Treasure Valley:IT
Information Technology. Delivered FAST.

Security Assessment

Risk Report

self
bob

4/5/2016

Discovery Tasks

The following discovery tasks were performed:

	TASK	DESCRIPTION
✓	Detect System Protocol Leakage	Detect protocols that should not be allowed outbound.
✓	Detect Unrestricted Protocols	Detect system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determine if controls are in place for user web browsing.
✓	Detect Wireless Access	Detect and determine if wireless networks are available and secured.
✓	External Security Vulnerabilities	Perform detailed External Vulnerability Scan. List and categorize external security threats.
✓	Network Share Permissions	Document access to file system shares.
✓	Domain Security Policy	Document domain computer and domain controller security policies.
✓	Local Security Policy	Document and assess 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.
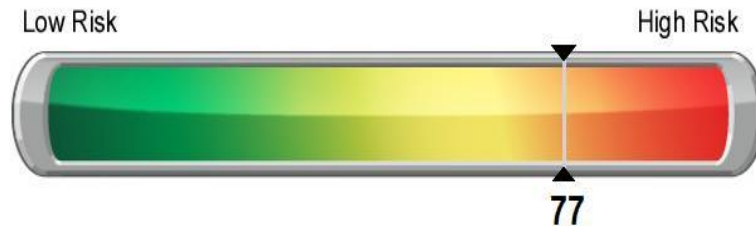
Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

Issues Summary

This section contains summary of issues detected during the Security Assessment. It is based on general best practices and may indicate existing issues or points of interest.

Overall Issue Score

Current (990)

| 110 | 220 | 330 | 440 | 550 | 660 | 770 | 880 | 990 | 1100 |
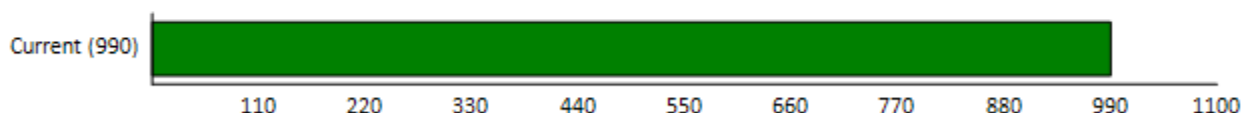
Account lockout disabled (77 pts)

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)

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: We recommend assessing the risk of each vulnerability and remediating all external vulnerabilities as prescribed.

Password history not remembered for at least 6 passwords (72 pts)

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 6 passwords.

Automatic screen lock not turned on. (72 pts)

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.

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

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

Recommendation: Eliminate inconsistencies and exceptions to the password policy.

Open or insecure WiFi protocols available (50 pts)

Issue: Open or insecure WiFi protocols may allow an attacker access to the company's network and resources.
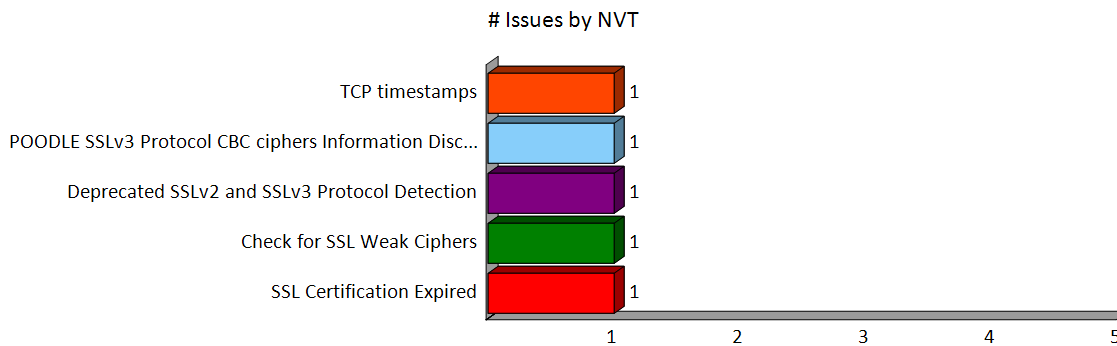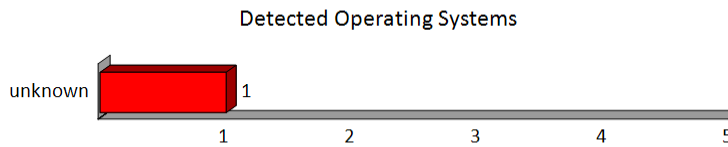
Recommendation: Ensure company's WiFi is secure and discourage the use of any open WiFi connections.

External Vulnerabilities
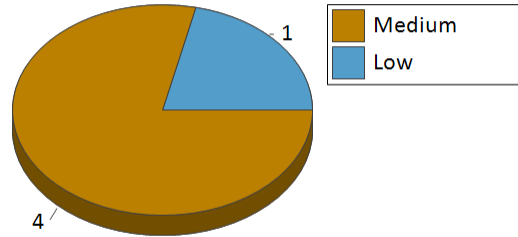
Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
50.248.236.185 (50-248-236-185-static.hfc.comcastbusiness.net)	2	0	4	1	0	5.0
Total: 1	2	0	4	1	0	5.0

Detected Operating Systems

Issues by NVT

Treasure Valley:IT
Information Technology. Delivered FAST.

Internal Vulnerabilities

Entertainment — 100%
Pornography — 100%
Shareware — 100%
Social Media — 100%
Warez — 100%
Web Mail — 100%

10 20 30 40 50 60 70 80 90 100

% Tested Sites Unrestricted
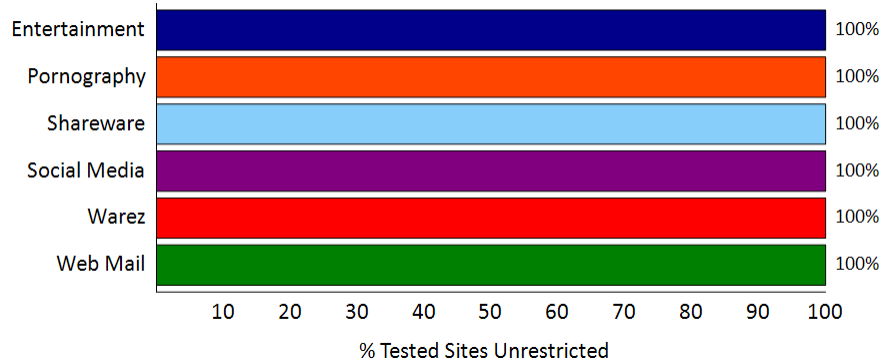
Local Security Policy Consistency

Policy Consistency

Password Policy — 83%
Account Lockout Policy — 0%
Audit Policy — 77%
User Rights Assignment — 63%
Security Options — 94%

10 20 30 40 50 60 70 80 90 100