Tenable One Scoring Explained

Quick Reference Guide

Last Revised: May 10, 2024

Table of Contents

Tenable One Scoring Explained: Overview

The building blocks for the Cyber Exposure Score (CES) in the Tenable One Exposure Management Platform are similar to those used for years in Tenable products (e.g., Tenable Vulnerability Management, Tenable Lumin). These mechanisms have to date only been used for vulnerability management data. Tenable One expands these concepts into new realms of the attack surface: **Web Applications** (Tenable Web App Scanning), **Cloud Resources** (Tenable Cloud Security), and **Identity** (Tenable Identity Exposure).

The following concepts are foundational to the scoring utilized in Tenable One:

- Vulnerability Priority Rating (VPR): The severity and exploitability of a given vulnerability. A vulnerability's VPR is expressed as a number from 0.1 to 10, with higher values corresponding to higher likelihood of the vulnerability leading to a compromise and a higher impact on the asset. This score is found in Tenable Vulnerability Management.
- Asset Criticality Rating (ACR): Rates the criticality of an asset to the organization. An asset's ACR is expressed as an integer from 1 to 10, with higher values corresponding to the asset being more critical to the business. This score is utilized in Tenable Lumin.
- Asset Exposure Score (AES): A combination of the VPR and ACR of a given asset.

Data Timing

Data within Tenable One refreshes on the following cadence:

- Asset Data: Asset information is updated every time the asset is seen as part of a scan.
- Tag Application: When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of asset and the tag's rules.
- Tag Reevaluation: Every 12 hours, Tenable One automatically reevaluates tags to ensure they apply to any new assets, and are removed from any inactive assets.

Scoring

The first step in the scoring process is to calculate the AES of assets, which are then aggregated to the CES by taking an average of the AES values across a group of assets.

For Tenable One, a consistent approach for computing the AES across the categories involves the following:

1. Calculate the **Vulnerability Density** for an asset based on whatever weaknesses are present and the associated severity of those weaknesses. Vulnerability Density is defined as the number of vulnerabilities on that asset, their severity as reflected in the VPR scores and whether or not those vulnerabilities are remotely discoverable.
2. Combine this result with the ACR (which can be model-generated or user-defined in the case of VM assets) and then scale the result to produce the AES.

In addition to a CES for each of the categories, a Global CES is also generated by considering the AES across the entire attack surface assessed by Tenable One (i.e. assets from Tenable Vulnerability Management, Tenable Web App Scanning, Tenable Identity Exposure, and Tenable Cloud Security). Such scores are updated within hours of running a scan.

Computing Resources (Tenable Vulnerability Management and Tenable Lumin)

The following scores can be found within Computing Resources data sources.

Vulnerability Priority Rating

The prioritization of vulnerabilities in Tenable Vulnerability Management is derived from the Vulnerability Priority Rating (VPR) which takes a risk based approach to prioritization based on the characteristics of the vulnerability and threat intelligence.

Asset Criticality Rating

The Asset Criticality Rating (ACR) found in Tenable Lumin rates the criticality of an asset to the organization. An asset's ACR is expressed as an integer from 1 to 10, with higher values corresponding to the asset being more critical to the business.

Asset Exposure Score Computation

In Tenable Lumin, each asset is given a score from 0 to 1000. These values are computed based on the weighting of the VPR values and the ACR.

Web Applications (Tenable Web App Scanning)

Vulnerability Priority Rating

In Tenable One, the concept of Vulnerability Priority Rating (VPR) extends to web application scanning. Where a web application detection is associated with a CVE, VPR scores already exist at the CVE level. For detections not associated with CVEs, such as OWASP Top 10 vulnerabilities, Tenable uses the Common Weakness Enumeration (CWE) as a surrogate to measure the threat for a given detection, and uses the CVSS vector for the detection to determine the potential impact.

Asset Criticality Rating

As with VPR, the concept of Asset Criticality Rating (ACR) extends to web applications. The algorithm is a function of three primary components:

- **Exposure**: Represents the extent to which the web application is exposed to external internet factors (e.g., "Crawler hidden, public internet facing web application")
- **Type**: Represents the character of the web application (e.g., "Moderately complex web application supporting legacy HTTP protocol access, using paid digital certificates with valid SSL certs")
- **Capabilities**: Represents the web application's abilities, hinting at purpose (e.g., "Web application supports user logins, significant API usage, and handles PCI data")

Tenable combines these features and components in a rules engine to produce the ACR for the web application.

Cloud Resources (Tenable Cloud Security)

Vulnerability Priority Rating

When calculating the VPR for Cloud policy violations (detections), Tenable uses the NIST Common Configuration Scoring System (CCSS). This scoring system addresses software security configuration issues. CCSS is largely based on CVSS and CMSS, and it is intended to complement them. The CCSS metrics are organized into three groups: base, temporal, and environmental. Base metrics describe the characteristics of a configuration issue that are constant over time and across user environments. Temporal metrics describe the characteristics of configuration issues that can change over time but remain constant across user environments. Tenable uses environmental metrics to customize the base and temporal scores based on the characteristics of a specific user environment.

For each policy category, such as Encryption and Key Management, Tenable derives the confidentiality, integrity, and availability (CIA) impact and exploitability parameters based on the nature of the configuration issue. In CCSS, the Exploitation Method metric can be either Active (A) or Passive (P). Active misconfigurations can be actively exploited by an attacker (e.g., unencrypted S3 bucket) while passive misconfigurations make life tougher for defenders (e.g., logging is disabled). For Temporal & Environmental metrics, Tenable derives the exploit level using external threat sources while the remediation level is based on internal policy violation data.

Asset Criticality Rating

For ACR, Tenable maps cloud assets to higher level categories of exposure based on the resource type and features (properties) extracted from cloud resource configuration data:

- Access Exposure
- Key/Data Exposure
- Private/Internal Exposure
- Public Exposure
- VPC Misconfig
- Potential Vulnerabilities

Tenable assigns weights to these exposure categories based on publicly available incident data.

Identity (Tenable Identity Exposure)

Vulnerability Priority Rating

Tenable Identity Exposure assigns the VPR at the deviance (vulnerability) level based on the existing severity levels created in Tenable Identity Exposure:

- **Critical:** Deviances that can be used by an attacker with unprivileged access to compromise the Active Directory.
- **High:** Post exploitation techniques or techniques that require chaining to be dangerous.
- **Medium:** Indicates a limited risk for the Active Directory infrastructures.
- **Low:** Deviances with low impact on the Active Directory. Certain business contexts may allow low-impact deviances that do not necessarily affect AD security.

Asset Criticality Rating

Tenable Identity Exposure calculates ACR for user and computer accounts using a rule based system. Rules fall into three broad categories depending on the properties evaluated:

- **Capabilities**: Represents an objects capabilities within Tenable Identity Exposure. This is inferred from various properties of the asset. For example, a KRBTGT account or managed service account receives a high capability score.
- **Group Permissions**: Assets can have greater or lower levels of permissions depending on the groups they are members of. In particular, administrative groups and groups that have write access to other important objects. Examples of groups are DomainAdmins, DomainUsers, Administrators, and BackupOperators.
- **Object Type**: Looks at the user account control attribute of the object to score it. If the attribute contains one or more of the listed values (normal, disable, workstation, server, interdomain), then Tenable Identity Exposure assigns the asset a score.

Once Tenable Identity Exposure assigns each feature a score, it calculates the ACR by taking the maximum score observed and penalizing disabled accounts.