VMO NOTES - BLOCK 1

Contents

> Insights

> L1 - Vulnerability Scanning

> L2 - Orders Process

> L3 - Generalized Troubleshooting Concepts

Insights

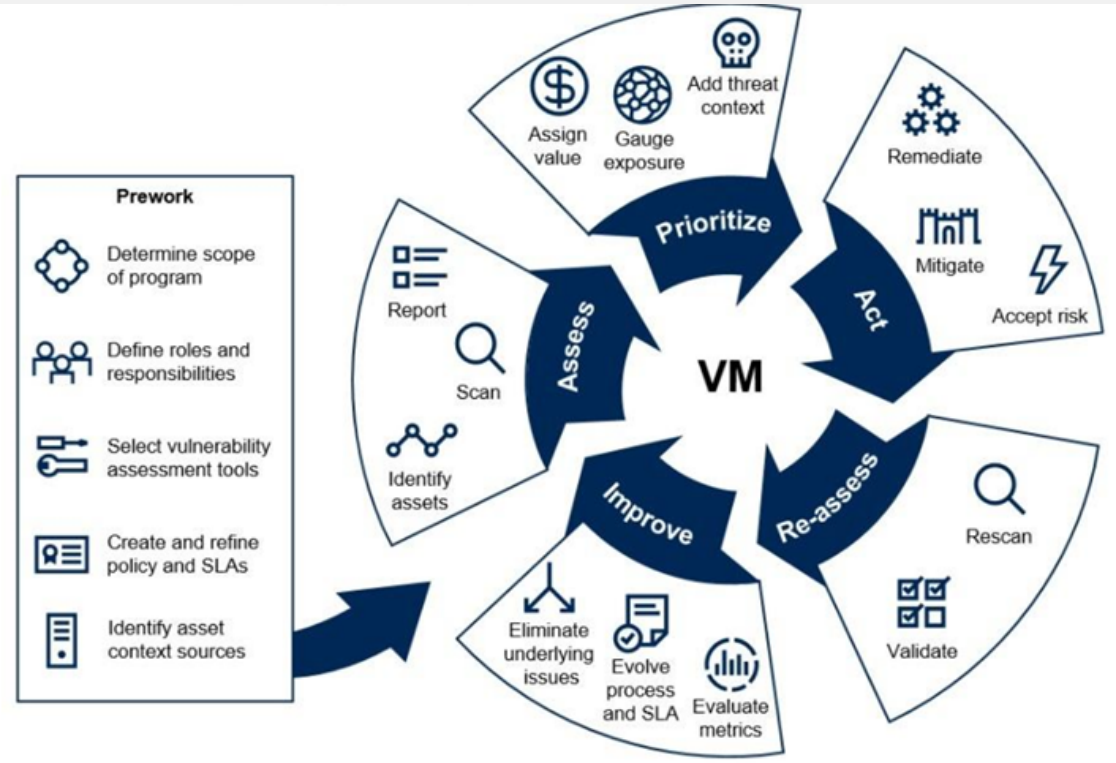
> -

L1 - Vulnerability Scanning

> - Goals
>   - Differentiate scanning for Vulnerability vs Compliance
>   - Vulnerability: Inspection of potential exploits to identify security holes
>   - Compliance: Ensures system configuration complies to security policy controls
>   - Difference: Vuln. scans inspects systems for exploits, Comp. scans check security policy compliance
>   - Differentiate Detection vs Remediation
>   - Detection: Used in the identification & detection of vulnerabilities due to misconfiguration or flawed programming within a network-based asset
>   - Remediation: Mitigates risk to the AFIN via the implementation of vulnerability countermeasures
>   - Difference: Detection finds vulnerabilities, which Remediation then attempts to fix
>   - Identify active scans
>   - Active scans prompt a system for information, such as system config or open ports, or test vulnerabilities by performing known attacks against a system. There is a potential for a high yield of information, but these scans are high-cost and can lead to system down-time, with the risk of an improperly configured scan or system resulting in an inaccurate scan. They are best used during non-working hours or by specific demand.
>   - Differentiate Credentialed vs Non-Credentialed scans
>   - Credentialed: Use of priviledged access to perform a scan on a system, with higher-privilege access yielding more in-depth information
>   - Non-Credentialed: Assessment of a system without system privileges, scanning exposed services for outward-facing vulnerabilities. These scans can slow or halt service on the target.

        - Difference: Credentialed scans use privileged information to perform a more effecient, targetted scan of a system, while Non-Credentialed scans can perform a scan without privileged access at the cost of lower yield of information and potential disruption of resources

- Vulnerability Management
    - Vulnerability Management Cycle



        - CSCS VMOs are responsible for the Assess & Re-assess steps
    - Assessment & Authorization (A&A)
        - Authorization required of scanning tools before use on AF assets.
    - 16th AF directs use scanning solutions
        - MPTO 00-33A-1109
            - Assured Compliance Assessment Solution (ACAS)
            - NOS/COSs Vulnerability Remediation threshold is 95% per enclave
            - MECM

- Vulnerability Scanning
    - Assesses known weaknesses in endpoints, networks, & applications
    - Creates an inventory of assets on the network
    - Identifies OS versions, software, ports, & accounts/user activity

- Compliance Scanning
    - Enables high-level audits to identify & report weaknesses
        - Audits enable system hardening
    - Focusses on configuration & system hardening
    - Checks adherence to compliance framework
        - Examples
            - Risk Management Framework (RMF DoD 8500)
    - Audits OS configuration files
        - OS specific; audits on unix machines use unix audit files

    - Benefits of Compliance Scanning
        - Provides assurance that compliance regulations are being satisfied
        - Identifies gaps in compliance posture
        - Reduces risks of fines and lawsuits

- Vulnerability Detection
    - Designed for two methods of testing
        - Static analysis of code (source or binary)
        - Penetration testing of live system
    - Creates a catolog of software fault patterns (CVEs)
    - Identifies signature detection - learned behaviors/user baseline
    - Bug vs Flaw - Software Development Life Cycle (SDLC)
        - Bugs
            - Buffer overflows, SQL injections
        - Flaws
            - Broken access control, logic violations
    - Categories of Vuln. Detection - Based on assets scanned
        - Network-based scans
        - Host-based scans
            - Direct, physical access scan of a client
        - Wireless scans
            - Check configuration and identify rogue APs
        - Application scans
        - Database scans

- Vulnerability Remediation
    - Workflow for fixing or neutralizing detected weaknesses
    - 4 steps
        1. Find - Detect vulnerabilities via scanning & testing
        2. Prioritize - Understanding which vulnerabilities pose the greatest risk
            - NIST Common Vulnerability Scoring System (CVSS)
                - Scores vulnerabilities based on risk with a rating & a score
                - Critical (CVSS 9-10)
                    - Create action plan within 2 weeks
                    - Remediate within 1 month
                - High (CVSS 7-8.9)
                    - Create action plan within 1 month
                    - Remediate within 3 months
                - Other
                    - May be resolved with discretion based on availability of resources
        3. Fix - Patch, block, fix vulnerabilities at scale in real time
        4. Monitor - Continuous, automatic monitoring w/ real-time alerts

- Active Scans
    - Any scan currently configured to run, be it scheduled or on demand
    - Approach includes everything an organization does to hinder system breaches

            - Requires continuous monitoring
                - Examine responses to evaluate whether a node represents a weak point
        - Actively prompts a system for information
        - IAW MPTO 00-33A-1109 on Active Scans
            - An Active Scan object will have its Max Scan Duration (hours) set to 20, without exception
            - Any old or unused scans are deleted quarterly

- Credentialed & Non-Credentialed Scans
    - Credential-based
        - Uses the admin account to do a more thorough check by finding problems that can't be seen from the network
        - Maintaining an accurate list of credentials is difficult
    - Non-credentialed
        - Gives you a quick look at vulnerabilities by only looking at network services exposed by the host, but don't provide deeper insight into OS and application vulnerabilities that don't face the network
    - IAW MPTO 00-33A-1109 on Credentialed/Non-Credentialed Scans
        - Credentialed scan using on-site Nessus Scanners or a Nessus Network Monitor (NNM) to identify all live hosts, IP addresses & ranges within an enclave, and quickly checking authenticated access w/ provided credentials
        - Non-Credentialed DMZ device scans with Critical/High severity findings will be subject to quarantine and/or removal

- VMO CSCS Tools
    - ACAS (Assured Compliance Assessment Solution)
    - ARAD (Automated Remediation Asset Discovery)
    - MECM (Microsoft Endpoint Configuration Manager)

L2 - Orders Process

- Goals
    - Differentiate order types between TASKORD, IAVA, TCNO, & MTO
        - TASKORD - USCYBERCOM operation-level direction
        - IAVA - IAVM notification of an imminent/current vulnerability threat to DoD systems that requires acknowledgement & remediation
    - Define purpose of STIGs
        - DoD implementation guides for specific products/versions to meet DoD baseline requirements
    - Define CVEs in correlation with IAVAs
        - CVE Published -> ACAS Plugin -> New Vulnerability scanning capabilities -> New potential IAVAs for those vulnerabilities
    - Discuss CVE originating authorities
        - CVE authorities are segmented into partner roles & responsibilities, defining what they contribute to the CVE Program and what's expected of them

    - Define interaction of plugins within ACAS on addressing CVEs
        - ACAS plugins are CVEs translated into an automated scanning & remediation process, expanding ACAS capabilities to cover new CVEs

- Order Types
    - Cyber Control Orders (CCO) aka CTOs
        - Directive to build or shape cyberspace in support of AF or combatant commander's mission assurance objective
        - Highest priority
    - Time Compliance Network Orders (TCNO)
        - Direct immediate patching of systems to mitigate vulnerabilities
        - For sensitive vulnerabilities that need fixed in a timely manner
        - AMAC-assigned TCNO Priorities
            - Critical
                - Widespread, imminent/ongoing threat to AFIN & operations
            - Serious
                - Widespread threat to the AFIN, supported operations is expected
            - Moderate
                - Possible threat to the AFIN
                - May be mitigated by factors like difficulty of exploitation or limited use of vulnerable systems
        - AMAC generates TCNO internally or in response to IAVAs or IAVBs
            - Information Assurance Vulnerability Management(IAVM)
                - IVAM notifications announce software or OS vulnerabilities as Alerts (IAVA) & Bulletins (IAVB)
            - Information Assurance Vulnerability Alert (IAVA)
                - Notifications generated when a vulnerability may result in an immediate, severe threat to DoD systems & information
                - Requires acknowledgement & corrective action
            - Information Assurance Vulnerability Bulletin (IAVB)
                - Addresses new vulnerabilities that don't pose an immediate risk to DoD systems, but could be escalated by non-compliance
                - Requires acknowledgement, corrective action recommended, not required unless specified
    - Maintenance Tasking Orders (MTO)
        - Routine task that enhances network security
        - Medium/low risk task
    - 616 OC & AMAC may release informational reports
        - C4 NOTAM (C2, Communications & Computers Notice to Airmen)
        - Friendly Forces Information Requirements (FFIR)
        - Commander's Critical Information Requirements (CCIR)

- Security Technical Implementation Guides (STIGs)
    - Implementation guides geared for specific products & versions, based on DoD policy & security controls
    - Contains all requirements flagged applicable for the product that have been selected on a DoD baseline

    - Security Requirements Guides (SRGs)
        - Compilations of Control Correlation identifiers (CCIs), grouped in applicable, specific areas at various level of technology specificity
        - Contain all flagged requirements from the parent level regardless of if they are selected on a DoD baseline
    - Control Correlation Identifiers (CCIs)
        - Decompositions of NIST control into a single actionable & measurable statement
        - Bridges the gap between high-level policy & low-level technical implementations
    - DISA STIGs Word Soup
        - "*DoD cybersecurity & cyberspace defense data strategy will enable semantic, technical & policy interoperability through a standards-based approach*"

- Common Vulnerabilities & Exposures (CVEs)
    - Identify, define, & catalog publicly disclosed cybersecurity vulnerabilities
    - Vulnerabilities discovered, assigned, & published by CVE Program partners worldwide
    - CVE IDs
        - Unique alphanumeric identifiers that reference specific vulnerabilities, enabling automation and allowing multiple parties to discuss & correlate information about specific vulnerabilities
        - Typically included in IAVA/Bs that include publically disclosed vulnerabilities
    - CVE Records
        - Used by technology & CS professionals to ensure they are discussing the same issue & coordinate efforts to prioritize & address vulnerabilities
        - One per vulnerability in the catalog
        - Published by partners to communicate consistent descriptions of vulnerabilities
        - CVE Record States
            - Reserved
                - Initial state of a record; ID being reserved for later use
            - Published
                - Data associated with an ID is populated to its Record
                - Must contain ID, prose description, & public reference
            - Rejected
                - Record should no longer be used, but is kept to prevent rediscovery of the same legacy data
            - CVE List
                - Catalog of all Records
    - National Vulnerability Database (NVD)
        - US government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
        - Data enables automation of vulnerability management, security measurement, & compliance
        - Includes databases of security checklist references, software flaws, misconfigurations, product names, & impact metrics
        - May have extra information on a CVE

- CVE Originating Authorities
    - CVE Program Partner Roles

            - Authorized Data Publisher (ADP)
                - Expand existing CVE Records (within scope)
            - CVE Numbering Authority (CNA)
                - Assigns IDs to vulnerabilities, creates/publishes information in the associated Record
            - CNA of Last Resort (CNA-LR)
                - Acts as CNA for vulnerabilities outside the scope of regular CNAs
            - Root
                - Recruitment, training, & governance of CNAs, CNA-LRs, & other Roots within governing Root's scope
            - Top-Level Root
                - Does not report to another root, responsible to the CVE Board
        - CVE Program Partner Responsibilities
            - Bug Bounty Programs - Assign CVE IDs to entities utilizing the Bug Bounty service
            - Hosted Services - Assign CVE IDs to vulnerabilities found in own services
            - National & Industry CERTs - Incident response & vulnerability disclosure services for nations & industries
                - May assign CVE CVE IDs
            - Vendors & Projects - Assigns CVE IDs for vulnerabilites found in their own products
            - Vulnerability Researchers
                - Independents - Assigns CVE IDs to products & projects, subject to review by the CVE Board
                - Organizations - Assigns CVE IDs to products & projects

- ACAS Plugins
    - Covers one or more CVE IDs, allowing an ACAS scan to include new vulnerabilities
    - Designed by Tenable Research
    - Contains vulnerability information, simplified remediation actions, and a testing algorithm for the security issue

---

L3 - Generalized Troubleshooting Concepts

- Goals
    - Comprehend Administrative Troubleshooting Tools
    - Comprehend Server Tool Troubleshooting
    - Comprehend Credential Troubleshooting

- Administrative Troubleshooting Tools
    - Wireshark
        - Network traffic monitoring tool
        - Compatable with many OSs & a majority of known protocols
        - Powerful filter system & clear, logical GUI
    - Microsoft Message Analyzer (MMA)
        - A Wireshark alternative

        - Can also report system call traces, allowing you to correlate local application & network activity
        - Allows you to save & reload captures, aggregate these saves, and analyze data from trace files
    - Clonezilla
        - Free & open-source disk cloning & backup/disaster recovery tool
        - 2 distributions
            - Clonezilla live
                - Single-machine backup & restore
            - Clonezilla SE
                - Server-scale deployments
        - High speed backup & cloning, quick & easy to start
        - Supports a variety of file systems
        - Great for one-time reservation operations
        - Does not distinguish software RAID, breaks files into separate devices
    - Notepad ++
        - Subjective quotes presented as Facts
            - "One of the best text editors ever."
            - "Great for working with code."
        - Customizable medium-dependent interface, custom highlighting of code syntax, colapsable blocks, & support for regular expressions in searches
        - Best feature is quick response time when working with large files
    - PuTTy
        - Lightweight, fast terminal emulator for configuring routers, switches, & servers remotely
        - Supports SSH, SCP, & rlogin protocols, multiple OSs, and many variations of the secure remote terminal
        - Provides user control over the SSH encryption key & protocol version, as well as alternate ciphers
        - Network communication layer supports IPv6
        - Comes bundled with pscp, psftp, & plink

- Server Troubleshooting
    - ping
        - Ideal command to confirm network connectivity at the IP level
        - Also gives packet loss reports
        - You can also ping your own machine to test the TCP/IP stack to find out if the issue isn't even on the network
    - ipconfig
        - Allows you to quickly & conveniently determine the machine's IP settings
        - Returns IPv4 & IPv6 addresses, subnets, & default gateways
    - netstat
        - Displays all active TCP connections on the machine, with paramaters to display aditional information, like the TCP & UDP ports being listened to
        - Useful when troubleshooting users being unable to connect to specific services
    - nslookup
        - Enables DNS troubleshooting & diagnostics

        - Available on Windows & Unix consoles
        - Returns information on the DNS server from the given address
    - nmap
        - Security auditing & network exploration tool
        - Most commonly used for security scans & penetration testing
        - Runs in the command line, but does have an official GUI, Zenmap