CYBR450-342N – Securing Networks Assignment

NAME: \_\_\_Chad Ballay\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_12/06/2020\_\_\_\_\_\_\_\_\_\_

**Research and explain the latest IEEE standard for Wi-Fi and the level of security it provides. Include at least one reference for more information.**

IEEE 802.11ac

Next step beyond 802.11n. Theoretically will have 4 times the bandwidth. Works on the 5ghz range. For some scenario's the 5ghz limitation will improve security due to how poorly the signal will propagate outward. (Laws of physics so not an intentional feature.) It implements on two new channels. 80MHz and 160MHz. This will complicate the scanning for rogue AP’s until new playbooks and tooling emerge. All in all it looks like the security features/flaws of 802.11ac wash out to a net zero. <https://www.youngupstarts.com/2014/04/05/wireless-network-security-what-802-11ac-means-to-you/>

**Provide at least three security measures for a Wide Area Network (WAN). How do they increase protection for the network? Include an explanation on how an Intrusion Detection System / Intrusion Protection System (IDS/IPS) works on a network. What security benefits does network segmentation, VLANs or virtual networking provide? In your answer, include at least 2 references outside of the textbook.**

VPN – Referenced multiple times as the first step due to how critical it is. Protects your traffic from being intercepted. This is a key risk due to the traffic flowing over and across networks you do not control. <https://en.wikipedia.org/wiki/Virtual_private_network>

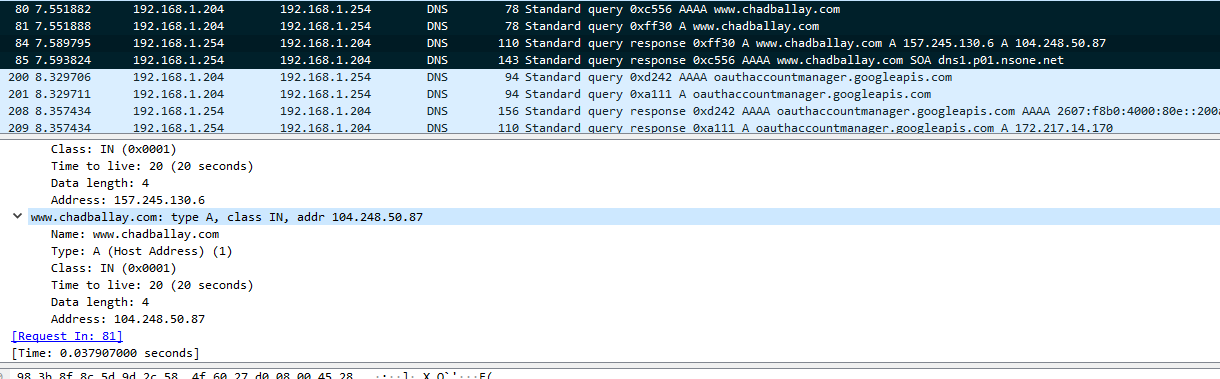
IDS – Intrusion Detection System. Looks within the network and notifies human operators. (Usually a SOC.) Usually works off of signature based monitoring. Works great for detecting attackers within the network. <https://en.wikipedia.org/wiki/Intrusion_detection_system>

IPS – Intrusion Prevention System. Looks along the perimeter of your network for anomalies and automatically responds. Works great for stopping attackers at the gates. <https://www.barracuda.com/glossary/intrusion-prevention-system>

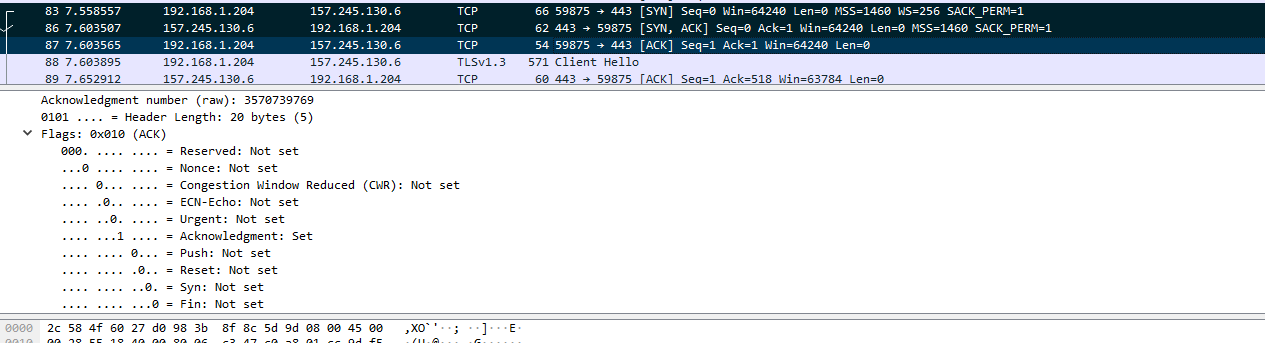
Network Segmentation – Just like on a ship where various compartments are isolated to prevent the loss of one being catastrophic to the whole ship, network segmentation divides and isolates your network so that one part of it doesn’t bring down the whole. This compartmentalization is implemented through various means. Firewalls, VLANs and SDN’s are some of the usual tools. <https://en.wikipedia.org/wiki/Network_segmentation>

**Use the Wireshark application to investigate the network traffic to/from a website. You may use your own computer or the Virtual Cybersecurity Desktop (see separate instructions).**

DNS resolution



Threeway Handshake

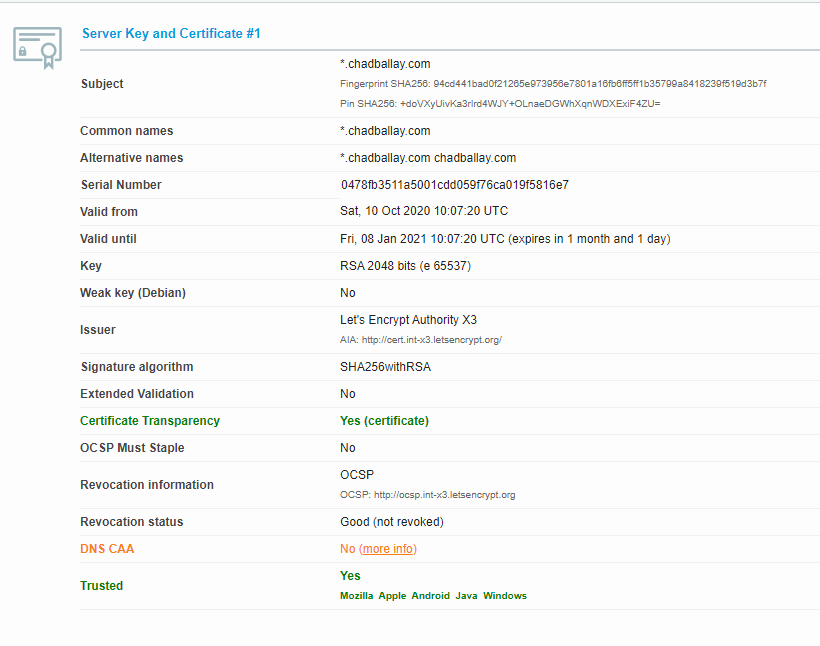


**Use the Qualys SSL labs (https://www.ssllabs.com/ssltest/) to evaluate a website. You can pick one that you work on or use www.bellevue.edu. Show and explain the results. What can we learn from this service?**

Testing <http://chadballay.com>

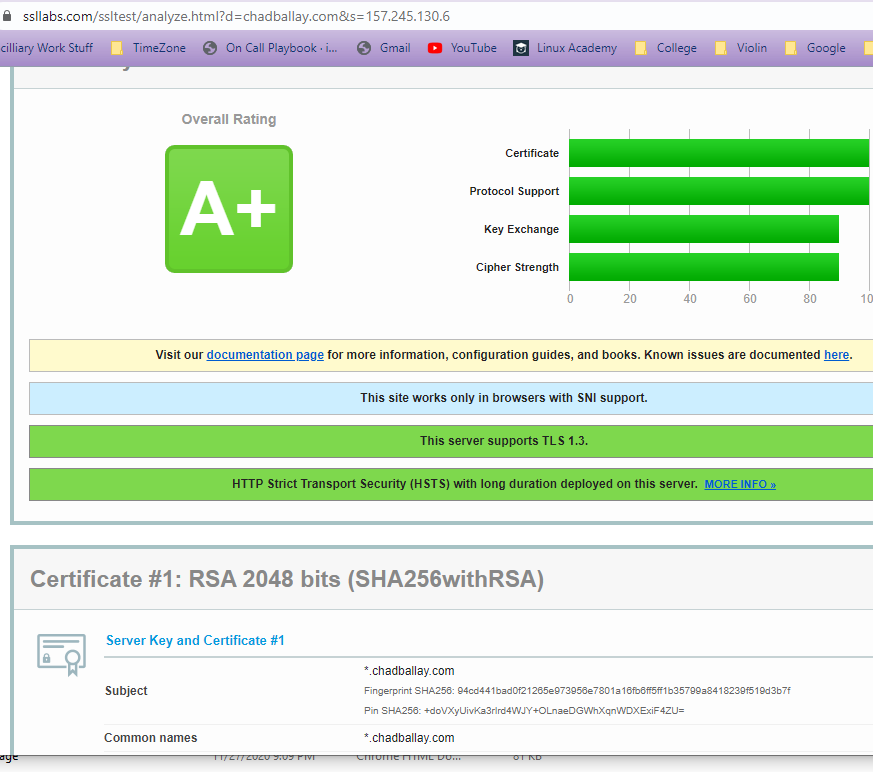
<https://www.ssllabs.com/ssltest/analyze.html?d=chadballay.com&latest>

Verified that my cert came through Let’s Encrypt.



An indepth copy of the report

<https://www.ssllabs.com/ssltest/analyze.html?d=chadballay.com&s=157.245.130.6>



We can see what ciphers are implemented as well as which ones would be likely to no support. We can gather the cert chain back to our own local trust store. You can figure out where this is hosted though Netlify.

