**CAPSTONE 3**

**Task1:** **Identify the possible issues and solution for the raised tickets.**

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?

**Answer:**

**Likely Issue:**

SSL/TLS certificates are **domain-bound**, meaning they are issued to specific **fully qualified domain names (FQDNs)** like www.example.com, not to raw **IP addresses**.

When accessing a website using its IP address over HTTPS:

* The browser checks if the SSL certificate presented by the server matches the requested URL (here, the IP).
* Since certificates are typically issued for domain names, there's **no match**, causing the certificate to be flagged as invalid.
* Additionally, the certificate may not be signed by a trusted Certificate Authority (CA), leading to the ERR\_CERT\_AUTHORITY\_INVALID message.

**Likely Solution:** Connect using domain name like [www.simplilearn.com](http://www.simplilearn.com)

* Ask Bob to use the **fully qualified domain name (FQDN)** instead of the IP address (e.g., https://www.google.com if 142.250.76.174 belongs to Google).
* Click "Advanced" in the warning and proceed unsafely (only in controlled environments).

**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?

**Answer:**

**Likely Issue:**

The most probable reason for this mismatch is that Sheila’s **system date and time are incorrect**, specifically **set to a future date** (after June 19, 2022). This causes the browser to think the certificate is already expired.

This is evident because:

* The certificate shown is issued by Amazon and valid until **June 19, 2022**.
* The error message states the certificate is **expired**, even though the current ticket date is **January 10, 2021** — well before expiration.
* Therefore, the local system's date is likely misconfigured.

**Likely Solution:**

* Clear browser cache.
* Verify and correct system date, time and time zone settings.

**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?

**Answer:**

**Likely Issue:**

Yes, this is a **client-side issue**.

The client system (James’s device) does **not have Amazon Root CA 1** installed or trusted in its **Trusted Root Certification Authorities store**. As a result, any certificate issued by that root CA is treated as **untrusted**, even if it's valid and used correctly.

**Likely Solution:**

* Download the **Amazon Root CA 1** certificate from a reliable source. Manually **add and trust** the certificate in the system’s certificate/keychain store.
* After installation, restart the browser or system to ensure the new trust settings take effect.
* Resolving it requires adding **Amazon Root CA 1** to the system’s trusted certificate authorities list. Once done, the error should no longer appear.

**TASK 2: Create appropriate Inbound rules.**

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).

Adding the appropriate Inbound rules in the given format.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** |
| **RDP** | TCP | 3389 | 18.66.78.112/32 |
| **SSH** | TCP | 22 | 18.66.78.112/32 |
| **HTTPS** | TCP | 443 | 0.0.0.0/0 |

**TASK 3: Design VPN connectivity based on given requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OS** | **VPN Type** | **VPN Protocol** | **Tunnel method** | **Firewall Port** |
| Ubuntu 20.04 | Host-to-Host | Open VPN UDP | Full Tunnel | UDP 1194 |
| Windows 10 | Remote Access | SSTP (Microsoft proprietary) | Split Tunnel | TCP 443 |