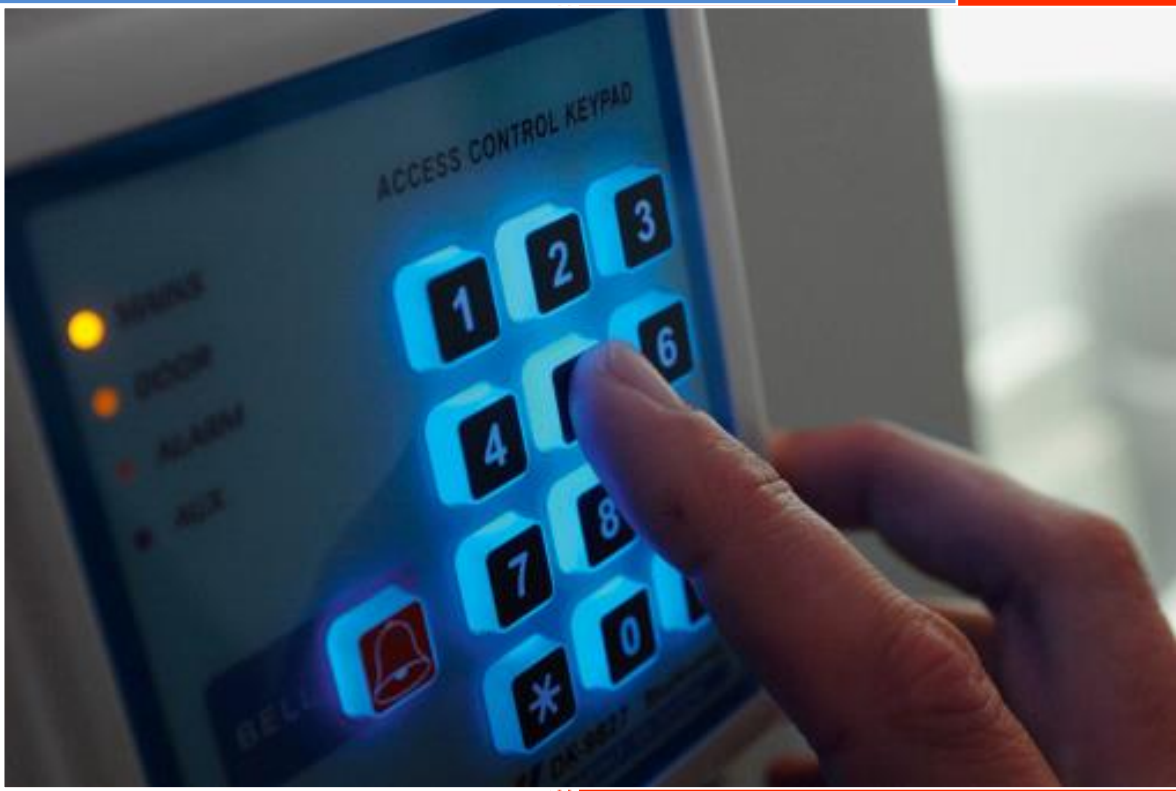
Visualnet Media Inc.

Security Assessment

Risk Report



Scan Date: 10/25/2016

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

10/27/2016

Table of Contents

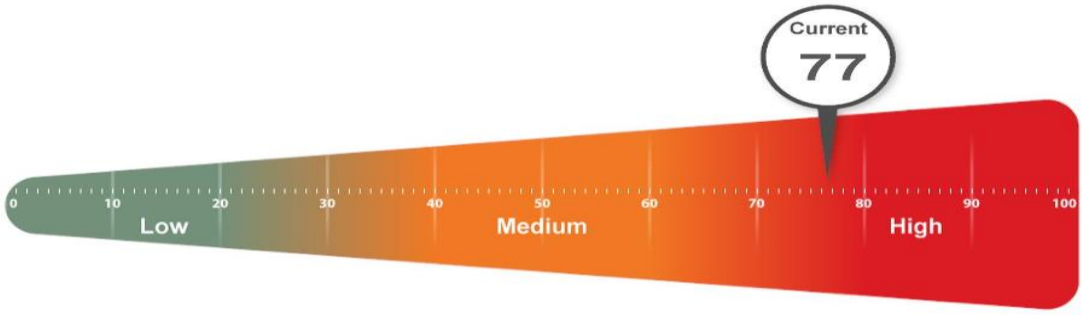
Discovery Tasks

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 detailed External Vulnerability Scan. List and categorize 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

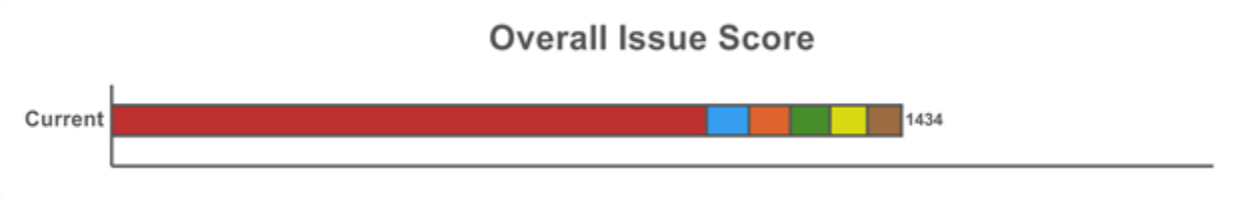
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



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, 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 (%)

	Automatic screen lock not turned on. (72 pts each)
1080	***Current Score:*** 72 pts x 15 = 1080: 75.31%
	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.

	Account lockout disabled (77 pts each)
77	***Current Score:*** 77 pts x 1 = 77: 5.37%
	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 severity external vulnerabilities detected (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 5.23%
	Issue: 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.

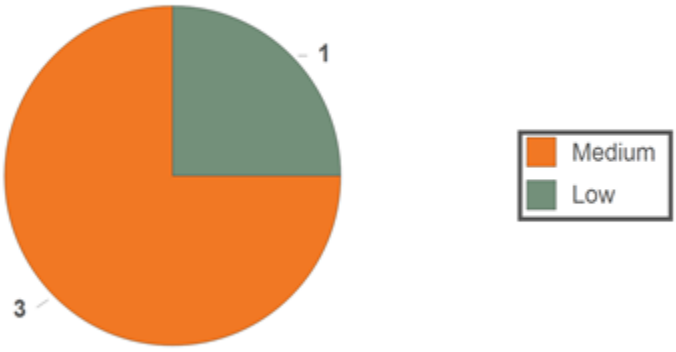
	Password history not remembered for at least six passwords (72 pts each)
72	***Current Score:*** 72 pts x 1 = 72: 5.02%
	Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.
	Recommendation: Increase 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: 4.74%
	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.

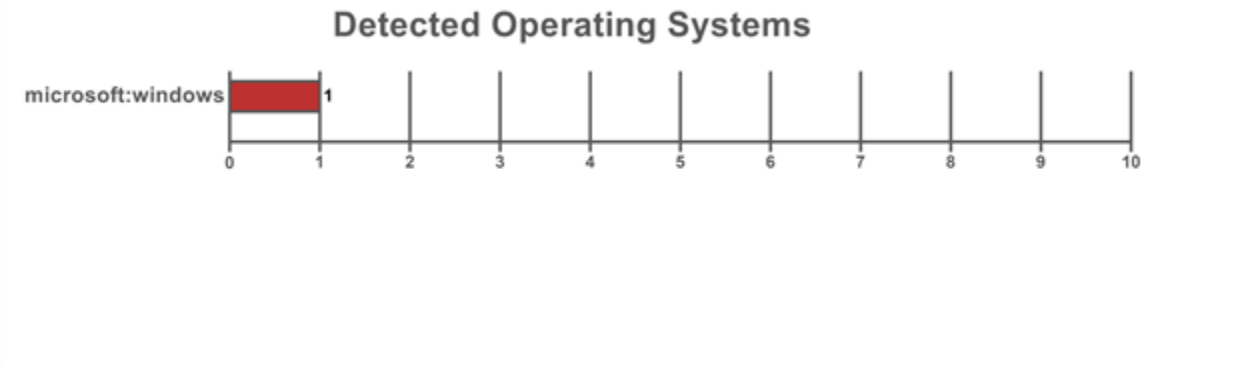
	Lack of web filtering (62 pts each)
62	***Current Score:*** 62 pts x 1 = 62: 4.32%
	Issue: Access to all websites appears to be unrestricted. This issue does not imply that any particular user is currently accessing restricted sites, but rather that they can. Controlling access to the Internet and websites 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.

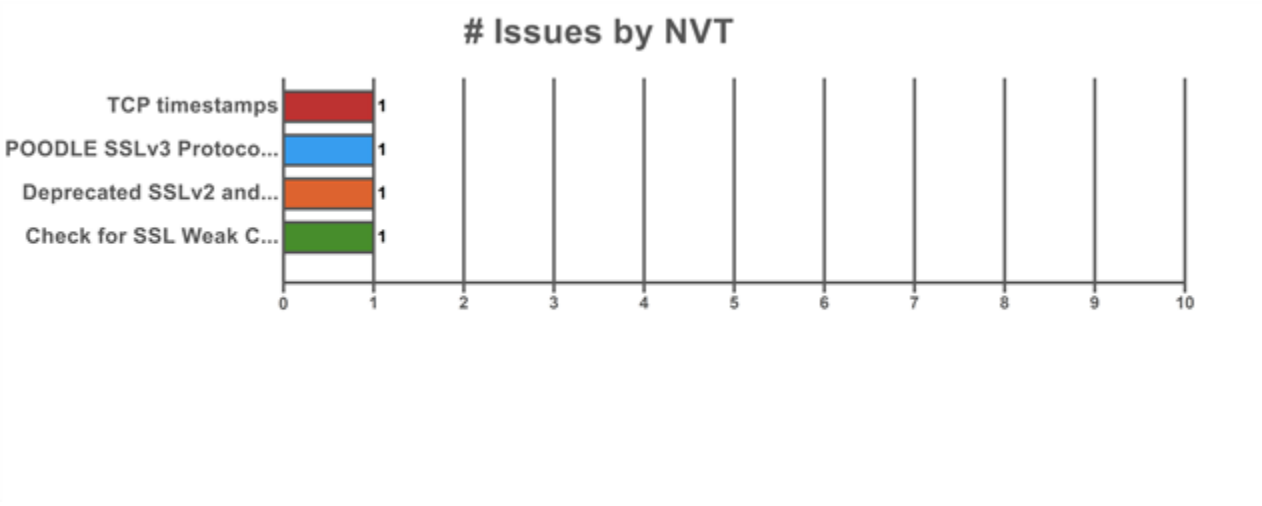
External Vulnerabilities



Host Issue Summary

Host	Open Ports	High	Med	Low	False	
50.248.236.185 (50-248-236-185-static.hfc.comcastbusiness.net)	2	0	3	1	0	4.3
: 1	2	0	3	1	0	4.3




Issues by NVT
TCP timestamps
POODLE SSLv3 Protoco...
Deprecated SSLv2 and...
Check for SSL Weak C...
1
1
1
1
0
1
2
3
4
5
6
7
8
9
10

Internal Vulnerabilities

Local Security Policy Consistency