Public

Office of the Chief Information Officer

OCIO Scanning and Penetration Test Guidelines for Clients

January 2022 v0.4

Purpose

This document is to provide clients with a guideline to prepare for security scans or penetration tests to ensure risks to government assets are minimized. Also, appropriate change management is followed, as required, per scan.

Table of Contents

Vulnerability Scanning

Overview

Vulnerability scanning, when properly configured, is a security technique that will identify security weaknesses and vulnerabilities within a computer network, device, or application. Vulnerability scanning can be used by individuals to identify vulnerabilities in systems in order to secure them or to exploit them. Clients may request vulnerability scanning through OCIO Information Security Branch (ISB) or through third party vendors.

Types of Scans

Port Scan

Port Scanning is the name for the technique used to identify open ports and services available on a network host. It does not identify vulnerabilities in applications beyond the port or service being available.

Vulnerability Scan

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses which could be exploited by an attacker.

- A vulnerability scan does not validate whether identified vulnerabilities can be exploited.
- Additional analysis is required to determine if the identified vulnerability presents an unacceptable risk to the system.

There are two common types of vulnerability scans:

- Network vulnerability scanning
- Web application vulnerability scanning

Network Vulnerability Scan

Network vulnerability scanning is a rapid, coarse-grain vulnerability scan that interrogates the identified open ports to identify whether there is a response, attempts to identify the application and the version that responds, and identifies vulnerabilities known to affect that version.

Web Application Scan

Web application scanning is a type of vulnerability scan which is not concerned with underlying infrastructure but is rather focused on the application being delivered.

There are two types of web application scans:

- Dynamic analysis
- Static analysis

Dynamic Analysis

A web application security scanner is a program which communicates with a web application through the web front-end to identify potential security vulnerabilities and architectural weaknesses in the web application. The act of performing a web application scan against the running application is also commonly referred to as a dynamic assessment.

Static Analysis

- An application scan can also occur against the static source code of an application (i.e., not the running application itself). This is also commonly referred to as a static code assessment.

Additional types of vulnerability scans include database scanning.

Penetration Tests

Penetration tests, also known as pen testing or ethical hacking, is the practice of gaining access to a location, computer system, network, and web applications by exploiting security vulnerabilities.
A penetration test is an authorized attack on a computer system or network to exploit vulnerabilities to gain access to system information.

There are three common types of penetration tests:

- Zero-knowledge testing, also known as Behavioral Testing, is a software testing method in which the internal structure/design/implementation of the item being tested is not known to the tester.
- Full-knowledge testing also known as Clear Box Testing, Open Box Testing, Glass Box Testing, Transparent Box Testing, Code-Based Testing or Structural Testing is a software testing method in which the internal structure/design/implementation of the item being tested is known to the tester. The tester chooses inputs to exercise paths through the code and determines the appropriate outputs.
- Partial-knowledge testing is a software testing method which is a combination of the Zero-knowledge testing method and the Partial-knowledge testing method. In Zero-knowledge testing, the internal structure of the item being tested is unknown to the tester and in Full-knowledge Testing the internal structure is known. In Partial-knowledge Testing, the internal structure is partially known.

Vulnerability Risk Rating

The Common Vulnerability Scoring System (CVSS) provides an international standard framework for assessing the impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.[I] When available, VRM will provide a Common Vulnerabilities and Exposures (CVE) as the authoritative reference for the notification process. CVE is a database of reported vulnerabilities that are uniquely identified; contain a technical description; mitigation techniques; and links to vendor patches.

Risk Rating	Examples *(*If criteria is met apply patches as required)*	CVSS Score	ISB Patching Recommendation
CRITICAL	Vulnerability allows remote code execution Critical business system/information affected Exploits exist and are in use System is connected to the Internet without having mitigating controls in place	**9.8 - 10**	**Within 72 Hours** **Formal acceptance of risk is required for all instances in which patching cannot be completed during the recommended time frame*
HIGH	Vulnerability allows remote code execution Essential business system information affected Proof of Concepts exist and are in use The system is in a protected enclave with strong access controls	**7.0 – 9.7** *****PCI-DSS Systems with a score of 6.0 or higher follow this standard*****	**Within 14 Calendar Days** **Formal acceptance of risk is required for all instances in which patching cannot be completed during the recommended time frame*
MEDIUM	Vulnerability allows an attacker with access to impersonate a legitimate user System is exposed to unauthenticated users System requires two-factor authentication and administrator level remote login is disallowed	**4.0 – 6.9**	At the next major update or within 3 months whichever is sooner
LOW	A vulnerability requires authenticated users to perform malicious actions, such as SQL injection Affected system contains non-sensitive, publicly-available information Mitigating controls exist that make exploitation unlikely or very difficult	**0.1-3.9**	At the next major update or within 12 months whichever is sooner

The OCIO Patch Guidelines provide recommended timelines for vulnerability mitigation. The timelines above are the maximum allowable time from notification to patching. Critical vulnerabilities ideally would be patched immediately; however, the guideline time recommendation considers the need for testing prior to applying vendor patches and mitigation techniques.

Scanning Providers

Scanning Providers and Capabilities

	Security Operations	Ministry	3rd Party Vendor
Scan Types			
Corporate Port Scanning			
External Corporate-wide Vulnerability Scans			
Internal Corporate-wide Vulnerability Scans			
Web Application Scans			
Database Scan			
Penetration Test			

BC Government Change Management Procedures for Scanning

Scanning may cause unintended consequences, overwhelm firewalls or appearing as a denial-of-service attack. Additionally, threat actors are scanning the government network 24/7. These potentially adverse effects demand that **ALL** scans of the government network be preceded by an approved Request for Change (RFC) or a Request for Special Processing (RSP) prior to the commencement of any scanning activity.

OCIO Information Security Branch Scanning Services

ISB Vulnerability and Risk Management Unit and Security Operations Unit provide some vulnerability scanning capability across Government:

- Routine scans: Port scanning, as well as external and internal vulnerability scanning of the government network is a routine process performed by OCIO ISB that proactively assesses the government's risk.
- Non-routine scans: The Web Application Vulnerability Assessment (WAVA) service assists clients in identifying security weaknesses and vulnerabilities pertaining to Web Applications through a scan of the application and a report produced based on the scan results.

Routine Scans

ISB Security Operations Unit (Sec Ops) routinely port scans and vulnerability scans across Government networks, with an emphasis on being non-disruptive. There is a standing RFC which authorizes Sec Ops to conduct port scanning and internal and external scanning on a continuous basis. Scan information is parsed by VRM, who notify owners of vulnerabilities found.

VRM notify with timelines to mitigate based on the OCIO Patch Guidelines. VRM utilizes CVSS in applying metrics to the vulnerability.

Once VRM notifications are sent, the business owner owns the risk until patching or other mitigation is complete.

Non-Routine Scans

The WAVA service assists clients in identifying security weaknesses and vulnerabilities pertaining to Web Applications through a scan of the application and a report produced based on the scan results.

The WAVA service consists of specialized web application scanning tools. Detailed results are provided to assist developers in understanding and remediating vulnerabilities. The scanning can be either unauthenticated or authenticated scan of the website using user credentials provided by the client.

iStore requests from Government and Broader Public Sector to Sec Ops for each application initiate WAVA Scans.

OCIO ISB can provide assistance for clients and their developers to confirm, assess and prioritize vulnerabilities, as follows:

	Gold Standard	Silver Standard	Bronze Standard
RFC completed by Security Operations			
iSTORE			
Dedicated Analyst			
Executive Summary			
Detailed Report			
Re-scan to confirm Mitigation			
Estimated Time	>30 days	18 days	14 days

Web Application Vulnerability Assessment Form

BPS iStore Request Forms

Consulting Services

Vulnerability assessments conducted by third-party vendors may include internal and external vulnerability scans targeting web, network, system, application, and database, and reporting on findings. Please note that consultants' service is limited in scope to the devices, network and applications of the organization requesting the service.

Service providers for vulnerability scanning services are provided at IM/IT Security Services.

OCIO does not conduct penetration testing. Service providers for penetration testing services are provided at IM/IT Security Services.

Important Information

- Orders exceeding $75,000 must be tendered through the Procurement Services Branch
- *Pricing information is confidential and must not be shared with suppliers.

[i] CVSS Vulnerability Metrics https://nvd.nist.gov/vuln-metrics/cvss accessed December, 6, 2018