CIST 3381: Information Assurance & Security

Spring 2022

Project Status Update

1. Name

Michael Chillemi

1. Name of pen testing application/tool approved

-Metasoloit

-Security Onion

- Dradis

-Wapiti

1. Project Scenario & goal (including how / for what purpose you are using the application for?)

I have not composed a scenario yet. But my goal is to utilize every application assigned to me. The purpose of each application is as followed, metasploit will be used to conduct the actual attack on the windows machine. Security onion will be used to conduct network security monitoring and intrusion detection. Wapiti is a tool used to audit the security of web sites. Also it will be used for vulnerability check. The last tool is Dradis which is will be used tot maintain information that can be shared to other parties. It will be the tool that I will be using to document every step in the project.

1. Allocated static IP address range

192.168.154.0/24

1. An informal project update (*points to consider*)
2. What do you plan?
3. Where do you stand (What have you done until now?)?
4. Your plan ahead?
5. Any issues you are facing / What have you tried to tackle the issue
6. Anything else / experience so far you want to share?

a. My plan would be to use wapiti to scan the windows machines basic website find the vulnerabilities in the website. Conduct the attack with metasploit. Use security onion to monitor the network security and test the intrusion system built in by having the victim conduct a counter attack and showing what happens when the security onion detects it. Last use Dradis to document every step of the process to be shared later on.

b. Currently I have both machines talking to each other. I need to understand a bit more how to implement security onion and how the victim will conduct the counter attack. Once I figure that part out I can fully start the attack.

c. My plan ahead will be getting more information about security onion. Also finalizing the plans on the counter attack. Once that is complete the rest of the project should be smooth sailing.

d. In the beginning I faced some issues getting the machines to talk to each other once I conducted one small change in the windows machines network settings then the machines were able to communicate with each other.

e. I am very excited to finalize my plans and start conducted my attack and really get involved in my very own attack on my own.

1. Help/Assistance I can provide for the project

I would really appreciate any knowledge or pointers on how to use security onion. Also maybe your thought about my plan I explained or some tips on how to make it go smoothly.

1. Attach Draft Report *(Optional)*