VMO NOTES - BLOCK 2

Contents

Insights

> -

L1 - ACAS Overview

> - Goals
>   - Differentiate the tools within the ACAS tool suite
>   - Describe purpose of Repositories with ACAS
>   - Define definition of Plugins within ACAS
>   - Discuss function of Plugins within ACAS

>   - Discuss ACAS Capabilities and Limitations

> - ACAS Tools/Software Components
>   - Tenable.sc (previously Security Center)
>   - Central console for ACAS. Offers automation & scale vulnerability/compliance scanning infrastructure. Allows management, altering, & reporting against vulnerability/compliance requirements
>   - Nessus Scanner
>   - Covers a breadth of checks, including unique CVEs, & operates across different environments. Can meet active scan requirements
>   - Nesus Network Monitor (NNM)
>   - Monitors network traffic in real-time, determining client & server vulnerabilities & sending them to Tenable. Continuously looks for new hosts, applications, & vulnerabilities w/o active scanning. Can meet passive scan requirements
>   - Nessus Manager
>   - Manager for Nessus agents & linked to Tenable, allowing Tenable to query the manager for agent scans. Can meet active scan requirements
>   - Nessus Agents
>   - Installed locally on a host, collecting vulnerability, compliance, & system data, & reports that info to a manager. Can perform Non-Credentialed scans on hosts, offline assets, & endpoints that intermittently connect to the internet
>   - Log Correlation Engine (LCE)
>   - Server
>   - Collects & normalizes data from clients, which is then analyzed using Tenable. Both raw & normalized data are available to the user
>   - Interface
>   - Web-based interface provided by each LCE server, for monitoring LCE server/client health & status, configuring LCE servers, managing clients, creating & assigning policies, & managing users
>   - Clients
>   - Installed on hosts to monitor & collect events, which are sent to the LCE Server and are both stored as raw logs & normalized & correlated with vulnerabilities

> - Repositories
>   - "*Scan data is stored in a proprietary data file format called a repository*"
>   - When a scan is initiated, results are imported into a repository
>   - Data is retained according to Admin-defined expiration settings
>   - Repositories are defined by an IP range or the Mobile Device Manager (MDM) data type they accept
> - 2 Categories, 5 Types
>   - Local - IPv4, IPv6, Mobile
>   - External - Remote, Offline

> - ACAS Plugins Defined
>   - Developed by Tenable Research to detect new vulnerabilities
>   - Written in the proprietary Nessus Attack Scripting Language (NASL)

>   - Contain vulnerability information, simplified remediation actions, & the algorithm to test for vulnerability presence
>   - Families - Named by attack type, device family, or plugin action; used to manage large groups of plugins, enabling/disabling potentially thousands of plugins, with the option to manually enable or disable specific plugins within a family
>   - Backdoors
>   - CISCO
>   - Databases
>   - Denial of Service
>   - Will be executed when Safe Checks are disabled
>   - Firewalls
>   - Deals with firewall devices & software that don't have a specified family
>   - Gain a shell remotely
>   - Port Scanners
>   - SCADA
>   - Service Detection
>   - Plugins that detect specific protocol or application listening on a port
>   - Web Servers
>   - Windows
>   - Windows: User Management
>   - Local security checks that specifically cover user information
>   - Categories for specific protocols
>   - DNS
>   - FTP
>   - RPC (Remote Procedure Call)
>   - SMTP
>   - SNMP (Simple Network Management Protocol)

> - Functions of ACAS Plugins
>   - Plugins typically cover 1 or more CVE IDs, allowing an ACAS scan to detect new vulnerabilities
>   - Configure Plugin Options
>   - Required User Role: Admin or organizational user w/ permissions
>   - VMO can configure plugin options within a scan policy to enable or disable them on a family or individual level

> - ACAS Capabilities
>   - Nessus Scanner Capabilities
>   - Agentless
>   - Scalable Solution
>   - Vulnerability Scanning
>   - Network Discovery
>   - Perform mandated discovery scans
>   - ID computers, server, printers, switches, routers, & IP phones on base
>   - Compliance Reporting
>   - Perform mandated compliance scans of security configuration checks
>   - Nessus Scanner Limitations

        - Does not remediate vulnerabilities
        - Shared resources among multiple bases limits concurrent data import
        - Scans can be time-consuming
        - Scans can utilize high network bandwidth
        - Scans only for known vulnerabilities
        - Most mandated scans require credentials

L2 - ACAS Hierarchy Structure

- Goals
    - Explain ACAS Hierarchy Structure

- Hosting
    - It is recommended that all ACAS components be deployed on discrete hosts with no non-cybersecurity software installed, as these components will likely utilized the entire resource pool of the host
    - In small environments (<2000 hosts>), deploying 2 or 3 components on a single host may be feasible
    - In virtualized environments, a 35% overage in CPU & RAM is recommended to cover loss due to virtualization
- Licensing
    - Tenable.sc, Nessus Manager, & LCE require a separate license or activation code, which are requested by deployed sites & fulfilled by DISA
    - Tenable.sc is licensed by the total number of unique active IP addresses it manages & the hostname of the system on which it is installed
- Interface
    - The Tenable, Nessus, & NNM web interface can be launched via browser & uses HTML5
    - To launch the web interface on a STIG-configured browser, the URL must be added to the browser's trusted sites

- Tenable Requirements
    - The more active users there are, the more memory & processor cores you want
    - RAID arrays and/or SSDs are ideal
    - Adequate disk space is critical
        - Tenable saves snapshots of the vulnerability archive daily
        - Vulnerability data size varies with the number & types of vulnerabilities, in adition to number of hosts
        - The output for some plugins are much larger than others
        - Active scan sessions of 35000-50000 hosts can consume as much as 150 GB of disk space, which is taken until the scan is complete & results are imported
- Nessus Scanner Requirements
    - Resource requirements to consider include raw IP address count & the configuration of the scanner deployment
    - No configuration can be assured to scan a specific number of hosts per hour

> - The ability to scan a given number of hosts rests heavily on the memory & processor power; more hadware = more speed
> - Bandwidth Availability & Latency
>   - Seriously impacts scanner performance
>   - Scanning can easily overload networks that are at or near capacity
>   - Host processing power & number of vulnerabilities also affect performance; the scanner may wait longer on a slow host to return its results
>   - Deploy 1 scanner per 2000-4000 hosts and/or 16000 IPs
>   - A scanner should not be assigned to multiple scan zones
>   - The UI has options for this, but the feature is know to cause performance & availability issues
>   - IP ranges within a scan zone can overlap, which may slow overall performance, but is generally insignificant

---

L3 - ACAS Tool Functions

> - Goals
>   - Discuss ACAS tool deployment considerations
>   - Discuss ACAS OPORD
> - ACAS OPORD
>   - JFHQ-DODIN TASKORD 20-0020
>   - *Implementation requirements & obligations*
>   - Structure
>   - Identify Organizational / Site IP Space and Hosts
>   - Global IP Space Documentation
>   - Program of Record IP Space Documentation
>   - Conduct Discovery Operations
>   - Active Discovery Operations
>   - Passive Discovery Operations
>   - Monitoring Network Services and Server Subnets/VLANs
>   - Monitoring Egress Points and External Network Connections
>   - Monitoring Network Core for Unused IP Space
>   - Discovery Scan Result Review
>   - Conduct Active Scans
>   - Active Scan Policy
>   - Active Scan Settings
>   - Active Scan Deviations
>   - Credential Use
>   - Vulnerability Scan Result Review
>   - Good Data
>   - Bad Scan, Local Checks Failed (Unsatisfactory)
>   - Plugins for Troubleshooting
>   - Host Coverage and Data Retention
>   - Configuration Scanning Requirements
>   - Agent Scanning

>   - Viewing Agent Scan Data in Tenable Security Center
>   - Scan Data in Tenable Security Center
>   - NNM TASKORD Requirement
>   - Publishing Compliance Objectives
>   - Area of Operations Modification for Report Attribute Configurations
>   - TASKORD Exemption Criteria
> - Each site must ID, document, & scan DoD owned or operated endpoints
> - Each organization/site will maintain a master Asset List covering the organization/site IP space
> - If an organization maintains multiple Tenable servers, they will maintain asset lists on each of them which includes the portion of the IP space the Tenable is responsible for

---

L4 - ACAS Administrator Responsibilities

> - Goals
>   - Define an organization within ACAS
>   - Explain how organizations are used within ACAS
>   - Define a scan zone within ACAS
>   - Explain how scan zones are used within ACAS
>   - Define a repository within ACAS
>   - Explain how a repository is used within ACAS
>   - Define the role of a Security Manager
>   - Explain the function of the status circle within ACAS

> - ACAS Organization
>   - A distinct set of users & groups, and the resources available to them

> - Organization Functions
>   - The organization is managed primarily by administrator users & security manager users
>   - Administrator users create organization & creates, assigns, & maintains security manager user accounts
>   - Security managers (or any org member with permisions) creates other users within the org
>   - Groups allow you to manage users & share permissions to resources & objects among the group
>   - Multiple orgs can share the same repos, & the vulnerability data within the overalapping ranges is shared between the orgs
>   - Orgs can be given their own discrete repos to facilitate situations where data must be kept confidential between different orgs

> - Scan Zones
>   - Scan zones are areas of your network that you want to target in a scan
>   - Scan zones associate an IP address, or range, with 1 or more scanners in a deployment
>   - Scan zones must be created to run active scans in Tenable

> - Repositories
>   - Databases within Tenable that contain vulnerability data

> - Repos are a proprietary format
> - Repos can be shared w/ users & orgs based on admin-defined assets
> - Repos provide scalable & configurable data storage
> - Repo data can be shared between multiple Tenable instances

> - Security Manager
>   - An account that manages an individual organization, with a broad range of security roles within said org, including complete access to all the org's data
>   - The initial user that is created when a new org is created
>   - Has the ability to launch scans, configure users that aren't the admin, set vulnerability policies, and alter other objects in the org
>   - The initial Sec Manager can't be deleted except by deleting the organization

> - Status Circle
>   - Within the settings of a Nessus scanner, the scanner health page provides info about a scanner
>   - Real-time health & performance data can be used to assist scanner troubleshooting
>   - Scanner alerts provide error information, updated every 30 seconds
>   - Scanner status can be visualized into graphs, such as a circle graph of scanners grouped by status

---

L5 - Role-based Access Control

> - Goals
>   - Recall usage of organizations within ACAS
>   - Define roles within ACAS
>   - Explain when roles are useful within ACAS
>   - Define groups within ACAS
>   - Explain when groups are useful within ACAS

> - ACAS Organizations
>   - A set of distinct groups & users and the resources they have access to
>   - Users are assigned repositories & zones within 1 or more IP network

> - ACAS Roles
>   - Roles determine what a user has access to
>   - Tenable.sc comes with 8 system-provided roles
>   - VMO can customize permissions on some, but not all system-provided roles
>   - VMO can configure linked user accounts
>   - Administrators can switch to one or more Security Manager user accounts without logging out & back into Tenable
>   - Administrator users can create Administrator or Security Manager user accounts
>   - Organizational users can create Auditor, Credential Manager, Executive, No Role, Security Analyst, Security Manager, or Vulnerability Analyst accounts at their own privilege level or lower

> - ACAS Groups
>   - Refers to collections of users with the same permissions within an organization
>   - User groups are a way to group rights to objects
>   - Quickly assign & alter rights to one or more users
>   - Group membership determines a user's access to security data
>   - User creates various objects such as reports, scan policies, dashboards, & other similar items
>   - Objects are automatically shared among the group members if the group permissions allow view & control

---

L7 - ACAS Repository Functions

> - Goals
>   - Explain ACAS repository function
>   - Discuss ACAS interaction with Continuous Monitoring Risk Scoring (CMRS)
>   - Discuss ACAS interaction with other security solutions

> - Continuous Monitoring Risk Scoring (CMRS)
>   - Web-based system that aggregates data from DoD end-point sensors
>   - Endpoint Security System (ESS)
>   - Assured Compliance Assessment Solutions (ACAS)
>   - Near real-time risk assessment & continuous monitoring
>   - CMRS's objective is to assess & measure the risk state of DoD IT systems in accordance w/ enterprise security controls like software/hardware inventory
>   - Built to host DoD security info of mobile devices, workstations & servers, networked user support devices, network infrastructure
>   - Platform ITs in a centralized location0
>   - CMRS displays the status of what ESS modules & versions are deployed on devices across the DoD, & summaries of what extensions each ESS instance has installed
>   - Device Search
>   - CMRS allows users to find any info it contains about devices on the DoDIN by searching by MAC, IP, hostname, org, location, system, etc.
>   - Software Inventory
>   - CMRS can do enterprise-wide searches for vulnerable, outdated, or required software deployment
>   - Collected from Asset Configurationn Compliance Module (ACCM) sensors by CMRS
>   - At least 1 Tenable Security Center instance is required to publish data to CMRS
>   - A base's entire Credentialed Repository will be published to CMRS weekly
>   - Multiple orgs can share the same repo, & overlapping vulnerability data may be shared between them
>   - Discrete repositories can facilitate situations where data musn't be available outside of your org

> - Security Solutions with ACAS

> - The Nessus scanner forges packets & performs other tasks that will look malicius to most security software, which can cause problems if the Endpoint Security System (ESS) on a device isn't configured properly
>   - The ACAS ESS Integration Guide provides guidance for properly configuring ESS
> - In instances where ESS is not used, it is on VMO to understand that deviations in configuration may cause unexpected scan results

---

L8 - ACAS Repositories

> - Goals
>   - Discuss deployment considerations for ACAS repositories
>   - Explain the containable data types for local ACAS repositories

> - Deployment Considerations
>   - Each repository can take up to 32 GB of storage
>   - Tenable SC doesn't limit the number of repos, but it is a significant performance factor
>   - Different file system options for Red Hat Enterprise Linux have different limitations on maximum partition size and maximum file count

> - Data Types
>   - Repos can only contain one of these data types
>   - IPv4 addresses
>   - IPv6 addresses
>   - Mobile Device Management (MDM)
>   - Nessus Agent
>   - DISA recommends separate repos for these data types
>   - Production Active scan,
>   - Passive traffic analysis data
>   - Non-production (diagnostic or test) scan data
>   - Ad-hoc scans
>   - Agent data

L9 - DEMO - ACAS Repositories

> - Goals
>   - Discuss remote Repositories within ACAS

> - Remote Repositories
>   - A repo copied from another Tenable SC system
>   - Remote repos can allow a central Tenable SC to analyze & perform reporting against data copied from other Tenable SC systems
>   - No scan data can be written into a Remote repo
>   - VMO may only use remote repos for reporting purposes
>   - Repo replication can copy up to the full repo size (32 GB) each day

        - Data volume & available bandwidth should be considered when multiple repos are being sync'd or if the source Tenable SC'sconnection has limited bandwidth
    - It may be tempting to create a centralized storage for sites with multiple Tenable SC deployments, but using replication to store two SC's worth of data into a single SC is unlikely to be successful

---

L10 - ACAS Active Scan Objects

- Goals
    - Define an Asset within ACAS
    - Differentiate template-based assets & custom asset types
    - Define credentials
    - Explain impact on credential availability by the user role of the credential creator
    - Discuss credential types supported within ACAS
    - Discuss authentication methods supported for credentials
    - Define audit files
    - Recall scanning for Vulnerability vs Compliance
    - Explain how audit files are used within ACAS
    - Recall usage of Scan Zones
    - Define Scan Policies
    - Discuss Advanced Options for configuration of Scan Policies

- Active Scan Objects
    - Assets, Credentials, & Policies

- Assets
    - Lists of devices within a Tenable SC organization
    - Assets can be added to group devices that share common attributes, whic can then be used to target those devices during scan configuration
    - Template-based Assets
        - Vendor-provieded asset templates, customizable for an environment
        - Updated via Tenable SC feed & visible depending on other configurations
    - Custom Asset Types
        -

Type	Description
Static	List of IPs
DNS Name List	DNS hostnames for the asset
LDAP Query	Uses results from LDAP query string
Combination	Asset created based on existing assets & the AND/OR/NOT operators
Dynamic	Meets a flexible group of condition statements & refreshes based on scans

> | Type | Description |
> |---|---|
> | Watchlist | List of IPs NOT in managed range (ex. known external source of malicious activity) |
> | Import | Imports previously exported asset file |

> - Credentials
>   - Reusable objeccts that facilitate a login to a scan target
>   - Various types of credentials can be configured for use with scan policies
>   - Tenable SC supports an unlimited number of SSH, Windows, & database credentials, & 4 SNMP credential sets per scan configuration
>   - Credentials created by an admin are available to all orgs; ones created by org users are only available in that org
>   - Users can share credentials, allowing them to scan remote hosts without knowing the host's credentials
>   - If a scan contains multiple instances of one type of credential, it will go through the list in order added, stopping at the first one that works even if another credential has greater privileges
>   - Supported Credential Types
>   - API Gateway
>   - Database
>   - SNMP
>   - SSH
>   - Windows
>   - Authentication methods within credential types have their own sets of authentication options
>   - General Authentication Options
>   - Name (Required) - Name of the credential
>   - Description - Description of the credential
>   - Tag - Tags of the credential
>   - Tags label assets, policies, credentials, or queries with a custom descriptor to improve filtering & object management
>   - After a tag is created & applied to an object, the tag is visible to all users who can view or modify the object, but tags are not shared across object types

> - Audit Files
>   - Proprietary formatted XML files that define how ACAS should check for compliance with a benchmark
>   - Benchmarks describe a configuration specification; the DoD standard specification uses STIGs
>   - Tenable distributes audit files via the Tenable SC Feed that is used to update the SC
>   - SCAP files can be uploaded & used in the same way as an audit file
>   - Still XML, but used a protocol defined by NIST
>   - Audit files are used to perform authenticated configuration scans of all active IP space to include all IP addresses & ranges owned, operated, managed, or maintained by a DoD entity to conduct or support operations

>   - Includes external contractor/vendor assets in DoD enclaves, both classified & unclassified, that align with DoD Component AOR
>   - At a minimum, all DoD Components must run all DISA STIG audit files & custom audit files developed to support DoD secure configuration requirements
>   - Includes audit files developed to check JFHQ-DODIN / CYBERCOM order compliance
>   - Additional audits may be required based on OS, applications, & devices within a host

> - Scan Policies
>   - Contain plugin settings & advanced directives for active scans
>   - Admin-created scan policies are available to all organizations within the Tenable deployment, while org user-created policies are only availabe to their org
>   - Policy options specify granular configurations for active scans

---

L11 - ACAS Active Scan Management: Nessus Scanner

> - Goals
>   - Explain endpoint discovery within Nessus Scanner
>   - Explain active scan scheduling

> - Endpoint Discovery
>   - Performed to get an accurate picture of network assets
>   - Examples
>   - Scans using the Host Discovery template
>   - Scans using discovery plugins
>   - Scans are not scheduled by default; the Enable Schedule setting defaults to off
>   - Schedule settings
>   -
>
> | Setting | Description |
> |---|---|
> | Frequency | How often the scan is launched (Once, Daily, Weekly, Monthly, Yearly) |
> | Starts | Specifies the exat date & time when a scan launches |
> | Timezone | Specifies the timezone for Starts setting |
> | Repeat Every | Specify relaunch interval (defaults by Frequency) |
> | Repeat On | For Weekly Frequency, specifies day of week |
> | Repeat By | For Monthly Frequency, specifies day of month |
> | Summary | Provides summary of schedule settings |

L12 - DEMO - ACAS Active Scan

> - Goals
>   - Explain resource considerations for scanning within Nessus Scanner
>   - Explain how a plugin is used within ACAS
>   - Explain the update process for a plugin

> - Resource Consideration
>   - Scans, reports, & dashboards all require RAM & CPU allocations on run, which may cause the UI to slow down when they run
>   - Moving reports & scans to after-hours will minimize impact to users
>   - System administrators should periodically review scheduled tasks to ensure they do not overlap
>   - Tenable SC doesn't try to distribute tasks scheduled for the same time
>   - Tenable SC will attempt to distribute the load for simultaneous tasks across available Nessus scanners, but this may adversely affect performance
>   - When possible, sites should avoid concurrent scan jobs, ensuring a 15 minute buffer between scheduled tasks

> - Plugins Purpose & Usage
>   - In adition to vulnerabilty scanning, plugins are also used to obtain configuration information from authenticated hosts for configuration audit purposes
>   - Plugin options let you select security checks by individual plugins or plugin family
>   - When a scan policy is created or altered, it records all selected plugins
>   - When a plugin update is recieved, new plugins are automatically enabled if they fall under an enabled plugin family; they are automatically disabled in the case they fall under a disabled or mixed plugin family

> - Plugin Updates
>   - Plugins for Tenable SC can be updated from a plugin server automatically, by manual refresh, or via individual plugin downloads from the DoD Patch Repository
>   - DISA plugin servers & Patch Repositories are updated daily
>   - Contractually, plugins should be updated with IAVM data within 48 hours of the IAVM announcement

---

L13 - Queries & Reports: Demo Query within ACAS

> - Goals
>   - Define a query within ACAS
>   - Explain how filters are used within a query or report
>   - Descibe the types of data that can be extracted using a query
>   - Describe dashboard customization within ACAS

> - Query
>   - Provides the ability to save custom views of vulnerability, event, ticket, user, & alert data for repeated acess

> - Filters & queries can be used to manipulated data seen in analysis tools & save views
> - Workflow Actions (alerting, ticketing, accepting/recasting risk) can be performed from some analysis tools
> - After a filter is built & applied, the filter icon number indicates the number of filters applied to the list
> - Filters can be built using 1 or more components (types of data, ex. CVE IDs) with defined filter component criteria (specific data, ex. a specific CVE ID)
> - Create a Query to save a filter for repeated use
> - Queries can be components within other ACAS capabilities, like automating emails for alerts that meet a query, or generating a daily report with a query of active alerts
> - Analysis tools for analyzing & responding to Tenable SC data

Tool	Description
Scan Results	View a table of scan results from active & agent scans
Dashboards	View graphical summaries of scans, scan results, & system activity
Solution Analysis	Veiw recommended solutions for all vulnerabilities on your network
Vulnerability Analysis	View a table of cumulative or mitigated vulnerability data
Event Analysis	View a table of Log Correlation Engine security event data
Mobile Analysis	View a table of vulnerability data discovered by scanning an ActiveSync, Apple Profile Manager, AirWatch, Good, or MobileIron MDM server
Reports	Create custom or template-based reports to export Tenable SC data for further analysis
Assurance Report Cards	Create ARCs to develop security program objectives & assess your org's security posture

> - Dashboard ACAS
>   - Dashboard components are the product of queries of scan data from repositories
>   - It is more effective to have a single user develop & share dashboards suited to their tasks than to have each user create their own
>   - Users should be advised to configure dashboards with less frequent updates to lessen the performance impact of dashboard queries

---

L14 - Queries & Reports: Demo Reports within ACAS

> - Goals

>   - Explain what a report is within ACAS
>   - Explain when a report would be useful within ACAS
>   - Explain the different types of data you can collect in a report
>   - Explain the different report formats

> - Reports
>   - Tenable SC has custom & template reports
>   - Additional vendor-provided report templates are available on the SC feed
>   - Administrators can enable generation of reports with Cyberscope or DISA ASR/ARF/Consolidated data
>   - Supported Formats
>   - | Report Type | Description | | PDF | Portable Document Format, universally viewable | | CSV | Comma Separated Values, for import into spreadsheets or databases | | DISA ARF | Assessment Result Format DISA standard | | DISA ASR | Assessment Summary Results DISA standard | | DISA Consolidated ARF | Consolidated ARF DISA standard | | Cyberscope | Reporting standard for FISMA compliance |
>   - CyberScope
>   - Department of Homeland Security & DoJ web application designed to streamline IT security reporting for federal agencies Federal Information Security Modernization Act (FISMA) compliance.

L15 - ACAS Self-Diagnosis

> - Goals
>   - Differentiate ACAS Scanner Status errors
>   - Describe ACAS Scanner Status errors

> - Scanner Deployment Considerations
>   - Scanning a device behind a NAT or proxy can return distorted results with false negatives & positives

> - Status Errors
>   -
>
> | Error | Problem | Fix/Check |
> |---|---|---|
> | Authentication Error | Wrong auth for scanner | Confirm credentials match scanner configuration settings |
> | Certificate Mismatch | Can't confirm scanner SSL certificate | Select different authentication type in configuration; for Nessus Scanner, confirm Certificate option file |
> | Connection Error | Can't connect to scanner | Confirm scanner configuration IP/hostname; Confirm network traffic is permitted |
> | Connection Timeout (Red) | Timeout when waiting for a scanner reply | Base techs physical check/restart; Contact PMO |

> | Error | Problem | Fix/Check |
> |---|---|---|
> | Invalid Configuration | Scanner attempted to connect on port 0 | Confirm Port option uses a valid TCP port |
> | Plugins Out of Sync (Yellow) | Scanner plugins don't match SC plugins | Attempt manual plugin update; Contact PMO |
> | Protocol Error (Yellow) | HTTPS negotiation error | Base techs restart; Contact PMO |
> | Reloading Scanner | Nessus restarting | Wait for restart to complete |
> | Updating Plugins (Blue) | Plugin update in progress | If persistent, update may have been interrupted |
> | Updating Status | Status refresh in progress | Scans can continue to run in this status |
> | Upgrade Required | Nessus Scanner version outdated | Update to continue scanning |
> | User Disabled | Disabled by Tenable SC User | |