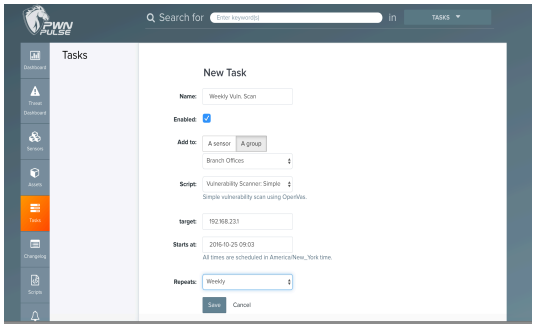
Best Practices – Vulnerability Scanning with OpenVAS in Pulse

Overview

Pulse includes a customized implementation of OpenVAS, the advanced open source scanner, to perform vulnerability scanning of network assets with the Pwn Pro sensor. This uncredentialed vulnerability scan is configured to target the network or specified network assets for a breadth of vulnerability types and score them based on their criticality. Whether running vulnerability scans for remote offices, or supplementing a commercial vulnerability scanner, Pulse makes it easy to centrally manage scans covering your entire organization.

Configure

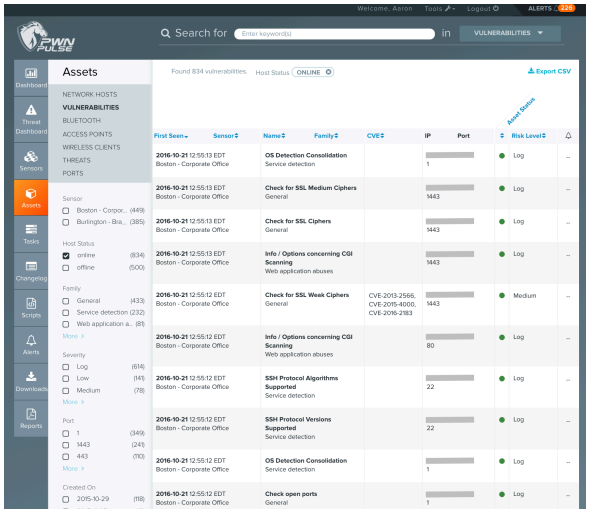


- Scans are easily configured through the Pulse User Interface. Simply create a new **Task** to perform a Vulnerability Scan. Select Vulnerability Scan Script from dropdown, specify the frequency of the scan (see more info below), and the network target(s) in CIDR notation.

- To ensure you are scanning for the most current vulnerabilities, ensure your sensor is up-to-date. This can be done automatically through Pulse by setting a weekly **Task**, to run a sensor update each week. See the *Pulse User Manual* (available from the help tab of Pulse), for more detail on sensor updates.

- Scanning with OpenVAS Vulnerability Scanner in Pulse:

    - **Simple Scan** - a scan that has removed various categories of vulnerabilities for which are known to likely result with service disruption or denial of service. Default method available for use when testing a single asset or the subnet.
    - **Connections Needed**- Allow TCP port 80 to www.openvas.org, Allow TCP/873 to feed.openvas.org



Validate

- Prior to scheduling a vulnerability scan on a full network, create a Task for a scan on a single target host on that subnet by IP address. This is to ensure that the traffic will be properly routed to the target from the sensor, with no filtering or IDS/IPS systems blocking traffic. Once the scan on the individual target has returned results (approximately 1 hour), proceed with scheduling larger scans on that network.

Schedule

- Schedule a single sensor to scan up to 254 hosts (/24 network) weekly.

- If performing vulnerability scans on multiple subnets, where possible, use multiple, staggered tasks – set to run at different times – to perform the scans. Where possible, schedule Vulnerability Scans at night to minimize any potential network impact.

Review & Remediate

- Results of the scan will be displayed in Pulse once the scan is complete. Vulnerabilities will be displayed on individual assets in the **Assets – Network Hosts** view, and can be listed, filtered, and exported as a csv from **the Assets – Vulnerabilities** view. Where applicable, CVE numbers will be assigned.

- Review Vulnerabilities in the Assets – Vulnerabilities view, and sort using filters based on Severity (Log/Low/Medium/High), Vulnerability Family, Created Date, and associated port.

- Apply patches and remediate vulnerabilities, and validate remediation with follow-on scans.