**Name**

**Lab#8: Advanced Cryptography**

**Step-1:** First we opened the website

Graphical user interface, application, email

Description automatically generated

Then we click first website under Recent best

Graphical user interface, application

Description automatically generated

**Step3: then we selected the first ip address**

**Table

Description automatically generated**

**Step-4:**

We note the overall rating is A+. for certificate it has 100 points. For protocol support it has 100. Key exchange and cipher strength holds above 80 points.

**Step-5:**

We see the reason why the website does not received A because site only work in browsers that supportrs SNI.

Graphical user interface, application

Description automatically generated

**Step 6:**

After scrolling down we note the authentication information. It has digital certificate RSA using SHA256. It shows common names and alternative names. Serial number is also mentioned. Validity is mentioned from Tue 7 jun to Mon 5 Sep as well as other information you can see below in the image.

Graphical user interface, text, application, email

Description automatically generated

**Step 7:**

When we scroll down it shows configuration. It supports TLS 1.2.TLS 1.1 could also not be supported because NIST currently suggests everyone upgrade to at least version TLS 1.2 so it depends on which security protocols that want to establish going forward. I would say that TLS 1.0 would be the next to not be supported . Because it has been found to be susceptible to the BEAST attack. As TLS is continuation of SSL.It has been discovered in the deprecated SSl and Tls protocls. For this reason we should disable SSlv2, SSlv3, TLS 1.0 and TLS 1.1. leaving only Tls 1.2 and Tls 1.3 enabled.

Graphical user interface, text, application

Description automatically generated

**Step 8**

As we know security protocols use cipher suites such as TLS and its deprecated predecessors SSL. They are a set of algorithms used to secure network. They should be placed in sequence to ensure security. There order is as follows Risk, Probability and impact. They should be listed as the lower bit suites first then the higher bit.

Graphical user interface, text, application, email

Description automatically generated

**Step 9:**

Now we test with browser and operating system that we use.

Graphical user interface, text, application, email

Description automatically generated

**Step 10:**

Now we click on worst case scenario after clicking scanning back

Graphical user interface, text, application, email

Description automatically generated

**Step 11:**

Now we review summary authentication and configuration, cipher suites and handshake simulation.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Step 12:**

As by reviewing according to my opinion top 5 vulnerabilities are

* Server Vulnerability to attack,
* certificate for a trusted cite,
* a strong key exchange,
* Protocol support,
* Cipher strength

**Step 13:**

Now I generate the report for the organization where I work. As you can see below we receive A score

Graphical user interface, application, email

Description automatically generated

**Step 14:**

 I completely agree with this site's score because, even though some cipher suites are week, which makes the cipher strength be lower than 100, the site has a perfect protocol control, a good key exchange and all the handshake simulations

**Step 15:**

Now we review other factors

Summary

Graphical user interface, application, email

Description automatically generated

Authentication

Graphical user interface, text, application, email

Description automatically generated

Configuration and cipher

Graphical user interface, text, application, email

Description automatically generated

Handshake

Graphical user interface, text, application, email

Description automatically generated

**Step 15:**

* Protocols TLS 1.1 and TLS 1.0 vulnerable to beast attack.
* No handshake compatibility
* Cipher strength
* Certificate for trusted cite
* Strong key exchange.

**Step 16:**

Now we test our own brower.

Graphical user interface, text, application, email

Description automatically generated

**Step 17:**

Graphical user interface, application

Description automatically generated

**Step 18:**

We closed the browse now

**Step 19:**

Now we opened internet explorer to check vulnerabilities

**Step 20:**

We see that there are too many vulnerabilities in Internet Explorer also it supports depreciated protocols that’s why google chrome is better then IE.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Text, application

Description automatically generated

**Step 21:**

All browsers closed.

**Q1:**

A1: I observed that a good website needs to use new protocols and stronger cipher suites to tackle vulnerabilities. Also cipher suite should be placed according to risk, probability and impact.

**Exercise 2:**

We use command given to show certificates

Graphical user interface, text, application

Description automatically generated

Certificate authority approved is show

Graphical user interface, text, application

Description automatically generated

Intermediate Certificate authorities

Graphical user interface, text, application, email

Description automatically generated

Revoking certificates

It shows when was certificate revoked and also its serial number value.

Graphical user interface, text, application, email

Description automatically generated

Untrusted Certificates

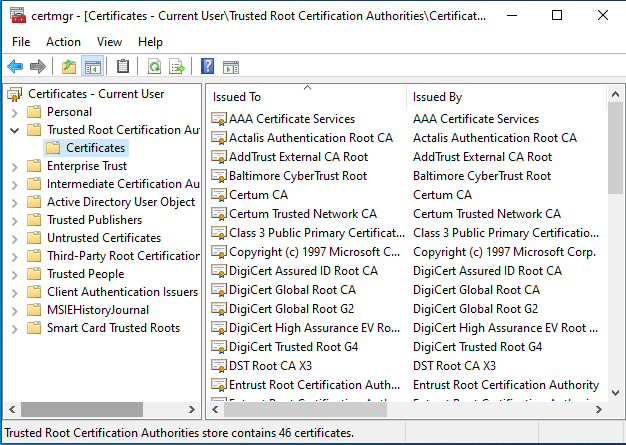
This shows certificates that are no longer trusted and are

Graphical user interface, text, application, email

Description automatically generated

Q2:

**Digital certificates:**

****

Digital certificates can be described as electronic files that are used to identify people and resources over network such as the internet. They enable secure,confidential communication between two parties using encryption. They are issued by CA. They have advantage over ink signatures. As they are given to data types based on their categories.