VULNERA

DATA SHEET

Common Vulnerability Management Terminology

Agent-Based Scan
A software package deployed to each device that needs to be tested. Once installed, the agent collects data that indicates whether the device may have security issues. The agent passes this data back to collection servers and information gathered across the entire infrastructure is then consolidated into a 'single pane of glass' interface for analysis.

Agentless Scan
Agentless scanning does not require agents to be installed on each device and instead reaches out from the server to the assets. While the data collected is similar to an agent-based approach, it eliminates installing and managing additional software on all devices

Asset
Any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.

Blue Team Assessment
A blue team that consists of incident responders who work within the security unit to identify, assess and respond to the intrusion and to provide guidance to the security team on where to make improvements to stop sophisticated types of cyberattacks and threats.

Breach
A disclosure of confidential information.

Cloud
Servers that are accessible over the internet that provide availability of resources such as data storage and processing.

Compliance
Adherence to a particular compliance framework such as NIST, ISO, or CIS. Compliance is a typical reason for organizations to conduct vulnerability assessments.

CVSS
The Common Vulnerability Scoring System is a cyber industry standard vulnerability scoring method.

Exploit
The method (typically a script or tool) used in an attack to take advantage of a flow (vulnerability).

Exfiltrate
Where an attacker transfers data from an application or network to their own system post-exploitation.

External Scan
Vulnerability scan conducted from outside the organization's perimeter firewall.

Hostname
A name or label that is used to identify a device connected to a network.

Infrastructure
Often used to refer to the IT network within an organization.

Internal Scan
Vulnerability scan conducted from within the organization's perimeter firewall.

Inventory (Asset) Management
You can't patch what you don't know you have. Tracking your inventory of assets is crucial for verifying that you have addressed all vulnerabilities in your network.

IP Address
A unique address the identifies a device on a network.

Incident
A breach of a security policy that impacts confidentiality, integrity or availability.

Incident Response
Actions taken in response to an incident.

Managed Security Services Provider (MSSP)
IT service businesses that specialize in providing security-as-a-services offerings for their customers.

Managed Services Provider (MSP)
Delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data center (hosting), or in a third-party data center.

Patching
the installation of a patch or fix from a vendor that has a bug/vulnerability

Patch Management
How will you deliver security patches to your network assets? When will patches be applied? Will you have to disable some or all of your network to apply fixes to your major vulnerabilities?

Penetration Test
An attempt to evaluate the security of an IT infrastructure by safely trying to check for exploitable vulnerabilities. Also known as a pentest.

Ransomware
Ransomware is a type of malicious software that disrupts computers, servers, and other devices by installing itself and then blocking access, deleting, or otherwise compromising legitimate data and applications. It typically demands a payment, or ransom, to "unlock" the computer and grant full access to the device and any related data and applications.

Remediation
While patching is applying a fix or patch, remediation is a little more holistic in the sense that it may be applying some kind of compensating control e.g. network segregation.

Remediation Validation
Allows organizations to assess the success of remediation efforts and whether site objectives have been met. It also enables systemic documentation of conclusions, decisions, and rationale for the remediation plan.

Red Team Assessment
A goal-based adversarial activity that requires a big-picture, holistic view of the organization from the perspective of an adversary. The purpose is to demonstrate how real-world attackers can combine seemingly unrelated exploits to achieve their goal.

Retest
Manual point-in-time validation of vulnerabilities removed. Often performed as an add-on to a one-time vulnerability assessment or penetration test.

Risk
The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a threat would exploit a vulnerability, with the associated consequences.

Risk Assessment
The identification, analysis and evaluation of risk. It takes into consideration the impact and likelihood of a threat exploiting a vulnerability.

Scanning
The act of running an automated tool to identify security vulnerabilities.

Security Assessment
An assessment that takes an extensive look at the organization's network and provides risk reduction techniques for each vulnerability found. A vulnerability assessment is a component of a security assessment.

Service
An open network port (TCP or UDP) that represents a process (database, web server, file server, etc). Services are enumerated on IP addresses and scanned during assessments to uncover vulnerabilities.

Threats
A combination of tools and methods involved in a cyberattack. These threats are not inherent to the network. Instead, they leverage vulnerabilities on the network.

Vulnerabilities
A potential weakness in a security architecture that opens an organization or individual to cyberattacks.

Vulnerability Assessment
Part of the vulnerability management process. An organization's network is assessed to identify misconfigurations, missing patches, and active attacks that put information at risk.

Vulnerability Management
The practice of proactively finding and fixing potential weaknesses in an organization's network security. Involves identifying, classifying, mitigating and fixing known vulnerabilities within a system.

Vulnerability Management Program
An ongoing process for detecting and addressing vulnerabilities and gaps in cybersecurity protection.

Vulnerability Remediation
Corrective action to address a weakness or flaw in a product, system's design or implementation that could be exploited. Examples of remediation efforts could include installation of a software patch, adjustment of a configuration setting or removal of the affected software.

Vulnerability Scanning
How will you check for vulnerabilities? It's important to have a comprehensive suite of vulnerability scanning tools for detecting weaknesses and logging them for future fixes. Checking external network assets (such as vendor networks, cloud-based applications, and external servers) with vulnerability scanners is also crucial for modern vulnerability testing.

Zero-Day
A newly discovered vulnerability or flaw which is identified before a patch has been released to mitigate the vulnerability or flaw. Once a patch is available the vulnerability or flaw is no longer called a zero-day.

+1 626.515.5523
www.vulnera.com | info@vulnera.com

VULNERA.