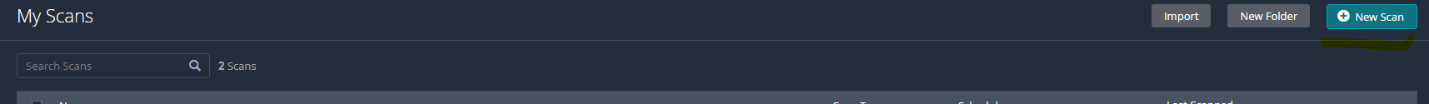
Nessus Vulnerability Scan:

The process below will specifically identify how to run a vulnerability scan utilizing Nessus. This will be a basic network scan targeting a host target IP (provided by try hack me).

Key Takeaways-

1. Configuring Nessus to target a host machine.
2. Interpreting results of the vulnerability scan.
3. Deciphering further actions based upon scan results.

Steps:

1. In Nessus, top right hand corner click on “New Scan”  
   
2. In scan templates, choose “Basic Network Scan”  
   A screenshot of a computer

   AI-generated content may be incorrect.
3. In the Basic>General tab, fill out applicable information.   
   \*Be sure to put the target IP address of the host you are scanning.

A screenshot of a computer

AI-generated content may be incorrect.

1. Navigate to the Discovery tab and choose the drop down for all ports. This will allow us to scan **all** ports related to that host.  
   A screenshot of a computer program

   AI-generated content may be incorrect.

1. Navigate to the advanced section, and choose the option scan type for “scan low bandwidth links”. This option will allow us to scan using the least amount of bandwidth.  
   \* In the save section bottom left hand corner, click the dropdown and click launch.  
   A screenshot of a computer program

   AI-generated content may be incorrect.
2. When the scan concludes, you have the option to click on a few different tabs. Host, vulnerabilities, and history.   
    - Click on vulnerabilities. Here you can see all of the vulnerabilities related to this specific host. It is good practice to click on “report” to get a comprehensive overview of spotted vulnerabilities.   
   - In this example, there was more information. If there were vulnerabilities, vulnerabilities can be assed based upon level of concern and remediation plans.  
   A screenshot of a computer

   AI-generated content may be incorrect.