tenable network security

PVS passive vulnerability scanner™

Continuous network monitoring uncovers unauthorized devices, vulnerabilities and untrusted relationships with deep packet inspection.

Product Overview

Tenable's Passive Vulnerability Scanner™ (PVS™) is a patented network discovery and vulnerability analysis technology that delivers continuous network scanning and profiling non-intrusively. PVS monitors IPv4, IPv6 and mixed network traffic at the packet layer to determine topology, services and vulnerabilities. PVS can be used alone to effectively target network segments or small networks, and is also an integrated component of Tenable's SecurityCenter Continuous View™. PVS continuously discovers and tracks users, applications, cloud infrastructure, trust relationships and vulnerabilities. It also automatically discovers users, infrastructure and vulnerabilities across operating systems, network devices, hypervisors, databases, tablets, phones, web servers, cloud applications and critical infrastructure.

PVS Benefits

Core and distinguishing benefits of continuous scanning with PVS include identifying all devices and applications, identifying their vulnerabilities and detecting BYOD/mobile devices:

- Always know what devices, applications, services and relationships are active on your network
- Protect sensitive systems unavailable to active scans by effectively scanning without credentials and without possible disruption of service
- Automatically pinpoint potential security risks posed by vulnerable assets and new or rogue systems
- Demonstrate compliance with both internal policies and key regulatory requirements by validating configuration management
- Uncover inappropriate use and pinpoint "insider threats" not detectable by perimeter devices
- Focus on incident response by alerting on "real" compromises
- Accelerate threat remediation and eliminate gaps between active scans
- Fill gaps between scheduled active scans with continuous scanning

Tenable's Passive Vulnerability Scanner delivers real-time network monitoring and profiling for continuous scanning and assessment of an organization's security in a non-intrusive manner. PVS monitors network traffic at the packet level to provide visibility into both server and client-side vulnerabilities with full asset discovery.

PVS easily installs in networks and passively detects devices on your network, including virtual- and cloud- based devices, BYOD/mobile devices and even discovers jailbroken iOS devices. PVS scales to meet future demand of monitoring virtualized systems, cloud services and the proliferation of devices.

Key Features

Real-Time Vulnerability Monitoring

Tenable PVS continuously monitors network traffic for a variety of security-related
information including:

- Tracking all client and server application vulnerabilities
- Identifying when an application is compromised or subverted
- Detecting and documenting new hosts added to a network
- Discovering when an internal system begins to port scan other systems
- Highlighting all interactive and encrypted network sessions
- Spotting ports served and which ports browsed for each individual system
- Passively determining the operating system of each active host
- Detecting vulnerabilities on communicating systems and the protocols and applications used
- Summarizing top hosts, vulnerabilities, applications, operating systems and connections
- Available support for 10 Gbps networks.

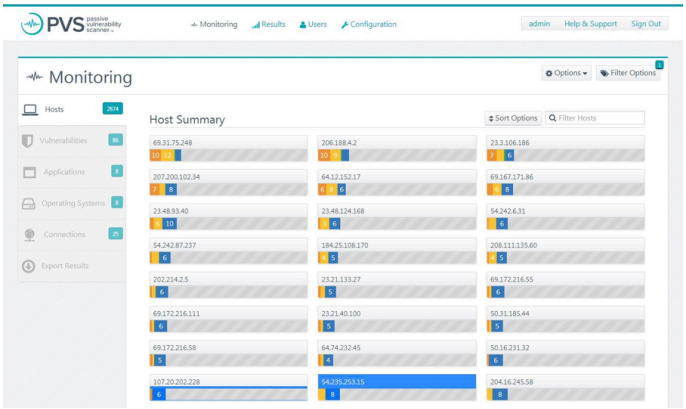
PVS connects to the network segment on a hub, spanned port, ERSPAN connection or network tap and continuously monitors the data stream, generating real-time alerts and comprehensive reports for the security, IT and management teams.

Network, Web and FTP Monitoring

PVS offers extensive web and FTP activity monitoring through direct analysis of the packet stream. By passively monitoring any HTTP or FTP transaction, PVS can determine and report useful information about each host on your network such as:

- All client and server web-based vulnerabilities and applications
- Complete list of all web-agents used on each host
- Passive enumeration of all files shared via FTP
- Real-time logging of every web GET, POST, or file download
- Real-time logging of every FTP file GET or PUT
- Real-time logging of every DNS query monitor

This data is useful to analyze insider activity, employee activity and malware infection or advanced threat compromise. Many of these logs can be sent to the Tenable Log Correlation Engine™ for further analysis, correlation search and long term storage.



Agentless Scanning and Clientless Access

PVS offers advanced protocol analysis of the Microsoft SMB protocol. If PVS is deployed on the interior of a network where it can see Active Directory network traffic, it can automatically learn:

- Each system's hostname and workgroup name
- A list of all files shared on any folder
- Logins and file downloads from a network share in real-time

The ability to passively determine this information in real-time has tremendous forensic and situational awareness value. For large networks, passively determining all shared folder contents makes identification of potentially sensitive data much easier. Using SecurityCenter Continuous View, with the integrated PVS and Log Correlation Engine modules, enables forensic analysis of employee activity and malware activity by examining records of files shared over the network.

SQL Database Logging & Monitoring

PVS can also look at network traffic and identify SQL devices and the vulnerabilities associated with them, and log this activity in real-time. Real-time logs for SQL queries can be sent to the Log Correlation Engine for search, storage and analysis of attacks, including SQL injection from web services. Full instrumentation of all SQL activity can be achieved by combining the PVS data with Nessus® SQL database configuration and vulnerability auditing data, as well as log data gathered from an SQL database server with a Log Correlation Engine agent.

Passive Topology Discovery & Service Identification Analysis

Data analysis for specific client or server vulnerabilities is performed by reconstructing both sides of network communications. Unique protocols, such as HTTP, SMTP and FTP, have specific strings that identify the version of the service. PVS identifies these and associates them with specific vulnerability plugins or tests.

PCI DSS Compliance

The PCI DSS requires accurate and comprehensive identification of all systems involved in the transmission, processing, or storage of credit card data. These systems collectively comprise the "cardholder data environment" (CDE) where the PCI DSS controls must be consistently applied and validated on an annual basis. Organizations must also provide evidence of procedures to maintain the integrity of the CDE. PVS not only monitors known data flows in/out of the CDE but also identifies undocumented data flows, particularly of unencrypted payment card information.

Deployment Options

The Tenable Passive Vulnerability Scanner is available at two performance levels; standard (1 Gbps) and high (10 Gbps) PVS is available at both levels as either a self- contained scanner or as part of SecurityCenter Continuous View. SecurityCenter Continuous View provides a comprehensive view of enterprise security by uniquely combining security eventswith active and passive vulnerability scanning.

tenable® network security

For More Information: Please visit tenable.com
Contact Us: Please email us at subscriptionsales@tenable.com or visit tenable.com/contact