CS53A Hands-On Project

Threat Identification and Vulnerabilities

Part I.

Refer to the spreadsheet entitled Real Threat Logs 2018 in Files/Hands-On Projects and answer the following questions. Note you can easily sort on individual columns which is often more flexible than viewing events on the actual firewall.

What is the time period for the listed threats?

Which country do most of the threats appear to come from?

What is the most common threat name?

Approximately how many events have a severity level of critical?

When was the most recent threat received from 66.240.205.34?

How many threats have been received from this IP address in 2018?

Where is this threat located? Use ip2location.com.

What is the abuse contact for this IP address? Use appropriate RIR Whois.

Where is threat 185.98.6.98 located?

What is the abuse contact for this IP address?

Part II.

Use the Qualys SSL Test Tool to determine the Security Grade for two secure websites that you use, don’t use large well-known sites like Facebook. Check the box labeled “Do not show results on the boards” before you run the tests.

Test Tool: <https://www.ssllabs.com/ssltest/>

Site 1 Name:

Site 1 Grade:

Site 1 Deficiency Reason:

Site 2 Name:

Site 2 Grade:

Site 2 Deficiency Reason:

Step 2: Select two sites from the list below and repeat the test.

<https://secure.hsabank.com>

<https://www.ncua.gov>

<https://www.onecu.org>

<https://content.dccu.com>

<https://www.pbccuvirtual.org>

<https://www.intrustbank.com>

Site 3 Name:

Site 3 Grade:

Site 3 Deficiency Reason:

Site 4 Name:

Site 4 Grade:

Site 4 Deficiency Reason:

<https://www.ssllabs.com/ssltest>

Always check “Do not show results.”

