

Metasploit Pro



PCI-DSS version 3.2.1
Compliance Findings

Report generated:

Fri, 5 Mar 2021 13:11:46 +0530

Total Pages: 3

Executive Summary

This report is an appendix for a more complete PCI-DDS compliance audit, performed by Metasploit Pro from Rapid7, Inc. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

The table below summarizes the pass/fail status of each of the tested PCI compliance requirements.

Requirements Status Summary

PCI Requirement	Result
2.2.1	PASS
2.3	PASS
6.2	PASS
8.2	PASS
8.2.1	PASS
8.2.3	PASS
8.5	PASS

Hosts Status Summary

Host	Test status
10.70.43.235	PASS
124.4.204.21 (usa-cin-gsd-bus-pa-fw-02.genpact.com)	PASS

Detailed Findings

PCI Requirement 2.2.1

PASS

Description: Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers. http and https are considered the same service in this context.)

Results: All surveyed hosts satisfy this requirement.

PCI Requirement 2.3

PASS

Description: Encrypt all non-console administrative access such as browser/Web-based management tools.

Results: All surveyed hosts satisfy this requirement.

PCI Requirement 6.2

PASS

Description: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Results: All surveyed hosts satisfy this requirement.

PCI Requirement 8.2

PASS

Description: Employ at least one of these to authenticate all users: password or passphrase; or two-factor authentication (e.g., token devices, smart cards, biometrics, public keys).

Results: All surveyed hosts satisfy this requirement.

PCI Requirement 8.2.1

PASS

Description: Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

Results: All surveyed hosts satisfy this requirement.

PCI Requirement 8.2.3

PASS

Description: Passwords must require a minimum password length of at least seven characters and contain both numeric and alphabetic characters, or at least equivalent complexity and strength.

Results: All surveyed hosts satisfy this requirement.

PCI Requirement 8.5

PASS

Description: Do not use group, shared, or generic accounts and passwords, or other authentication methods.

Results: All surveyed hosts satisfy this requirement.