CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 2

Vulnerability Management

Implementing Vulnerability Management Processes

Chapter 5

Outline

- Vulnerability Management Requirements
- Common Vulnerabilities
- Frequency of Vulnerability Scans
- Tool Configuration

Vulnerability Management Requirements

- **Vulnerability management**
  - **A process used to mitigate potential, common, or known threats when protecting a network**
    - **Identify Requirements**
    - **Establish scanning frequency**
    - **Properly configure tools utilized**
    - **Execute scanning**
    - **Generate reports**
    - **Remediation**
    - **Ongoing scanning and continuous monitoring**

[1]

Vulnerability Management Requirements

- Vital requirements to identify
  - External authorities (laws, regulations)
  - Internal authorities (organizational policies, executive directives)
  - Best practices (prevent risk of liability issue)
- Key to creating the vulnerability management process is
  - Understanding the requirements
  - Applying these requirements to a specific organization or network being monitored

[1]

Regulatory Environments

- Regulatory Environment
  - An environment in which an organization operates that is controlled by laws, rules, or other regulations put in place by governments, industry groups, or other organizations
- Three regulatory standards
  - International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 Standard
  - Payment Card Industry Data Security Standard (**PCI DSS)**
  - Health Insurance Portability and Accountability Act (HIPPA)

[1]

Regulatory Environments

- **ISO/IEC 27001 Standard**
  - **Covers every aspect of developing and maintaining information security**
  - **Provision A.12.6.1 deals with vulnerability management in three stages for timely identification and mitigation of known vulnerabilities**
    1. **Desk-side audit verifies the organization has documented a process for managing vulnerabilities**
    2. **An implementation audit assures the documented process is being carried out**
    3. **Surveillance audits confirms the process continues to be followed and improved**

[1]

Regulatory Environments

- PCI DSS version 3.2
  - Applies to any organization that processes credit card payments using cards branded by
    - Visa, MasterCard, American Express, Discover, and JCB
      - These five companies worked together to create PCI DSS
  - PCI DSS is periodically updated
- PCI DSS Requirement 11, Regularly Test Security Systems and Processes
  - Section 2 goes over vulnerability scanning
    - Every quarter or when there are significant changes there should be internal and external scans
    - Internal scans should be preformed by a qualified member of the organization
    - External scans should be performed by approved scanning vendors (ASVs)
    - All personnel involved must have necessary skills
    - Any "high risk" vulnerability discovered during required scans must be resolved
      - A final scan is necessary to demonstrate that risks have been properly mitigated

[1]

Regulatory Environments

- HIPPA
  - Safeguard protected health information (PHI)
  - Section 164.308(a)(1)(i) requires that
    - Organizations to perform accurate vulnerability assessment
    - Implement security measures that reduce the risk of assessed vulnerabilities
  - There are steep civil penalties for any organization that violates HIPPA, either intentionally or unintentionally

[1]

Vulnerability Management Requirements

- Corporate Security Policy
  - A general statement created by senior management to dictate how security will be implemented within an organization
  - Management establishes the security program such as
    - Develops the program goals
    - Delegates responsibilities
    - Shows the strategic/tactical value of security
    - Outlines how the policy should be enforced
  - Issue-specific policy (functional policy)
    - Addresses security issues requiring detailed explanation
    - Presents decisions specific to the actual computers, networks, and applications

[1]

Vulnerability Management Requirements

- **Data Classification**
  - **Classification Level**
    - **An item of metadata to attach to all data to determine the protective controls applied to the information**
    - **Assigning value to data enables a company to gauge the resources to be allocated for each type of data**
  - **Typical classification levels can include**
    - **Private**
      - **Information whose improper disclosure could raise personal privacy issues**
    - **Confidential**
      - **Data that could cause grave damage to the organization**
    - **Proprietary/Sensitive**
      - **Data that could cause some damage, such as loss of competitiveness to the organization**
    - **Public**
      - **Data whose release would have no adverse effect on the organization**

[1]

Vulnerability Management Requirements

- **Data Classification**
  - Should be unique and separate from others
  - The classification process outlines how information is controlled and handled from creation to termination
  - Criteria parameters an organization may use to determine data's sensitivity
    - Level of damage that can be caused by the data's disclosure
    - Level of damage by the data's modification or corruption
    - Lost opportunity costs incurred if data is unavailable or corrupted
    - Legal, regulatory, or contractual responsibility to protect the data
    - Effect of data on security
    - Age of data

[1]

Data Classification Exercise

- **Company X is an online retailer that sells a variety of every-day goods to the public. Below is a table of some of the types of data stored on their servers. Classify each data type into these three categories: Public, Sensitive, and Confidential.**

DATA	CLASSIFICATION
Customer name	
Wholesale suppliers	
1985 Employee IDs	
Credit card information	
Customer address	
Customer orders	
Company address	

Data Classification Exercise

- **Company X is an online retailer that sells a variety of every-day goods to the public. Below is a table of some of the types of data stored on their servers. Classify each data type into these three categories: Public, Sensitive, and Confidential.**

DATA	CLASSIFICATION
Customer name	Public
Wholesale suppliers	Public
1985 Employee IDs	Sensitive
Credit card information	Confidential
Customer address	Confidential
Customer orders	Sensitive
Company address	Public

- **University X is a public, four-year university with a large population. Below are some of the different types of data hosted on their servers. Classify these different types of data into these three categories: Public, Sensitive, and Confidential**

DATA	CLASSIFICATION
Student name	
Student ID	
Employee SSN	
Student GPA	
Financial aid status	
Employee salary	
Student address	

- **University X is a public, four-year university with a large population. Below are some of the different types of data hosted on their servers. Classify these different types of data into these three categories: Public, Sensitive, and Confidential**

DATA	CLASSIFICATION
Student name	Public
Student ID	Sensitive
Employee SSN	Confidential
Student GPA	Sensitive
Financial aid status	Confidential
Employee salary	Sensitive
Student address	Confidential

Vulnerability Management Requirements

- Asset Inventory
  - Is necessary for managing vulnerabilities in an information system
  - Center for Internet Security's (CIS's) Critical Security Controls (CSC)
    - CSC #1 is the inventory of authorized and unauthorized devices
    - CSC #2 covers the software running on those devices
  - As a reminder, an asset is anything of worth to an organization, such as
    - People, partners, equipment, facilities, reputation, and information
    - The CySA+ exam focuses on hardware, software, and information assets

[1]

Vulnerability Management Requirements

- Critical Asset
  - Anything essential to performing the primary functions of an organization
  - Require a higher degree of attention through thoroughness and frequency of vulnerability scans
- Noncritical Asset
  - Not required for the accomplishment of an organization's main mission but still valuable
  - Prioritized lower than critical assets for resources

[1]

Common Vulnerabilities

- Unless a threat is specifically targeting an organization, there are common vulnerabilities that apply to most systems
  - Missing patches/updates
    - Any system that cannot reasonably update during operation should be noted and mitigated with alternative control
  - Misconfigured firewall rules
    - The ability to reach a device across a network should be restricted by appropriate, separate firewalls or means of segmentation
  - Weak passwords
    - It is not uncommon for default passwords to be forgotten or weak passwords to be chosen, even by the security team
- Eliminating the usual means of exploitation can completely deter a threat

[1]

Common Vulnerabilities

- **Servers**
  - **Common Vulnerabilities**
    - **Losing track of a server's purpose or existence on the network**
    - **Allowing unnecessary services and open ports to run**
    - **Misconfiguration of services**
      - **Ignoring "bonus" features and only configuring those deemed critical, exposes more vulnerabilities**
  - **Prevent these vulnerabilities**
    - **Remove, disable, or harden servers**
    - **Document servers' default applications and services**
    - **Ensure the full capability set of anything implemented on a network is known**
    - **Anything unneeded should be disabled completely**

[1]

Common Vulnerabilities

- Endpoints
  - Almost always user-end devices such as mobile devices
  - Most common entry point for threats to a network, with email attachments and web links as the most common vector
  - Typically lack up-to-date malware protection
  - Misconfiguration or default configuration; functionality favored over security in endpoint design
- To combat these weak points
  - Ensure there are baseline configurations that can be verified periodically by scanning tools
  - Baseline configurations should be driven by
    - The organization's risk management process
    - Appropriate regulatory requirements

[1]

Common Vulnerabilities

- **Network Infrastructure**
  - **Wireless Access Points (WAPs)**
    - **The most common vulnerability**
    - **Even with physically and electronically controlled WAPs, any rogue WAP/device can connect to a network unless prevented**
  - **Wired Equivalent Privacy (WEP) protocol**
    - **Is known to be insecure**
  - **Wi-Fi Protected Access 2 (WPA2) protocol**
    - **Is more secure than WEP**
  - **IEEE 802.1X Standard**
    - **For wireless and wired devices provides port-based Network Access Control (NAC)**
    - **Any client wishing to connect must authenticate itself**
    - **Subsequent access control is limited, and patches/requirements can be required for the endpoint**

[1]

Common Vulnerabilities

- Virtual Hosts
  - Virtualization of hosts brings unique vulnerabilities, most notably the virtual machines (VMs)
    - VMs can easily multiply, and organizations may have hundreds or thousands in many states of use or disrepair to dot their landscape
    - As requirements change, it can be easier for a VM to be copied than restarted
    - It is not uncommon to see poorly secured VMs running with no one tracking them
- Hypervisor
  - The virtualization environment
  - Responsible for ensuring that VMs are isolated from the OS of their host to prevent access to all other VM's on that host

[1]

Common Vulnerabilities

- Virtual networks
  - Commonly implemented in two ways:
    - Internally to a host using network virtualization software within a hypervisor
    - Externally using protocols such as the Layer 2 Tunneling Protocol (L2TP)
  - There are currently few known threats to virtual networks apart from those discussed with VM vulnerabilities
- Any Hypervisor Vulnerabilities
  - Could allows a user to escape a VM
    - This would provide access to the virtual networks implemented by the hypervisor
    - This would allow eavesdropping, modification of network traffic, or denial of service

[1]

Common Vulnerabilities

- **Management interface**
  - **The virtualization tools' mechanism by which a virtual device can be "plugged in with an ethernet cable or added memory"**
    - **Interfaces frequently allow remote access by administrators**
    - **Interfaces also suffer most vulnerabilities through misconfiguration**
- **Best Practice**
  - **Follow a security technical implementation guide to harden or properly configure these critical control devices**

[1]

Common Vulnerabilities

- **Mobile Devices**
  - **Common Vulnerabilities**
    - **Theft**
      - **With physical access to a device, there is little to be done to secure it, so it must be assumed that every mobile device will at some point be stolen**
    - **Passwords**
      - **Weak passwords are common vulnerabilities to all information systems, but a mobile device will often use short numeric codes**
    - **App store**
      - **Potential source of numerous malicious apps, despite Google's attempt to keep it safe. Even iOS users can be susceptible, especially if they jailbreak the device**
    - **Lack of updates**
      - **Carriers can often impose limitations on how and when a mobile device may be updated**

[1]

Common Vulnerabilities

- **Interconnected networks**
  - Example
    - Heating, Ventilation and Air Conditioning (HVAC) a vendor used by Target. This vendor had access for Targets network to monitor HVAC systems.
    - An attacker was able to use HVAC system vendors network as an entry point into Targets network
  - Ensure that your organization considers the possible vulnerabilities interconnected networks presents

[1]

Common Vulnerabilities

- Virtual private networks (VPNs)
  - Connect two or more devices that are physically part of separate networks to allow for the exchange or data as if they were part of the same LAN
- Common Vulnerability
  - Potentially allow connection to untrusted, unpatched, and possibly infected hosts in a network
    - Mitigated by requiring VPN client software only be on organizationally owned, managed devices
- Network Access Control (NAC) solution
  - Actively checks a device for patches, updates, and other required parameters before allowing network connection
  - May place noncompliant devices in "guest" network

[1]

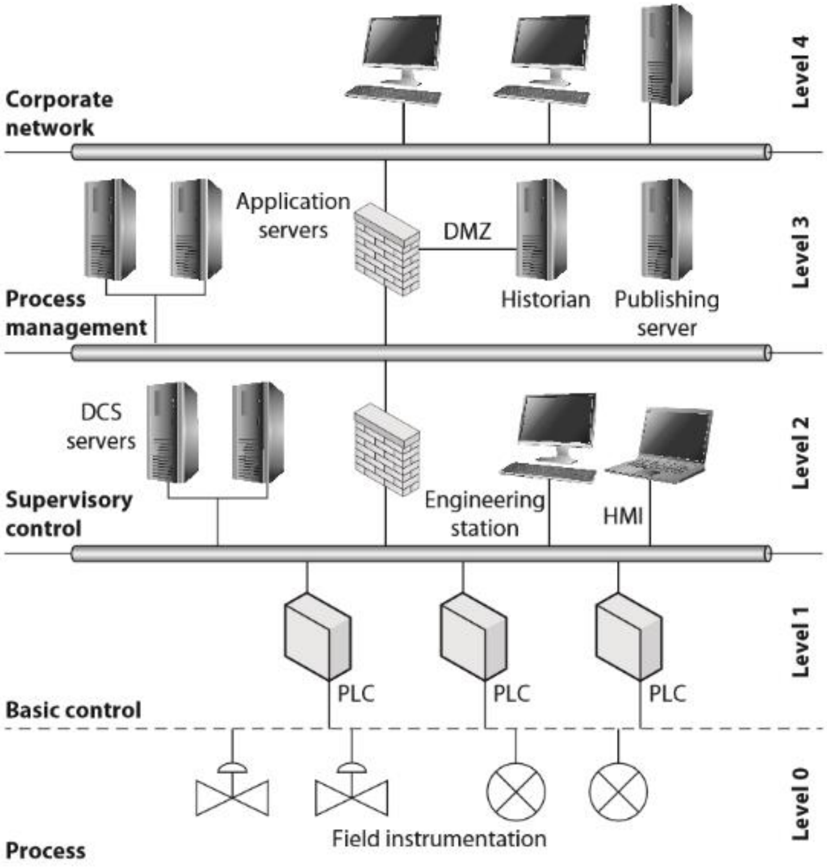
Common Vulnerabilities

- **Industrial Control Systems (ICSs)**
  - **Cyber-physical systems that allow specialized software to control the behaviors of a system**
  - **Used in automobile assembly lines, building elevators, and HVAC systems**
- **Common Vulnerabilities**
  - **ICS manufacturers set firmware passwords**
    - **Chosen passwords are often trivial and documented in plain text so all users have access**
    - **Often difficult or impossible to change**
  - **Software running an ICS is often burned into the firmware devices**
    - **E.g. The programmable logic controllers (PLC) that ran the uranium enrichment centrifuges targeted by Stuxnet**
    - **Patches and updates require a device brought offline, and updated by a qualified technician**
    - **Vendors may not provide patches or updates even for known, public vulnerabilities**

[1]

Common Vulnerabilities

- **Typical ICS Architecture**
  - **Level 0: actual physical devices like sensors and actuators**
  - **Level 1: remote terminal units or programmable logic controls**
  - **Level 2: database servers and human-machine interaction controllers and terminals**
  - **The operational technology (OT) network (levels 0-2)**
    - **Frequently bridged to the IT network (levels 3 and 4) to allow access to physical processes from anywhere on the internet**



[1]

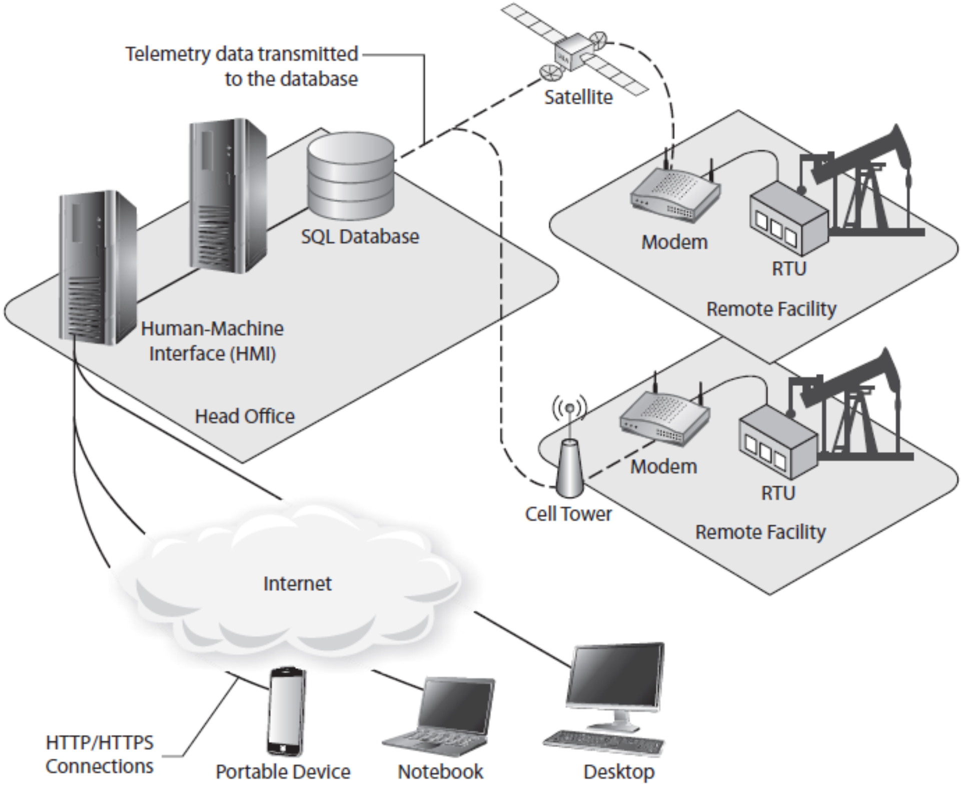
Common Vulnerabilities

- Supervisory Control and Data Acquisition (SCADA) systems
  - Specific type of ICS characterized by covering large geographic regions
  - Commonly associated with energy and utility applications
- Common vulnerabilities
  - Long distance communications relied on the obscurity of the communications protocols and radio frequencies involved
    - Wireless systems have since been hardened and modernized
  - Isolated and unattended facilities
    - Remote stations allow physical access to system components for attacks and delayed response, but camera and alarm protection has improved

[1]

Common Vulnerabilities

- **A typical SCADA system architecture**



[1]

Frequency of Vulnerability Scans

- Vulnerability scan frequency
  - How often should your organization scan for vulnerabilities
    - Depends on the organization
    - The process of vulnerability scans are important to knowing if vulnerability management is effective
  - Determining the frequency and scopes of various scans based on previously established requirements, allows the organization better control of its security posture

[1]

Frequency of Vulnerability Scans

- Risk Appetite
  - The amount of risk an organization's executives are willing to assume
    - Risk is a deliberate process that quantifies the chance of a threat being realized and the net effect it may have on an organization
- Risk cannot be driven down to zero
  - A threat always has the possibility of causing loss to an organization
  - Financial or opportunity cost of mitigating a threat may approach a point of diminishing returns
  - How expensive is too expensive is dictated by an organization's risk appetite

[1]

Frequency of Vulnerability Scans

- Regulatory Requirements
  - After identifying all applicable regulations of an organization's regulatory environment, the frequencies of various scans will be given
- Regulatory requirement examples
  - Requirement 11.2 of the PCI DSS requires vulnerability scans quarterly as well as after any significant change in the network
  - HIPPA imposes no frequency requirements

[1]

Frequency of Vulnerability Scans

- Technical Constraints
  - Vulnerability assessments require limited resources of personnel, time, bandwidth, hardware, and software
  - Top technical constraints: qualified personnel and technical capacity
    - Cycles of CPU time, bytes of primary/secondary memory, bits per second of network connectivity
    - Quantify the capacity required for scans
  - Carefully balance the mission and security requirements of an organization

[1]

Frequency of Vulnerability Scans

- **Workflow**
  - Workflow of security and network operations
    - Qualified personnel must review, analyze, and determine action after any vulnerability scan
    - This process is best incorporated into workflow of security and/or network operations centers personnel
  - Standardized and enforced repeatable vulnerability management processes enables effective risk management across a system
    - For example: A security operations center worker understands every Tuesday morning is the day to review the previous night's vulnerability scans, routine is established, and the organization benefits from consistent vulnerability scans and well document outcomes

[1]

Tool Configuration

- **Tool configuration**
  - Today's tools typically have more power and options than will be used
  - An information system may also impose limitations or requirements on which features of the tool can or should be applied
- **Main criteria when configuring scanning tools are**
  - Sensitivity levels
  - Vulnerability feed
  - Scope
  - Credentialed vs. Noncredentialled
  - Server based vs. Agent based
  - Types of Data
  - Tool Updates and Plug-ins
  - Security Content Automation Protocol (SCAP)
  - Permission and Access

[1]

Tool Configuration

- Sensitivity Levels
  - Tools must be configured to perform their job and appropriately protect assets
  - Required protections must always remain in place
    - If scanning an organization covered by HIPPA, no part of assessment can compromise protected health information
  - Scans must also protect the system on which information resides
    - E.g. If an organization processes thousands of dollars each second and scanning slows that down by an order of magnitude, the effect could be a significant loss of revenue
    - Understanding the sensitivity and nature of an asset helps with tool configuration to minimize risk, such as scheduling the scan during windows of time with no trading

[1]

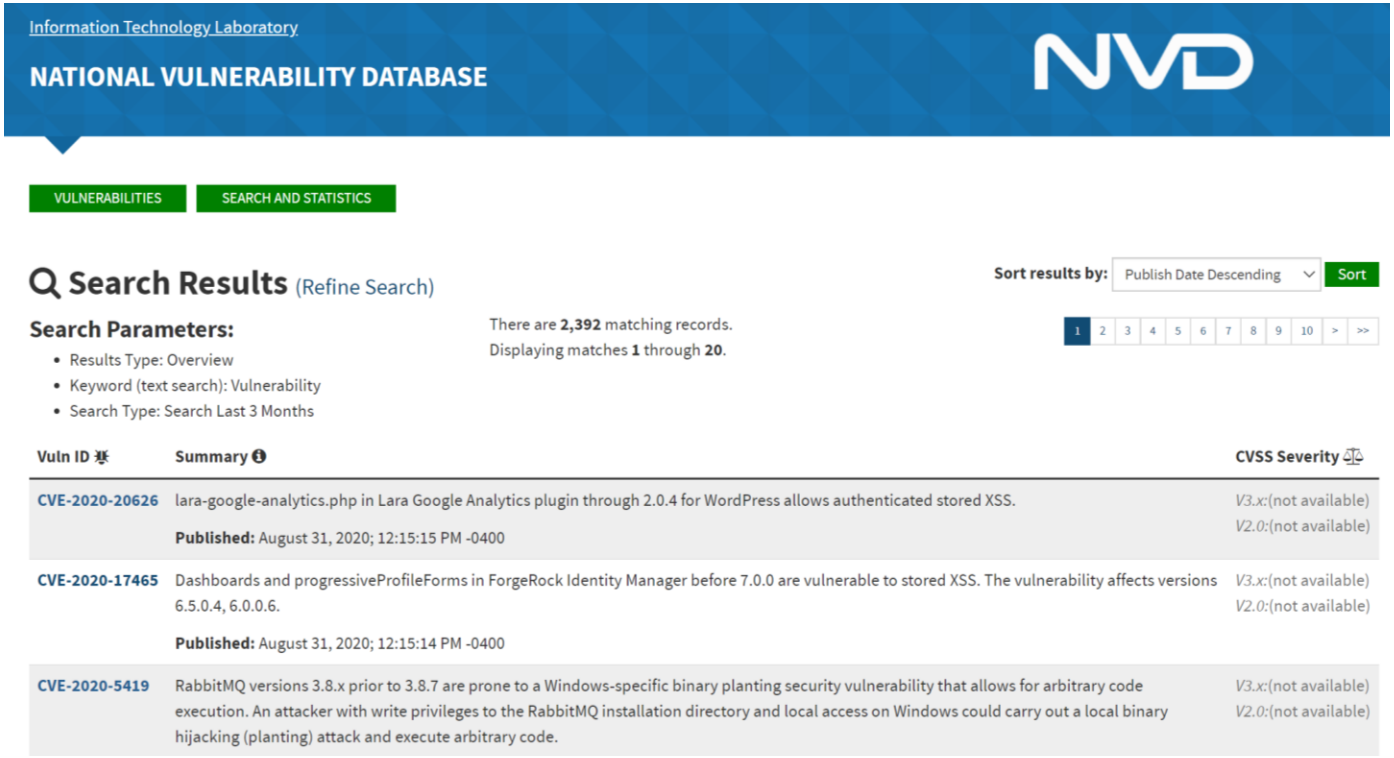
Tool Configuration

- Vulnerability Feed
  - Knowledge of vulnerabilities most typically comes from commercial or community feeds, each with update cycles ranging from hours to weeks
  - An ideal vulnerability feed is one that is about as frequent as the scanning cycle implemented
- Subscribe to vulnerability alerts other than the provider
  - National Vulnerability Database (NVD) provides two Rich Site Summary (RSS) feeds NVD
    - Will alert any new vulnerability reported, providing the bleeding edge of notifications
    - Only alerts reports that have been analyzed, providing specific products affected and additional analysis

[1]

Tool Configuration

- **Below is an example of a general NVD vulnerability search**


Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
SEARCH AND STATISTICS
Sort results by: Publish Date Descending
Sort
1 2 3 4 5 6 7 8 9 10 > >>

Search Results (Refine Search)

Search Parameters:

- Results Type: Overview
- Keyword (text search): Vulnerability
- Search Type: Search Last 3 Months

There are **2,392** matching records.
Displaying matches **1** through **20**.

Vuln ID	Summary	CVSS Severity
CVE-2020-20626	lara-google-analytics.php in Lara Google Analytics plugin through 2.0.4 for WordPress allows authenticated stored XSS. **Published:** August 31, 2020; 12:15:15 PM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2020-17465	Dashboards and progressiveProfileForms in ForgeRock Identity Manager before 7.0.0 are vulnerable to stored XSS. The vulnerability affects versions 6.5.0.4, 6.0.0.6. **Published:** August 31, 2020; 12:15:14 PM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2020-5419	RabbitMQ versions 3.8.x prior to 3.8.7 are prone to a Windows-specific binary planting security vulnerability that allows for arbitrary code execution. An attacker with write privileges to the RabbitMQ installation directory and local access on Windows could carry out a local binary hijacking (planting) attack and execute arbitrary code.	*V3.x:*(not available) *V2.0:*(not available)

[2]

Tool Configuration

- Scope
  - The set of devices that will be assessed constitutes the scope of the vulnerability scan
  - A carefully defined scope is necessary for both scheduled and special scans to appropriately configure tools
  - Best Practice
    - Series of scans with each scan has a different scope and parameters
      - Relieves the load from critical nodes or the entire system that may occur during a simpler, whole system scan
      - Tools must know which nodes to test and which to leave alone in both global and targeted scans

[1]

Tool Configuration

- Credentialed vs. Noncredentialled
  - Noncredentialled vulnerability scan
    - Evaluates the system from the perspective of an outsider
    - A black-box test in which the scanning tool does not get any special information or access into the target
    - Tends to be a quicker, realistic approach that can be more secure, but may not get full coverage of the target
  - Credentialed vulnerability scan
    - Tool is provided with credentials to log in remotely and examine the inside and outside
    - Can reduce the amount of network traffic and will always be more thorough

[1]

Tool Configuration

- **Server Based vs. Agent Based**
  - **Server-based scanner**
    - **Consolidates all data and processes on one or a small number of scanning hosts, depending on a fair amount of network bandwidth**
    - **Has fewer components and can detect and scan devices connected to the network**
      - **Makes maintenance tasks easier and more reliable**
  - **Agent-based scanner**
    - **Agents run on each protected host and report their results back to central scanner, requiring less bandwidth**
    - **Best for scanning mobile devices**
      - **Because agents run continuously on each host, mobile devices can still be scanned even when not connected to the corporate network**

[1]

Tool Configuration

- Types of Data
  - Consider information that should be included in a scanning tool's report
    - This information determines the data a scan must collect, in turn affecting the tool configuration
    - Each report is intended for a specific audience
- Tool Updates and Plug-Ins
  - Vulnerability scanning tools
    - Work by testing systems against lists of known vulnerabilities, which are frequently being discovered
    - If a list is not up-to-date, any tool being used will eventually fail to detect vulnerabilities known by others, especially adversaries
  - It is critical to keep tools updated

[1]

Tool Configuration

- Security Content Automation Protocol (SCAP)
  - A protocol that uses specific standards for the assessment and reporting of vulnerabilities in the information systems of an organization
    - Currently in version 1.2, incorporating a dozen different components that standardized everything from an asset reporting format to common vulnerabilities and exposures to the common vulnerability scoring system
  - Developed by National Institute of Standards and Technologies (NIST) and industry partners
  - Leverages baselines developed by NIST to define minimum standards for vulnerability management
    - For example: to ensure a system's Windows 10 workstations are complying with the requirements of the Federal Information Security Act (FISMA), the appropriate SCAP module that captures these requirements would be used. The module would then be provided to a certified SCAP scanner, which would report this compliance in a standard language
  - SCAP is a framework that has standardized full automation of the vulnerability management process

[1]

Tool Configuration

- Permissions and Access for Scanning Tools
  - Must have the correct permissions depending on
    - Network Access
      - Before scanning must examine the network to
        - Determine what ACLs need to be modified
        - Modify the IDS and IPS to not alert or stop the scan
        - Modify the HBSSs to prevent it from mitigating the effect of the scan
    - Reporting Interface
      - Ensure the right permissions are set for the reports generated by the vulnerability scanning tool
  - Best Practice
    - Have a dedicated account for the scanning tool
    - Do not run the scanning tool as root unless required
    - Only authorized users should be able to review the report [1]

Quiz

Chapter 5

Question #1

- **The popular framework that aims to standardize automated vulnerability assessment, management, and compliance level is known as what?**
  A. CVSS
  B. SCAP
  C. CVE
  D. PCAP

[1]

Answer #1

- **B**
  - **Security Content Automation Protocol (SCAP) is a method of using open standards, called components, to identify software flaws and configuration issues**

[1]

Question #2

- **An information system that might require restricted access to, or special handling of, certain data as defined by a governing body is referred to as a what?**
  - A. Compensating control
  - B. International Organization for Standardization (ISO)
  - C. Regulatory Environment
  - D. Production system

[1]

Answer #2

- C
  - A regulatory environment is the environment an organization exists/operates in controlled by laws, rules, or regulations put in place by a formal body.

[1]

Question #3

- **Which of the following are parameters that organizations should not use to determine the classification of data?**
  - A. The level of damage that could be caused if the data were disclosed
  - B. Legal, regulatory, or contractual responsibility to protect the data
  - C. The age of the data
  - D. The types of controls that have been assigned to safeguard it

[1]

Answer #3

- D
  - Common criteria parameters used to determine the sensitivity of data include level of damage caused if data were disclosed; legal, regulatory, or contractual responsibility to protect the data; and the age of the data
  - Classification should determine the controls used to protect data, not the other way around

[1]

Question #4

- **What is the term for the amount of risk an organization is willing to accept in pursuit of its business goals?**
  A. **Risk appetite**
  B. **Innovation threshold**
  C. **Risk hunger**
  D. **Risk ceiling**

[1]

Answer #4

- A
  - Risk appetite is a core consideration when determining your organization's risk management policy and guidance
  - Risk appetite will vary based on criticality of production systems, impact to public safety, and financial concerns

[1]

Question #5

- **Insufficient storage, computing, or bandwidth required to remediate a vulnerability is considered what kind of constraint?**
  1. **Organizational**
  2. **Knowledge**
  3. **Technical**
  4. **Risk**

[1]

Answer #5

- C
  - Any limitation on the ability to perform a task on a system due to limitations of technology is a technical constraint and must have acceptable compensating controls in place

[1]

Question #6

- **Early systems of which type used security through obscurity, or the flawed reliance on unfamiliar communications protocols as a security practice?**
  A. PCI DSS
  B. SCADA
  C. SOC
  D. PHI

[1]

Answer #6

- B
  - Early Supervisory Control and Data Acquisition (SCADA) systems had the common vulnerability of relying heavily on obscure communications protocols for security
  - This practice provides only the illusion of security and may place the organization in worse danger

[1]

Question #7

- **What is the reasoning that patching and updating occur so infrequently with ICS and SCADA devices?**
  A. These devices control critical and costly systems that require constant uptime
  B. These devices are not connected to networks, so they do not need to be updated
  C. These devices do not use common operating systems, so they cannot be updated
  D. These devices control systems, such as HVAC, that do not need security updates

[1]

Answer #7

- A
  - The cost involved and potential negative effects of interrupting business and industrial processes often dissuade these device managers from updateding and patching these systems

[1]

Question #8

- **All of the following are important considerations when deciding the frequency of vulnerability scans except which?**
  - A. Security engineers' willingness to assume risk
  - B. Senior executives' willingness to assume risk
  - C. HIPPA compliance
  - D. Tool impact on business processes

[1]

Answer #8

- A
  - An organization's risk appetite, or amount of risk it is willing to take, is a legitimate consideration to determine frequency of scans. However, only executive leadership can make that determination

[1]

Scenario for Questions 9-12

- A local hospital has reached out to your security consulting company because it is worried about recent reports of ransomware on hospital networks across the country. The hospital wants to get a sense of what weaknesses exist on the network and get your guidance on the best security practices for its environment. The hospital has asked you to assist with its vulnerability management policy and provided you with some information about its network. The hospital provides laptops to its staff and each device can be configured using a standard baseline. However, the hospital is not able to provide a smartphone to everyone and allows user-owned devices to connect to the network. Additionally, its staff is very mobile and relies on VPN to reach back to the hospital network.

[1]

Question #9

- **When reviewing the VPN logs, you confirm that about half of the devices that connect are user-owned devices. You suggest which of the following changes to policy?**
  - A. None, the use of IPSec in VPNs provies strong encryption that prevents the spread of malware
  - B. Ask all staff members to upgrade the web browser on their mobile devices
  - C. Prohibit all UDP traffic on personal devices
  - D. Prohibit noncompany laptops and mobile devices from connecting to the VPN

[1]

Answer #9

- **D**
  - **Allowing potentially untrusted, unpatched and perhaps even infected hosts onto a network via a VPN is not ideal**
  - **Best practices dictate that VPN client software be installed only on organizationally owned and managed devices**

[1]

Question #10

- **What kind of vulnerability scanner architecture do you recommend be used in this environment?**
  A. Zero agent
  B. Server based
  C. Agent based
  D. Network based

[1]

Answer #10

- C
  - Because every laptop has the same software baseline, an agent-based vulnerability scanner is a sensible choice.
  - Agent-based scanners have agents that run on each protected host and report their results back to the central scanner
  - The agents can also scan continously on each host, even when not connected to the hospital network

[1]

Question #11

- **Which vulnerabilities would you expect to find mostly on the hospital's laptops?**
    A. **Misconfigurations in IEEE 802.1X**
    B. **Fixed passwords store in plaintext in the PLC's**
    C. **Lack of VPN clients**
    D. **Outdated malware signatures**

[1]

Answer #11

- D
  - Malware signatures are notoriously problematic on endpoints, particularly when they are portable and not carefully managed
  - Although VPN client problems might be an issue, they would not be as significant a vulnerability
  - IEEE 802.1X problems would be localized at the network access points and not on the endpoints
  - PLC's are found in ICS and SCADA systems and not normally in laptops

[1]

Question #12

- **Which of the followings is not a reason you might prohibit user-owned devices from the network?**
  A. **The regulatory environment might explicitly prohibit these kinds of devices**
  B. **Concerns about staff recruiting and retention**
  C. **There is no way to enforce who can have access to the device**
  D. **The organization has no control over what else is installed on the personal device**

[1]

Answer #12

- B
  - Staff recruiting and retention are frequently quoted by business leaders as reasons to allow personal mobile devices on their corporate networks
  - Therefore, staffing concerns would typically not be a good rationale for prohibiting these devices

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. National Vulnerability Database, 2020.