

## Integrate Tenable.io

EventTracker v8.x and above

## Abstract

This guide helps you in configuring **Tenable.io** and EventTracker to receive **Tenable.io** events. You will find the detailed procedures required for monitoring Tenable.io.

## Audience

Administrators who are assigned the task to monitor and manage Tenable.io events using EventTracker.

*The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.*

*EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

Abstract .....	1
Audience .....	1
Overview .....	3
Prerequisites .....	3
Integration of Tenable events to EventTracker server .....	3
Verify Tenable.io Integration in EventTracker .....	6
EventTracker Knowledge Pack.....	11
Flex Reports .....	12
Import Tenable.io knowledge pack into EventTracker .....	18
Knowledge Objects .....	19
Flex Reports .....	20
Parsing Rule.....	21
Verify Tenable.io knowledge pack in EventTracker .....	23
Knowledge Objects.....	23
Flex Reports .....	23
Parsing Rule .....	24
Create Flex Dashboards in EventTracker .....	25
Schedule Reports.....	25
Create Dashlets.....	27
Sample Flex Dashboards .....	31

## Overview

Tenable provides comprehensive visibility into the security posture of container images as they are developed, enabling vulnerability assessment, malware detection, policy enforcement and remediation prior to container deployment. It gains visibility into the security of web applications with safe vulnerability scanning, complete with high detection rates to ensure you understand the true risks in your web applications. It brings clarity to your security posture through a fresh, asset-based approach that provides maximum coverage of your evolving assets and vulnerabilities in ever-changing environments.

## Prerequisites

- EventTracker v8.x should be installed.
- Tenable.io for cloud and Tenable.io on premises(Security Centre)
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

## Integration of Tenable events to EventTracker server

Following are the steps to integrate Tenable.io to Eventtracker.

- Please Contact the EventTracker support team for obtaining Tenable Integrator pack
- The Integrator package will be obtained in a Zip file format, extract the files to get the below file contents as shown in the image.

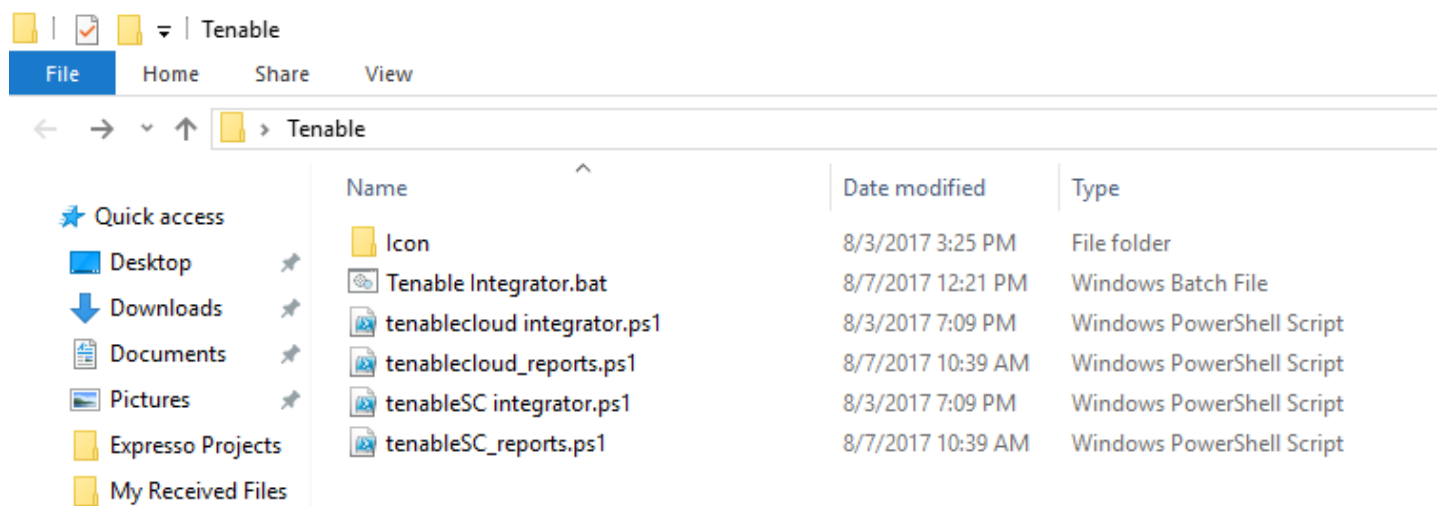


Figure 1

- Double-click on the Tenable Integrator.bat(for both cloud or Security centre) to start the integration process.
- Once the .bat starts running, you will get a pop up window as shown in below image.

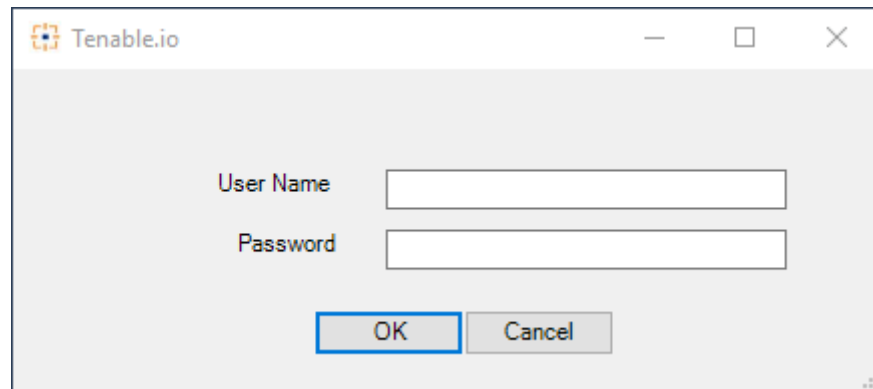


Figure 2

- In the pop-up window that appeared, enter your Tenable Username and Password.
- Once you enter the details, click on **OK**.
- Now a task scheduler trigger pop-up window appears as shown in below image

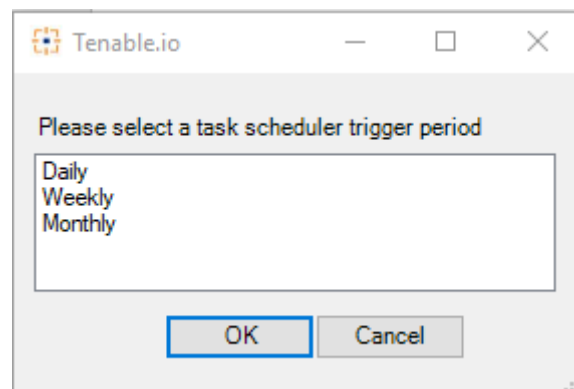


Figure 3

- In this task scheduler window, you need to choose how you want to schedule the Tenable reports, i.e. on a Daily, Weekly or Monthly basis.
- Click on **OK** once scheduling period is chosen.
- Once you click **OK**, an authentication pop up window will appear asking for Username and password as shown below:

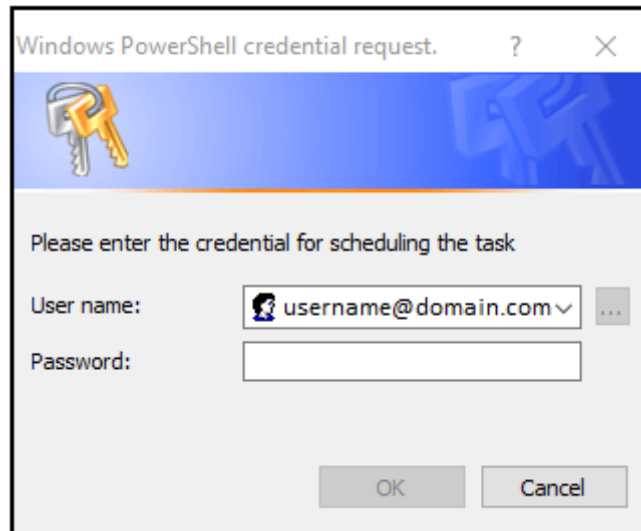


Figure 4

- Please enter your System Username and Password to proceed with the Task Scheduling.
- Click on **OK** to continue.

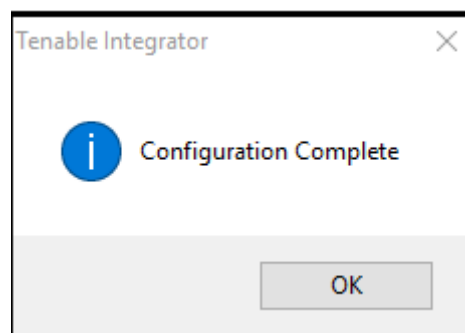


Figure 5

- Configuration is now complete.

**Note:** For the scans to be monitored, the permissions for the user scans should be set to 'Can view' as shown in the below image, otherwise the scans would not be saved or monitored.

The screenshot shows the Tenable.io interface for configuring a scan. The top navigation bar includes 'Vulnerability Management', 'Dashboards', 'Scans' (highlighted), 'Reports', and 'Settings'. The left sidebar lists folders like 'My Scans', 'All Scans', and 'Trash', and resources like 'Policies', 'Target Groups', 'Exclusions', 'Scanners', and 'Agents'. The main content area is titled 'scan 1 / Configuration' and has tabs for 'Settings', 'Compliance', and 'Plugins'. Under the 'Settings' tab, there are sections for 'BASIC', 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'BASIC' section is expanded to show 'General', 'Schedule', 'Notifications', and 'Permissions' (highlighted). The 'Permissions' section is further expanded to show 'Data Sharing' and 'User Sharing'. The 'Data Sharing' section has a dropdown for 'Scan results' set to 'Show in dashboard'. The 'User Sharing' section has a dropdown for 'Owner' set to 'Jacob.s@contoso.com' and a search box for 'Add users or groups'. Below this, a list of users is shown, including 'Default' and 'Karen.witmann@contoso.com'. A dropdown menu is open for the 'Default' user, showing options: 'Can view', 'No access', 'Can view' (highlighted), 'Can control', and 'Can configure'. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 6

## Verify Tenable.io Integration in EventTracker

- Launch the EventTracker web.
- Navigate to **Admin > Manager**.

The screenshot shows the EventTracker web interface. At the top left is the EventTracker logo. The top navigation bar includes 'Admin', 'Tools', 'Help', and 'Hello, Admin'. Below this is a secondary navigation bar with 'Dashboard', 'Incidents', 'Behavior', 'Search', 'Reports', 'My EventTracker', and 'Config Ass'. A 'NEWS' section is visible, followed by 'ANNOUNCEMENTS' with a 'No Announcements' button. The main content area features several articles: 'Latest Knowledge Packs', 'How to Succeed at SIEM', 'EventTracker Wins SC Magazine's Coveted 5-Star Rating for the Fourth Year in a Row', 'SIEMphonic and the Cyber Kill Chain', and 'Fishing'. A dropdown menu is open from the 'Admin' button, listing various configuration options: Active Watch Lists, Alerts, Behavior Rules, Behavior Settings, Category, Event Filters, Eventvault, IP Lookup Configuration, Knowledge Objects, Logbook Configuration, **Manager** (highlighted), Parse Rules, Report Settings, RSS, Systems, Users, Weights, and Windows Agent Config.

Figure 7

- Go to the **Direct Log Archiver** Tab and check if the configurations are replicating as show in the below image.
- Please select the checkbox **Direct log file achieving from external sources**, if not selected by default, as shown in the below image.



## MANAGER CONFIGURATION

CONFIGURATION    syslog / VIRTUAL COLLECTION POINT    **DIRECT LOG ARCHIVER / NETFLOW RECEIVER**    AGENT SETTINGS

E-MAIL CONFIGURATION    STATUSTRACKER    NEWS

Direct log file archiving from external sources

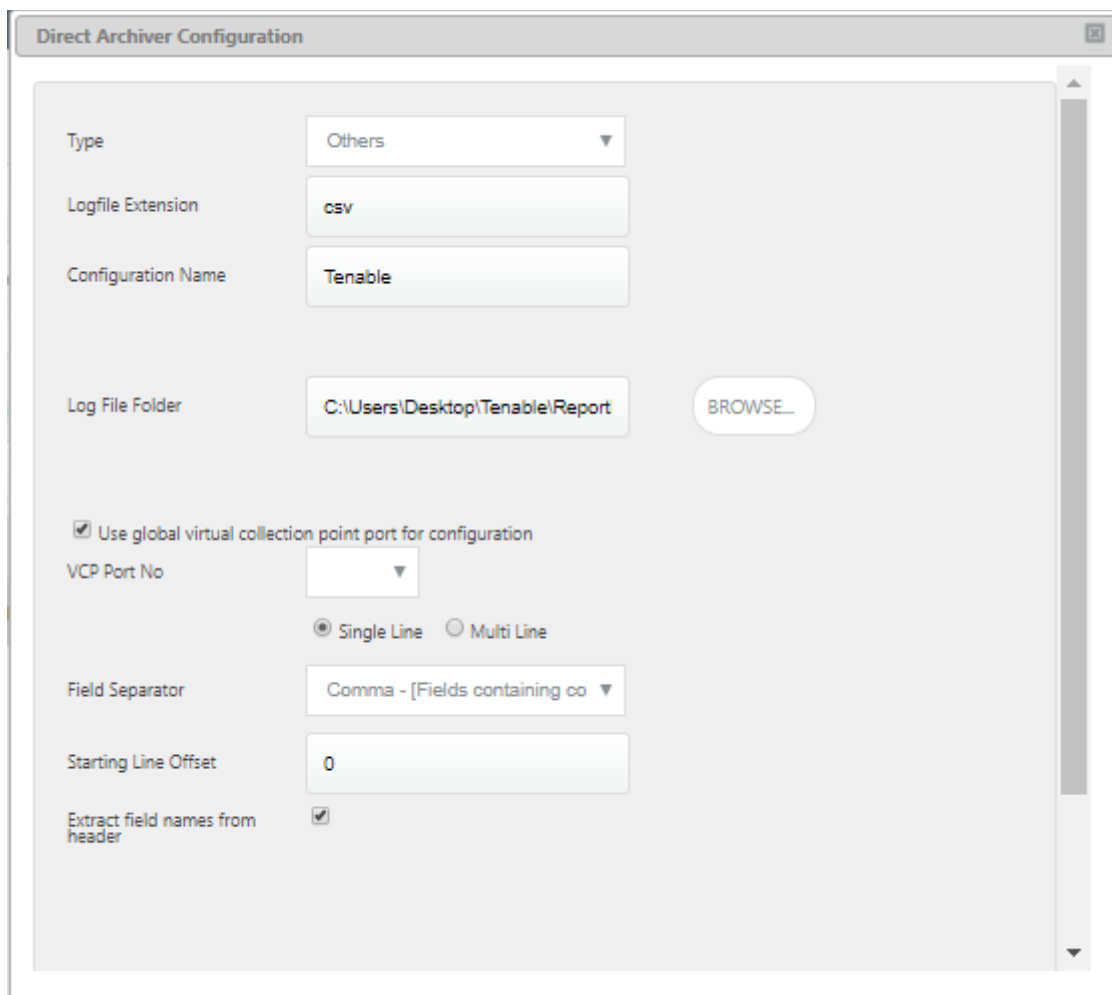
Purge files after  days    Maximum files per cycle     Global virtual collection point

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	VCP PORT	FIELD SEPARATOR	LOG TYPE
C:\Users\etadmin\Desktop\Tenable\ReportDLA	Tenable	csv	GLOBAL	Comma - [Fields containing comma are wrapped in double quotes]	

ADD    EDIT    REMOVE

Figure 8

- Confirm if the Configurations are set right by clicking on **Edit**. You will get the below window once you click **Edit**.



The screenshot shows a dialog box titled "Direct Archiver Configuration". It contains the following fields and options:

- Type: Others (dropdown)
- Logfile Extension: csv (text input)
- Configuration Name: Tenable (text input)
- Log File Folder: C:\Users\Desktop\Tenable\Report (text input) with a BROWSE... button
- Use global virtual collection point port for configuration
- VCP Port No: (empty dropdown)
- Single Line  Multi Line
- Field Separator: Comma - [Fields containing co (dropdown)
- Starting Line Offset: 0 (text input)
- Extract field names from header:

Figure 9

- Click on **Configure** to check the Computer Name, Configuration name and system description.
- Click **Ok**.

**Direct Archiver Configuration**

**Log file configuration**

Configuration Name: C:\Users\Desktop\Tenable\ReportDLA\Tenable

Log Source: Tenable

Computer Name: Tenable.io

Computer IP: ::1 GET IP

System Type: Win 10

System Description: Tenable Scanner

Comment Line Token:

Entire Row as Description  Formatted Description

Log File Format: Custom Log File Format

Message Fields:  ADD

REMOVE

**Select Event Date and Time Fields**

No of Fields: 2

Date Field:

Time Field:

**Select Date Time Format Fields**

Format Value: AUTO i

**Select Column Mapping**

Computer:

<< BACK SAVE & CLOSE CANCEL

Figure 10

- Go to **Start** and open **Task Scheduler** to confirm if the scheduling action is created or not.
- Below image shows the Tenable Task that is created for scheduling.

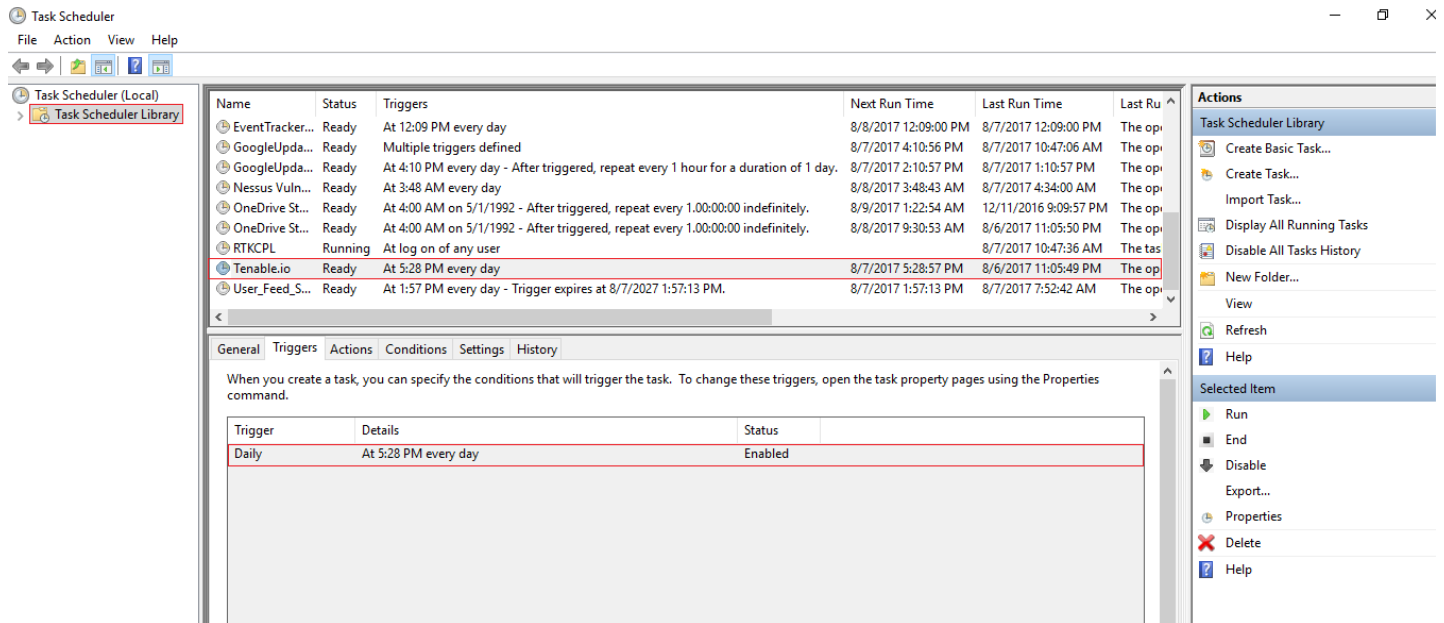


Figure 11

- Check if the Task Scheduler is configured correctly with the right conditions to trigger the task, with the specified date and time when it needs to be run.
- Tenable Integration is now completed with EventTracker to receive Tenable Events.

## EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories, reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

## Flex Reports

**1. Tenable-Basic Network Scan:** This report provides a full system scan suitable for any host.

LogTime	Plugin ID	CVE	CVSS	Host	Message	Protocol	Port	Plugin Output	Risk	Solution	Synopsis
01/25/2017 05:17:07 PM	78479	CVE-2014-3566	4.3	192.168.1.255	SSLV3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)	tcp	1433	Nessus determined that the remote server supports SSLV3 with at least one CBC cipher suite, indicating that this server is vulnerable.	Medium	Disable SSLV3.	It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.
01/25/2017 06:03:24 PM	10547	CVE-1999-0499	4.3	192.168.137.224	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure	tcp	161		Medium	Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets	The list of LanMan services running on the remote host can be obtained via SNMP.
01/25/2017 06:03:24 PM	94437	CVE-2005-1794	5.1	192.168.137.236	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	tcp	3389	Port 514/tcp was found to be open	Medium	Force the use of SSL as a transport layer for this service if supported, or	It may be possible to get access to the remote host.
01/25/2017 06:03:24 PM	10114	CVE-1999-0524	6.1	192.168.1.255	ICMP Timestamp Request Remote Date Disclosure	tcp	1433	This host returns non-standard timestamps (high bit is set)	Medium	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).	It is possible to determine the exact time set on the remote host.

Figure 12

## Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/7/2017 11:08:12 AM	3230	PNPL-6-KP / Contoso...	N/A	N/A	Tenable

**Event Type:** Information  
**Log Type:** Application  
**Category Id:** 0

**Description:**  
 Plugin ID: 94437  
 CVE: CVE-2016-6329  
 CVSS: 2.6  
 Risk: Low  
 Host: 192.168.1.118  
 Protocol: tcp  
 Port: 3389  
 Name: SSL 64-bit Block Size Cipher Suites Supported(SWEET32)  
 Solution: Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.  
 Synopsis: The remote service supports the use of 64-bit block ciphers.  
 Plugin Output:

Figure 13

**2. Tenable-Credentialed Patch Audit:** This report provides the ways that a host can be authenticated and enumerates missing patch updates.

LogTime	Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Message	Vulnerability Description	Synopsis	Solution
01/27/2017 10:39:52 AM	94741	CVE-2016-6313	5.0	Medium	192.168.137.236	tcp	0	CentOS 6 / 7 : libgrypt (CESA-2016:2674)	An update for libgrypt is now available for Red Hat Enterprise Linux	The remote CentOS host is missing one or more security updates.	Update the affected libgrypt packages.
01/27/2017 10:39:52 AM	95321	CVE-2016-6327	10.0	Critical	192.168.10.100	tcp	214	CentOS 7 : kernel (CESA-2016:2574)	An update for kernel is now available for Red Hat Enterprise Linux 7.	The remote CentOS host is missing one or more security updates.	Update the affected kernel packages.
01/27/2017 10:39:52 AM	95320	CVE-2016-3075	5.0	Medium	192.168.137.236	tcp	88	CentOS 7 : glibc (CESA-2016:2573)	An update for glibc is now available for Red Hat Enterprise Linux 7.	The remote CentOS host is missing one or more security updates.	Update the affected kernel packages.
01/27/2017 10:39:52 AM	94981	CVE-2016-8635	9.3	High	192.168.1.140	tcp	0	CentOS 5 / 6 / 7 : nss / nss-util (CESA-2016:2779)	An update for nss and nss-util is now available for Red Hat Enterprise	The remote CentOS host is missing one or more security updates.	Update the affected kernel packages.

Figure 14

## Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/10/2017 5:51:16 PM	3230	PNPL-6-KP / Contoso...	N/A	N/A	Tenable
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Plugin ID: 94741 CVE: CVE-2016-6313 CVSS: 5.0 Risk: Medium Host: 192.168.137.236 Protocol: tcp Port: 0 Name: CentOS6/7:libgrypt CESA-2016:2674 Solution: Update the affected libgrypt packages. Synopsis: The remote CentOS host is missing one or more security updates. Vulnerability Description: An update for libgrypt is now available for Red Hat Enterprise Linux			

Figure 15

- 3. Tenable-Badlock Detection:** This report provides the badlock vulnerability for Windows and the Linux/Unix application Samba for network file sharing.

LogTime	Plugin ID	CVE	CVSS	Risk	Host	Port	Protocol	Message	Synopsis
01/25/2017 10:30:40 AM	90510	CVE-2016-0128	6.8	Medium	192.168.1.118	49450	tcp	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	The remote Windows host is affected by an elevation of privilege
01/25/2017 11:01:46 AM	90516	CVE-2015-5370	6.8	Medium	192.168.1.255	49410	tcp	MS16-047: Multiple errors in DCE-RPC code (3148527) (Badlock) (uncredentialed check)	The remote Windows host is affected by an elevation of privilege
01/25/2017 11:01:46 AM	90510	CVE-2016-2118	6.8	Medium	192.168.1.255	49410	tcp	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	The remote Windows host is affected by an elevation of privilege
01/25/2017 11:01:46 AM	90516	CVE-2016-2113	6.8	Medium	192.168.1.255	49410	tcp	MS16-047: Missing TLS certificate validation (3148527) (Badlock) (uncredentialed check)	The remote Windows host is affected by an elevation of privilege

Figure 16

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0	<b>Description:</b> Plugin ID: 90510 CVE: CVE-2016-0128 CVSS: 7.1 Risk: High Host: 192.168.1.140 Protocol: tcp Port: 49455 Name: MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) Solution: Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. Synopsis: The remote Windows host is affected by an elevation of privilege vulnerability. Plugin Output:				

Figure 17

4. **Tenable-Host Discovery:** This report provides a simple scan to discover live host and open ports.

LogTime	Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Message	Vulnerability Description	Synopsis	Plugin Output	Solution
01/06/2017 12:37:24 PM	10180	NA	NA	None	192.168.137.236	Tcp	0	Ping the remote host	This plugin attempts to determine if the remote host is alive using one or more ping types. An ARP ping, provided the host is on the local subnet and Nessus is running over ethernet. A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK. A UDP ping (DNS, RPC, NTP, etc).	It was possible to identify the status of the remote host (alive or dead)	The remote host is up. The host is the local scanner.	NA
01/06/2017 12:37:24 PM	10180	NA	NA	None	192.168.1.140	Tcp	0	OS Identification	Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.	It was possible to identify the status of the remote host (alive or dead)	NA	Update the affected kernel packages.

Figure 18

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/10/2017 6:02:36 PM	3230	PNPL-6-KP / <u>Contoso</u>	N/A	N/A	Tenable
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0	<b>Description:</b> Plugin ID: 10180 CVE: CVSS: Risk: None Host: 192.168.1.140 Protocol: tcp Port: 0 Name: Ping the remote host. Vulnerability Description: This plugin attempts to determine if the remote host is alive using one or more ping types. An ARP ping, provided the host is on the local subnet and Nessus is running over ethernet. A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK. A UDP ping (DNS, RPC, NTP, etc). Solution: NA				

Figure 19

5. **Tenable-Malware Detection:** This report provides the scan results of malware on windows and unix systems.



LogTime	Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Message	Vulnerability Description	Synopsis	Solution	Plugin Output
01/00/2017 03:02:14 PM	24786	NA	NA	None	192.168.1.118	tcp	0	Nessus Windows Scan Not Performed with Admin Privileges	The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.	The local security checks are disabled.	Reconfigure your scanner to use credentials with administrative privileges.	#NAME?
01/00/2017 03:02:14 PM	70329	NA	NA	None	192.168.1.140	tcp	0	Microsoft Windows Process Information	Report details on the running processes on the machine. This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.	Use WMI to obtain running process information.	Address the problem(s) so that local security checks are enabled.	Process_Modules_csv : lists the loaded modules for each process.

Figure 20

**Logs Considered:**

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Plugin ID: 70329 CVE: CVSS:  Host: 192.168.1.140 Port: 0 Name: Microsoft Windows Process Information Description: Report details on the running processes on the machine. This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies. Solution: Address the problem(s) so that local security checks are enabled. Synopsis: Use WMI to obtain running process information. Plugin Output: Process_Modules_csv : lists the loaded modules for each process.			

Figure 21

**6. Tenable-Bash Shellshock Detection:** This report provides the vulnerability that affects Bash, a common component known as a shell that appears in many versions of Linux and Unix. It allows the user to type commands into a simple text-based window, which the operating system will then run.

LogTime	Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Message	Vulnerability Description	Solution	Synopsis	Plugin Output
08/03/2017 06:15:20 PM	10180	CVE-2014-6277	8.1	High	192.168.137.224	tcp	445	Ping the remote host	This plugin attempts to determine if the remote host is alive using one or more ping		It was possible to identify the status of the remote host (alive or dead).	The remote host 192.168.137.224 is considered as dead-not scanning the remote host 192.168.137.224 is
08/03/2017 06:15:20 PM	11219	CVE-2014-6278		None	192.168.137.236	tcp	22	Tenable SYN scanner	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a	Protect your target with an IP filter.	It is possible to determine which TCP ports are open.	Port 80/tcp was found to be open

Figure 22



**Logs Considered:**

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/10/2017 6:08:17 PM	<a href="#">3230</a>	PNPL-6-KP / <a href="#">Contoso...</a>	N/A	N/A	Tenable

**Event Type:** Information  
**Log Type:** Application  
**Category id:** 0

**Description:**  
 Plugin ID: 11219  
 CVE: CVE-2014-6278  
 CVSS:  
 Risk: None  
 Host: 192.168.137.236  
 Protocol: tcp  
 Port: 22  
 Vulnerability Description: This plugin is a SYN "half-open" port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP(full connect)scans against broken services, but they might cause problems for less robust firewalls and also leave e unclosed connections on the remote target, if the network is loaded.  
 Solution: Protect your target with an IP filter.

Figure 23

- 7. Drown Detection:** DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security.

LogTime	Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Message	Vulnerability Description	Solution	Synopsis	Plugin Output
08/03/2017 06:20:17 PM	83705	CVE-2016-0702	9.0	High	192.168.1.140	tcp	80	Tenable Drown detection	A key disclosure vulnerability exists due to improper handling of cache-bank conflicts on the Intel Sandy-	Upgrade to OpenSSL version 1.0.2g or later.	The remote service is affected by multiple vulnerabilities	

Figure 24

**Logs Considered:**

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/3/2017 6:20:17 PM	<a href="#">3230</a>	NTPLDTBLR38 / <a href="#">Tenabl...</a>	N/A	N/A	Tenable

**Event Type:** Information  
**Log Type:** Application  
**Category id:** 0

**Description:**  
 Plugin ID: 83705  
 CVE: CVE-2016-0702  
 CVSS: 9.0  
 Risk: High  
 Host: 192.168.1.140  
 Protocol: tcp  
 Port: 80  
 Name: Tenable **Drown** detection  
 Vulnerability Description: A key disclosure vulnerability exists due to improper handling of cache-bank conflicts on the Intel Sandy-bridge microar chitecture. An attacker can exploit this to gain access to RSA key information.  
 Solution: Upgrade to OpenSSL version 1.0.2g or later.  
 Synopsis: The remote service is affected by multiple vulnerabilities

Figure 25

- 8. Tenable-Scap and Oval Auditing:** This report provides details about how to generate SCAP and Oval content audit scan results.

LogTime	Plugin ID	Ip Address	Port and Protocol	Repository	Severity	Plugin Name	Mac Address	NetBios Name	Check Name	Information	Actual Value	Reference Information
02/06/2017 11:28:52 AM	1000370	192.168.1.100	80/tcp	RonLab	High	CCE-9136-3:xccdf_gov.nist_rule_store_account_lockout_threshold:xccdf_gov.nist_benchmark_USGCB-Windows-7_v1.2.3.1	C1:18:86:b1:E3:43	WORKGROUP:TARGET-WIN7	CCE-9136-3=Account Lockout Threshold	Account Lockout Threshold,if this setting is enabled it gives the number of failed sign-in attempts taht will cause an Juser account to be locked.	xccdf_gov.nist_rule_store_account_locou_t_threshold:Passed	OVAL-DEF:oval.gov.nist.usgcb.windoseven.def.9r CCE-CCE-9136-3 Generated Date-2017/02/4T09:30:00 Updated Date: 2017/02/05t12:20:36
02/06/2017 11:28:52 AM	1000378	192.168.10.26	104/tcp	RonLab	High	CCE-9253-6:xccdf_gov.nist_rule_store_access_this_computer_from_remote_network:xccdf_gov.nist_benchmark_USGCB-Windows-7_v1.2.3.1	a3:46:ec:b1:85:0d	WORKGROUP:TARGET-WIN7	CCE-9253-6=Access this computer from remote network	Access this computer from remote network,if this setting is enabled it allows only administrators to access the remote computer or the user who are assigned with specific roles and rights by administrator.	xccdf_gov.nist_rule_store_access_this_computer_from_remote_network:Passed	OVAL-DEF:oval.gov.nist.usgcb.windoseven.def.9r CCE-CCE-9253-6 Generated Date-2017/02/1T09:30:00 Updated Date: 2017/02/05t12:20:36
02/06/2017 11:28:52 AM	1000337	192.168.1.11	108/udp	RonLab	High	CCE-9260-1:xccdf_gov.nist_rule_store_passwords_using_reversible_encryption:xccdf_gov.nist_benchmark_USGCB-Windows-7_v1.2.3.1	00:2f:70:fh:38:9f	WORKGROUP:TARGET-WIN7	CCE-9260-1=Reversible Password Encryption	Reversible Password Encryption,if this setting is enabled password will be stored in a decrypted format,putting them at a higher risk of compromise.This setting should be disabled.	xccdf_gov.nist_rule_store_passwords_using_reversible_encryption:Passed	OVAL-DEF:oval.gov.nist.usgcb.windoseven.def.9r CCE-CCE-9260-1 Generated Date-2017/02/9T10:00:00 Updated Date: 2017/02/10t10:00:00

Figure 26

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/8/2017 4:52:10 PM	3230	PNPL-6-KP / Contoso-	N/A	N/A	Tenable

**Event Type:** Information  
**Log Type:** Application  
**Category Id:** 0

**Description:**  
 PluginID: 1000378  
 Ip Address: 192.168.10.26  
 Port/Protocol: 0/tcp  
 Repository: RonLab  
 Severity: High  
 Plugin Name: CCE-9253-6:xccdf\_gov.nist\_rule\_store\_access\_this\_computer\_from\_remote\_network:xccdf\_gov.nist\_benchmark\_USGCB-Windows-7\_v1.2.3.1  
 First Discovered: Feb 1,2017 05:43  
 Last Observed: Feb 1,2017 12:43  
 DNS Name: Win7-pc-lab  
 Mac Address: a3:46:ec:b1:85:0d  
 NetBios Name: WORKGROUP:TARGET-WIN7

Figure 27

9. Tenable-User activities: This report provides details about all the user activities.

LogTime	Computer	User Name	Email ID	Last Login	Last Observed Login Attempt	Account Permission	Account Enabled	Account Lockout
08/04/2017 05:49:14 PM	TENABLE	Gilbert.jercos@contoso.com	Gilbert.jercos@contoso.com	1/1/1970 5:30:00 AM	8/4/2017 5:14:28 PM	32	0	0
08/04/2017 05:49:14 PM	TENABLE	Karen.manor@acme.com	Karen.manor@acme.com	8/4/2017 5:05:16 PM	8/4/2017 5:03:09 PM	64	1	0
08/04/2017 05:49:15 PM	TENABLE	Jiren.rakota@adf.com	Jiren.rakota@adf.com	8/4/2017 5:28:49 PM	8/4/2017 5:13:14 PM	16	1	0

Figure 28

**Logs Considered:**

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/7/2017 2:47:33 PM	<a href="#">3230</a>	NTPLDTBLR38 / <a href="#">Tenabl...</a>	N/A	N/A	Tenable

**Event Type:** Information  
**Log Type:** Application  
**Category Id:** 0

**Description:**  
 logout: 0  
 enabled: 1  
 uuid\_id: de12b754-ba64-4a1b-b430-13d98f3b9c5c  
 login\_fail\_total: 1  
 login\_fail\_count: 0  
 last\_login\_attempt: 8/4/2017 5:13:14 PM  
 lastlogin: 8/4/2017 5:28:49 PM  
 permissions: 16  
 type: local  
 name: Jiren  
 email: jiren.rakota@adf.com  
 username: jiren.rakota@adf.com

Figure 29

## Import Tenable.io knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Knowledge Objects
- Flex Reports
- Parsing Rule

**NOTE:** Export knowledge pack items in the following sequence:

- Knowledge Objects
- Flex Reports
- Parsing rule

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



Figure 30

3. Click the **Import** tab.

## Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **All Tenable.io group of Knowledge object.etko**, and then click **Import** button

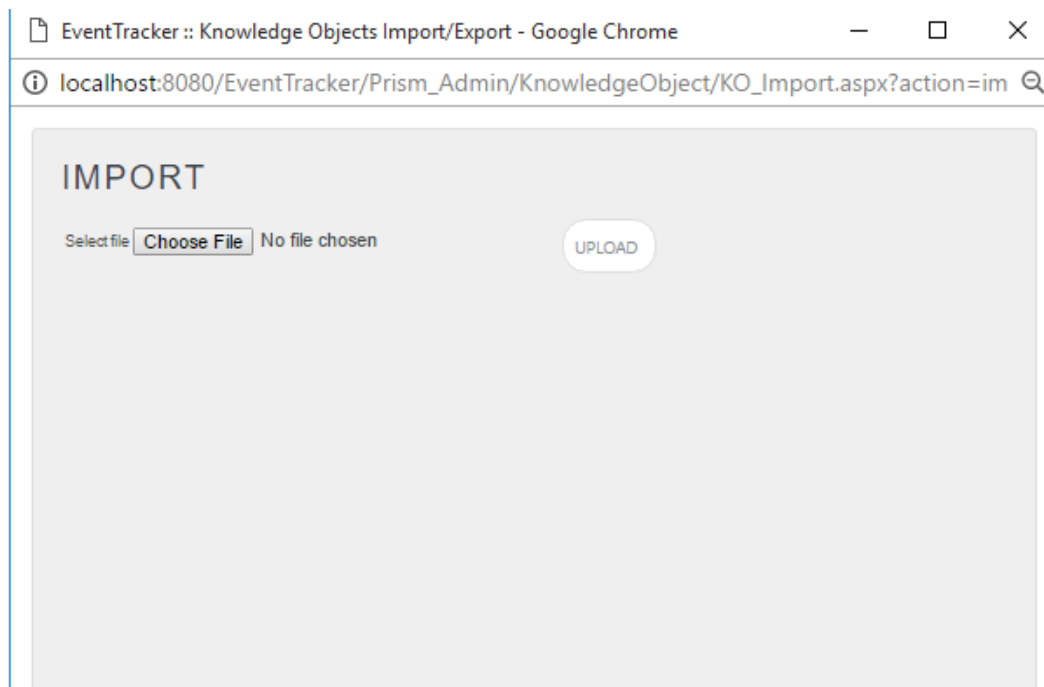


Figure 31

3. Choose the Knowledge objects that needs to be imported and click on **upload**.

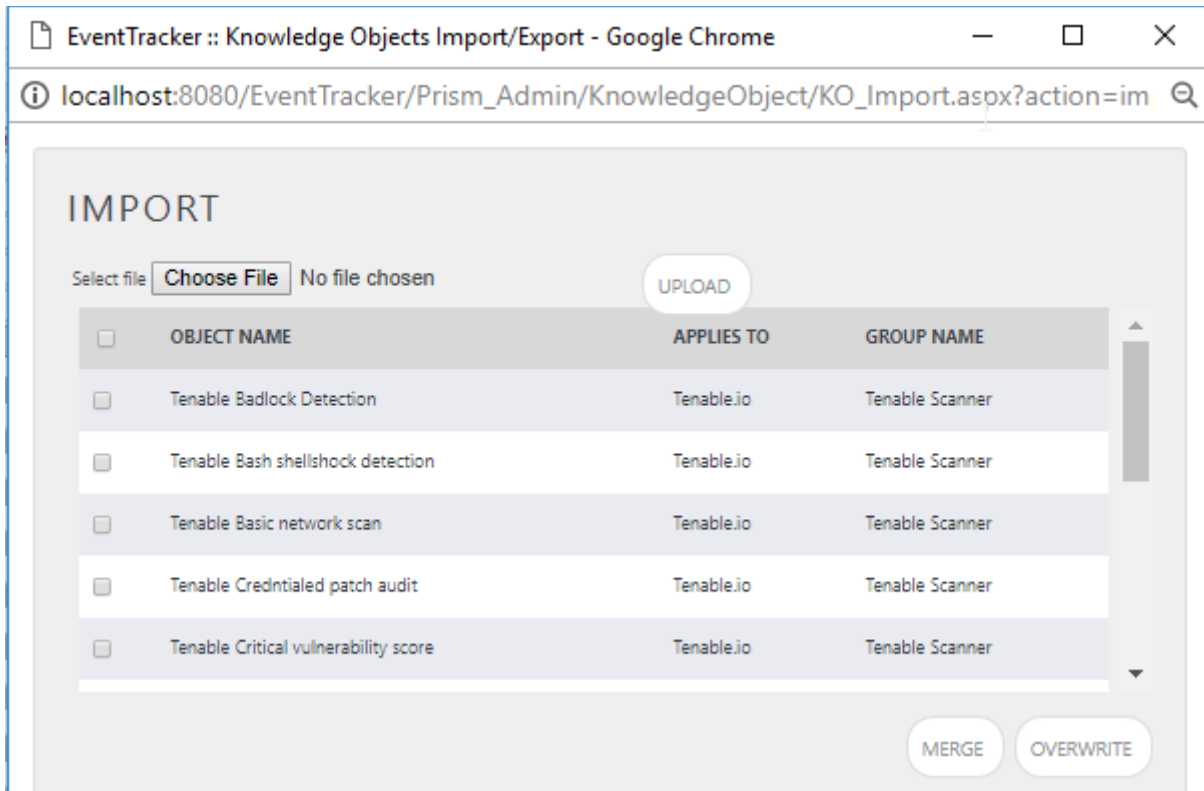


Figure 32

4. Knowledge objects are now imported successfully.

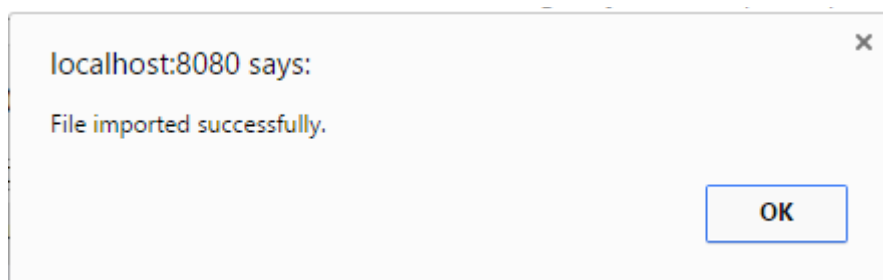



Figure 33

## Flex Reports

1. Click **Reports** option, and then click the browse  button.
2. Locate the **All Tenable.iogroup of flex reports.issch** file, and then click the **Open** button.

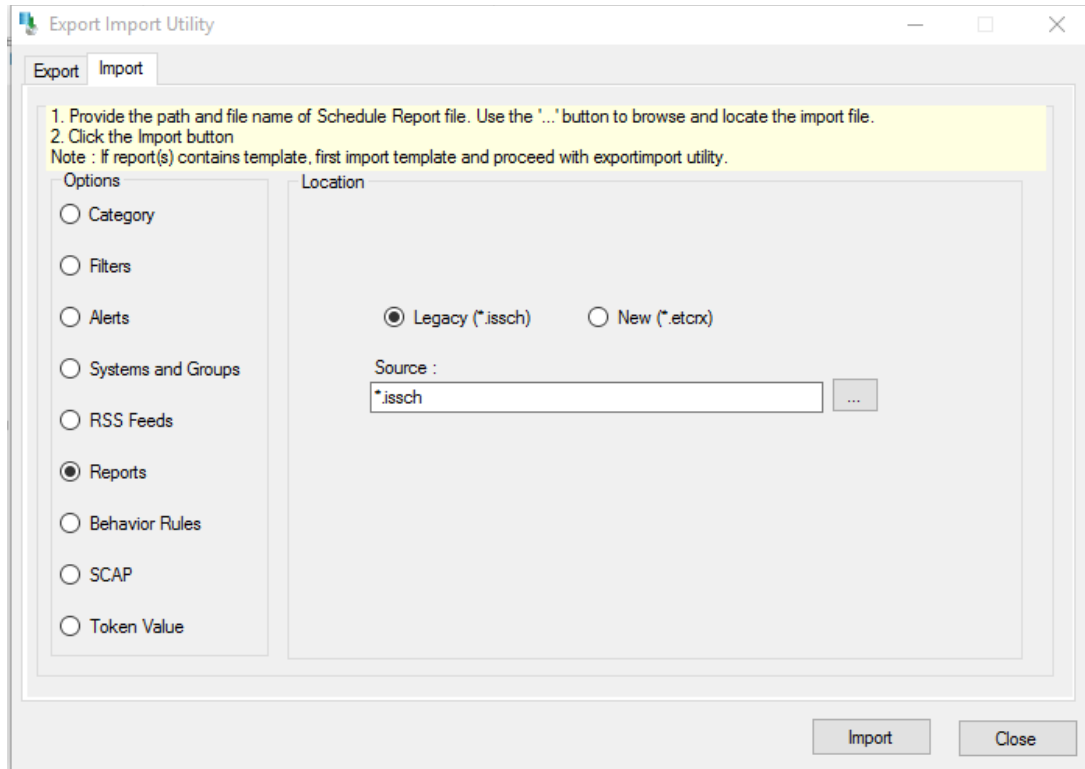


Figure 34

3. Click the **Import** button to import the reports. EventTracker displays success message.

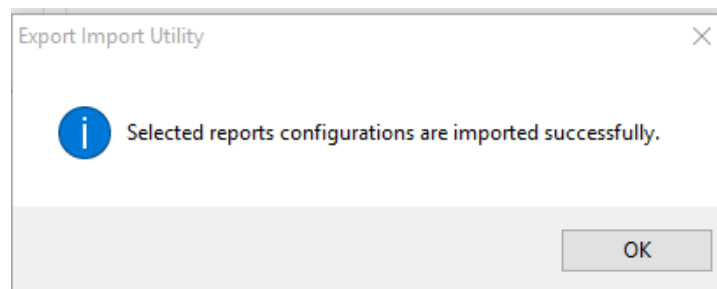



Figure 35

## Parsing Rule

1. Click **Token Value** option, and then click the browse  button.
2. Locate the **All Tenable.io group of Token Value.issch** file, and then click the **Open** button.

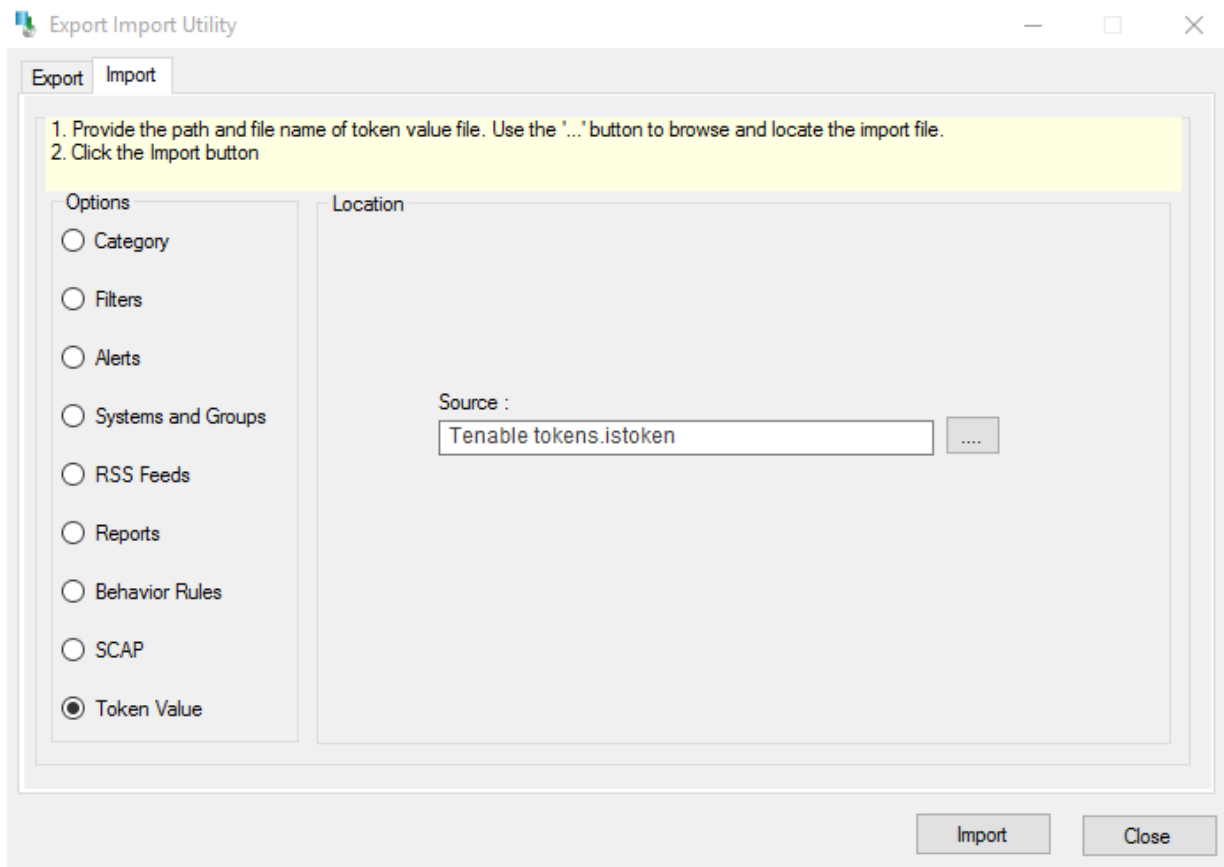


Figure 36

4. Click the **Import** button to import the tokens. EventTracker displays success message.

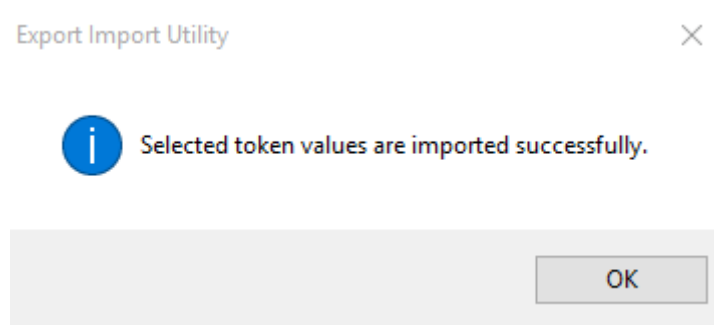


Figure 37

# Verify Tenable.io knowledge pack in EventTracker

## Knowledge Objects

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.

In the **Knowledge Object tree**, expand **Tenable.io** group folder to see the imported Knowledge objects.

The screenshot displays the 'KNOWLEDGE OBJECTS' interface. On the left, a 'GROUPS' sidebar lists various categories, with 'Tenable Scanner' expanded to show a list of objects including 'Tenable Badlock De...', 'Tenable Bash shells...', 'Tenable Basic netw...', 'Tenable Credntialed...', 'Tenable Critical vuln...', 'Tenable Drown Det...', 'Tenable Host Disco...', 'Tenable Malware D...', and 'TenableScap and O...'. The main panel shows the details for the 'Tenable Badlock Detection' object. It includes a search bar at the top, a 'GROUPS' sidebar, and a main content area with the following sections:

- OBJECT NAME:** Tenable Badlock Detection
- APPLIES TO:** Tenable.io
- RULES:** A table with columns: TITLE, LOG TYPE, EVENT SOURCE, EVENT ID, EVENT TYPE. One rule is listed: 'Tenable-Badlock Detection' with event source 'Tenable' and event ID '3230'.
- MESSAGE SIGNATURE:** (?s)Plugin\sID:\*(CVE\sCVE\(-2015\)-5370)(CVE\(-2016\)-2110)(CVE\(-2016\)-2111)(CVE\(-2016\)-2112)(CVE\(-2016\)-2113),...
- MESSAGE EXCEPTION:**
- EXPRESSIONS:** A table with columns: EXPRESSION TYPE, FORMAT STRING, EXPRESSION 1, EXPRESSION 2. One expression is listed: 'Key Value Delimiter' with format string ':' and expression 2 '\n'.

Figure 38

## Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**Tenable Scanner**', and then click the **Search** button.  
EventTracker displays Flex reports of '**Tenable Scanner**'



## REPORTS CONFIGURATION

Scheduled
  Queued
  Defined

Search

### REPORT GROUPS

- Sonicwall UTM
- Sophos Enterprise Co...
- Sophos UTM
- Suricata IDS
- Syslog
- Tenable.io
- Teradata Database
- Terminal Services
- Trend Micro Deep Sec...
- Trend Micro InterSca...

### REPORTS CONFIGURATION : TENABLE.IO

Total: 9

<input type="checkbox"/>	TITLE	CREATED ON	MODIFIED ON	
<input type="checkbox"/>	Tenable-User activity	8/4/2017 6:02:47 PM	8/4/2017 6:02:47 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable -Badlock detection	8/3/2017 5:48:22 PM	8/3/2017 5:56:52 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Credentialed patch audit	8/3/2017 5:48:22 PM	8/3/2017 6:04:27 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Host discovery	8/3/2017 5:48:22 PM	8/3/2017 6:11:05 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Malware detection	8/3/2017 5:48:22 PM	8/3/2017 6:51:08 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Bash shellshock detection	8/3/2017 5:48:22 PM	8/3/2017 6:16:05 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Drown detection	8/3/2017 5:48:22 PM	8/3/2017 6:20:58 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Scap and oval auditing	8/3/2017 5:48:22 PM	8/4/2017 12:24:10 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	Tenable-Critical vulnerability score	8/3/2017 5:48:22 PM	8/3/2017 6:21:37 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="+"/> <input type="button" value="🗑️"/>

Figure 39

## Parsing Rule

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Parsing rule**.

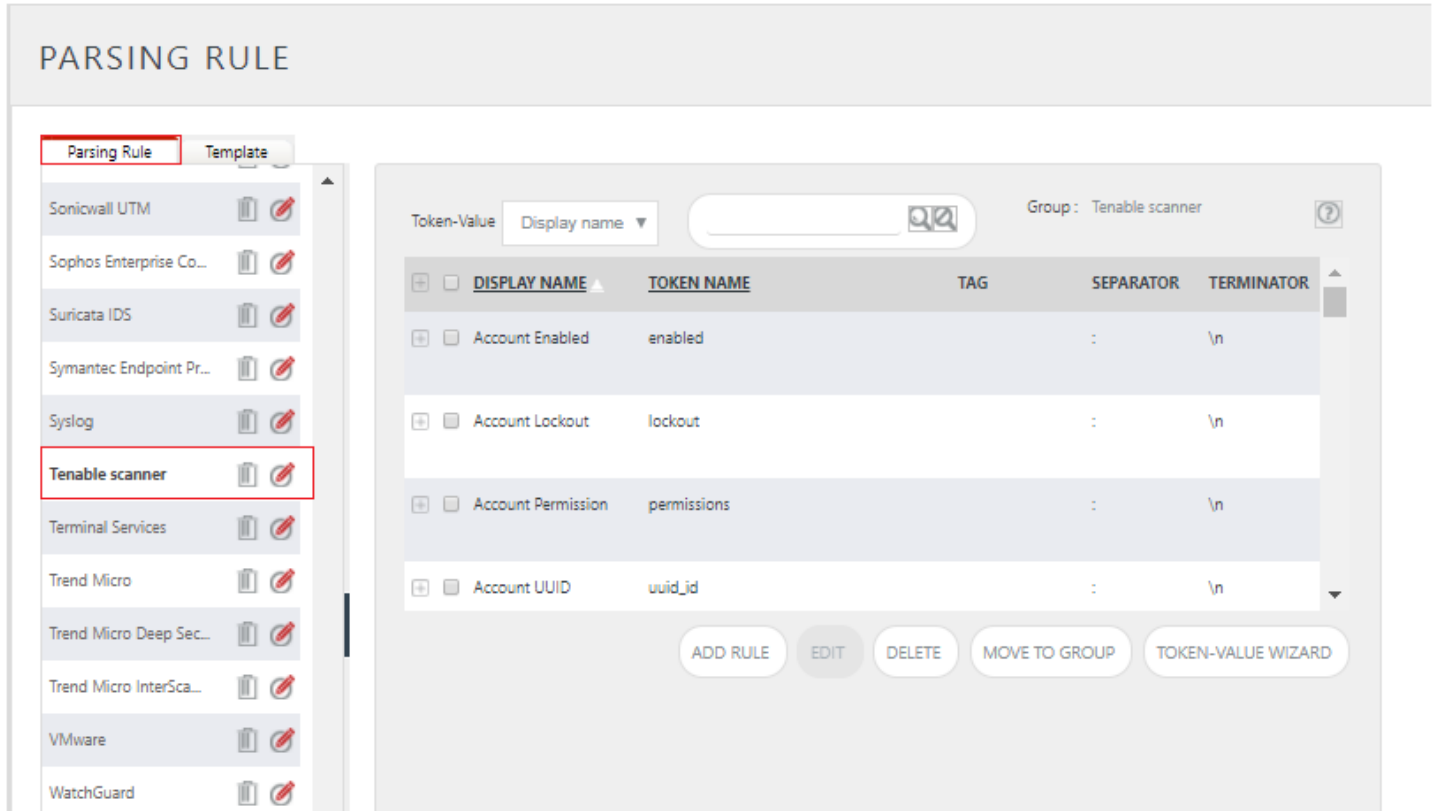


Figure 40

## Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

### Schedule Reports

1. Open **EventTracker** in browser and logon.

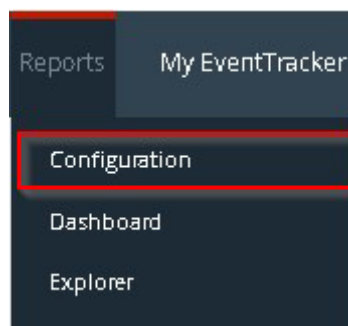



Figure 41

2. Navigate to **Reports>Configuration**.
3. Select **Tenable.io** in report groups. Check **Defined** dialog box.

The screenshot shows the 'REPORTS CONFIGURATION' page. At the top, there are radio buttons for 'Scheduled', 'Queued', and 'Defined', with 'Defined' selected. A search bar is on the right. On the left, a 'REPORT GROUPS' sidebar lists various groups, with 'Tenable.io' highlighted in a red box. The main area shows a table of reports for 'TENABLE.IO', with a 'Total: 9' badge in the top right. The table has columns for 'TITLE', 'CREATED ON', and 'MODIFIED ON'. A red box highlights the first three rows of the table.

TITLE	CREATED ON	MODIFIED ON
Tenable-User activity	8/4/2017 6:02:47 PM	8/4/2017 6:02:47 PM
Tenable -Badlock detection	8/3/2017 5:48:22 PM	8/3/2017 5:56:52 PM
Tenable-Credentialed patch audit	8/3/2017 5:48:22 PM	8/3/2017 6:04:27 PM
Tenable-Host discovery	8/3/2017 5:48:22 PM	8/3/2017 6:11:05 PM
Tenable-Malware detection	8/3/2017 5:48:22 PM	8/3/2017 6:51:08 PM
Tenable-Bash shellshock detection	8/3/2017 5:48:22 PM	8/3/2017 6:16:05 PM
Tenable-Drown detection	8/3/2017 5:48:22 PM	8/3/2017 6:20:58 PM
Tenable-Scap and oval auditing	8/3/2017 5:48:22 PM	8/4/2017 12:24:10 PM
Tenable-Critical vulnerability score	8/3/2017 5:48:22 PM	8/3/2017 6:21:37 PM

Figure 42

4. Click on 'schedule'  to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

## REPORT WIZARD

TITLE: TENABLE-USER ACTIVITY  
LOGS

CANCEL < BACK NEXT >

Review cost details and configure the publishing options. Step 8 of 10

### DISK COST ANALYSIS

Estimated time for completion: 00:00:44(HH:MM:SS)  
 Number of cab(s) to be processed: 7  
 Available disk space: 167 GB  
 Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)

Deliver results via E-mail  
 Notify results via E-mail

To E-mail:  [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:

Show in:

Persist data in Eventvault Explorer

Figure 43

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

## Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

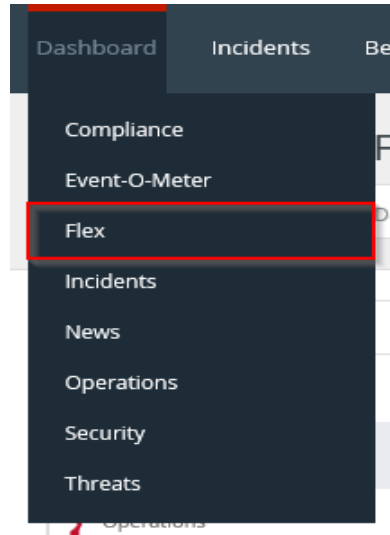


Figure 44

2. Navigate to **Dashboard>Flex**.  
Flex Dashboard pane is shown.

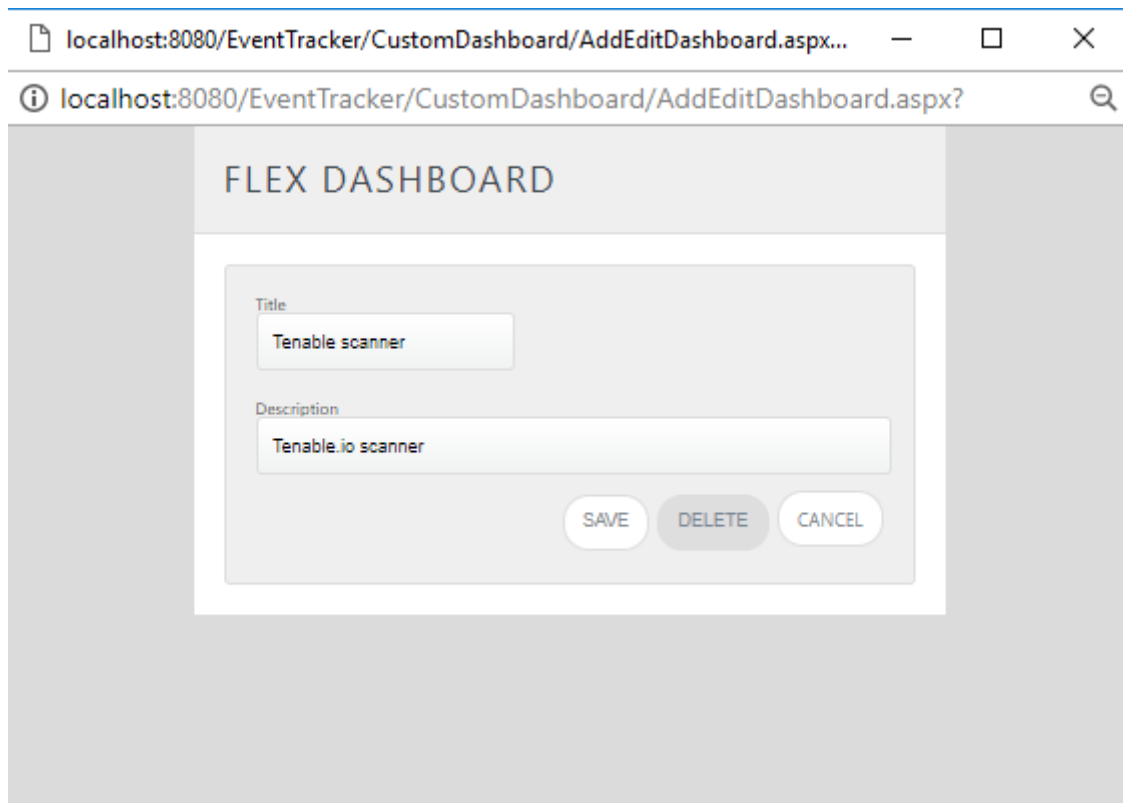



Figure 45

3. Fill suitable title and description and click **Save** button.
4. Click  to configure a new flex dashlet. Widget configuration pane is shown.

## WIDGET CONFIGURATION

**WIDGET TITLE**

**NOTE**

**DATA SOURCE**

**CHART TYPE**    **DURATION**    **VALUE FIELD SETTING**    **AS OF**  
           

**AXIS LABELS [X-AXIS]**    **LABEL TEXT**  
   

**VALUES [Y-AXIS]**    **VALUE TEXT**  
   

**FILTER**    **FILTER VALUES**  
   

**LEGEND (SERIES)**    **SELECT**  
   

1/1/1970 5:30:00 AM     8/4/2017 5:05:16 PM     8/4/2017 5:28:49 PM

Figure 46

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.

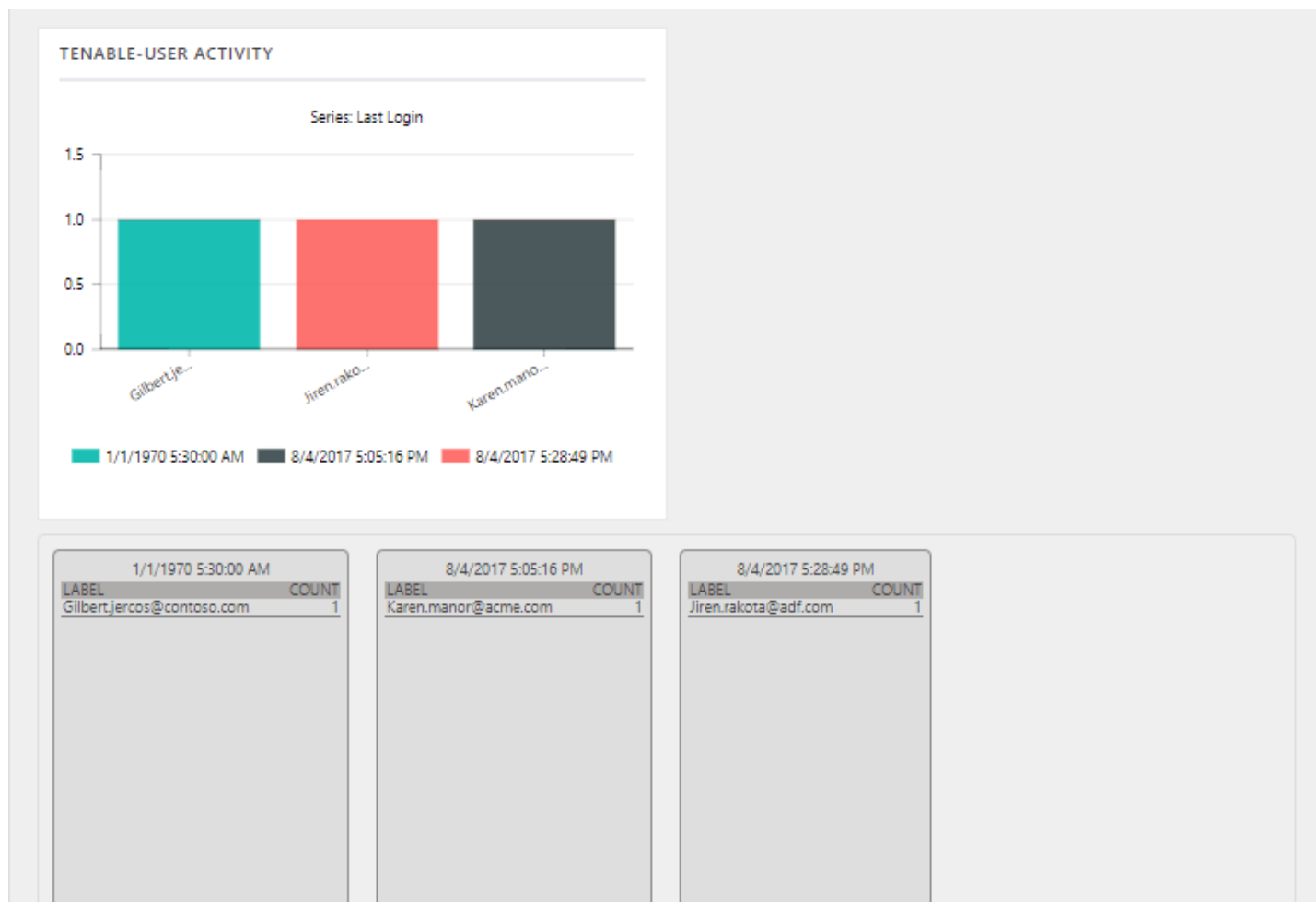


Figure 47

14. If satisfied, click **Configure** button.

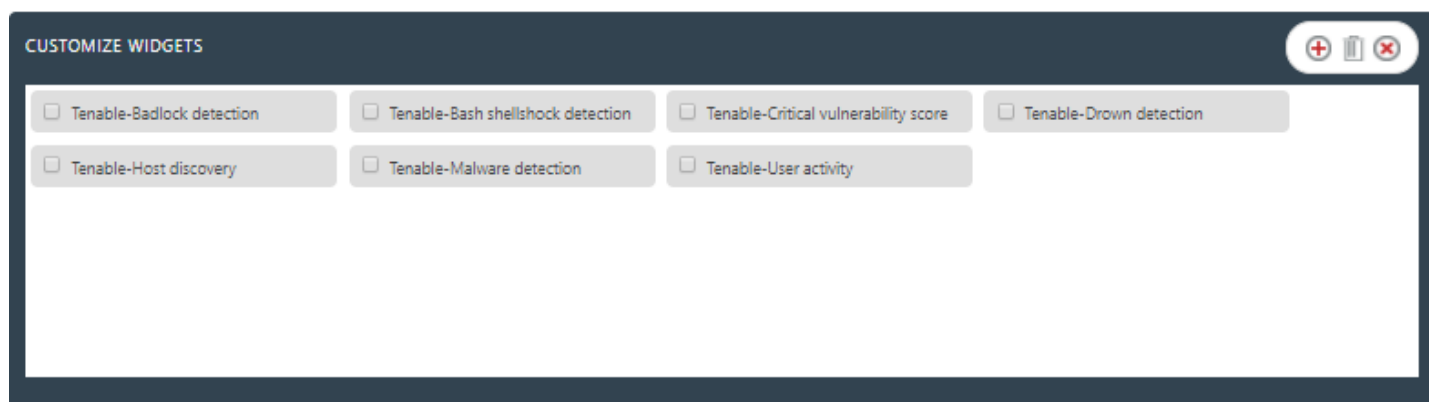



Figure 48

15. Click 'customize'  to locate and choose created dashlet.

16. Click  to add dashlet to earlier created dashboard.

## Sample Flex Dashboards

For below dashboard

### Report Name: Tenable-Credentialed Patch Audit

- **WIDGET TITLE:** Tenable-Credentialed Patch Audit  
**CHART TYPE:** Stacked Column  
**AXIS LABELS [X-AXIS]:** CVE  
**LEGEND:** Vulnerability description

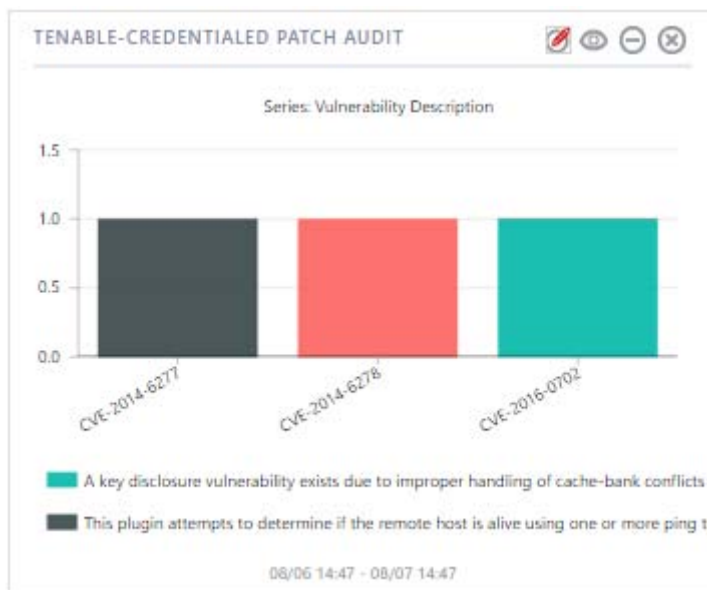


Figure 49



**Report Name: Tenable-Badlock Detection**

- **WIDGET TITLE:** Tenable-Badlock Detection  
**CHART TYPE:** Pie  
**AXIS LABELS [X-AXIS]:** CVE  
**LEGEND:** Host

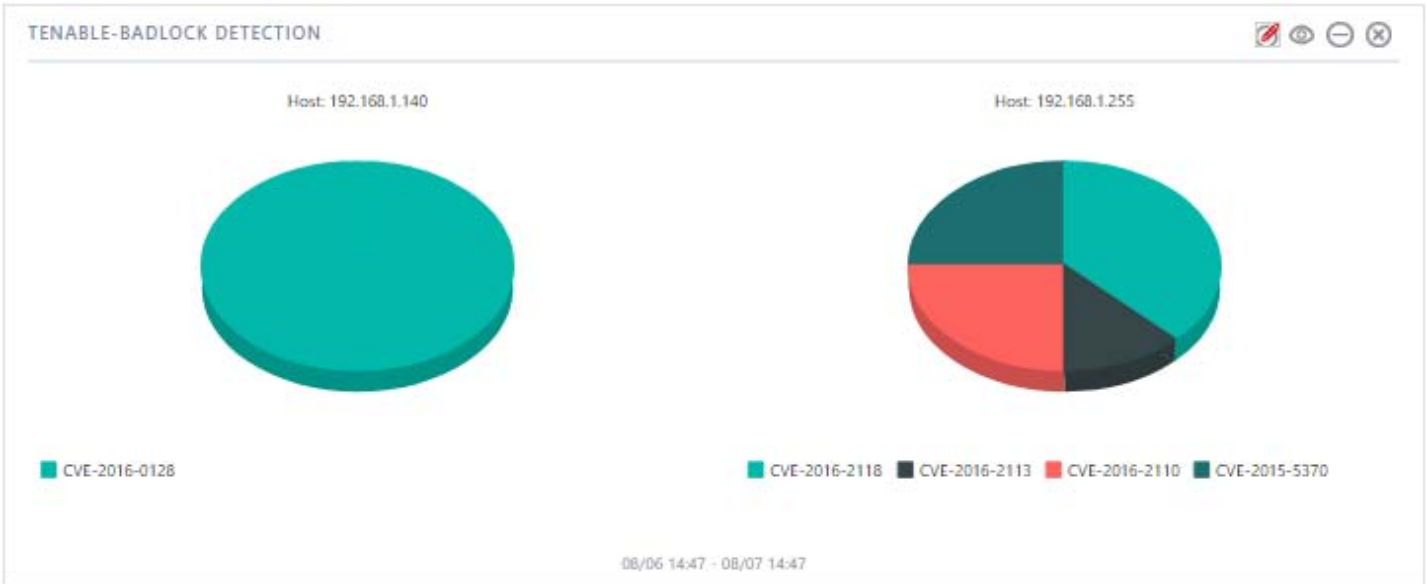


Figure 50

**Report Name: Tenable-Host Discovery**

- **WIDGET TITLE:** Tenable-Host Discovery  
**CHART TYPE:** Stacked Column  
**AXIS LABELS [X-AXIS]:** IP Address  
**LEGEND[SERIES]:** Message

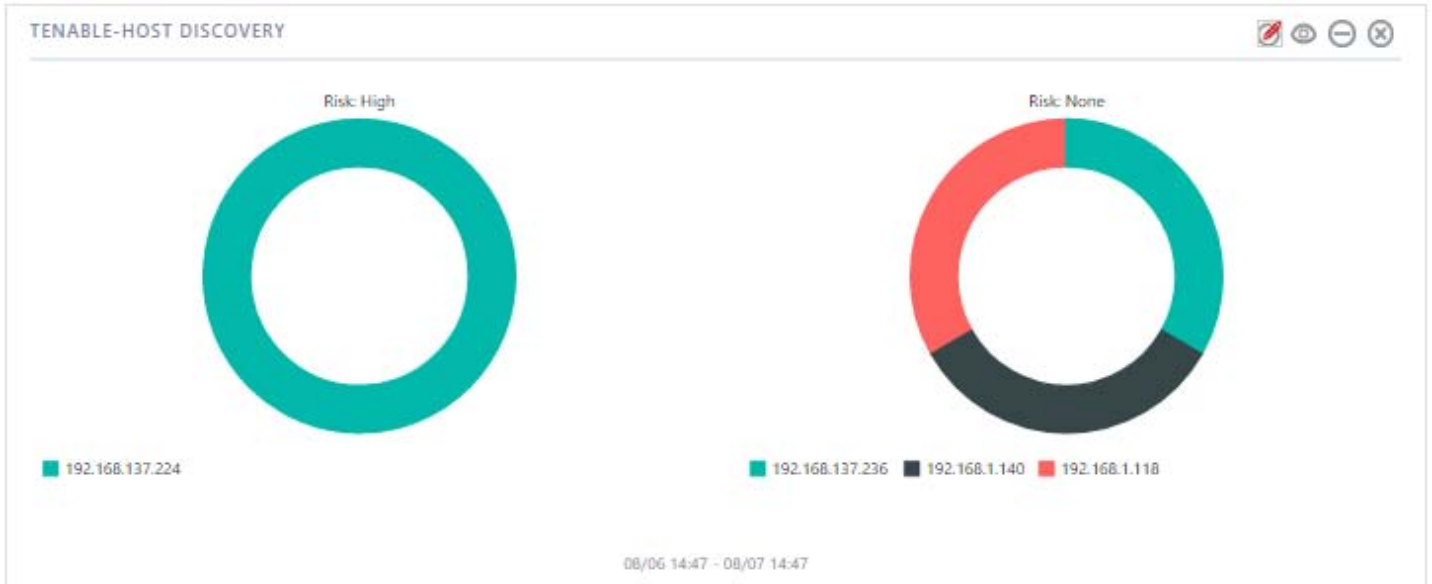


Figure 51

**Report Name: Tenable-Malware Detection**

- **WIDGET TITLE:** Tenable-Malware Detection  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** HOST  
**LEGEND:** Message

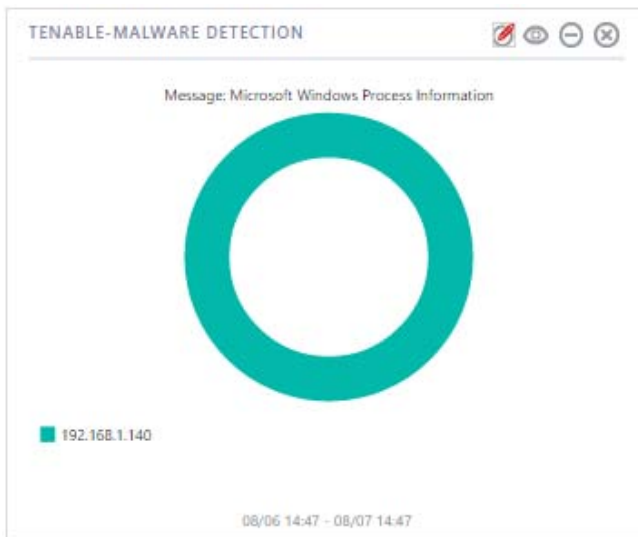


Figure 52

**Report Name: Tenable-Bash Shellshock Detection**

- **WIDGET TITLE:** Tenable-Bash Shellshock Detection  
**CHART TYPE:** Stacked Column  
**AXIS LABELS [X-AXIS]:** CVE  
**LEGEND:** Risk



Figure 53

**Report Name: Tenable-Drown Detection**

- **WIDGET TITLE:** Tenable- Drown Detection  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** CVE  
**LEGEND[SERIES]:** Risk

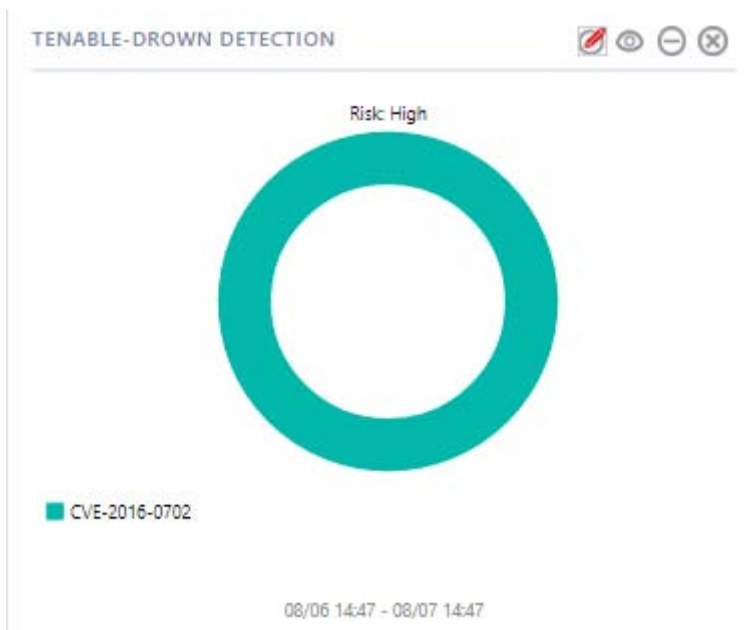


Figure 54

**Report Name: Scap and Oval Auditing**

- **WIDGET TITLE:** Tenable- Scap and Oval Auditing  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Mac Address  
**LEGEND[SERIES]:** Severity

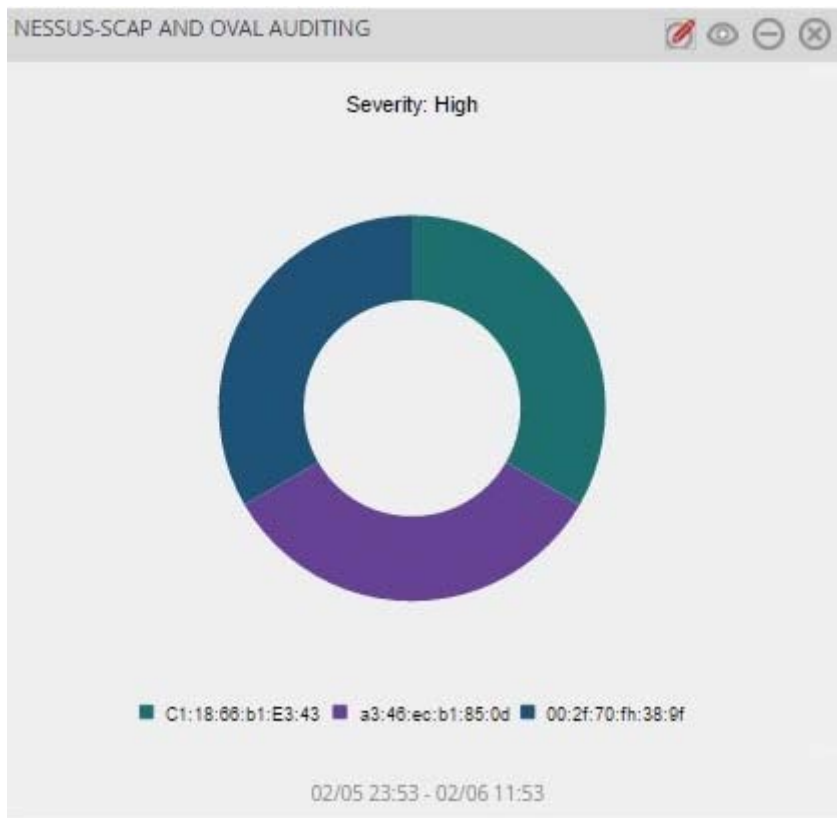


Figure 55

**Report Name: Critical vulnerability score**

- **WIDGET TITLE:** Critical vulnerability score  
**CHART TYPE:** PIE  
**AXIS LABELS [X-AXIS]:** CVE  
**LEGEND:** HOST

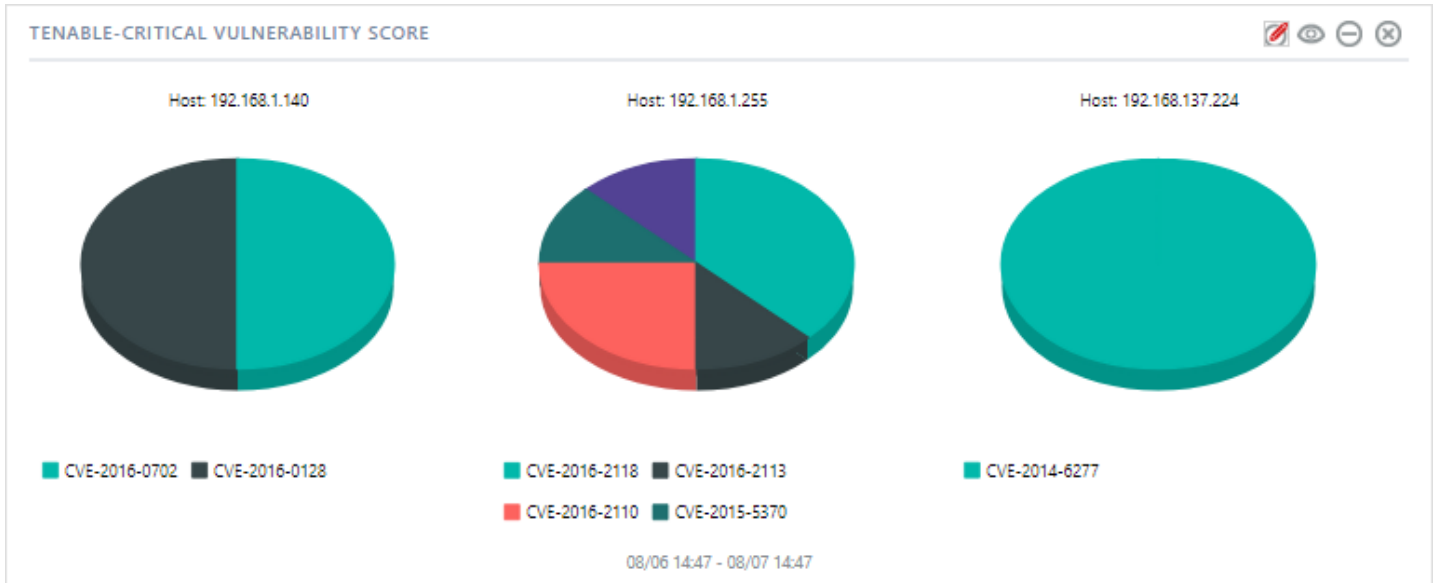


Figure 56