tenable
Web App Scanning

QUICK START FOR TENABLE WEB APP SCANNING

SERVICES BRIEF

Table of Contents

1. INTRODUCTION

This Services Brief ("Brief") incorporates and is governed by the Master Agreement located at http://static.tenable.com/prod_docs/tenable_slas.html, or any negotiated agreement between the parties that covers Professional Services ("Agreement"). Any capitalized terms used herein but not defined will have the definitions ascribed to them in the Agreement.

Any installation, configuration, knowledge transfer, or instruction not specifically referenced in this Brief is considered out of scope for this engagement. This includes, but is not limited to, any integrations related to third party products.

All services outlined in this brief will be delivered by a Tenable Certified Security Consultant, or by one of Tenable's qualified partners (hereinafter "Consultant").

2. SERVICE OVERVIEW

The Tenable Web App Scanning (formerly Tenable.io Web Application Scanning) Quick Start is a tailored service to streamline the identification and configuration of web application scanning.

This Tenable Web App Scanning (WAS) Quick Start Service is designed to provide five (5) outcomes within the scope defined in this Brief:

(a) **Plan and prepare the Customer**. Consultant will pre-plan, review and validate Tenable's approach and customer's prerequisites to ensure a smooth transition to Phase 2 activities.

(b) **Configure Tenable Vulnerability Management**. Tenable WAS will be initialized and configured by Consultant based on requirements captured during Phase 1 - Pre-Call.

(c) **Identified Scanning**. Consultant will scan up to ten (10) web applications (URLs) to provide a high-level assessment of the component vulnerabilities, HTTP security header, SSL/TLS and web application vulnerabilities.

(d) **Implement Tuning and Optimize Best Practices**. Consultant will implement and orient you to Tenable's best practices for future effective scanning

(e) **Provide Tenable Deliverable Document**. Document will provide a summary of your deployment requirements, deployed scanner resources and the web applications (URLs) identified for scanning.

Prerequisites

In order to receive the WAS Quick Start services, the Customer must ensure before Tenable begins work that all of the following actions have been performed, are available or are accessible, as applicable:

(a) Tenable software covered by this Brief is downloaded and accessible to Engineer

(b) Customer has valid administrative usernames and passwords for software applicable to this Brief

(c) Tenable port requirements must be reviewed at: https://community.tenable.com/s/article/What-ports-are-required-

for-Tenable-products and the necessary ports are open

(d) Access to Tenable's Community and/or Support Portal

(e) All necessary hardware and appliances are mounted and in place

(f) Customer has identified web application(s) to be in scope to be scanned

(g) Customer must have legal authorization to scan the identified web applications

(h) Credentials for web application to be scanned

(i) Customer Tenable Vulnerability Management user list for access to scans and scanning (i.e., RBAC)

(j) A customer representative with knowledge of the structure and makeup of the web applications (ideally, a developer)

(k) The web application is accessible from the cloud-based WAS scanner or from the local WAS scanner. The list of Tenable cloud scanners is available at: https://docs.tenable.com/tenableio/webapplicationscanning/Content/Scans/CloudScanners.htm

Definitions

WAS

Tenable Web App Scanning – The Tenable web application scanning tool to be used in this engagement

DAST

Dynamic Application Security Testing – The type of testing performed by WAS, in which the web application is in an operating state

SAST

Static Application Security Testing – A type of security testing that relies on inspecting the source code of an application. Tenable WAS does ***not*** perform this type of testing.

URL

Uniform Resource Locator – A reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. Commonly referred to as a web address.

RBAC

Role-Based Access Control - a method of restricting network access based on the roles of individual users.

3. SCOPE

The Tenable WAS Quick Start will be delivered across four (4) phases, split into multiple categories:

Phase 1 - Pre-Call:

Requirements around WAS scanning and wider security objectives will be gathered during the pre-call, including an understanding of what environments are to be scanned (Development, QA, Pre-Production, Production). Prerequisites for scanning will be discussed to ensure that the customer environment is correctly prepared and configured for the Phase 2 activities.

Phase 2 - Initialization, Identification and Scanning Workshop:

The activities in Phase 2 may have been completed fully or partially in Proof of Value (PoV) deployment, but will be reviewed to ensure that operation is suitable for ongoing business activities.

(a) Access to the Tenable Vulnerability Management platform and WAS application will be confirmed.

(b) Consultant will ensure that the appropriate users have access to the Tenable WAS product for scanning and viewing of results. Role-Based Access Control (RBAC) will need to be defined to allow this access, and administrative credentials will be required for this configuration.

(c) If on-premises or remote scanner(s) are to be deployed, up to three (3) will be deployed and connected to Tenable Vulnerability Management. These scanners can be used for scanning internet-facing web applications or, if firewall rules are suitably configured, can be used to scan Development or Pre-Production environments. Tenable also offers the Tenable Core + WAS virtual appliance that can be deployed locally on-premises or within a cloud-based development environment to scan non-internet-facing web applications. The virtual appliance is available in .ova, .zip and .iso format from https://www.tenable.com/downloads/tenable-io-was-scanner. (Login is required.) The scanner needs access to https://cloud.tenable.com on port 443.

Following the Initialization, Consultant will review the customer's security objectives gathered from the pre-call and recommend best practices. Consultant will explain the methodologies recommended to be used in Phase 3.

(a) The customer will identify up to ten (10) target web applications (URLs) to be within the scope of quick and detailed scanning.

(b) Methods for identifying further (possibly unidentified) web servers, services and applications using Tenable Vulnerability Management or Tenable Security Center will be discussed.

(c) Consultant will utilize a preconfigured Python script to read an XLSX file to create a URL scan targeting the ten (10) URLs identified. The script requires Tenable Vulnerability Management access.

(d) Quick scans will be configured and deployed (or scheduled to be scanned) to provide a high-level assessment of the component vulnerabilities, HTTP security header, SSL/TLS and web application vulnerabilities.

(e) A review of the results from the quick scans will be done to:

(i) appraise the findings of the applications covered in "quick scan" only

(ii) review in detail the sitemap crawled as an input to the detailed scanning, tuning and optimization

(f) Of the ten (10) target web applications (URLs) identified, the customer may select three (3) for detailed scanning. Overview scans will be performed on these three (3) URLs for tuning in Phase 3. This is conducted by analyzing the sitemap .csv output.

(g) An optimized vulnerability scan will be created and deployed for each of the three (3) URLs identified for detailed scanning.

Phase 3 - Tuning and Optimization:

Across two separate sessions, Consultant will tune the three (3) web applications (URLs) identified for detailed scanning while demonstrating Tenable's best practices for Web App Scanning. This includes:

(a) An optimized vulnerability scan will be created and deployed for each of the three (3) URLs identified for detailed scanning.

(b) Consultant will optimize the scanning configuration and apply authentication while adhering to Tenable's best practices.

(c) Customer will learn techniques to optimize the scan for efficiency and ensure it covers all areas of the application.

(d) Depending on the size of the web application (URL), the scan may complete and the results will be further analyzed and potentially further optimized.

Phase 4 - Documentation:

Documentation will consist of a templated report that documents the deployment requirements, deployed scanner resources (if any) and the web applications identified for scanning.

4. DELIVERABLES

Deliverable documentation will be completed remotely at the end of the engagement, and includes:

(a) Tenable Web App Scanning Documentation with the deployment setup and port requirements

(b) Scanning outcomes of up to ten (10) quick scans and the analysis of the three (3) detailed scans highlighting the coverage of the web applications (URLs)

(c) Information to help you maintain your deployment, with future recommendations and links to appropriate documentation

5. ASSUMPTIONS AND CONSTRAINTS

Tenable will rely on the following assumptions, together with those stated elsewhere in this Brief, in performing the service in this Brief. Should any of these assumptions prove incorrect or incomplete, or should Customer fail to comply with any of the responsibilities set forth in this Brief, Tenable reserves the right to modify the price, scope, level of effort, or schedule for the service in this Brief.

(a) Customer has valid licenses for all Tenable software covered by this Brief.

(b) Tenable may perform the service both remotely and on-site at a mutually agreed upon Customer location.

(c) Customer will provide Tenable access to key individuals, information and network resources at Customer site that are required in order for Tenable to perform the required tasks and deliverables of this Brief. Timely access to these key Customer individuals is required during the duration of this Brief, either onsite or remotely.

(d) When at a Customer facility, the Customer will provide Tenable Consultant with a professional workspace such as a conference room and access to personnel with sufficient privileges to the relevant hardware and software required to perform the engagement.

(e) Customer shall provide the Tenable Consultant with reasonable and safe access to Customer's facilities and ensure that its facilities constitute a safe working environment.

(f) The Customer systems meet or exceed the specifications found in the Tenable General Requirements document, available at https://docs.tenable.com/generalrequirements/.

(g) All workdays under this Brief are based upon an eight (8) hour workday and all work will be completed during normal working hours defined as Monday through Friday.

(h) Tenable personnel will not be exposed to hazardous environments. Customer will provide any safety equipment needed. Customer personnel will mount the hardware in the appropriate locations.

(i) Tenable is not responsible for any impact caused by Active Querying or any other network communication.

ABOUT TENABLE

Tenable® is the Exposure Management company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com