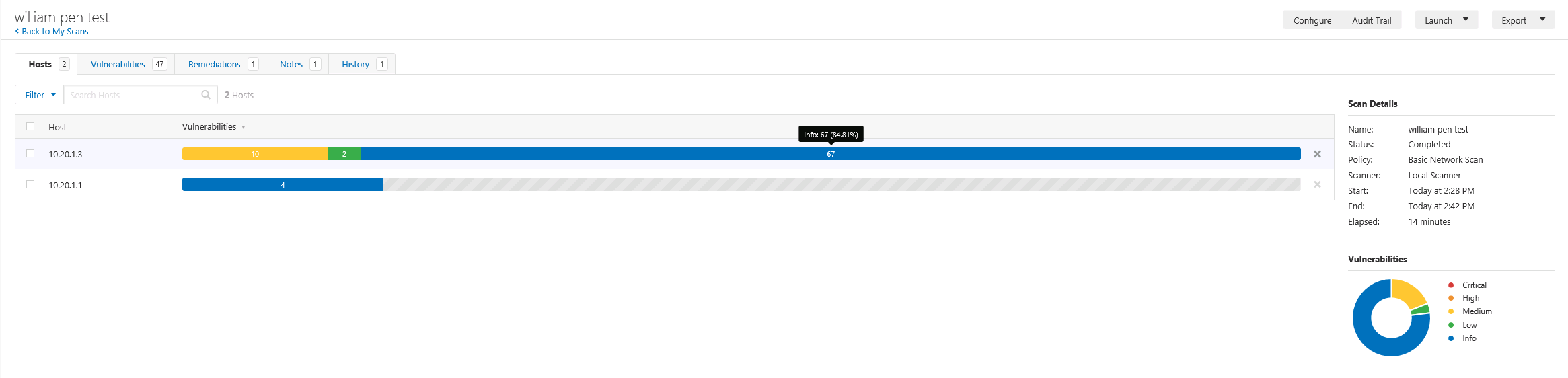
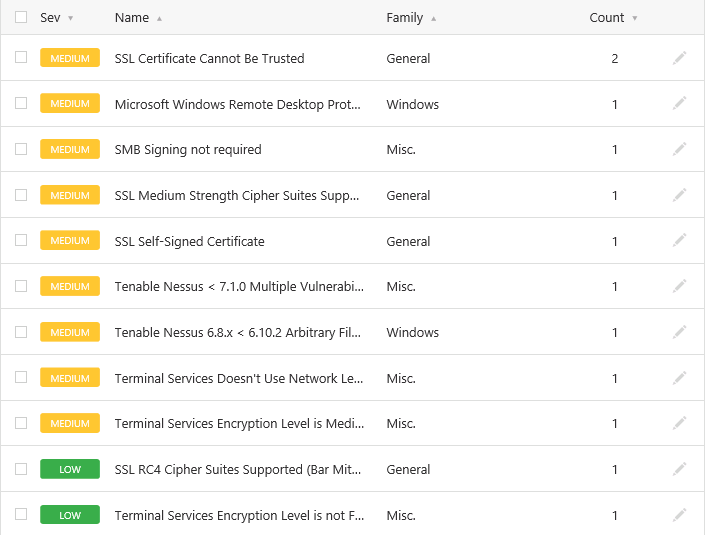
William Chen IST 323 – M002

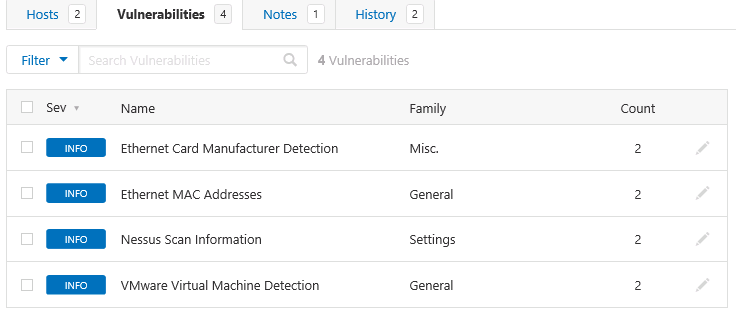
Professor Christopher Croad 11/02/2020

Lab #4 – Penetration Testing a pfSense Firewall

1. **Section 1, Part 2 #11: Vulnerability report summary**
2. **Section 1, Part 2 #13: Medium and low vulnerabilities**



1. **Section 1, Part 2 #27: Updated vulnerability report summary**



**Nessus scanning tool**

The Nessus scanner is a tool developed by Tenable that scans for any vulnerabilities. Some of the vulnerabilities that Nessus can scan for are “vulnerabilities that could allow unauthorized control or access to sensitive data on a system, misconfigurations like a missing patch, common passwords, default passwords, and denial of service vulnerabilities” (Wikipedia). Nessus scans various things such as operating systems, network devices, databases, webservers, and infrastructures. In an article written by Thorin Klosowski for LifeHacker, he taught users how to scan for vulnerabilities using Nessus, and one of the vulnerabilities he had was an Apple TV not on the latest firmware (even though he never used the device). Along with the certificates and other vulnerabilities we found in the lab, Nessus can be used to find any vulnerabilities among all technologies.

A benefit that Nessus has is when you click into a vulnerability to learn more, and it gives you a description and solution. For example, in the lab, I clicked on the “SSL Certificate Cannot Be Trusted,” and it explained the vulnerability with three possible reasons why the problem might’ve come up and how hackers could exploit it. As a solution, it recommended me to purchase a certificate. Despite how great Nessus is at detecting vulnerabilities, there are limitations. Nessus doesn’t actively scan for vulnerabilities, which means that at any point between the first scan and a future scan, many vulnerabilities can arise, but Nessus won’t tell you unless you do a scan. One can use a firewall and/or anti-malware with active scanning and update software and apps to combat this. Another limitation is the cost. Although Tenable offers a free version of Nessus, there are limitations on how many devices it can scan (limited to sixteen IP addresses per scanner). An additional limitation is a bad actor needing to be in your network in the first place. Along with this, the hacker would need to know how to use the tools to attack the vulnerabilities. Most of these limitations are user-based.

**Sources**

<https://lifehacker.com/how-to-use-nessus-to-scan-a-network-for-vulnerabilities-1788261156>

<https://www.cs.cmu.edu/~dwendlan/personal/nessus.html>

<https://www.tenable.com/products/nessus/nessus-faq>

https://en.wikipedia.org/wiki/Nessus\_(software)