NIH External Tenable Nessus System Scanning Procedure

By default, NIH and the NCI run regular agent-based Nessus scans against all servers within the NIHNetwork. Tenable Nessus scans can also be run by NIH against external IPs/networks that are used to support NIH applications by following these instructions. Before you submit your request, you will need to know or have the following:

- IP(s) to be scanned
- Scan policy to be used (i.e., host discovery, patch audit, SCAP compliance, etc.)
- Administrative Credentials (if needed for the desired scan policy)
- Scanning instructions such as if the scan must be run after hours or on a weekend, or any special details that IRT should know
- Written approval from your company to scan the remote network/IP

When you are ready to schedule the Tenable Nessus scan you should do the following:

1. Email the NCI ISSO (link sends email). to obtain written approval to scan your network(s). Be sure to specify the IP(s) or IP range(s) you wish to have scanned in order to avoid any ambiguity.

2. Once you have received written approval from the NCI ISSO, send an email to IRT (irt@nih.gov) and ask them to create a new ticket on your behalf. Please be prepared to include the following information in the request:

- IP(s) or IP range(s) to be scanned
- Tier (production or non-production)
- Credentials (if the website requires authentication). See the tip below about the type of account you should use for scanning
- Copy of the NCI ISSO's approval (as an attachment)
- Copy of your company's approval from an authorized officer (i.e., ISSO, CIO, CEO, etc.) of your company
- NCI Point of Contact or an email where you would like the report forwarded. NIH will only send external reports in encrypted format. NIH uses their Secure Electronic File Transfer email service to send to external recipients

4. IRT will send notice for the time the scan will start, and when the scan is complete.

Tips

- In addition to an initial scan, NCI recommends setting up quarterly Nessus scans with IRT to ensure new vulnerabilities are identified as they emerge as part of an overall continuous monitoring strategy.
- We recommend creating designated credentials that will be used solely for scanning purposes and that will be shared only with NIH IRT. The account should be a user account with adequate privileges to perform scans across the designated IPs.
- You should promptly address all High/Critical findings as well as those Moderate risk findings that are valid. You ultimately are the arbiter of which findings are valid and which are false positives.