Student: Katie Dillan

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?

09/1/2016 to 2/12/2018

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

China

What is the most common threat name?

"FTP: login Brute Force attempt (40001)" 8706 times

Approximately how many events have a severity level of critical?

11255

When was the most recent threat received from 66.240.205.34?
2/10/2018 - Spyware: ZeroAccess.Gen Command and Control Traffic (13235)

How many threats have been received from this IP address in 2018?
41

Where is this threat located? Use ip2location.com.

San Diego, CA 92123

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

No abuse contact found. Customer Name: CariNet, Inc

Where is threat 185.98.6.98 located?

Abdirova, 5, 514, KZ

What is the abuse contact for this IP address?

Denis S Suhachev, AR31908-RIPE, +7-727-2-584-584

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: penfed.com
Site 1 Grade: F
Site 1 Deficiency Reason:

This server is vulnerable to the Return Of Bleichenbacher's Oracle Threat (ROBOT) vulnerability. Grade set to F. MORE INFO »

This server's certificate is distrusted by Google and Mozilla. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server's certificate chain is incomplete. Grade capped to B.

Site 2 Name: smcu.org
Site 2 Grade: A
Site 2 Deficiency Reason:
none

Site 2 Name: fidelity.com
Site 2 Grade: A
Site 2 Deficiency Reason:

This server supports anonymous (insecure) suites (see below for details). Grade set to F.
This server supports insecure cipher suites (see below for details). Grade set to F.
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »
This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

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: https://www.pbccuvirtual.org
Site 3 Grade: C
Site 3 Deficiency Reason:

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »
This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »
HTTP request to this server failed, see below for detail

Site 4 Name: www.ncua.gov
Site 4 Grade: F
Site 4 Deficiency Reason:

This server is vulnerable to the OpenSSL Padding Oracle vulnerability (CVE-2016-2107) and insecure. Grade set to F.
This server's certificate chain is incomplete. Grade capped to B.
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

https://www.ssllabs.com/ssltest

Always check “Do not show results.”