**Information required to run Nessus scan on applications in the VAEC.**

**The VAEC Security Team will run an unofficial scan for your ATO to determine your vulnerability remediation and an unofficial scan once you have done your remediation. Once your ATO is received, all Nessus scans must be requested from the CSOC.**

For each server (template available – change “APPLICATION” in file name to the application name):

1. IP address and Hostname
2. Type of Operating System
3. Admin credentials for Windows Server – one of the following
   1. Provide admin account and password
   2. Create a local administrative account called “**nessusadmin”** on server and provide credentials
4. Admin credentials for Linux Server
   1. Use SSH Key pair and account (Keys need to be created on a Linux server, keys generated with Putty or Reflections do not work)
      1. Provide private key, user account and paraphrase/password
      2. Account will need Sudo rights
      3. Permissions need to be set:
         1. **#chmod 0600 ~nessus/.ssh/authorized\_keys**
         2. **#chmod 0700 ~nessus/.ssh/**

Open a ServiceNow General Request (Make a Request/Create General Request) to request a scan. In the description, be sure to ask that the ticket be assigned to **OIT VAEC Security**. The assigned engineer will have you send them an encrypted email with the required information.

ADDITIONALLY:

On your Windows scan targets make sure that:

* WMI is be enabled
* Ports 139 and 445 are both be open between scanner and target
* File & print sharing enabled
* Remote registry service enabled
* Default admin shares enabled ($ADMIN, $IPC…)

On Linux hosts and Network devices make sure that:

* Port 22 is open
* You can ssh into the scan target
* The account has enough privileges to perform all checks
* The account can do privileges escalation via: su, sudo su, cisco enable etc.