Lab 6

Lab 6 – Vulnerability Scanning & Patching – Nessus

By

Lukas Fuller

IAE-201-D02

IA-201: Introduction to Information Assurance

**Abstract**

The objective of this lab is to introduce students to Nessus. Students will understand what vulnerabilities are and what risk they pose to a network. Students will understand how to scan a host and network using Nessus to find vulnerabilities and other network information.

**Materials**

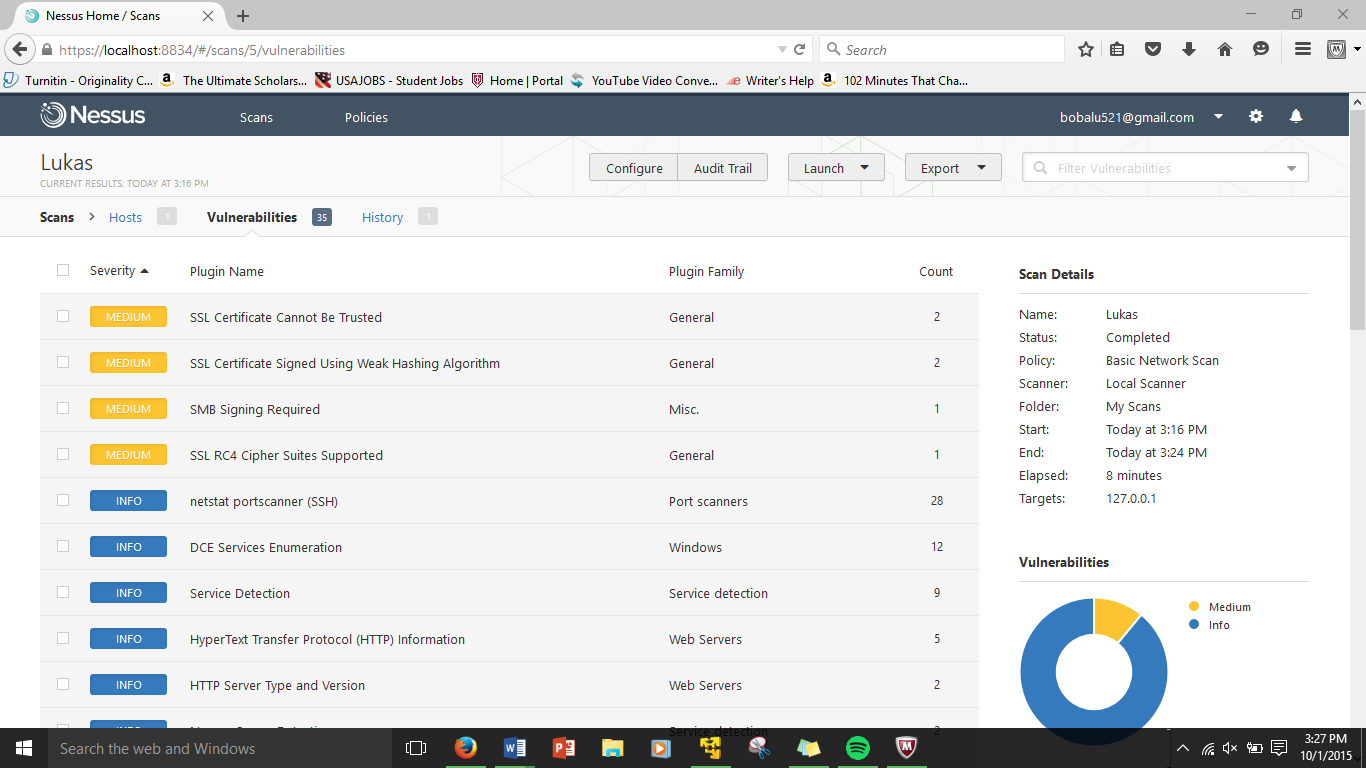
1. Windows VM
2. Metasploitable VM

**Conclusion**

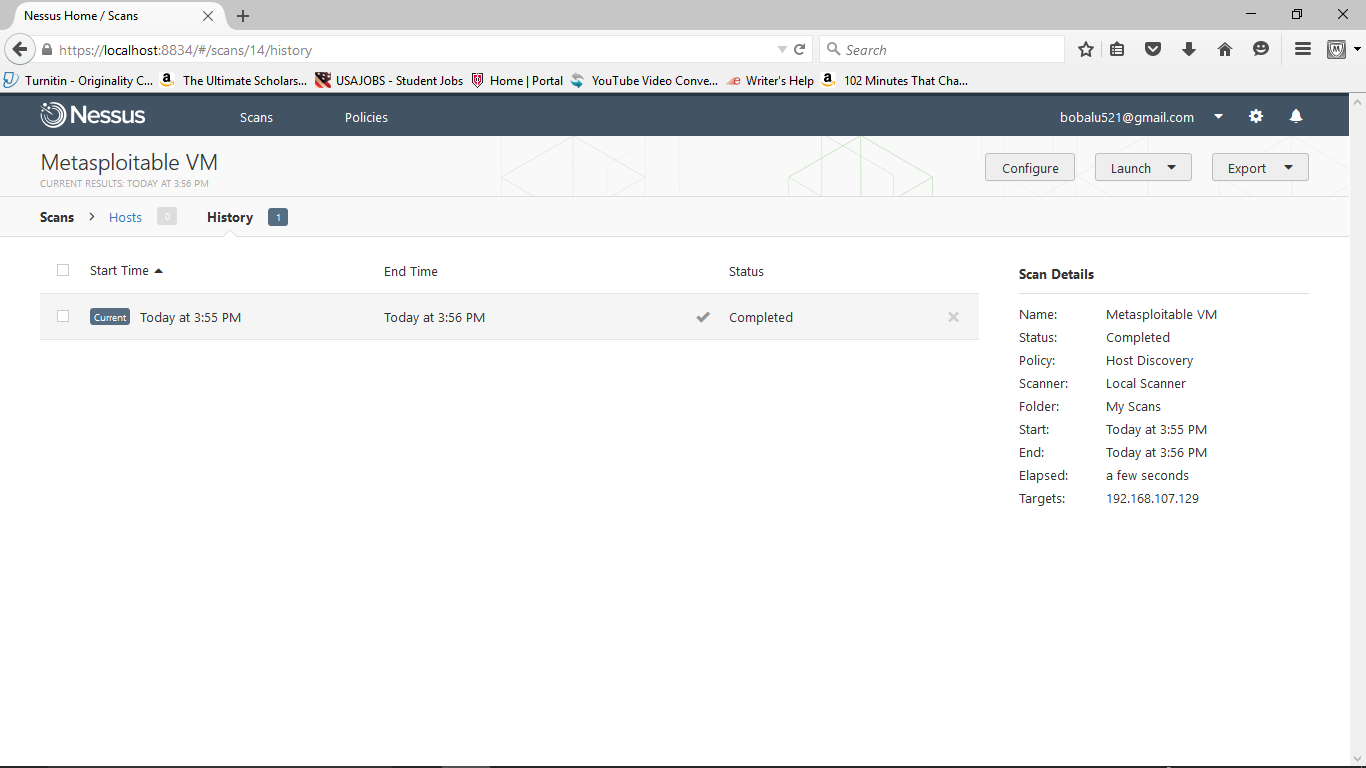
Although I had a few troubles with my Metasploitable VM being detected (probably since I created a VM with Linux on it and the metasploit program so it isn’t exactly the same). Regardless, I learned the risks that lurk on the network especially without a firewall. Nessus showed how many potential threats my computer has, and that’s with a firewall so I assume that a metasploitable VM would have quite a few more. So far I am understanding the basics of the networking environment that I’ve been presented with, and hopefully by the end of the class I will have a grasp on all of the basics in computer security.

**Screenshots**

1. Screenshot of vulnerabilities on Windows box.



2. Screenshot of vulnerabilities of Metasploitable box.



**Questions:**

1. What is Nessus?  **A network vulnerability scanner that searches for known exploits on hosts.**
2. Why is a tool like Nessus important? **It allows for constant current network monitoring**
3. How many vulnerabilities did Windows have? **35**
4. How many vulnerabilities did Metasploitable have? **0**
5. What critical leveled vulnerabilities are there on the Metasploitable box? **0**
6. What is the solution to fix each of the critical leveled vulnerabilities? **NA**
7. Do you see any non-critical vulnerabilities in the Metasploitable box that you find interesting or might pose a risk? What are they? What are the solutions to fix them? **NA**