tenable.sc™

Remediation Instructions by Host Report (Scan: External Scan - Gary Request)

November 29, 2021 at 7:21pm UTC

Sable Cantus [scantus@riohondo.edu]
MASTER ORGANIZATION

tenable

Table of Contents

About This Report

Identifying vulnerable hosts in a network is only the first step in securing an organization. Unaddressed vulnerabilities on hosts can provide attackers with easier access to an otherwise secure network. Determining and implementing remediation measures is key to properly securing any network. By leveraging the capabilities of SecurityCenter, Nessus, and the Passive Vulnerability Scanner (PVS), security teams can more easily identify hosts with vulnerabilities requiring remediation in order to more effectively secure their network.

The Remediation Instructions by Host report provides detailed information on the most vulnerable hosts identified on the network. The report is organized by plugin type (Active, Passive, and Compliance) and broken down by host. For each of the top 20 most vulnerable hosts, detailed steps to mitigate the risk of the vulnerabilities, including CVE, BID, and vendor knowledgebase articles, are provided. Additionally, this report provides information about the top services and ports on each vulnerable host.

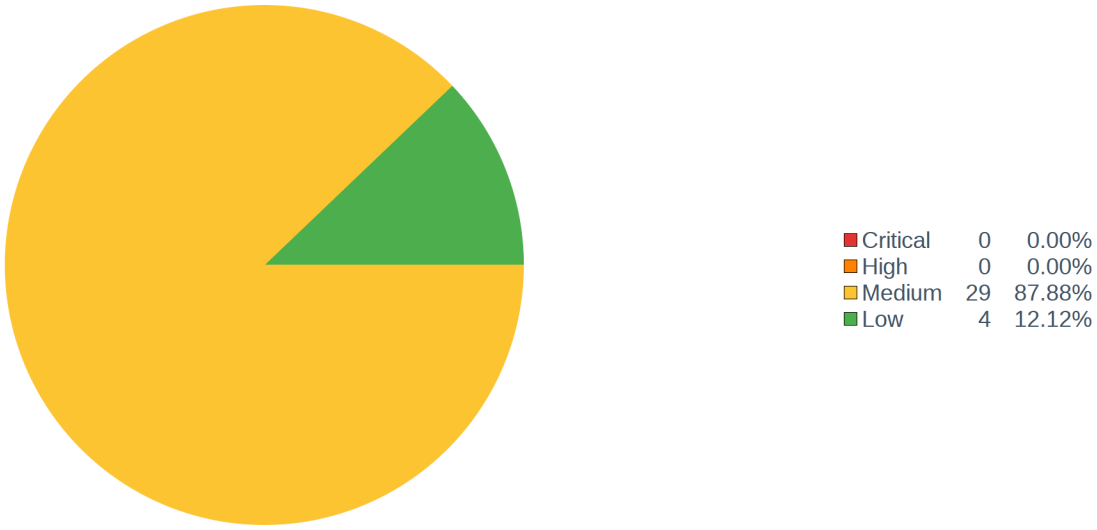
The chapters in this report provide distinct views of the vulnerable hosts detected on the network. Each chapter focuses on a specific plugin type: active, passive, or compliance. For each type, the 20 most vulnerable hosts and suggested steps to remediate vulnerabilities on them are detailed. Security teams can use these chapters to understand the vulnerable hosts that could impact their network and implement the steps necessary for remediation.

Executive Summary

This chapter provides an overview of the vulnerability statuses of hosts covered in this report. The topics addressed include active vulnerabilities, passive vulnerabilities, and compliance checks.

The Active Vulnerability Summary pie chart depicts the breakdown of vulnerability severities detected by active scanning. The Active Vulnerability Summary table presents an overview of the active vulnerabilities detected within an organization's network by subnet. These components can be used to quickly understand the balance of severities found on the network by Nessus vulnerability scans.

Active Vulnerability Summary

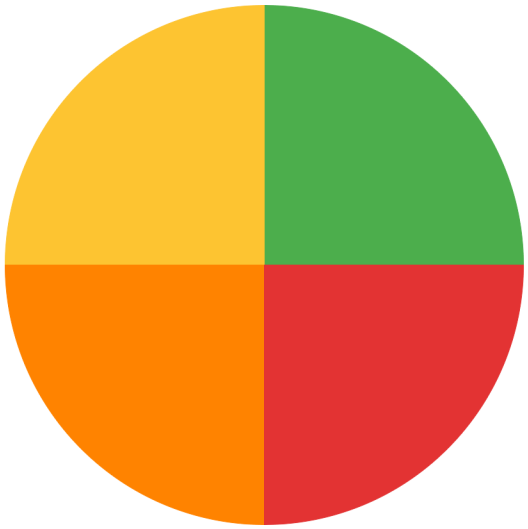


Active Vulnerability Summary

IP Address	Low	Med.	High	Crit.	Total	Vulns
207.233.58.0/24	4	29	0	0	33	29 4

The Passive Vulnerability Summary pie chart depicts the breakdown of vulnerability severities detected by passive scanning. The Passive Vulnerability Summary table presents an overview of the active vulnerabilities detected within an organization's network by subnet. These components can be used to quickly understand the balance of severities found on the network by passive vulnerability scans.

Passive Vulnerability Summary



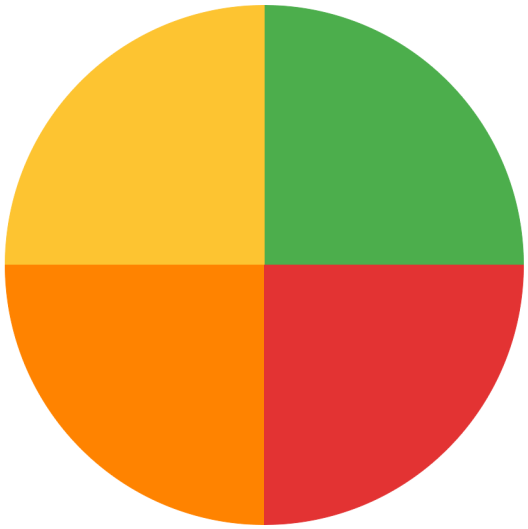
Critical	0	25.00 %
High	0	25.00 %
Medium	0	25.00 %
Low	0	25.00 %

Passive Vulnerability Summary

IP Address	Low	Med.	High	Crit.	Total	Vulns

The Compliance Summary Pie Chart depicts the breakdown of vulnerability severities detected during compliance checks. A high severity is assigned to failed compliance checks and a medium severity is assigned to compliance checks that require manual verification. The Compliance Summary table presents an overview of compliance checks applied within an organization's network by subnet. These components can be used to quickly understand the balance of severities found on the network by Nessus vulnerability scans.

Compliance Summary



Critical	0	25.00 %
High	0	25.00 %
Medium	0	25.00 %
Low	0	25.00 %

Compliance Summary

IP Address	Low	Med.	High	Crit.	Total	Vulns

Active Remediation Instructions by Host

This chapter provides a top 20 summary of the most vulnerable hosts discovered through active scanning. Active vulnerability scanning uses Nessus to send packets to target machines, providing a snapshot of the network services and applications installed. Active scanning also determines whether vulnerabilities are present. Active scanning can perform highly accurate patch, configuration, and vulnerability audits across many systems, including Unix, Linux, Windows, network devices, and database systems.

Top 20 Host Summary

IP Address	DNS Name	OS CPE	MAC Address	Score	Total	Vulns

This section uses an iterator to provide detailed information about each of the top 20 most vulnerable hosts by score. The vulnerability score for each host is calculated by totaling the count of vulnerabilities at each severity level then multiplying it by the severity score. The default severity scores are: Info - 0, Low – 1, Medium – 3, High – 10, Critical – 40. Administrators can customize the severity scores as necessary. For each host, several components are included.

The Vulnerability Summary pie chart shows the ratio of vulnerabilities by severity detected on that host.

The Top Services Discovered table provides a list of the top 20 services identified by Nessus. The Nessus Service Detection plugin (ID 22964) aims to fingerprint all services it encounters. SecurityCenter can process this information and create a summary of unique services discovered by Nessus.

The Top Port Findings table provides a summary of the top ports in use is displayed for all matched vulnerabilities. Each port has its count of vulnerabilities as well as a breakdown for each severity level.

The Top 10 Critical Severity Vulnerabilities List provides a table of the top critical severity vulnerabilities found on that host. The table displays the name, severity level and count of each vulnerability.

The Top 10 Critical Severity Remediation Plan table provides detailed information on each of the top 10 critical severity vulnerabilities and how to remediate them.

The Top 10 High Severity Vulnerabilities List provides a table of the top high severity vulnerabilities. The table displays the name, severity level and count.

The Top 10 High Severity Remediation Plan table provides detailed information on each of the top 10 high severity vulnerabilities and how to remediate them.

Passive Remediation Instructions by Host

This chapter provides a top 20 summary of the most vulnerable hosts discovered through passive scanning. The Passive Vulnerability Scanner (PVS) is an advanced network monitoring application designed to detect vulnerabilities on the network by listening to network communications. Through passive monitoring, PVS can reveal devices and software on the network that are not authorized, or that may indicate a network compromise.

Top 20 Host Summary

IP Address	DNS Name	OS CPE	MAC Address	Score	Total	Vulns

This section uses an iterator to provide detailed information about each of the top 20 most vulnerable hosts by score. The vulnerability score for each host is calculated by totaling the count of vulnerabilities at each severity level then multiplying it by the severity score. The default severity scores are: Info - 0, Low – 1, Medium – 3, High – 10, Critical – 40. Administrators can customize the severity scores as necessary. For each host, several components are included.

The Vulnerability Summary pie chart shows the ratio of vulnerabilities by severity detected on that host.

The Top Port Findings table provides a summary of the top ports in use is displayed for all matched vulnerabilities. Each port has its count of vulnerabilities as well as a breakdown for each severity level.

The Top 10 Critical Severity Vulnerabilities List provides a table of the top critical severity vulnerabilities found on that host. The table displays the name, severity level and count of each vulnerability.

The Top 10 Critical Severity Remediation Plan table provides detailed information on each of the top 10 critical severity vulnerabilities and how to remediate them.

The Top 10 High Severity Vulnerabilities List provides a table of the top high severity vulnerabilities. The table displays the name, severity level and count.

The Top 10 High Severity Remediation Plan table provides detailed information on each of the top 10 high severity vulnerabilities and how to remediate them.

Compliance Remediation Instructions by Host

This chapter provides a top 20 summary of compliance check failures and checks that require manual verification by host, which are reported through performing scans with audit files in SecurityCenter. The compliance checks may vary in importance, depending on the environment. In this report, the checks that failed are listed as high severity and checks that require manual verification are listed as medium severity.

Top 20 Host Summary

IP Address	DNS Name	OS CPE	MAC Address	Score	Total	Vulns

This section uses an iterator to provide detailed information about each of the top 20 hosts with the highest compliance failure rates by score. The vulnerability score for each host is calculated by totaling the count of vulnerabilities at each severity level then multiplying it by the severity score. The default severity scores are: Info - 0, Low – 1, Medium – 3, High – 10, Critical – 40. Administrators can customize the severity scores as necessary. For each host, several components are included.

The Audit Summary pie chart shows the ratio of audit checks by severity detected on that host. An information severity designates a passed audit check, a medium severity requires manual verification, and a high severity is assigned for failed audit checks. The pie chart legend provides a percentage and a severity count of identified vulnerabilities.

The Top 10 Failed Audit Checks List provides a table of the top high severity compliance vulnerabilities. The table displays the name, severity level and count.

The Top 10 Failed Audit Checks Remediation Plan provides detailed information on each of the top 10 failed compliance checks and how to remediate them.