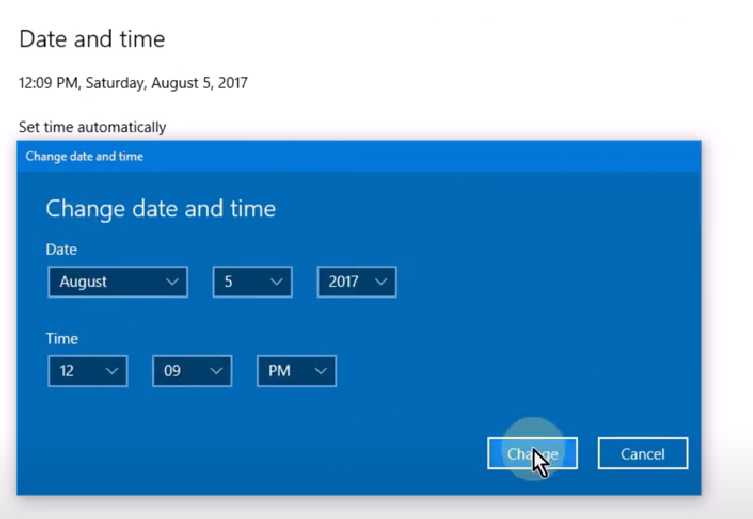


**ANS:** ITS SHOWING DUE TO TIME AND DATE OF YOUR SYSTEM UNMATCHED TO THE RECENT TIME.

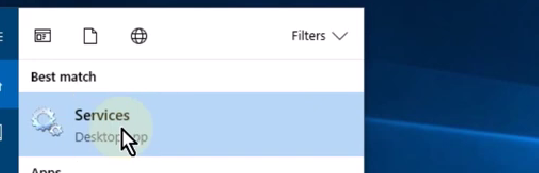
**STEP 1 :** **Go to windows Time and Date section in setting** 

If the time and date is incorrect please turn of these two options as above by “ automatically “

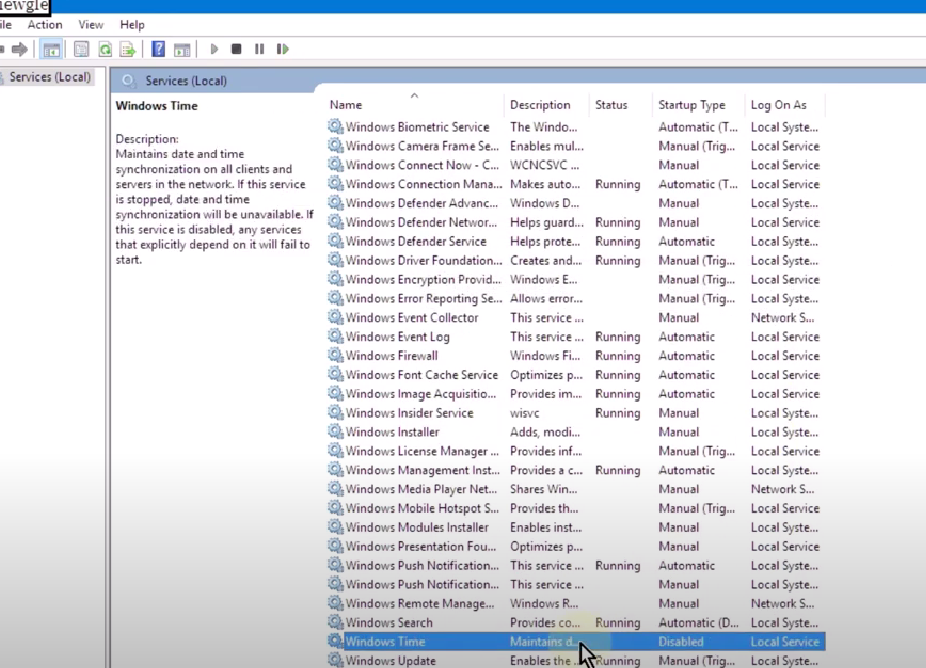
Do it manually by selecting hover the “Change” But and you will get the pop as below.



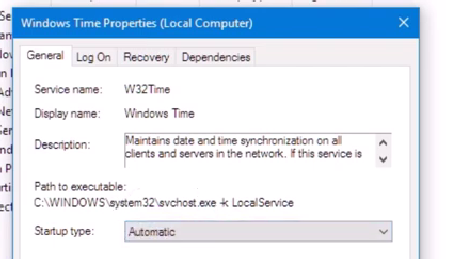
**Step 2 : Open Services**



Open windows time:



Set it to automatic



Then do right- click on the Windows time then Hit the “START”



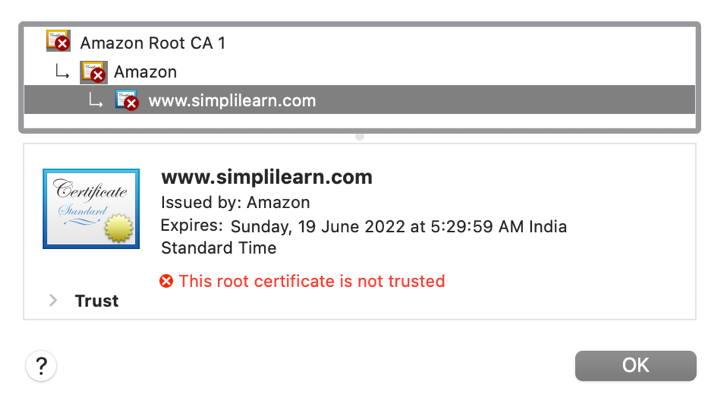
DONE! RESTART YOUR WINDOW.

**Ticket 3:**

Date: 2/12/2021

Submitted By: James Clay (Software Developer)

I am trying to browse this website, but my browser displays an error that the root certificate is not trusted. Is this issue client related?



Client Machine Root Certificates

Table

Description automatically generated

**Ans :** To resolve this problem, install the intermediate certificate (or chain certificate) file to the server that hosts your website. To do that, log into your DigiCert Management Console, click the order number, and then select the certificate download link. This file should be named DigiCertCA.crt. Then follow your[server-specific installation instructions](https://www.digicert.com/kb/ssl-certificate-installation.htm) to install the intermediate certificate file.

Once you import the intermediate certificate, check the installation again using the [SSL Certificate tester](https://www.digicert.com/help/). In the tester, an incomplete installation shows multiple certificate files connected by an unbroken blue chain.

We can also import the certificate and rest all will be sanitized trusted clients.

**TASK 2:**

You are reviewing the inbound rules of a VM in the cloud. The VM is used to host the bank’s website. For additional security, a valid digital certificate has been configured.

The cloud administrator is authorized to access the VM using RDP and SSH connections, but access should only be allowed from the authorized system with a fixed public IP (18.66.78.112).

Add the appropriate Inbound rules in the given format.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** |
|  |  |  |  |

**Note:**

1. Use 0.0.0.0/0 to indicate anywhere (IPv4).
2. Subnet mask /32 indicates only one host whereas /0 indicates all the hosts in the network.

**TASK 3:**

As a network security consultant, you are designing the VPN connectivity requirements so that users working remotely from home can access the corporate network. The business has provided the following connectivity requirements:

**VPN Connection 1:**

This VPN will be used by software developers working on Ubuntu 20.04 from home to connect only to the main software repository server in the enterprise network. Use an open-source VPN protocol that is designed for speed. Configure all the network traffic to go through the enterprise network.

**VPN Connection 2:**

This VPN will be used by remote users working on Windows 10 from home to connect to the enterprise network. Use a Microsoft proprietary VPN protocol for ease of configuration. Users should be able to watch Netflix directly without connecting through the enterprise network, which would otherwise block this kind of traffic.

Diagram

Description automatically generated

For these VPN connections, you will need to perform the following:

1. Determine the VPN types, VPN protocols, and the tunnel methods
2. Select the Firewall ports to allow
3. Both VPN connections must support strong 256-bit encryption and use the SSL/TLS for key exchange