Akshatha K

Network Security Consultant

TASK 1:

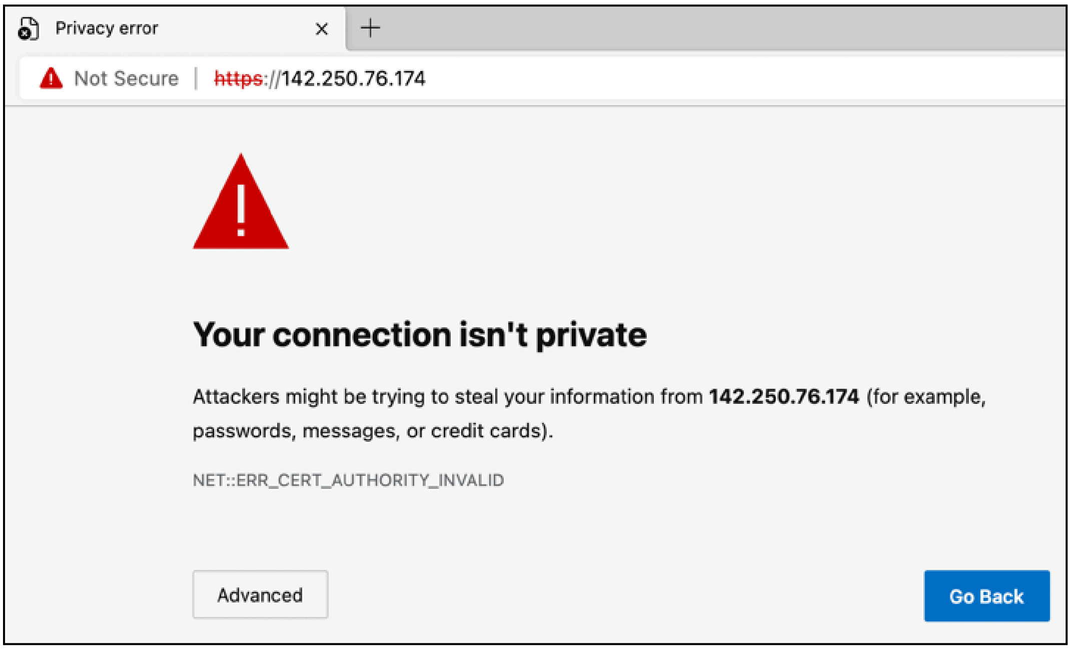
As a network security consultant, you have to review tickets raised by users due to digital certificate issues. To help them resolve these issues, you need to understand the organization's certificate information. Identify the likely issue and the possible solution for the following tickets:

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

ANSWER for ticket 1:

Likely Issue:

The primary issue here is that SSL/TLS certificates are generally issued for specific domain names (FQDNs) rather than IP addresses. When you access a website using an IP address, the certificate presented by the server may not match the IP address, causing a certificate error. This is because the certificate's Common Name (CN) or Subject Alternative Name (SAN) fields include only domain names and not IP addresses.

Possible Solutions:

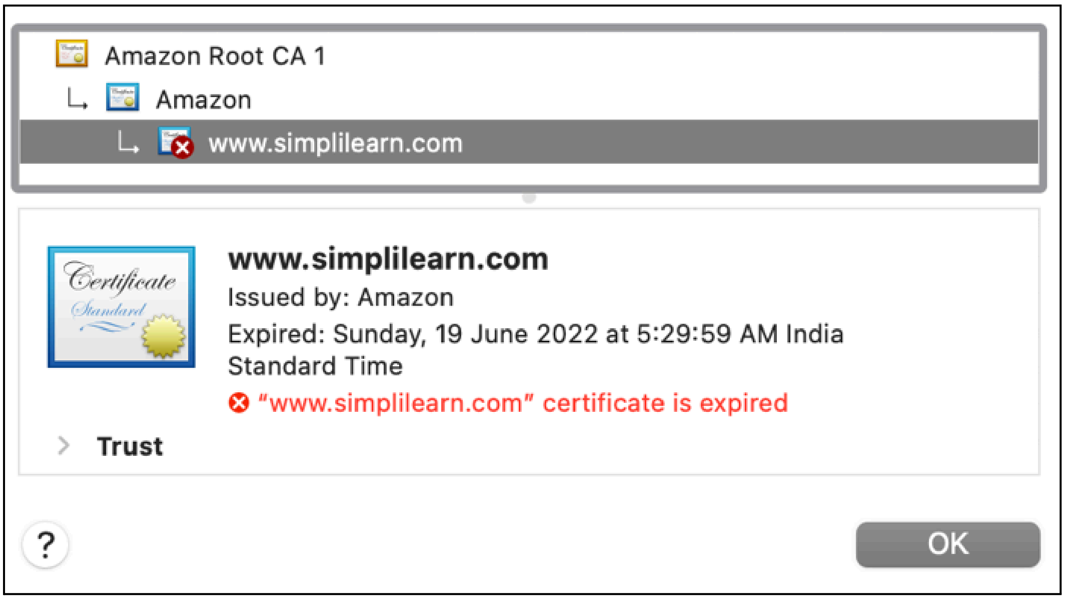
1. **Use the Domain Name**: Always access the website using its domain name rather than the IP address. The digital certificate is valid for the domain name specified in the certificate, so accessing the website using this domain will ensure that the certificate validation succeeds.
2. **Verify Certificate Details:**If accessing via the FQDN still results in errors, check the certificate details. Ensure that the FQDN is correctly listed in the certificate's CN or SAN fields. You can view certificate details by clicking on the padlock icon in the browser's address bar.
3. **Check for Expiration or Revocation:**Ensure that the certificate has not expired and is not revoked. If there are issues related to the certificate's validity period, renew or replace the certificate as needed.
4. **Intermediate Certificates:**Verify that the server is correctly presenting the full certificate chain, including any intermediate certificates. Sometimes, missing intermediate certificates can cause trust issues.

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?



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

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

ANSWER for Ticket 2:

Likely Reasons and Solutions:

Old Certificate Still in Use:

- **Issue:** The web server might still be serving the old, expired certificate rather than the newly renewed one.

- **Solution:** Verify that the new certificate has been properly installed and configured on the web server. Restart the web server after installation to ensure that it is using the latest certificate. You can also use online tools like SSL Labs' SSL Test to confirm which certificate is being served.

Date and Time Settings:

- **Issue: The system time on the server or client device may be incorrect, which can lead to incorrect certificate validation.**
- **Solution: Verify that the date and time settings are accurate on both the server and client devices. Synchronise with a reliable time source if necessary.**

Incorrect Certificate Configuration:

- **Issue:** The new certificate might not have been correctly bound to the appropriate domain or service.
- **Solution:** Check the web server configuration to ensure that the new certificate is correctly associated with the domain name. Ensure that any intermediate certificates are also correctly installed if required.

Browser Cache Issue:

- **Issue:** The browser might be caching the old certificate, leading to a display of outdated information.
- **Solution:** Clear the browser cache and restart the browser. You might also want to check the site in incognito mode or using a different browser to rule out local caching issues.

Certificate Chain Issues:

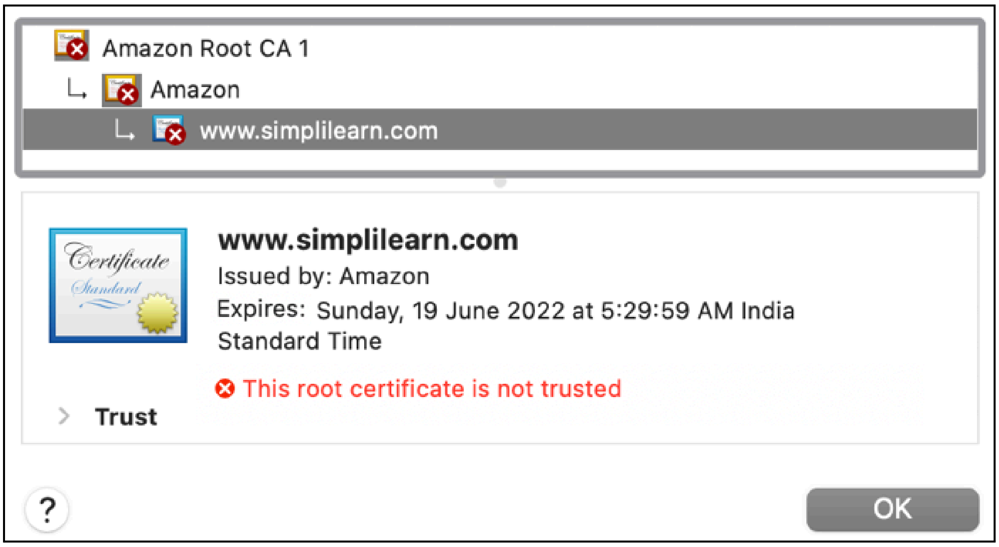
- **Issue:** There may be issues with the certificate chain if intermediate certificates are not properly configured or installed.
- **Solution:** Verify that the full certificate chain is correctly installed and configured on the server. Missing intermediate certificates can cause trust issues and lead to certificate errors.

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

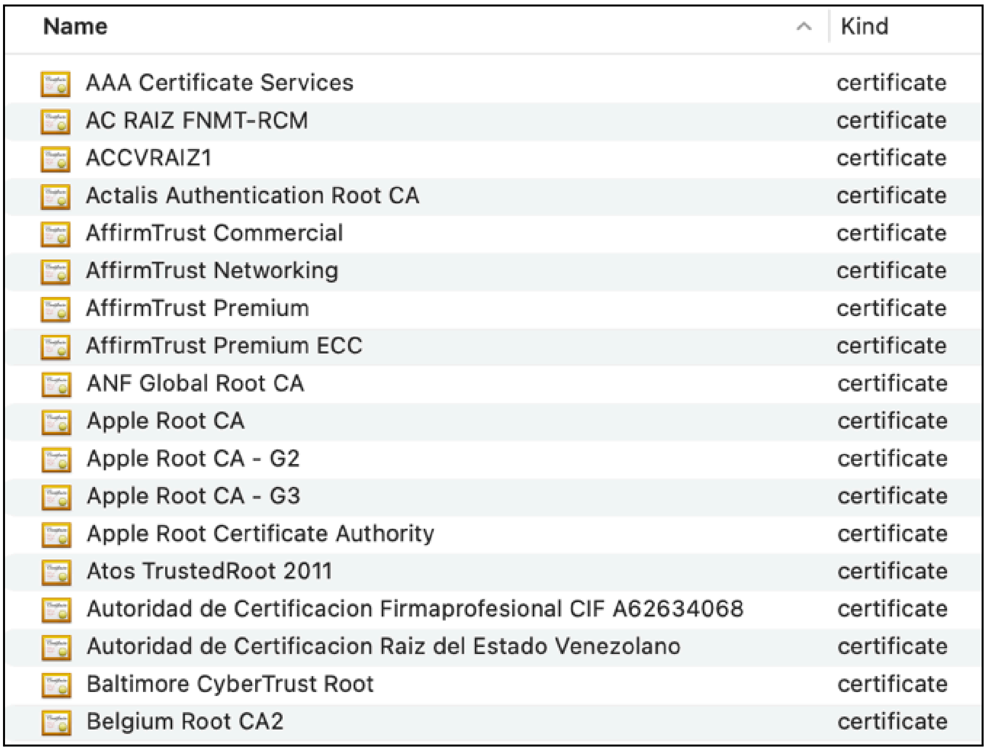
www.simplilearn.com

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

ANSWER for Ticket 3:

Possible Solutions:

1. **Update Your Browser**: Make sure you're using the latest version of your browser, as updates often include new root certificates and security patches.
2. **Check System Root Certificates**: Ensure that your operating system has up-to-date root certificates. On Windows, you can update these via Windows Update. On macOS, check for system updates.

3. **Install Missing Certificates**: If you know the certificate authority used by the website, you can manually install their root certificate. This is usually not necessary unless you're dealing with an internal or less common CA.
4. **Clear Browser Cache**: Sometimes clearing your browser's cache and cookies can resolve certificate-related issues.
5. **Try a Different Browser**: See if the issue persists across different browsers. This can help determine if it's a browser-specific issue.
6. **Verify the Website's Certificate**: Use online tools to check the website's SSL certificate to ensure it's properly configured and not expired. Websites like SSL Labs' SSL Test can be useful.
7. **Check for Interception**: Ensure that there isn't any software or network configuration (like a corporate proxy or antivirus with SSL scanning) intercepting and altering your SSL traffic.

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.

ANSWER for task 3:

Type	Protocol	Port Range	Source
RDP	TCP	3389	18.66.78.112/32
SSH	TCP	22	18.66.78.112/32
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

TASK 3:

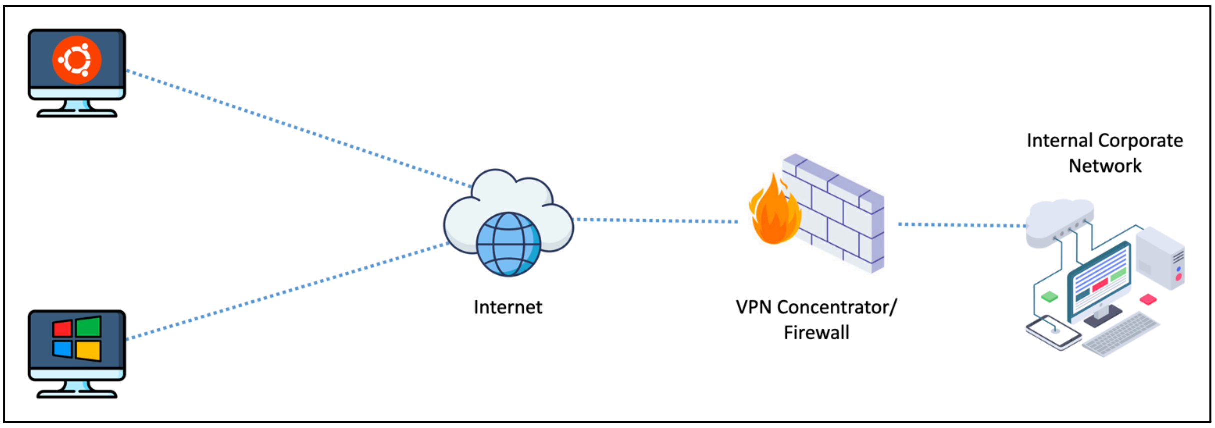
As a network security consultant, you are designing the VPN connectivity requirements so that users working remotely from home can access the corporate network. The business has provided the following connectivity requirements:

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

ANSWER for Task 3:

Requirement	VPN Connection 1 (Ubuntu 20.04 Developers)	VPN Connection 2 (Windows 10 Users)
VPN Type	Remote Access VPN	Remote Access VPN
VPN Name	OpenVPN	L2TP/IPsec

VPN Protocol	OpenVPN	L2TP/IPsec
Tunnel Method	Full Tunnel	Split Tunnel
Firewall Ports	UDP 1194	UDP 500, UDP 4500, UDP 1701
Encryption	256-bit AES	256-bit AES
Key Exchange	SSL/TLS	SSL/TLS
Configuration Notes	- Install and configure OpenVPN. - Route all traffic through the corporate network. - Restrict access to the main software repository server.	- Set up and configure L2TP/IPsec VPN. - Allow split tunneling for non-corporate traffic. - Ensure proper pre-shared keys or certificates. - Configure Windows 10 to connect using L2TP/IPsec.