Security Assessment

Risk Report

CONFIDENTIALITY NOTE: The information contained in this report is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If you are not the client or addressee, you are strictly prohibited from reading, photocopying, distributing, or otherwise using this report or its contents in any way.

Scan Date: 2019/01/18

Prepared for: Your Customer / Prospect

Prepared by: Your Company Name

2021/02/03

Table of Contents

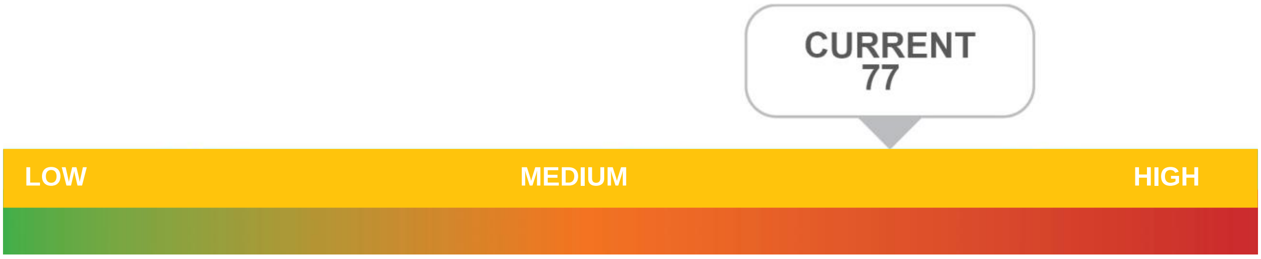
Discovery Tasks

The following discovery tasks were performed:

	TASK	DESCRIPTION
✓	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determines if controls are in place for user web browsing.
✓	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✓	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.
✓	Network Share Permissions	Documents access to file system shares.
✓	Domain Security Policy	Documents domain computer and domain controller security policies.
✓	Local Security Policy	Documents and assesses consistency of local security policies.

Risk Score

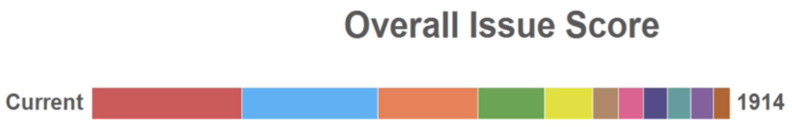
The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

Issues Summary

This section contains summary of issues detected during the Security Assessment. It is based on general industry-wide best practices and may indicate existing issues or points of interest. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Overall Issue Score: Risk Score x Number of Incidents = Total points: Total percent (%)

450 Medium External Vulnerabilities Detected (75 pts each)

Current Score: 75 pts x 6 = 450: 23.51%

Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.

Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

408 Screen lock time is > 15 minutes (68 pts each)

Current Score: 68 pts x 6 = 408: 21.32%

Issue: Even though screen lockout has been activated, extensive lockout times may lead to authorized access when users leave their computers.

Recommendation: Reduce screen lockout to 15 minutes or less on the specified computers.

300 Password complexity not enabled (75 pts each)

Current Score: 75 pts x 4 = 300: 15.67%

Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.

Recommendation: Enable password complexity to assure that network user account passwords are secure.

200

Compromised Passwords found on the Dark Web (50 pts each)

Current Score: 50 pts x 4 = 200: 10.45%

Issue: A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2019.

Recommendation: Ensure the compromised passwords are no longer in use. We recommend having all users reset their password as the extent of the compromise is difficult to assess. Only the first 5 per domain are listed here.

144

Automatic screen lock not turned on (72 pts each)

Current Score: 72 pts x 2 = 144: 7.52%

Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.

Recommendation: Enable automatic screen lock on the specified computers.

77

Account lockout disabled (77 pts each)

Current Score: 77 pts x 1 = 77: 4.02%

Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.

Recommendation: Enable account lockout for all users.

75

Passwords less than 8 characters allowed (75 pts each)

Current Score: 75 pts x 1 = 75: 3.92%

Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to more than 8 characters.

72

Password history not remembered for at least six passwords (72 pts each)

Current Score: 72 pts x 1 = 72: 3.76%

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

Recommendation: Increase password history to remember at least six passwords.

70 Maximum password age greater than 90 days (70 pts each)

Current Score: 70 pts x 1 = 70: 3.66%

Issue: Passwords that are not changed regularly are more vulnerable to attack and unauthorized use. Minimizing the allowed password age greatly reduces the window of time that a lost or stolen password poses a threat.

Recommendation: Modify the maximum password age to be 90 days or less.

68 Inconsistent password policy / Exceptions to password policy (68 pts each)

Current Score: 68 pts x 1 = 68: 3.55%

Issue: Password policies are not consistently applied from one computer to the next. A consistently applied password policy ensures adherence to password best practices.

Recommendation: Eliminate inconsistencies and exceptions to the password policy.

50 Open or insecure WiFi protocols available (50 pts each)

Current Score: 50 pts x 1 = 50: 2.61%

Issue: Open or insecure WiFi protocols may allow an attacker access to the company's network and resources.

Recommendation: Ensure company's WiFi is secure and discourage the use of any open WiFi connections.

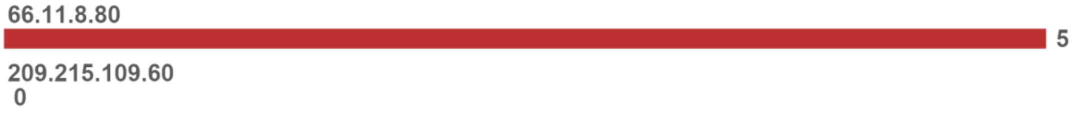
External Vulnerabilities

High (0) | Medium (6) | Low (1)

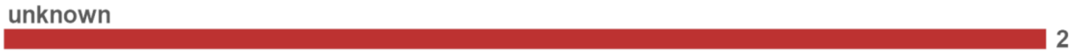
Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	FALSE	HIGHEST CVSS
209.215.109.60 (60.32.109.215.209.in-addr.arpa)	0	0	0	0	0	0.0
66.11.8.80 (66-11-8-80.orf.contbb.net)	3	0	6	1	0	5.0
Total: 2	3	0	6	1	0	5.0

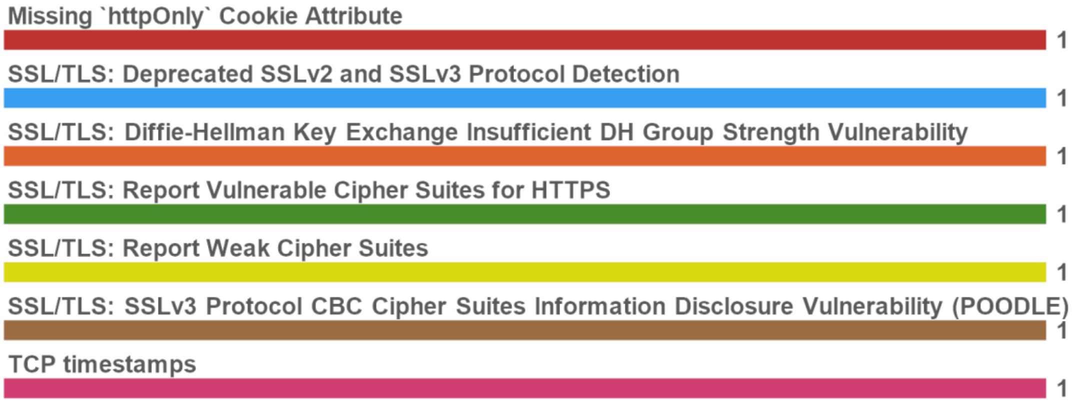
Top Highest Risk (By CVSS Score)



Detected Operating Systems



# Issues by NVT



ISSUE	COUNT
TCP timestamps	1
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	1

ISSUE	COUNT
SSL/TLS: Report Weak Cipher Suites	1
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	1
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1
Missing `httpOnly` Cookie Attribute	1

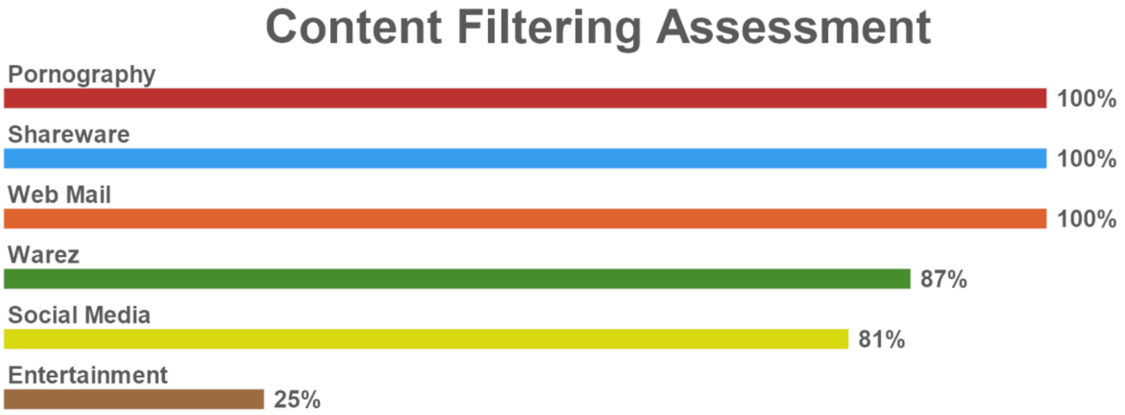
Internal Vulnerabilities

This section details the issues discovered in order of severity. For each issue, the affected nodes are also listed.

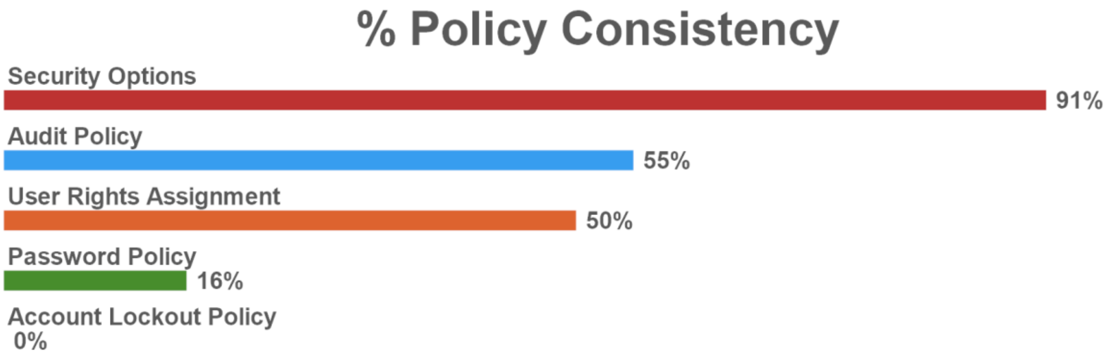
Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	FALSE	HIGHEST CVSS
Total: 0	0	0	0	0	0	0.0

Unrestricted Web Content



Local Security Policy Consistency



Dark Web Scan Summary

The following results were retrieved using a preliminary scan of the Dark Web using ID Agent (www.idagent.com).

Only the first 5 per domain are listed here.

EMAIL	PASSWORD/SHA1	COMPROMISE DATE	SOURCE
dstaar@ircpa.org	jord************	2019/10/02 10:15:00 AM	file-upload
lchavis@ircpa.org	chie************	2019/10/02 10:12:00 AM	file-upload
mstrickland@ircpa.org	mont************	2019/10/02 10:15:00 AM	file-upload
nneill@ircpa.org	vero************	2019/10/02 10:14:00 AM	file-upload