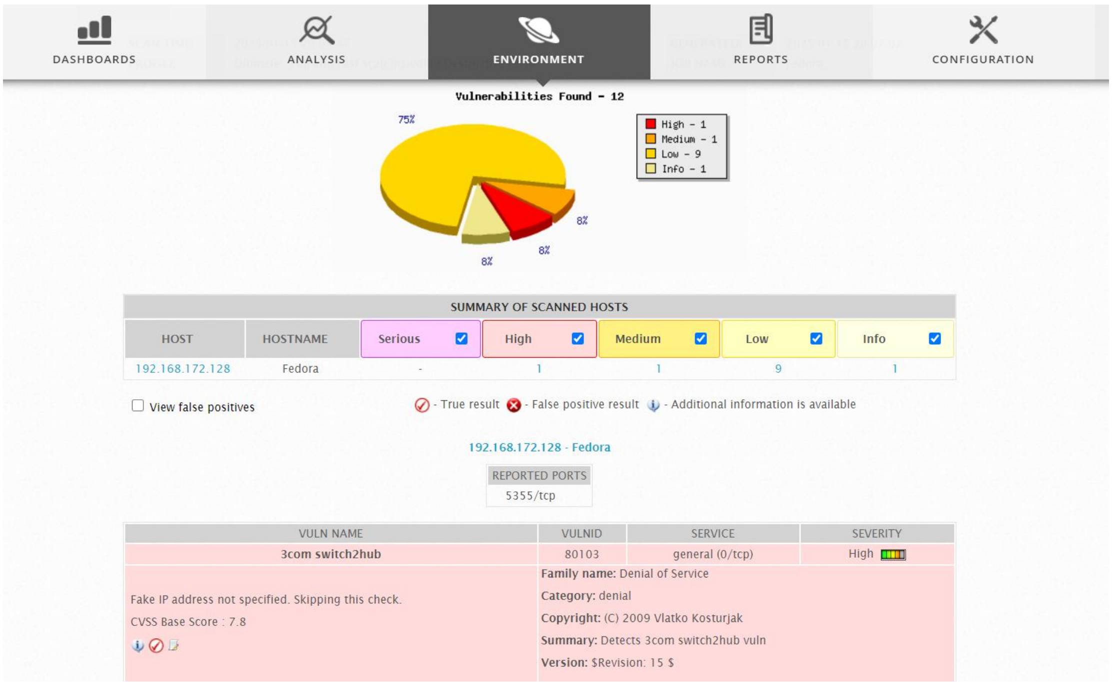
Security Fundamentals Assignment 1

ZHENGZHENG LI

1. Screenshots from Alienvault OSSIM that list the top CVSS results from a security assessment on two hosts:



SUMMARY OF SCANNED HOSTS

HOST	HOSTNAME	Serious ☑	High ☑	Medium ☑	Low ☑	Info ☑
192.168.172.128	Fedora	-	1	1	9	1

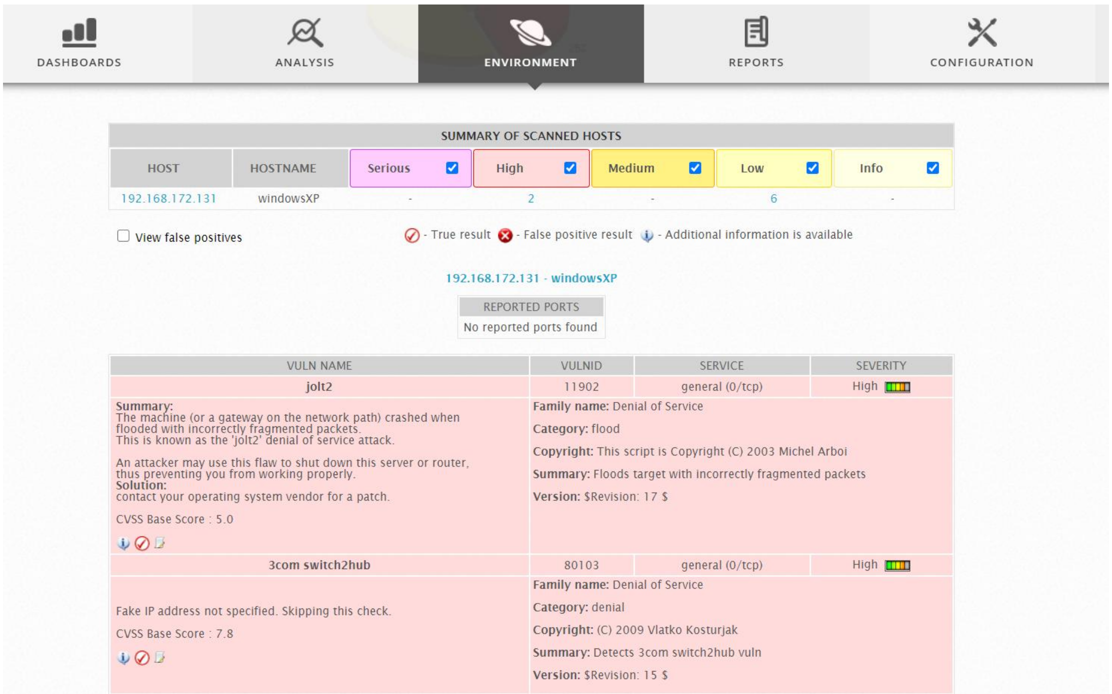
☐ View false positives

- True result - False positive result - Additional information is available

192.168.172.128 - Fedora

REPORTED PORTS
5355/tcp

VULN NAME	VULNID	SERVICE	SEVERITY
3com switch2hub	80103	general (0/tcp)	High
Fake IP address not specified. Skipping this check. CVSS Base Score : 7.8	Family name: Denial of Service Category: denial Copyright: (C) 2009 Vlatko Kosturjak Summary: Detects 3com switch2hub vuln Version: $Revision: 15 $		



SUMMARY OF SCANNED HOSTS

HOST	HOSTNAME	Serious ☑	High ☑	Medium ☑	Low ☑	Info ☑
192.168.172.131	windowsXP	-	2	-	6	-

☐ View false positives

- True result - False positive result - Additional information is available

192.168.172.131 - windowsXP

REPORTED PORTS
No reported ports found

VULN NAME	VULNID	SERVICE	SEVERITY
jolt2	11902	general (0/tcp)	High
Summary: The machine (or a gateway on the network path) crashed when flooded with incorrectly fragmented packets. This is known as the 'jolt2' denial of service attack. An attacker may use this flaw to shut down this server or router, thus preventing you from working properly. Solution: contact your operating system vendor for a patch. CVSS Base Score : 5.0	Family name: Denial of Service Category: flood Copyright: This script is Copyright (C) 2003 Michel Arboi Summary: Floods target with incorrectly fragmented packets Version: $Revision: 17 $		
3com switch2hub	80103	general (0/tcp)	High
Fake IP address not specified. Skipping this check. CVSS Base Score : 7.8	Family name: Denial of Service Category: denial Copyright: (C) 2009 Vlatko Kosturjak Summary: Detects 3com switch2hub vuln Version: $Revision: 15 $		

2. What types of devices can Alienvault OSSIM monitor?

AlienVault OSSIM can monitor the following types of devices:

Servers: Includes physical or virtual servers running Windows or Linux.

Network Devices: Such as routers, switches, and firewalls.

Security Devices: Includes IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems).

Applications and Databases: Such as web applications and database servers.

Cloud Services: Resources on platforms like AWS, Azure, etc.

Endpoint Devices: Such as workstations and laptops.

3. Is it agent-based or agentless?

AlienVault OSSIM supports both agent-based and agentless modes:

Agent-based: By deploying HIDS agents (e.g., OSSEC) on hosts to collect detailed system information and event logs.

Agentless: Through network traffic monitoring and log collection for device status analysis.

4. What are the differences between the free and paid version?

The key differences between the free OSSIM and paid USM Anywhere versions are:

Free OSSIM:

- Provides basic SIEM features like event correlation, vulnerability assessment, and HIDS support.
- Lacks support for cloud services and machine learning-based analytics.
- Only community support is available; no official technical support.

Paid USM Anywhere:

- Supports cloud platform monitoring (e.g., AWS, Azure, and Google Cloud).
- Offers advanced threat intelligence and automated response features.
- Includes professional technical support.

5. List 3 other commercial SIEM products on the market that provide similar functionality to Alienvault OSSIM.

Other commercial SIEM products with similar functionalities include:

Splunk Enterprise Security: A widely-used enterprise-grade SIEM platform with powerful log analysis and data visualization capabilities.

IBM QRadar: A sophisticated SIEM solution focusing on threat detection and incident management, suitable for enterprise-level networks.

ArcSight (Micro Focus): An enterprise-grade solution providing real-time threat detection and incident management, designed for complex IT environments.