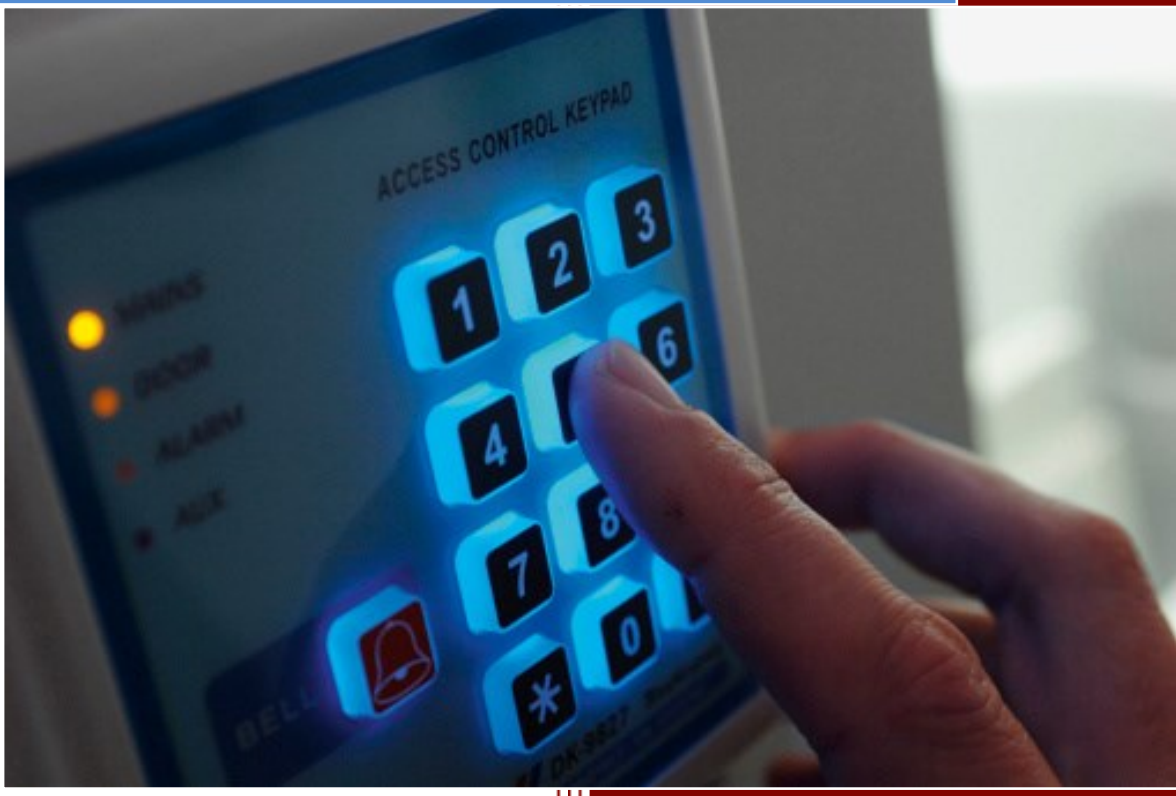
YourIT!
Your Logo Goes Here

Security Assessment

Risk Report



Scan Date: 12/03/2018

Prepared for:
Your Customer / Prospect
Prepared by:
Your Company Name

12/06/2018

Table of Contents

1 - Discovery Tasks

2 - Risk Score

3 - Issues Summary

4 - External Vulnerabilities

5 - Internal Vulnerabilities

6 - Unrestricted Web Content

7 - Local Security Policy Consistency

8 - Dark Web Scan Summary

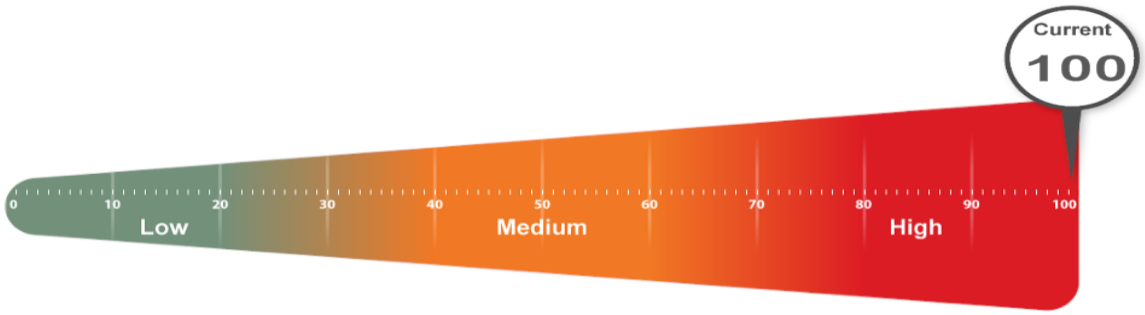
Discovery Tasks

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

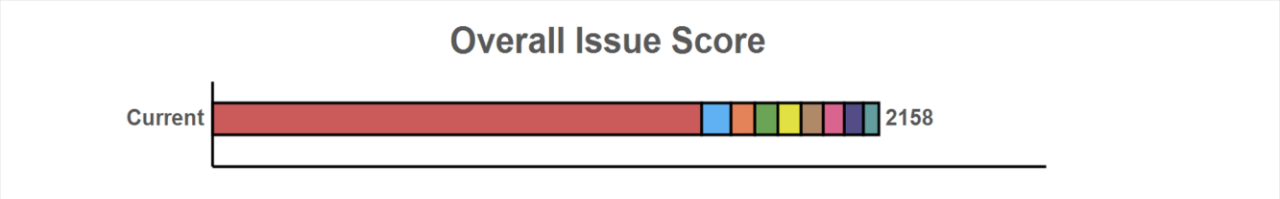
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



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 (%)

	Compromised Passwords found on the Dark Web (100 pts each)
600	***Current Score:*** 100 pts x 6 = 600: 92.31%
	Issue: A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2018.
	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.

	Critical External Vulnerabilities Detected (95 pts each)
95	***Current Score:*** 95 pts x 1 = 95: 4.4%
	Issue: Critical 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 remediating all external vulnerabilities as prescribed.

	Account lockout disabled (77 pts each)
77	***Current Score:*** 77 pts x 1 = 77: 3.57%
	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.

	Medium External Vulnerabilities Detected (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 3.48%
	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 remediating all external vulnerabilities as prescribed.

	Password complexity not enabled (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 3.48%
	Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.
	Recommendation: Enable password complexity to assure domain account passwords are secure.

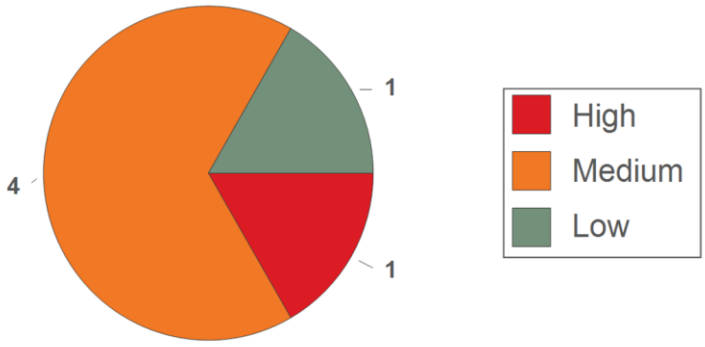
	Password history not remembered for at least six passwords (72 pts each)
72	***Current Score:*** 72 pts x 1 = 72: 3.34%
	Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.
	Recommendation: Increase password history to remember at least six passwords.

	Inconsistent password policy / Exceptions to password policy (68 pts each)
68	***Current Score:*** 68 pts x 1 = 68: 3.15%
	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.

	Lack of web filtering (62 pts each)
62	***Current Score:*** 62 pts x 1 = 62: 2.87%
	Issue: Access to all websites appears to be unrestricted. This issue does not imply that any particular user is currently accessing restricted sites, but rather that they can. Controlling access to the Internet and websites may help reduce risks related to security, legal, and productivity concerns. Lack of adequate content management filtering to block restricted sites may lead to increased network risk and business liability.
	Recommendation: Put access controls in place to block websites that violate the company's Internet use policy.

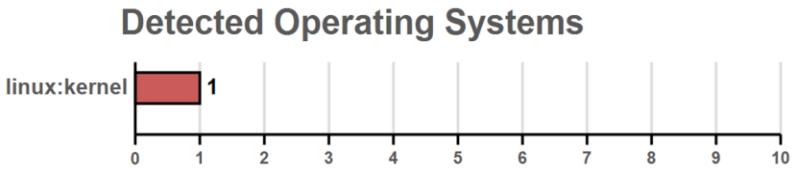
	Open or insecure WiFi protocols available (50 pts each)
50	***Current Score:*** 50 pts x 1 = 50: 2.32%
	Issue: Open or insecure WiFi protocols may allow an attacker access to the company's network and resources.
	Recommendation: Ensure company's WiFi is secure and discourage the use of any open WiFi connections.

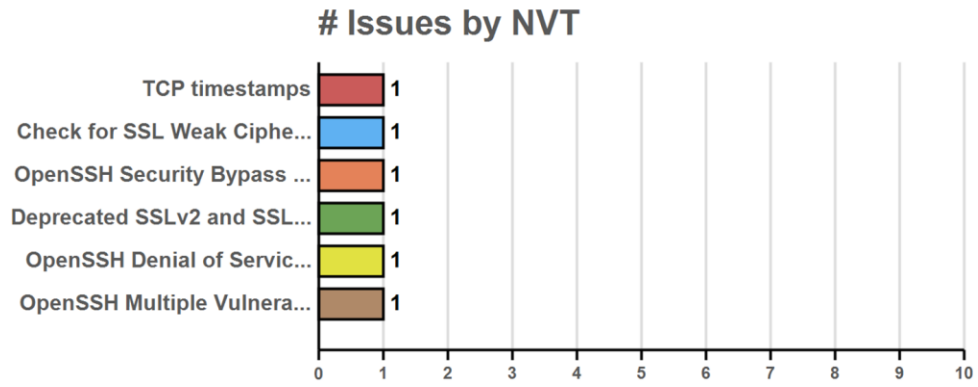
External Vulnerabilities



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
182.161.179.152 (ip-182-161-179-152.ip.securesvr.net)	4	1	4	1	0	8.5
Total: 1	4	1	4	1	0	8.5





Issue	Count
TCP timestamps	1
Check for SSL Weak Ciphers	1
OpenSSH Security Bypass Vulnerability	1
Deprecated SSLv2 and SSLv3 Protocol Detection	1
OpenSSH Denial of Service Vulnerability - Jan16	1
OpenSSH Multiple Vulnerabilities	1

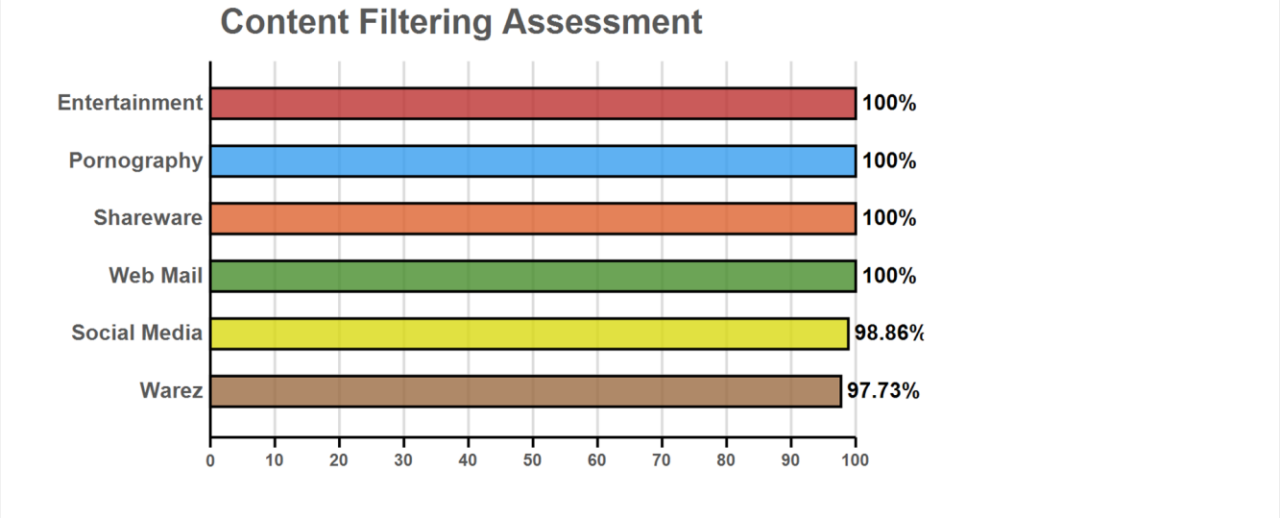
Internal Vulnerabilities

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

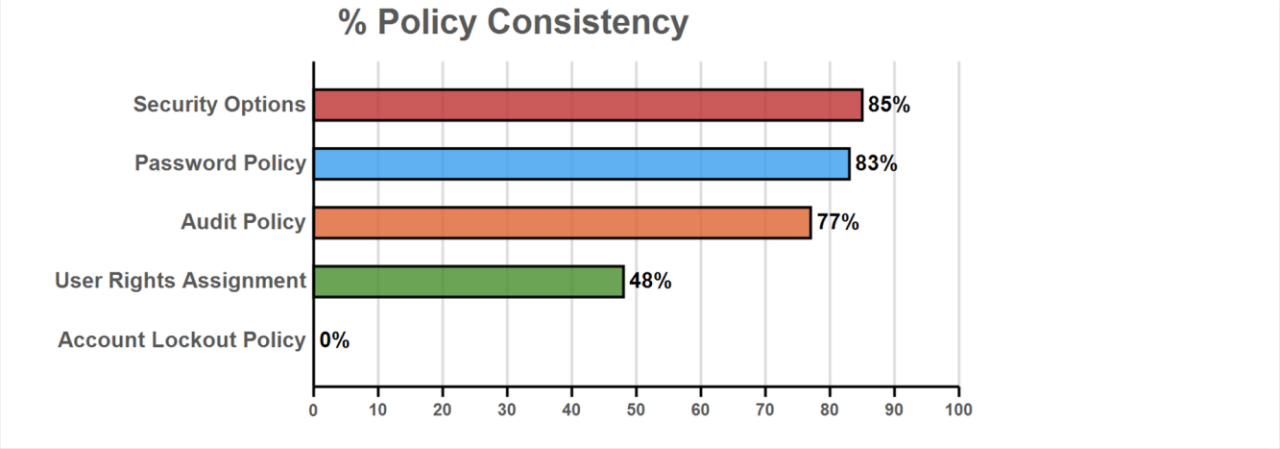
Host Issue Summary

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.

10 entries were found. Only the first 5 per domain are listed here.

Email	Password/SHA1	Compromise Date	Source
jsmith@example.com	password: 1race**********	03/23/2018 1:00:00 AM	id theft forum
rsimpson@myco.com	password: awart**********	03/23/2018 1:00:00 AM	id theft forum
bwillis@myco.com	password: moonl**********	03/23/2018 1:00:00 AM	id theft forum
frogers@myco.com	password: kingl**********	11/15/2017 1:00:00 AM	id theft forum
eknievel@myco.com	password: biker**********	03/23/2018 1:00:00 AM	id theft forum
rcrandon@myco.com	password: mypro**********	12/27/2016 1:00:00 AM	id theft forum