Advanced Executive Program in Cybersecurity

Virtual Internship Project Problem Statement

Submitted By :

DEEPAK SHARMA

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.

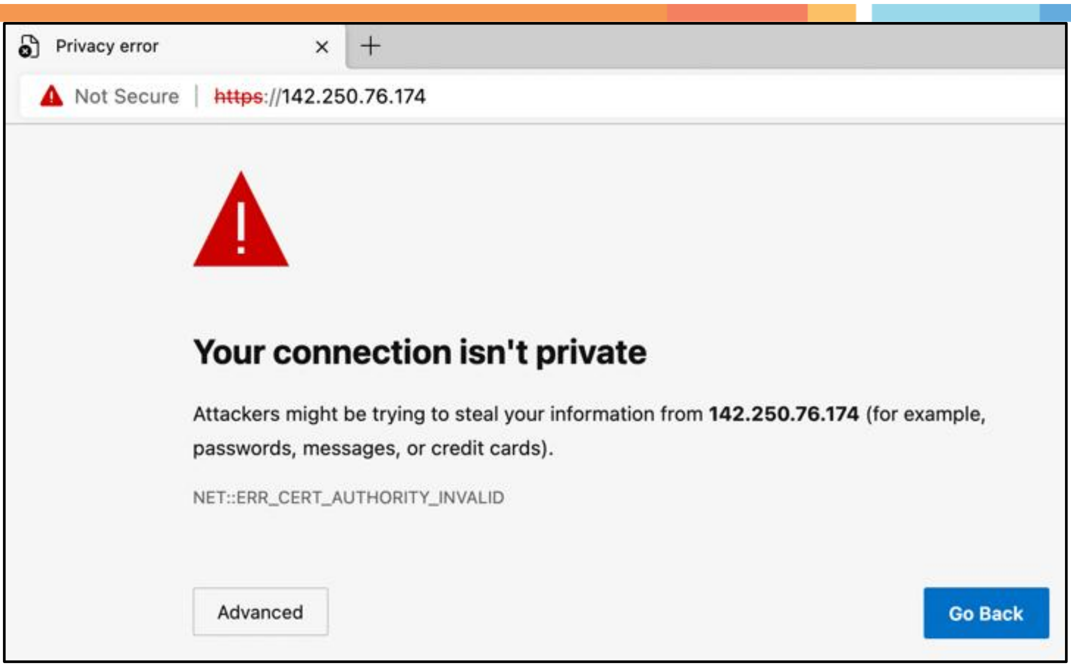
Expected Deliverables:

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?



Your connection isn't private

Attackers might be trying to steal your information from **142.250.76.174** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

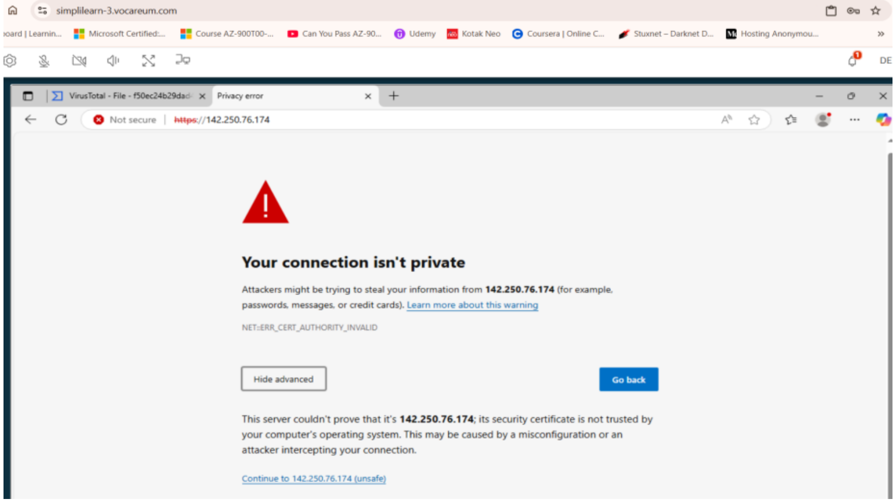
Solution:

SSL/TLS certificates are issued for domain names (FQDN), such as www.elbancobank.com, not for IP addresses.

When Bob tries to access the website using its IP address (e.g., https://142.250.76.174), the browser checks the certificate's Common Name (CN) or Subject Alternative Name (SAN). These fields usually contain the domain name. Since there is no match with the IP address, the browser throws a security error.

Recommendation: -

- **Always access the website via its domain name (e.g., https://www.elbancobank.com).**
- **Confirm that the domain name properly resolves to the IP using DNS.**



Your connection isn't private

Attackers might be trying to steal your information from **142.250.76.174** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **142.250.76.174**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

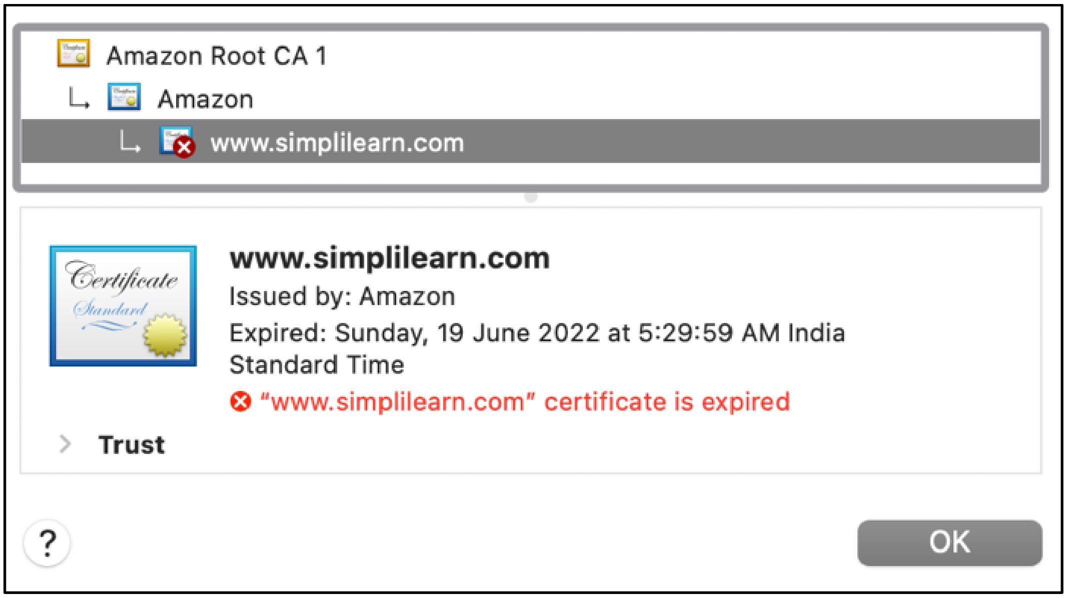
Continue to 142.250.76.174 (unsafe)

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?



www.simplilearn.com

Issued by: Amazon

Expired: Sunday, 19 June 2022 at 5:29:59 AM India Standard Time

"www.simplilearn.com" certificate is expired

Solution :-

Sheila submitted the ticket on **October 1, 2021**, but the certificate was recently renewed and is valid **until June 2022**. The certificate expiration error she is seeing is therefore **not due to actual expiration**, but likely due to **other technical causes** such as:

Likely Root Causes

Cause	**Description**
Old certificate still being served	The web server was not restarted after installing the new certificate, so it continues to serve the old (expired) one.
Client/browser cache	The browser may be caching the old certificate and displaying an outdated error.
System clock incorrect on client machine	If the client machine’s clock is set ahead (e.g., Jan 2023), it will see the June 2022 expiry as already passed.

Client-side (Sheila should try):

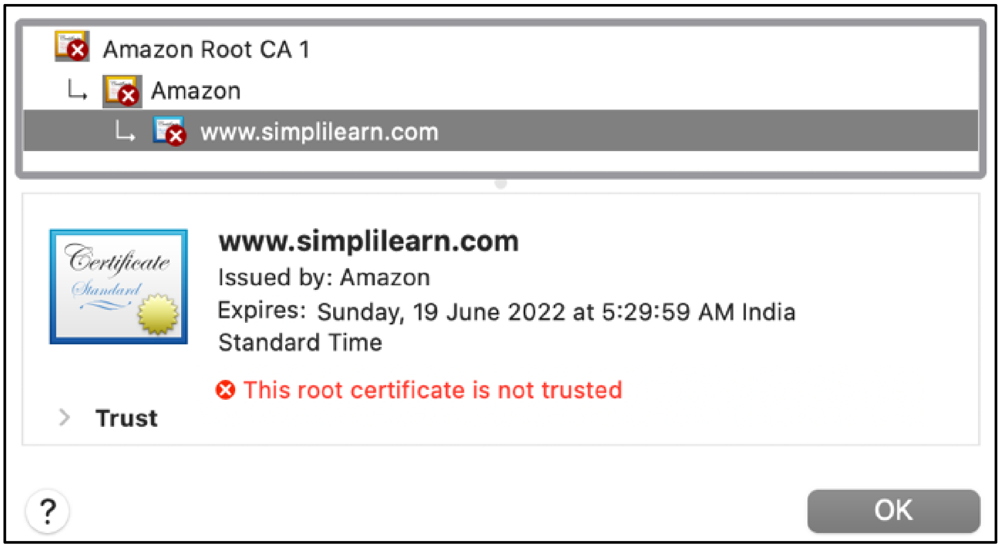
1. **Clear browser cache or test in incognito mode.**
2. **Use another browser or device to rule out local caching.**
3. **Check and correct the system clock:**

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?

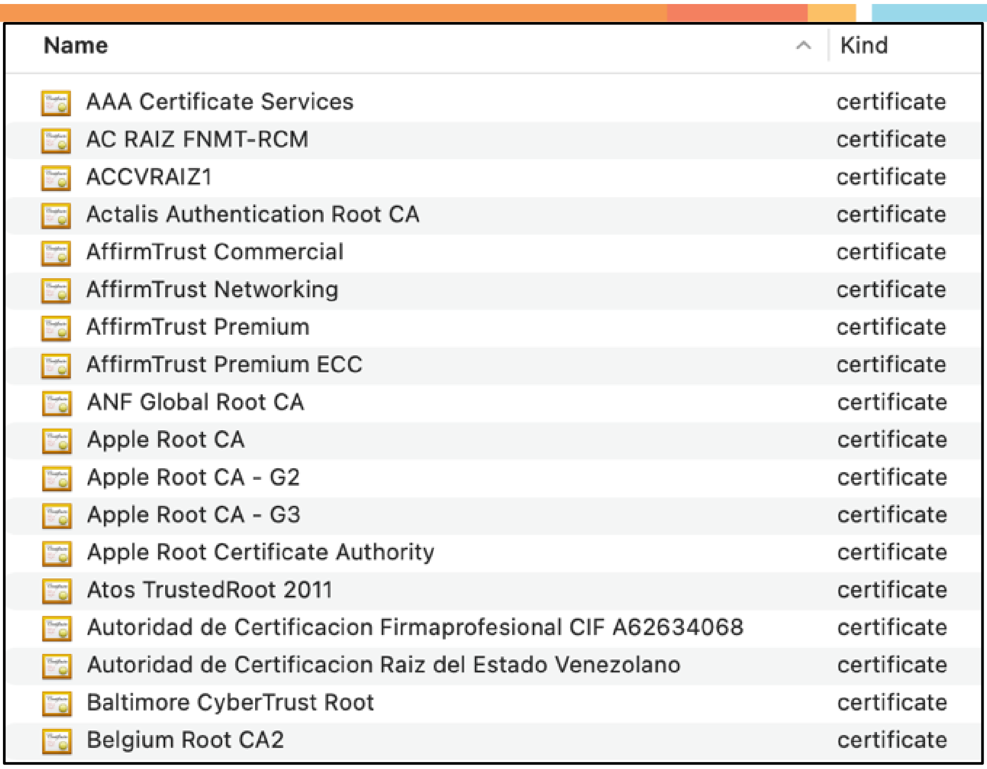


Amazon Root CA 1
└ Amazon
└ www.simplilearn.com

www.simplilearn.com
Issued by: Amazon
Expires: Sunday, 19 June 2022 at 5:29:59 AM India Standard Time

ⓧ This root certificate is not trusted

Client Machine Root Certificates



Name	Kind
AAA Certificate Services	certificate
AC RAIZ FNMT-RCM	certificate
ACCVRAIZ1	certificate
Actalis Authentication Root CA	certificate
AffirmTrust Commercial	certificate
AffirmTrust Networking	certificate
AffirmTrust Premium	certificate
AffirmTrust Premium ECC	certificate
ANF Global Root CA	certificate
Apple Root CA	certificate
Apple Root CA - G2	certificate
Apple Root CA - G3	certificate
Apple Root Certificate Authority	certificate
Atos TrustedRoot 2011	certificate
Autoridad de Certificacion Firmaprofesional CIF A62634068	certificate
Autoridad de Certificacion Raiz del Estado Venezolano	certificate
Baltimore CyberTrust Root	certificate
Belgium Root CA2	certificate

Root Cause and Solution :- The browser does not trust the SSL certificate because the root CA is not present in the client's trusted certificate store. This is a client-side issue, often caused by a missing or self-signed root certificate.

- **Confirm which root CA is being used.**
- **If it's a public CA, ensure client OS/browser is updated.**
- **If it's a private CA, install the CA root certificate on the client machine.**

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
WebSites	TCP	443	0.0.0.0/0
RDP Service	TCP	3389	18.66.78.112/32
SSH Service	TCP	22	18.66.78.112/32

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:

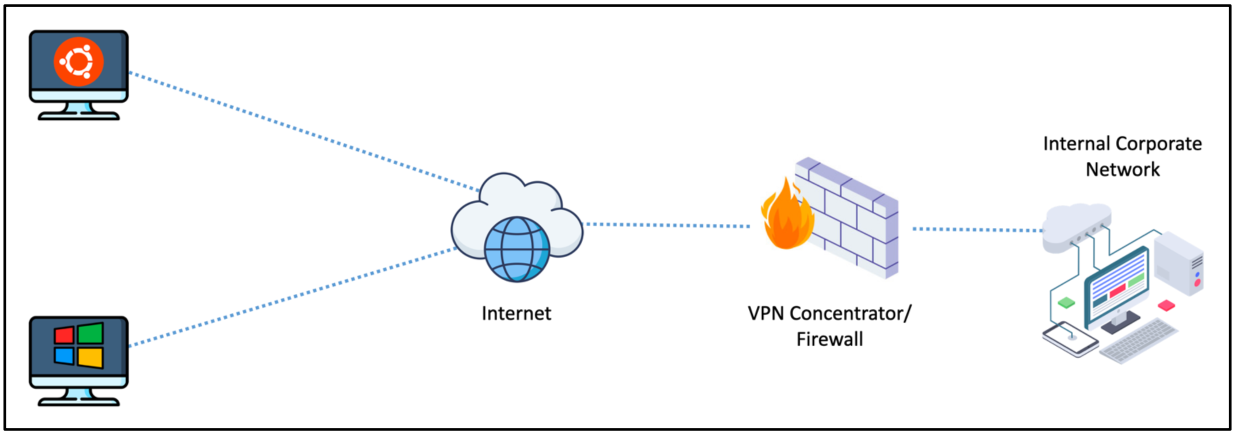
As a network security consultant, you are designing the VPN connectivity requirements so that users working remotely from home can access the corporate network. The business has provided the following connectivity requirements:

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.



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

Task 3 – VPN Configuration Table

Operating System	VPN Type	VPN Protocol	Tunnel Method	Firewall Port	Security Justification
Ubuntu	Host to site	OpenVPN (UDP)	IPsec VPN	1194	OpenVPN is a secure, modern VPN using SSL/TLS encryption. Port 1194 is used by default for UDP-based VPN traffic. Only trusted clients with certs can connect.
Windows	Host to site	PPTP	Split	1723	PPTP allows lightweight VPN access. However, it is less secure; best used in controlled environments. Port 1723 must be restricted to trusted IPs only.