INFOTC 3001: Computer Network Security
Spring 2019

FINAL PROJECT

I. Objectives.

Implement a vulnerability scanner to detect attacks (we will not focus on preventing/ blocking the attacks, just detecting them).

II. Material Required.

Access to the *credentials file* --> file

III. Activity and requirements.

You are hired by a company to install and configure a vulnerability scanner for their cloud infrastructure allocated in Amazon Web Services (AWS). The company decided to hire you because they received a threaten (apparently from a former employee) who said that their systems will be hacked in the next days.

The company already changed all the passwords for all the users according to their password policy. The company is expecting you to provide a detailed technical report of your finding that includes recommended solutions.

The company who hired you said that there should be 4 instances running in total, all connected to each other, and possibly using the 192.168.100.32/27 subnet which means that the systems should be using IP addresses in the range of 192.168.100.32 to 192.168.100.62.

Start.

1. Select the first available row in the *credentials file* and add your pawprint next to it, so no other student can use those credentials.
2. From the row you selected, download the file to access through RDP to the Windows instance by using the username and password assigned to it.
3. Install Nessus vulnerability scanner on that Windows instance.
4. Find out the IP addresses of the systems (tip: one option is to use *Host Discovery* Template in Nessus with the network ID 192.168.100.32/27).
5. In Nessus create and execute a scan for each of the four systems. Take screenshots of results.

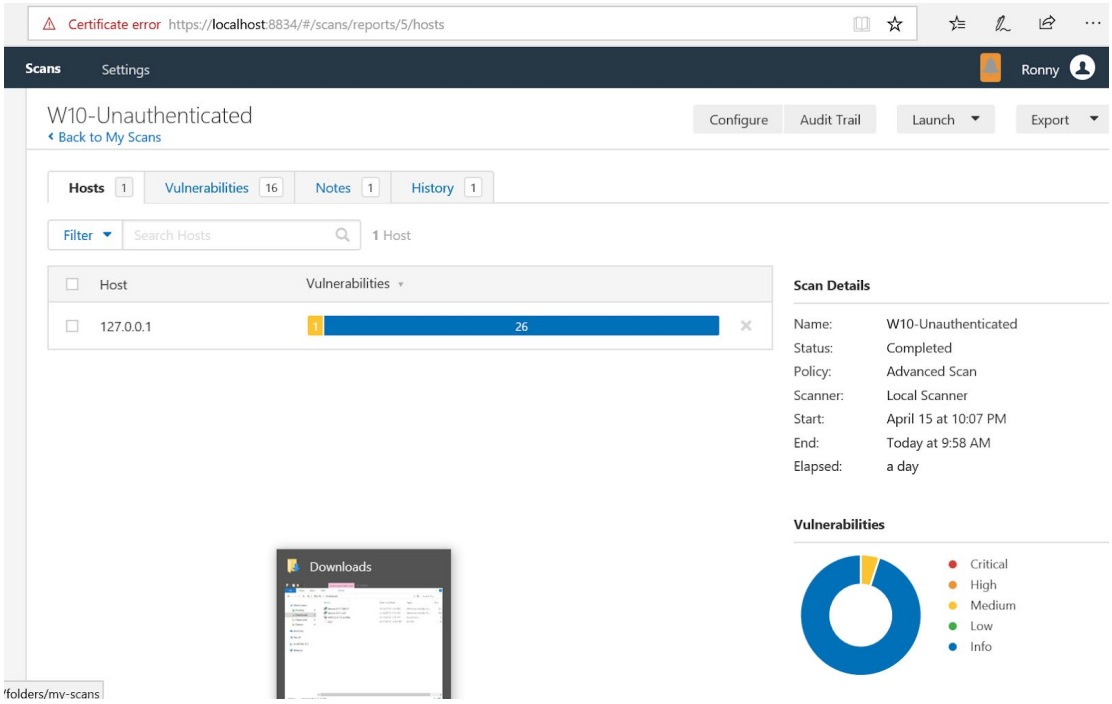
6. Install Snort IDS (https://www.snort.org/) in the Windows and make sure to create rules for UDP, TCP, and ICMP, store the logs in files. (windows video).

IV. Technical Report.

PART 1. By Wednesday, April 24th.

Present a 'Preliminary Report' recommendations to fix medium, high and critical vulnerabilities found by Nessus for each of the four systems.

Add screenshots for each scan i.e.



SSH to the Red Hat instance and obtain information such as user accounts created, type of accounts (root-type or not), total memory, total HDD, Red Hat release version, when the instance was created and network configuration. Take screenshots of each command execution and results.

Based on the /var/log/secure* files list the 2 most common IP addresses (per log) that failed to ssh to the Red Hat instance (tip: sudo egrep "Failure|Failed" /var/log/secure-DATE)

Add a screenshot of Snort being executed.

PART 2. By Friday, May 3rd.

Exactly on Friday, May 3rd.:

1. Ssh to the Red Hat Instance and list the files that were modified the last 7 days. Include screenshot.
2. List the 4 most common IP addresses that failed to ssh to the instance (filter only logs created the last 7 days in /var/log/secure*).
3. List the 4 most common user accounts that failed ssh to the instance (filter only logs created the last 7 days in /var/log/secure*).
4. Analyze the logs create by Snort IDS in the Windows system. What is the most important piece of information you were able to find from the logs?
5. RDP to the Windows instance and create again scans for the 4 systems, take screenshots and write a short summary based on the comparison with the previous scans screenshots. i.e. Did you find any difference?