CYBERSECURITY

Vulnerability Management Guide

By Shourooq Shaath

WHAT IS VULNERABILITY MANAGEMENT?

Vulnerability management is a term that describes the various processes, tools, and strategies of identifying, evaluating, treating, and reporting on security vulnerabilities and misconfigurations within an organization's software and systems. In other words, it allows you to monitor your company's digital environment to identify potential risks, for an up-to-the-minute picture of your current security status.

WHAT DOES A VULNERABILITY MANAGEMENT SOFTWARE DO?

Vulnerability management solution helps to monitor a system's security in real-time, detects breaches, and takes necessary actions to remediate the threat before it has the opportunity to cause harm to the system or application.

There are three phases to **Vulnerability Management**, they are as follow:

1. **Phase 1 -> Vulnerability Assessment**:
   A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

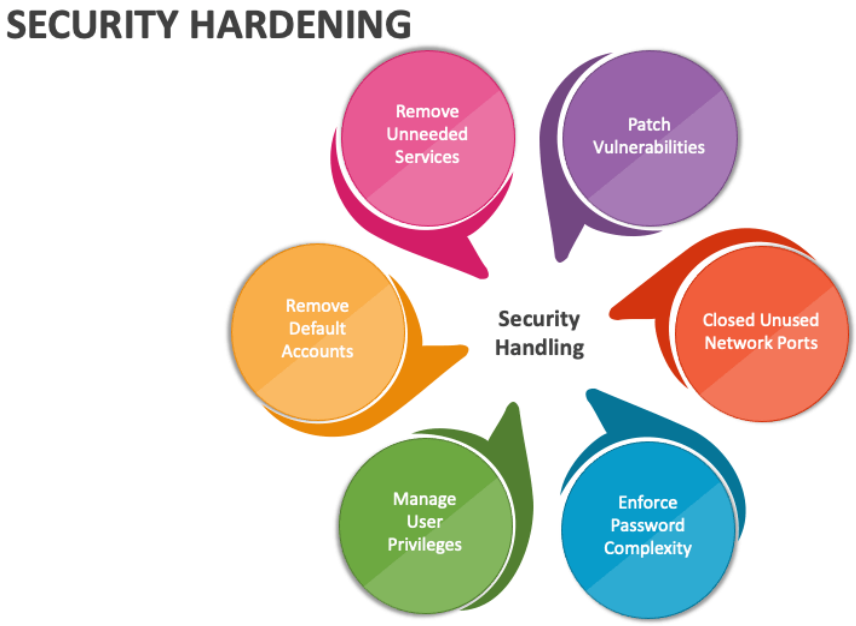
   Vulnerability assessment tools are designed to automatically scan for new and existing threats that can target your application. Types of tools include:

   Web application scanners that test for and simulate known attack patterns.
   Protocol scanners that search for vulnerable protocols, ports, and network services.
   Network scanners that help visualize networks and discover warning signals like stray IP addresses, spoofed packets, and suspicious packet generation from a single IP address.
   It is a best practice to schedule regular, automated scans of all critical IT systems. The results of these scans should feed into the organization's ongoing vulnerability assessment process.

2. **Phase 2 -> Vulnerability Remediation**:
   The vulnerability remediation process is a workflow that fixes or neutralizes detected weaknesses. It includes 4 steps: finding vulnerabilities through scanning and testing, prioritizing, fixing, and monitoring vulnerabilities. Here are the four steps to vulnerability remediation process.

3. **Phase 3 -> Vulnerability Hardening**: is the process of configuration and disabling features
   Is a process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services and disabling unnecessary features. This will reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vector s and condensing the system's attack surface.

   Things to consider with security hardening are …



There are several types of system hardening activities, including:

- Application hardening
- Operating system hardening
- Server hardening
- Endpoint hardening
- Database hardening
- Network hardening

VULNERABILITY MANAGEMENT SOLUTIONS

To create an effective vulnerability-management process, a top solution will include automated functionalities, *for* …

- *Scanning* – This includes network scanning, firewall, application system ..etc.
- *Finding* – This includes analyzing the result of your scan
- *Checking* – This includes assessing vulnerabilities to determining how threat actors can use them
- *Prioritize based on risk and impact* – This determine which bugs are highest risk, and thus should be placed at a higher priority for remediation or mitigation.
- *Patching* – This involves patching identified vulnerabilities, effectively eliminating them as potential threat vectors.
- *Measuring* – This involves assessing the effectiveness of the vulnerability-management solution and making changes to the process where necessary.

TOP VULNERABILITY MANAGEMENT SOFTWARE AND TOOLS

Tools	Description
A. Rapid7 Insight VM 9(Nexpose)	Is an open-source vulnerability scanning solution. It's able to automatically scan and assess physical, cloud and virtual infrastructures
B. Burp Suite	Is a web vulnerability scanner used in a great many organizations
C. Nmap	Is a port scanner that also aids pen testing by flagging the best areas to target in an attack.
D. Tenable Nessus	Is a widely used, open-source vulnerability assessment tool. It is probably best for experienced security teams, as its interface can be a little tricky to master at first.
E. Snyk	Is developer vulnerability scanning and security platforms tool that automatically

	fix vulnerabilities in your code, open-source dependencies, containers, and infrastructure as code —Snyk is industry leading security intelligence.

References

https://www.servicenow.com/products/security-operations/what-is-vulnerability-management.html

https://www.softwaretestinghelp.com/vulnerability-management-software/

https://www.imperva.com/learn/application-security/vulnerability-assessment/#:~:text=A%20vulnerability%20assessment%20is%20a,mitigation%2C%20if%20and%20whenever%20needed.

https://www.beyondtrust.com/resources/glossary/systems-hardening

https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#nmap