Passive Vulnerability Scanning Overview

November 11, 2015
Revision 3

Table of Contents

I. Introduction

Passive Vulnerability Scanner (U.S. patent 7,761,918 B2) from Tenable is a network discovery and vulnerability analysis software solution that delivers continuous and near real-time network profiling and monitoring in a non-intrusive manner.

Passive Vulnerability Scanner® (PVS™) monitors network traffic at the packet layer to determine topology, services and vulnerabilities and is tightly integrated with SecurityCenter® and Log Correlation Engine® from Tenable to centralize both event analysis and vulnerability management for a complete view of your security and compliance posture.

Elements of Passive Monitoring

PVS observes network sessions and builds a model of active hosts and their services and applications. Traffic to and from each client or server application, as well as common network services such as DNS lookups and Windows file browsing, are analyzed to discover new hosts, new applications, new connections and vulnerabilities in real time.

Easy and Continuous Data Gathering

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

PVS observes which systems are active, what protocols they communicate on, what systems they communicate with, what applications they run and what vulnerabilities exist. This information is used to efficiently monitor your network for compliance with corporate policy and support of business initiatives.

Passive Vulnerability, Topology and Application Identification

As PVS observes network packets, it builds a model of the active hosts on a network and their services. For example, observing a TCP port 25 SYN-ACK packet from one of the monitored hosts will cause PVS to re-evaluate the network model. It will determine if the server with port 25 open is new information and, if so, PVS updates the model. An alert message with this new information can also be sent when changes like this are found.

A similar process is used to evaluate all network information including passively discovered information, topology information, trust relationships and vulnerabilities.

PVS uses a variety of techniques to determine if a host is alive and what purpose the host serves. It also makes use of passive operating system identification by monitoring the SYN packets that may be sent from a system during network usage. Each operating system (e.g., Linux, Windows, Solaris, etc.) builds SYN packets in a unique way, which can be used to determine the operating system.

Real-time Network Activity Logging

Data is analyzed for specific client or server vulnerabilities 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 vulnerabilities.

More complex protocols such as DNS, Windows file sharing and SNMP require several steps to determine the actual version of the underlying service or client. PVS uses various pattern matching and protocol analysis techniques to accomplish this identification.

PVS includes a database of over 6,500 plugins (tests) that are designed to discover hosts, applications and their related client/server vulnerabilities. Client-side vulnerabilities can be found without the need for agents or credentialed scans. See the PVS plugin page on the Tenable website for the latest list of plugins: tenable.com/pvs-plugins.

The PVS database of vulnerabilities also makes use of an index of exploits. As PVS reports vulnerabilities, it will also report which are exploitable. This means you can sniff your network and find vulnerabilities that are exploitable without performing an actual penetration test or even a vulnerability scan. When combined with the reporting and analytics of SecurityCenter, this sort of information can be used to identify:

- Systems running clients that have public exploits available
- Internet facing services that are exploitable
- Applications hosted behind VPNs and on Extranets that are exploitable

Advantages of Passive Monitoring

Once PVS learns your network, there are many advantages that can greatly enhance your security monitoring program.

Vulnerability Monitoring

PVS can determine and identify vulnerabilities continuously, so threat remediation is accelerated, eliminating gaps between active scans. Monitoring network data, as opposed to performing an active scan, has no impact on the network and provides continuous information about all elements of the network transactions, including client side vulnerability information.

Client Application and Vulnerability Monitoring

PVS includes many different types of checks to look for which client applications are in use and if they have any vulnerabilities associated with them. PVS will identify:

- All email clients in use such as Outlook, Thunderbird, Mail.app and many others
- All Web browsers in use such as Internet Explorer, Firefox, Chrome and Opera
- Chat programs such as Trillian or Skype
- Media streaming applications such as iTunes and Apple QuickTime

PVS also reports each of these applications according to the U.S. government's Common Platform Enumeration (CPE) specification. Passively determined vulnerability (CVE) and platform (CPE) data can be leveraged for U.S. government CyberScope reporting.

In order to gather client-side vulnerability information with a scanner such as Tenable Nessus®, administrative credentials need to be supplied for a vulnerability scan. Traditional vulnerability scanning, which is server focused, won't identify most client-side vulnerabilities or even enumerate which browser or email client is in use.

Continuous Activity Monitoring

As PVS analyzes network traffic to update its model of known hosts, applications and vulnerabilities, it also can stream a real-time log of many different types of network activities. These include many types of file sharing, network browsing, and database queries. Following is a list of several of the common protocols and services that PVS can monitor data in real time:

- **DNS** – All DNS lookups and lookup failures are logged in real time.
- **Facebook** – All Facebook logins are analyzed such that the local user ID can be identified.
- **FTP** – All FTP GET and PUT file transfers are logged in real time.
- **Gmail** – All Google Mail logins are logged in real time to discover the local user ID for tracking.
- **HTTP** – Web GET and POST requests are logged in real time along with the URL and user agent.
- **IM** – All instant messaging logins are logged to identify the user ID of the session.
- **NFS** – All Unix files transferred via NFS are logged in real time.
- **SMB** (Windows file sharing) – All files that are downloaded via "domain" folders or "directory shares" are logged.
- **SMTP** – All source email addresses are sniffed and collected to report on all local email addresses.
- **SQL** – All MS SQL, Oracle and MySQL database insertions, deletions and queries are converted to a log and streamed in real time.
- **Twitter** – All Twitter logins are analyzed to identify the local user ID.

Log Correlation Engine (LCE®), a part of SecurityCenter Continuous View®, contains many types of normalization and correlation to process logs from PVS. For example, for each passive HTTP request, LCE will normalize this log to consider the type of file being downloaded such as a `.gif` image or a `.pdf` document. This makes it very easy to see overall trends of file activity. It is very useful to have access to all files, DNS lookups, database queries, web browsing activity and social networking activity during a forensics investigation or incident response.

Passive Monitoring Means Less Active Scanning

The passive nature of PVS operation reduces the need for scheduled "scanning windows" that are required for active scanners. Since PVS does not generate network traffic, there is no risk to sensitive systems. Very often, critical production systems are not actively scanned out of concern over the impact scanning may have. Many security applications generate so much network traffic that they themselves become part of the problem. PVS provides real-time event monitoring without generating traffic or requiring an administrator to initiate a scan. This aspect is critical in situations where it is important that network activity remains as static as possible.

When managed by SecurityCenter, policy alerts can be scheduled to look for unauthorized change. For example, with PVS sending vulnerability data to SecurityCenter in real time, it is trivial to alert when the expected number of hosts on a DMZ goes above a given threshold. Any type of query can be scheduled to look for vulnerabilities, number of open ports, new client-side vulnerabilities and much more.

In-Depth Web Application Security Monitoring

Most large enterprises have some sort of custom web applications and many more web enabled applications. Although these are web services, they don't always run on common HTTP ports such as 80 and 443. This can cause organizations to miss auditing many of their critical assets with web-based interfaces such as appliances, email gateways, custom applications, management consoles and more.

As PVS analyzes network traffic, it performs port-independent discovery. For example, if you have a web server on an uncommon port, such as 2200, the PVS will see it – regardless if your vendor placed it there or a hacker did. Beyond identification of web services, PVS also provides much more in-depth analysis of web-based applications including:

- Identification of all HTTP and HTTPS services regardless of port
- Identification of all websites hosted on a web server
- Identification of all SSL certificates, regardless of port, their certificate authority and if and when they will expire
- Web content that is potentially insecure or hostile including JavaScript commonly used to attack browsers and hostile ActiveX components
- Web content, such as JavaScript and cascading style sheets (CSS), that is hosted from a third-party server that may not be under your control

All of this data can be sent to SecurityCenter where it can be continuously trended, reported and alerted on. SecurityCenter can also manage vulnerability data, web application audits and configuration testing of web servers and applications with the Nessus vulnerability scanner.

II. Example Uses of Passive Monitoring

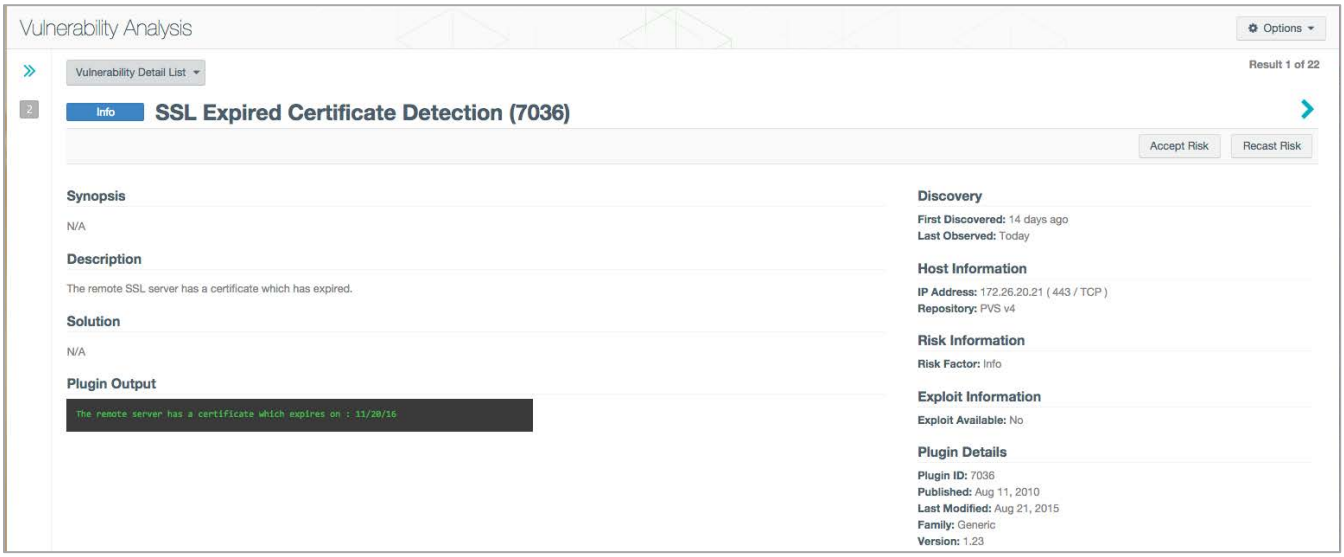
This section provides example of some typical applications of PVS and provides an overview of some of the available plugins. These screen captures were taken from various SecurityCenters and Log Correlation Engines that were managing vulnerabilities and logs from one or more PVS devices.

Identifying Policy Violations

The PVS has a number of plugins to identify violations to the organization's security policy that could introduce a security risk.

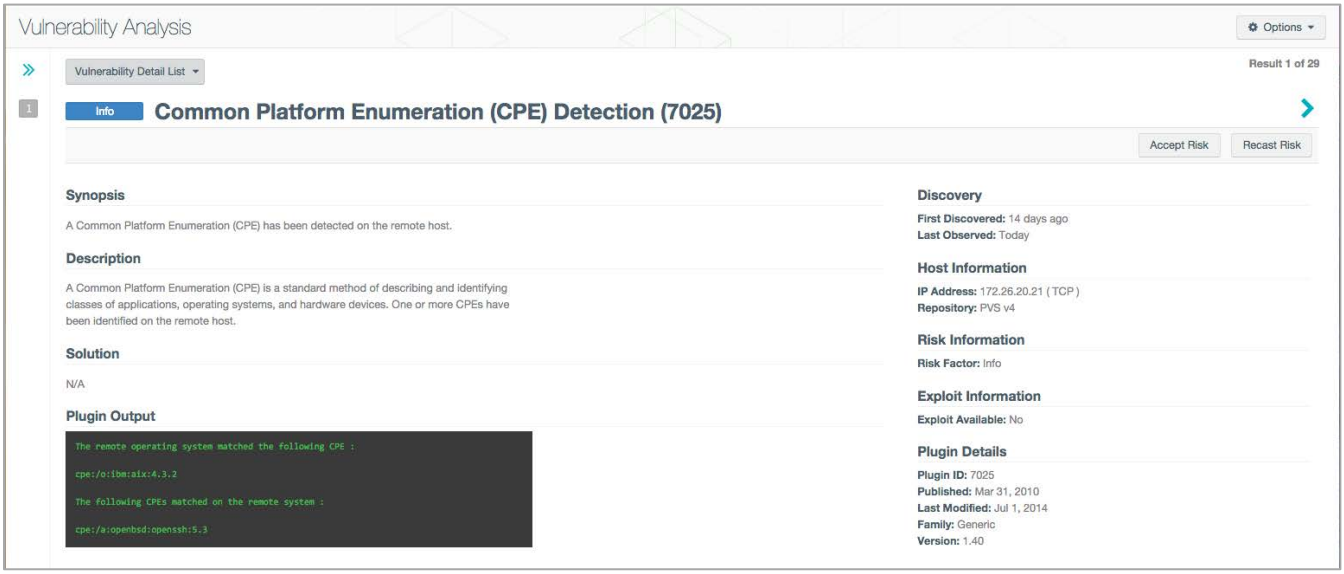
Identifying Expired SSL Certificates

Plugin 7036 – SSL Expired Certificate Detection – In this screen capture below, PVS sniffed an SSL service in use on a web server (port 443) and identified that the associated certificate had expired.



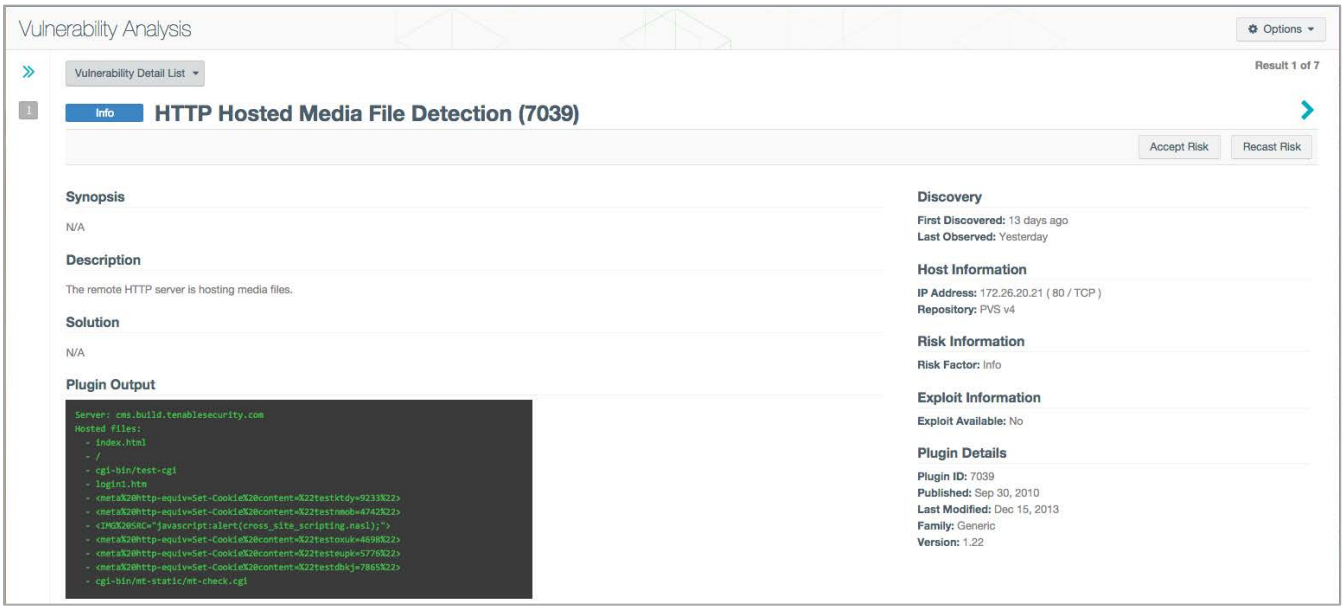
Common Platform Enumeration

Plugin 7025 – Common Platform Enumeration (CPE) Detection – Browser, email and several other classes of server and client applications are identified and reported with the US Government's official standard.



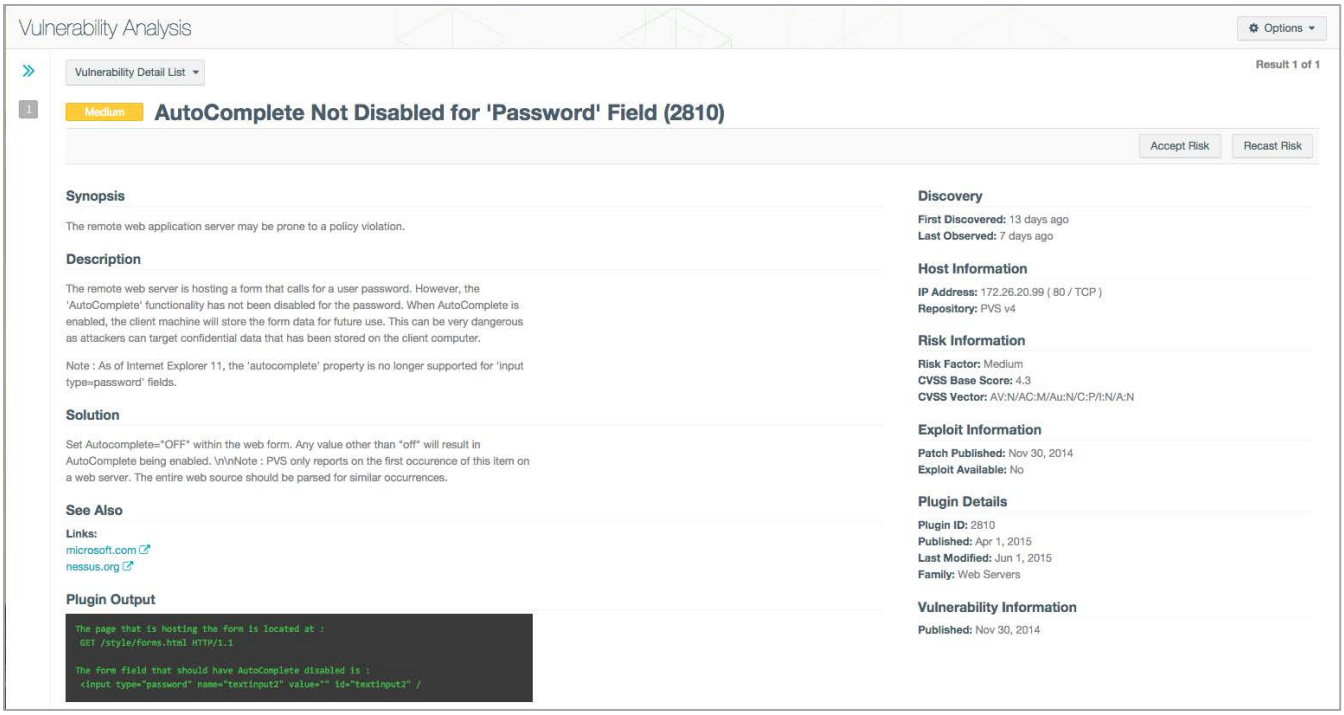
Hosted Media File Detection

Plugin 7039 – HTTP Hosted Media File Detection – PVS will monitor the actual file and directory structure of a web server and let you know the last 100 files or directories it has observed. There are similar reports that PVS will perform for FTP servers and SMB Windows file shares.



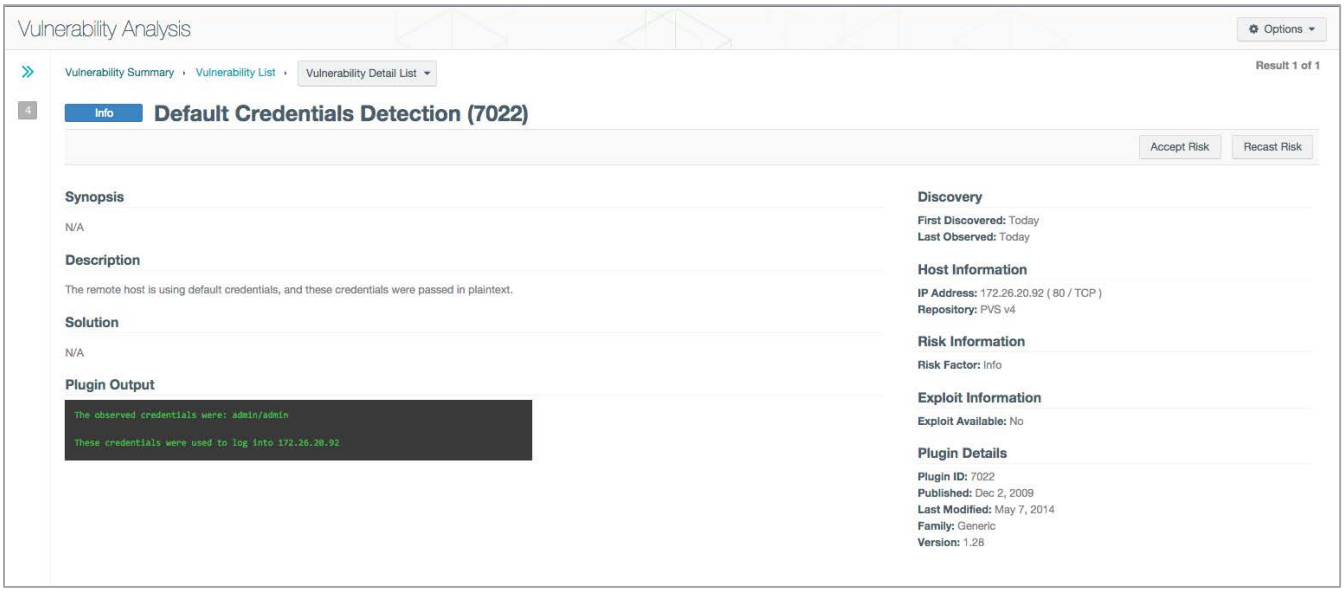
Autocomplete for Password Field

Plugin 2810 – Autocomplete Not Disabled for 'Password' Field – The remote web server is hosting a form that calls for a user password. However, the “Autocomplete” functionality has not been disabled for the password field.



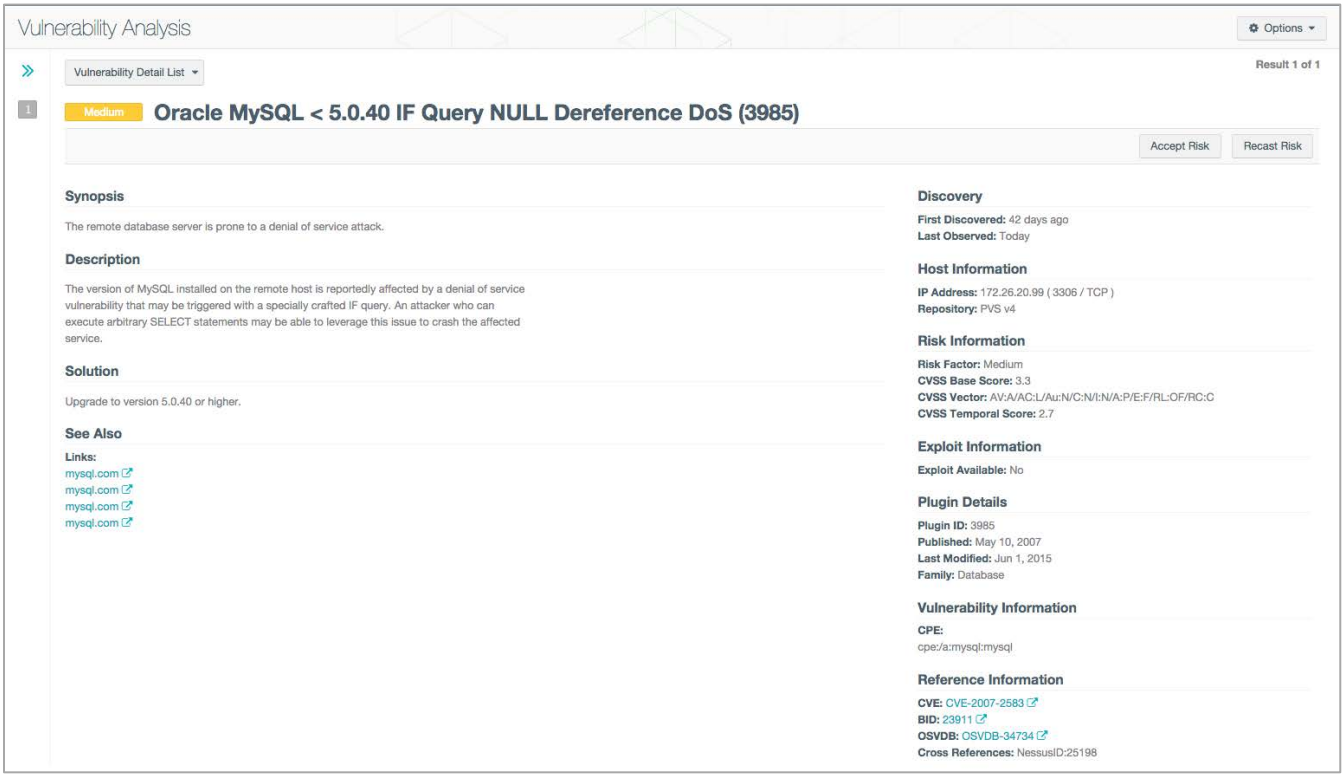
Default Credentials Detection

Plugin 7022 – Default Credentials Detection– The remote host is using default credentials, and these credentials were passed in plaintext.



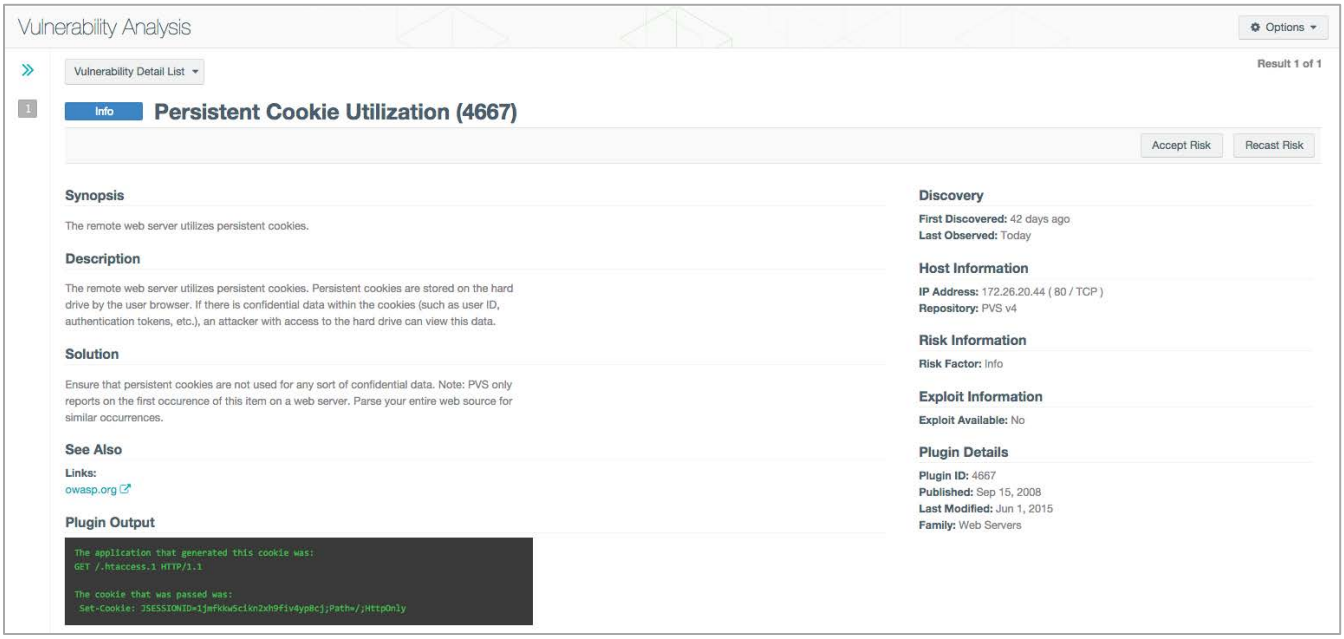
SQL Denial of Service Vulnerability

Plugin 3985 – Oracle MySQL NULL Dereference DoS– The remote database server is prone to a denial of service attack.



Persistent Cookie Utilization

Plugin 4667 – Persistent Cookie Utilization – The remote web server utilizes persistent cookies.



Incident Detection and Response

PVS can play a very important role in the incident response process from initial detection to determining the scope of the event.

HTTP Proxy Detection

Plugin 3389 – HTTP Proxy Detection – In some cases, simply finding a vulnerability may indicate that you have already been compromised. For example, consider this vulnerability report:

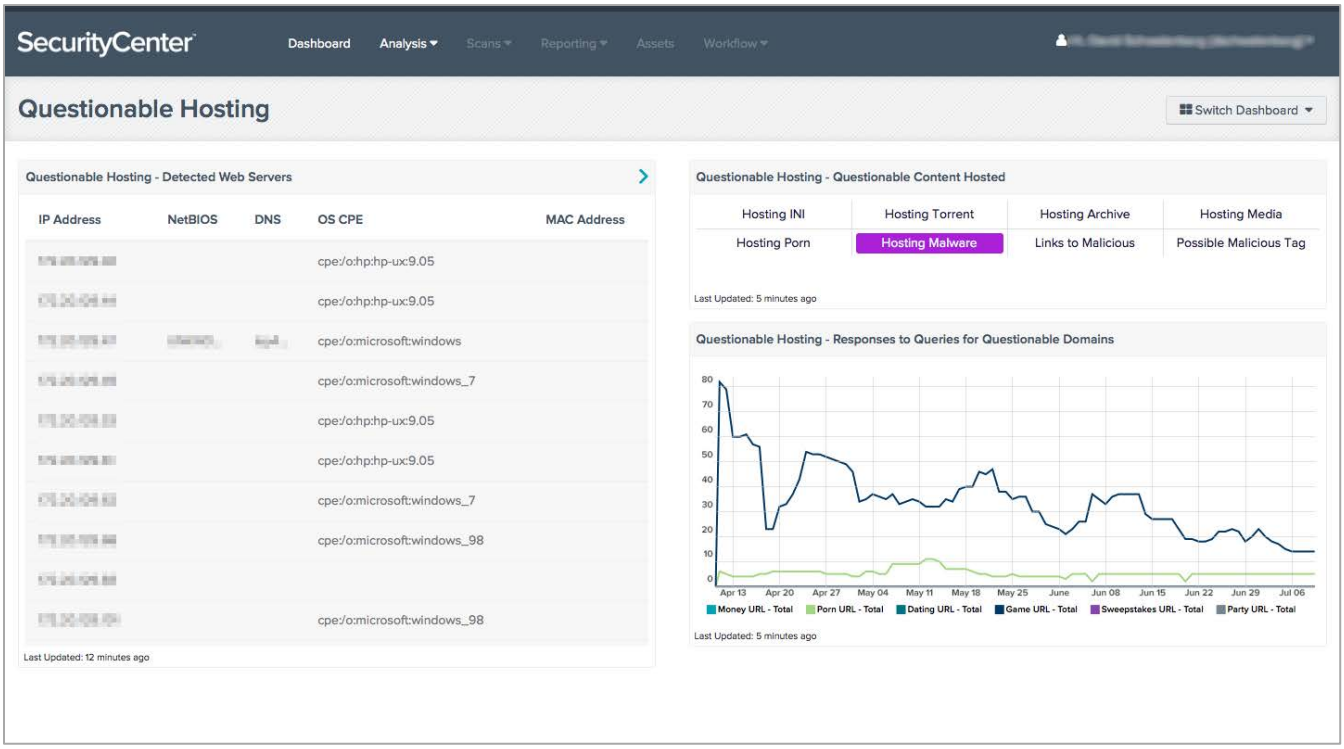
```
10.10.10.10|8011/tcp|3389|NOTE|Feb 16 03:14:57 - The remote host is a proxy
server.  PVS has determined this due to the format of the HTTP request.
PVS observed a client issuing this request: GET http://www.somesite.com
HTTP/1. The server replied with: Proxy-Connection:XXXXXXXX External
Access : The PVS has observed connections to this port from hosts
outside of the configured range of network addresses. This vulnerability
is likely accessible from external network addresses.
```

In this case, the server at 10.10.10.10 has a proxy running on port 8011 that will perform HTTP proxy connections. This sanitized log came from one of our customer web servers that was compromised and the intruders placed a high-port proxy to bounce off and attack other websites.

Tracking Malicious Websites

For a given web server, active web application scanning is no guarantee that all hosted websites will be found. There may be no links between two websites hosted on the same web server. Similarly, scanning a network for all ports to look for web servers that may have been installed as part of a botnet is difficult to do in real time. Because of this, it's very common for malicious web servers to be set up on university, home user and any type of large networks.

SecurityCenter's "Questionable Hosting" dashboard presents all web servers passively detected on the network, as well as questionable content that the web servers might be hosting and trend lines for detected websites that contain keywords not expected for the local network.



Real-time Traffic Analysis

The ability to analyze traffic in real time is one of the most powerful features of PVS. PVS identifies the type of traffic (web, DNS, database, Windows file sharing) and organizes the data for analysis.

Real-time Analysis of Web Traffic

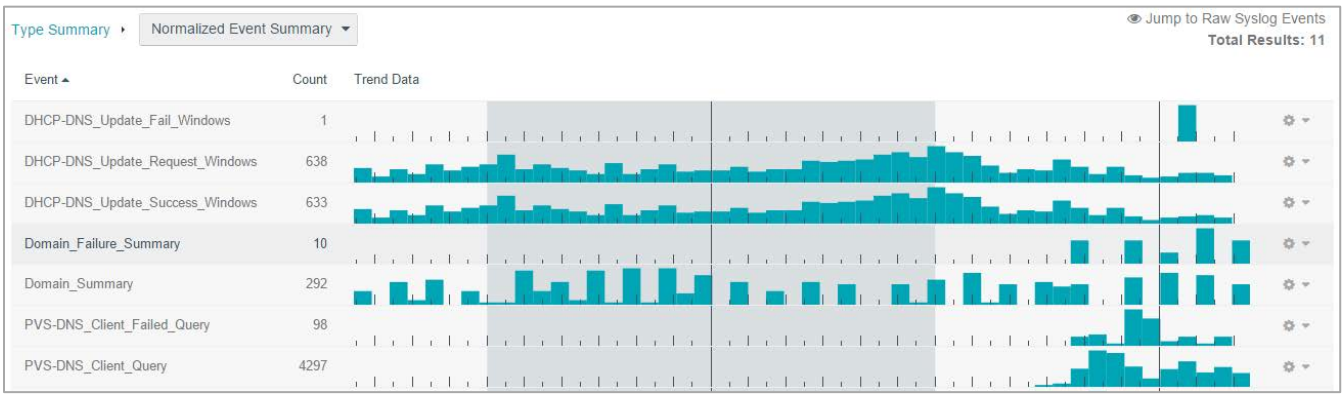
The PVS can monitor data for many types of live file sharing to LCE. In the screen below, web traffic activity has been displayed over the past 24 hours for a single host. There have been 303 JPEG images downloaded via HTTP, 56 PNG images and 86 files that had a `.txt` extension. If this were an employee under investigation, the analysts could drill into these screens and look at the actual image names.

This is very useful for analysis of web based “drive-by” malware infections. For example, if a system were known to be compromised, PVS and LCE could be used to see which sites and which potentially malicious PDF, movie or JavaScript file were downloaded. Then a search could be performed to see if any other systems on the network downloaded that same malicious file.

Real-time Analysis of DNS Traffic

When PVS sniffs data from DNS queries to LCE, it makes the data available for searching. This is an excellent forensic reference but can be difficult to comprehend when working with DNS logs from thousands of active nodes. To help with this, LCE will summarize all DNS lookups seen for a given host. This can make auditing which sites a host performed a DNS lookup for very efficient. LCE will also perform alerts on the statistic rates of DNS lookups, DNS lookup failures and can also alert when a node is continuously performing DNS lookups that are failing. All of these indicate changes in DNS usage that indicates abuse or a misconfiguration.

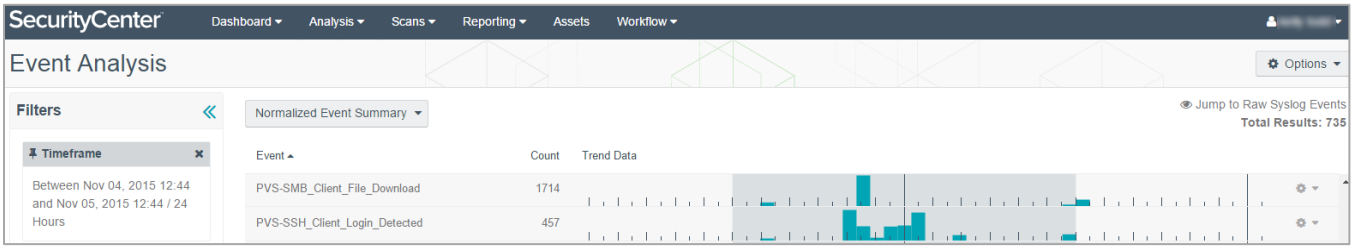
In the following screen capture, a single host has performed 4297 DNS lookups in the past 24 hours and generated 292 “Domain Summary” logs:



Real-time Analysis of Windows File Sharing Traffic

PVS can monitor data from file uploads or downloads via the Windows SMB protocol. This includes when a host gets patches pushed to it from the domain server or when someone uploads a file to a network share. LCE takes these logs and normalizes them by file extension, so that it can graphically display SMB file transfers of common “office” documents in text, PowerPoint, Adobe, Excel and Word documents.

In the following screen capture, all SMB file sharing logs have been graphed out from November 4, 2015 through November 5. There have been 1714 file downloads via SMB; drilling down to show the “List of Events” view will show the date and time of the download, the source and destination IP addresses involved in the transfer, and the sensor through which the download was detected.

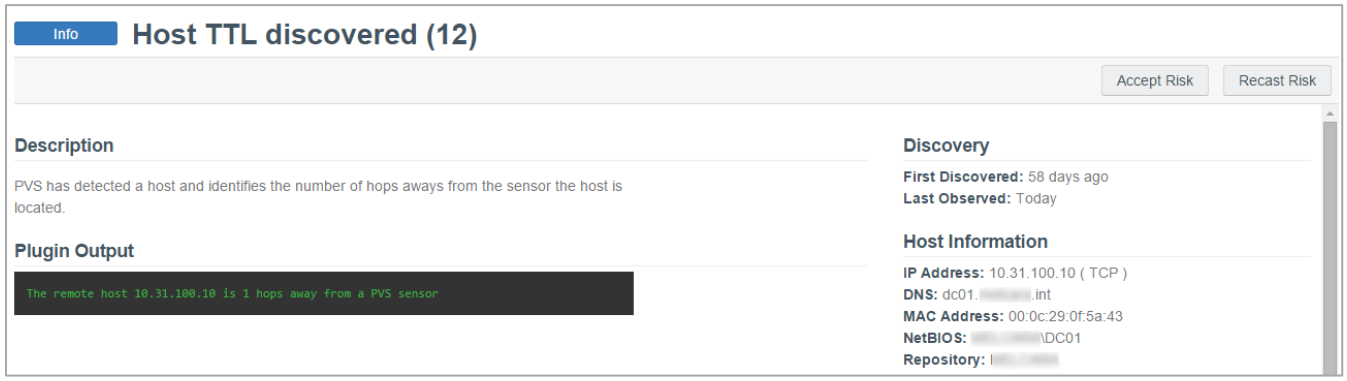


Real-time Analysis of Database Traffic

PVS can sniff data of database queries from Oracle, MySQL and MS SQL and send them to LCE for normalization and correlation. This type of logging can help analyze web application attacks that involve SQL injection as well as finding SQL traffic and SQL servers passively.

Detecting New or Rogue Systems

As new hosts are detected, PVS will generate “Host TTL discovered” events. See the screen capture below for an example event of this type:



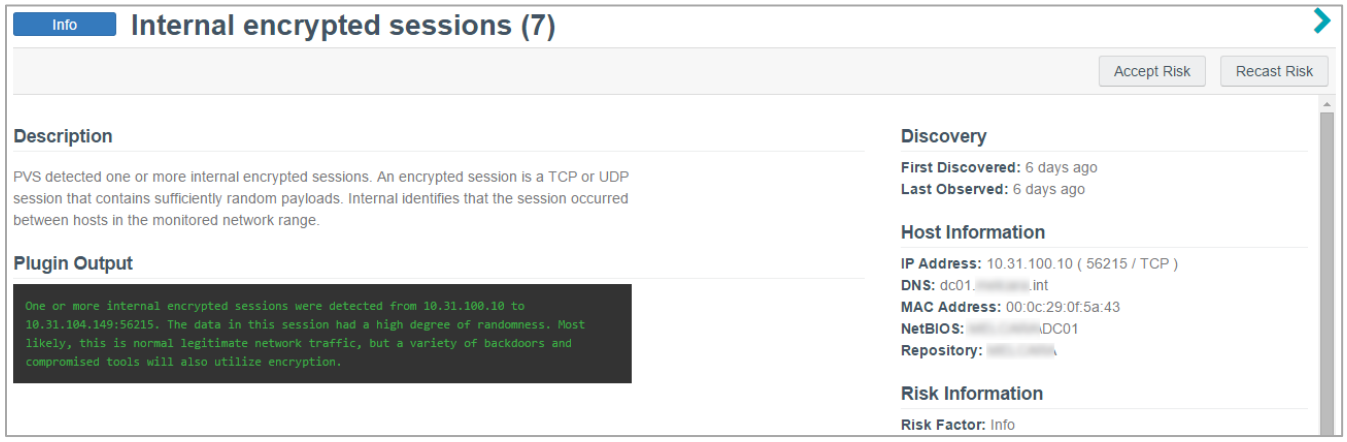
Once a new system is detected, PVS will monitor the host for unusual activity or vulnerabilities. When this event is generated, automated alerts can be created to notify affected personnel of the new potential threat.

Detecting Insider Threats

The following plugins can be used to detect insider threats whose activity may elude perimeter devices:

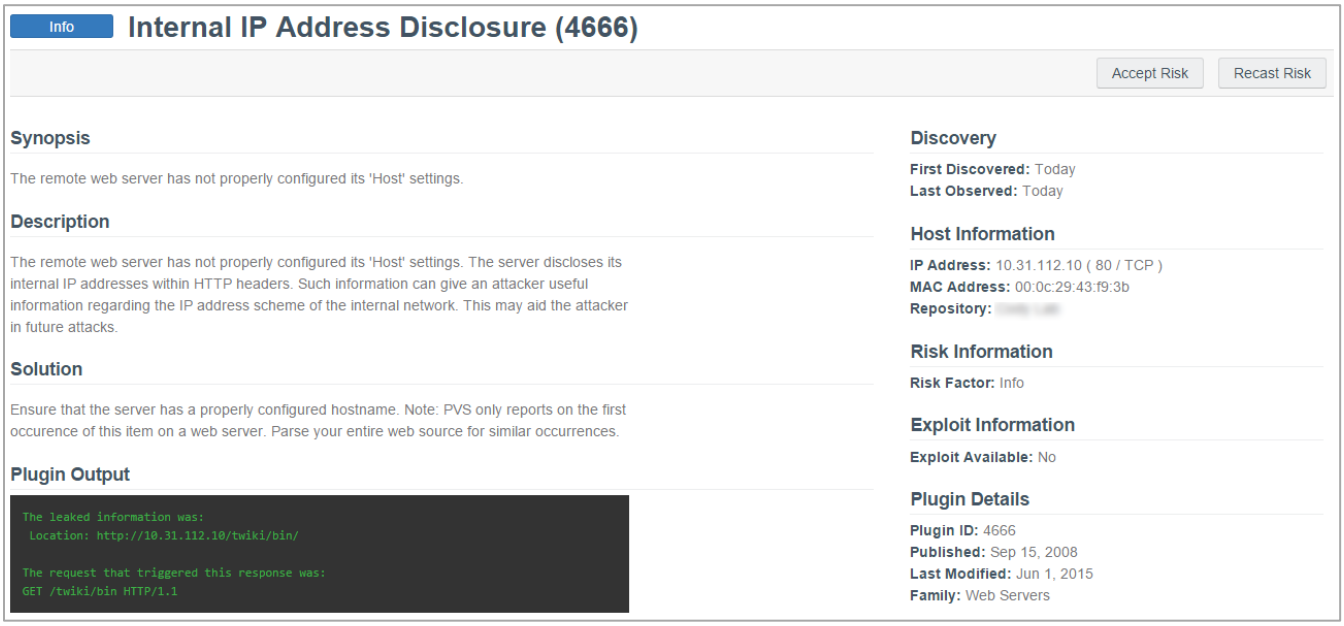
Detecting Encrypted Sessions

Plugin 7 – Internal encrypted sessions – PVS detected a port used for one or more internal encrypted sessions.



Disclosure of Internal IP Address

Plugin 4666 – Internal IP Address Disclosure – The remote web server has not properly configured its "Host" settings. The server discloses its internal IP addresses within HTTP headers.



III. Conclusion

Passive vulnerability monitoring is not a replacement for active vulnerability scanning, but it is an extremely useful enhancement that provides an advantage to a continuous network monitoring program. PVS is available on Red Hat Linux ES 5, ES 6 and ES 7, Microsoft Windows and macOS operating systems and supports CPE, CVSS and the exploitability index. Please contact sales@tenable.com for more information.

IV. About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.