Tenable’s Passive Vulnerability Scanner (PVS): Not an IDS or IPS

Rob Tessier/Ron Mullins – Tenable Network Security
11/3/15

The comparison of Tenable’s Passive Vulnerability Scanner (PVS) to an IDS has happened so often that our CEO, Ron Gula, a former NSA penetration tester and the creator of Dragon IDS (which was purchased by Enterasys), wrote a blog on this very topic differentiating PVS from an IDS. The blog can be found at https://www.tenable.com/blog/is-the-passive-vulnerability-scanner-an-intrusion-detection-system.

From our technical FAQ document on PVS (http://static.tenable.com/marketing/pvs-technical-faq.pdf), the same question was asked and answered as follows:

Q: Is PVS an IDS?

A: No. PVS is deployed similarly, in a strategic location, to see enough traffic to be effective, but PVS provides different results. An IDS is looking for known attacks as they occur. PVS is looking at the same traffic for real-time asset discovery and vulnerability detection, not attacks. PVS provides visibility into your network, the activity on your network, the assets attaching to your network and the various technical and business vulnerabilities these activities and assets create.

PVS is a passive vulnerability scanner. Do you know what happens between the last time a vulnerability scan is completed and the next time a scan is completed? New hosts, new ports, new services and new vulnerabilities can arrive on your networks faster than you may be allowed to scan for them. PVS can find out what is happening on your network without scheduling and waiting for an active scan. As PVS monitors your network, it also watches for potential application compromises, trust relationships and open or browsed network protocols.

PVS can be configured to monitor an entire network, a particular segment, or even a single server that you are interested in. For example, if you have a web server that you need to monitor 24/7, you can configure PVS to listen to all incoming and outgoing traffic to this server.

NetworkWorld reviewed Tenable’s PVS back in 2006 during PVS’s initial release, and had this to say:

Passive scanning, by its nature, is politically less sensitive and technically a dramatically lighter touch on the network. It provides accurate, up-to-date information as soon as a system appears and starts "talking."

Just by watching a network’s traffic flow, passive scanners can deduce a large amount of information about the communicating systems. Just as you can determine the type of cheese by tasting it (an "active" scan), you can also use passive techniques, such as reading the label or taking the aroma as it passes by.

With Tenable’s PVS, the goal is to detect and report on system applications and vulnerabilities. Tenable is home to the popular Nessus active vulnerability-scanning freeware. PVS (originally called NeVO) is the passive complement to Nessus. The latter product works by performing active scans of systems using a wide variety of techniques ranging from pinging to logging into a system and looking at the file system and registry, but PVS does its detection without sending a single packet.

These products will be of greatest use in larger networks with multiple subnets and 1,000 stations or more. For example, Tenable’s PVS provides less information than an active vulnerability scanner. However, PVS carries none of the risks of system crashes or the political problems of active scanning - problems that are magnified in large networks. PVS is also arguably more effective than active scanning for large networks, because it detects changes in configuration and topology as they happen. […]

Tenable’s Security Center makes it possible to combine the passive information of PVS and any active scan information you might be willing to gather from Nessus. Together, these can be managed, reported on, analyzed and even trended over time.
Although Tenable can use vulnerability information to help in IDS event management, the real sweet spot for this product is in networks where vulnerability information is an important part of security policy.

As a Sales Engineer for Tenable Network Security in South Florida AND a former end user of Tenable’s SecurityCenter with PVS, PVS is not an IDS. I’ll share my perspective.

1. Detecting a compromised system is very different from detecting a system that is under attack. Most intrusion detection systems detect attacks and not actual compromises. Tenable’s approach of monitoring files, system settings, logs, application processes, mobile devices, rogue access points, and network traffic as part of our continuous network monitoring is an excellent solution to hunt malware, compromised system accounts, and botnets.

2. Below is a screen shot of an indicators dashboard from SecurityCenter Continuous View depicting a wide variety of passive and active attack and compromise data in real-time. The full description of this dashboard (one of the 260+ dashboards available in SecurityCenter) can be found at http://www.tenable.com/sc-dashboards/indicators.

3. PVS is not a network intrusion detection system. It does not have a list of common or recently discovered attack patterns nor does it identify probes and scans. Instead, the focus is on auditing your network in real-time. PVS creates two types of data:
   - A real-time report of all mobile devices, IPv4 and IPv6 vulnerabilities, open ports, browsed ports, boundary traversing, and applications.
   - A real-time log of all network traffic, which is like an enhanced version of NetFlow that logs artifacts such as SSL certificate names, shared Windows files names, queried domain names, and browsed HTTP web sites.

4. Passive vulnerability data is useful for auditing activity on the network and identifying systems with applications and network connectivity that are suspicious, including:
   - Comparing all Internet browsing and served ports. While this does not detect attacks that occur 100% over common streams of network traffic, such as HTTP, attacks that communicate on “uncommon” ports such as IRC, DNS, or high ports, are readily identified regardless if they are client or server-based.
   - New web sites hosted on existing web servers. I’ve personally worked with organizations that have detected malware and compromised web servers by detecting new web sites being added to their Apache and Windows services.
• Auditing the web user-agents in use. While it is more than possible for malware to perfectly emulate Firefox and other common browsers, there is a large amount of malware that claims to be something that is still readily identified. PVS logs all user agent strings observed for each host in one spot, making this audit very easy to report against.
• Identifying unique client-side network activity. PVS logs all client-side network application usage such as SNMP, NFS, FTP, IRC, and Telnet. In environments where there is infrequent usage of these protocols, this activity is an indicator of suspicious activity.
• Identifying unique network services. PVS also logs all services running on every port. Regardless if a compromised system implements port knocking or only accepts connections from known hostile IP addresses, PVS will log the service. For example, if a system was compromised and an intruder placed a web server on port 31000 that only answers to IP addresses from a network block in China or Mississippi, PVS would report an HTTP speaking protocol there.
• Identifying the active DNS server in use. Compromised systems will often leverage DNS servers external to the organization. This can be done through direct re-configuration of the underlying operating system or simply performing DNS queries to known DNS servers.
• Changes in trust relationships. PVS keeps track of which clients connect to which servers and on which ports. Dramatic changes in client-server trust counts on different ports can indicate worms, scanning, and manual probing.

5. PVS’s real-time logs are another great resource to detect compromised systems. I’ve worked with many organizations that send their PVS real-time logs to applications such as Splunk. We also have organizations that deploy Tenable’s Log Correlation Engine (LCE) to process PVS real-time logs. There are many built-in correlations for the PVS within LCE. Some examples are listed below.

• Correlating all web, file sharing, network protocols, and SSL traffic with a real-time list of high quality botnet IP addresses.
• Correlating all web and DNS queries with DNS names and URLs that are known to be botnets.
• Tracking systems that perform proxies and leap-frog attacks based on the SSH, VNC, and Windows RDP protocols.
• Tracking anomalies and spikes in all types of logged PVS network sessions including SSL, DNS, NFS, web queries, and, in particular, spikes in failed DNS queries.
• Summarizing all executable files that have been downloaded on a daily basis.
• Summarizing all DNS domains queried on both an hourly and daily basis.
• Tracking all network traffic by learned user IDs. This facilitates analysis and reporting of any particular user’s network traffic.
• Tracking client-side network browsing activity including web, VNC, SSH, and Windows RDP.

As described above, PVS is not an IDS/IPS although it is a tool that identifies active real-time vulnerabilities and risk on the network.

I personally was able to stop several malware outbreaks on our network from the alerts triggered by PVS. From that initial alert, I reacted fast and isolated the machine before the malware could spread. Three months prior to installing PVS, we had another malware outbreak that caused 75% of the company machines to be reimaged, costing the organization tens of thousands of dollars in IT resources working overtime to clean up the mess, not to mention all of the lost employee productivity while we reimaged their machines.

As the Security Manager responsible for reducing risk, protecting assets, and meeting regulatory compliance, PVS was a welcomed addition to our vulnerability assessment program, ultimately reducing our attack surface.

From the PVS data sheet at http://www.tenable.com/data-sheets/passive-vulnerability-scanner-data-sheet:

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 nonintrusive 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 realtime 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 events with active and passive vulnerability scanning.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world’s largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.