Network Assessment

Risk Report

Scan Date: 9/13/2016

Prepared for:
ACME Company
Prepared by:
Sean Gaines

9/13/2016

Table of Contents

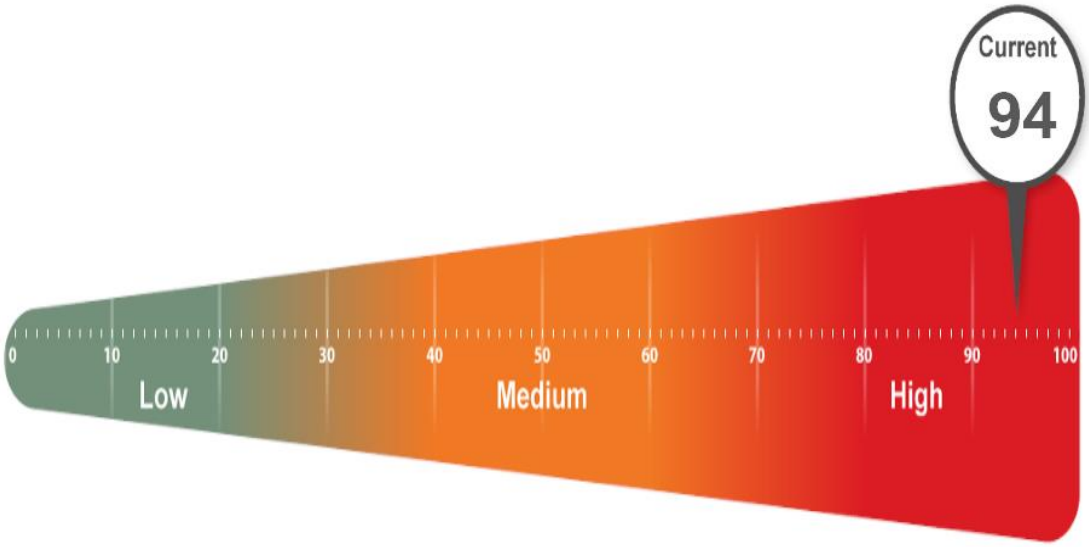
Discovery Tasks

The following discovery tasks were performed:

	Task	Description
✓	Detect Domain Controllers	Identifies Domain Controllers and Online status
✓	FSMO Role Analysis	Enumerates FSMO roles at the site
✓	Enumerate Organization Units and Security Groups	Lists the Organizational units and Security Groups with members
✓	User Analysis	List of users in AD, status, and last login/use, which helps identify potential security risks
✓	Detect Local Mail Servers	Mail server(s) found on the network
✓	Detect Time Servers	Time server(s) found on the network
✓	Discover Network Shares	Comprehensive list of Network Shares by Server
✓	Detect Major Applications	Major apps / versions and count of installations
✓	Detailed Domain Controller Event Log Analysis	List of event log entries from the past 24 hours for the Directory Service, DNS Server and File Replication Service event logs
✓	Web Server Discovery and Identification	List of web servers and type
✓	Network Discovery for Non-A/D Devices	List of Non-Active Directory devices responding to network requests
✓	Internet Access and Speed Test	Test of internet access and performance
✓	SQL Server Analysis	List of SQL Servers and associated database(s)
✓	Internet Domain Analysis	“WHOIS” check for company domain(s)
✓	Password Strength Analysis	Uses MBSA to identify computers with weak passwords that may pose a security risk
✓	Missing Security Updates	Uses MBSA to identify computers missing security updates
✓	System by System Event Log Analysis	Last 5 System and App Event Log errors for servers
✓	External Security Vulnerabilities	List of Security Holes and Warnings from External Vulnerability Scan

Risk Score

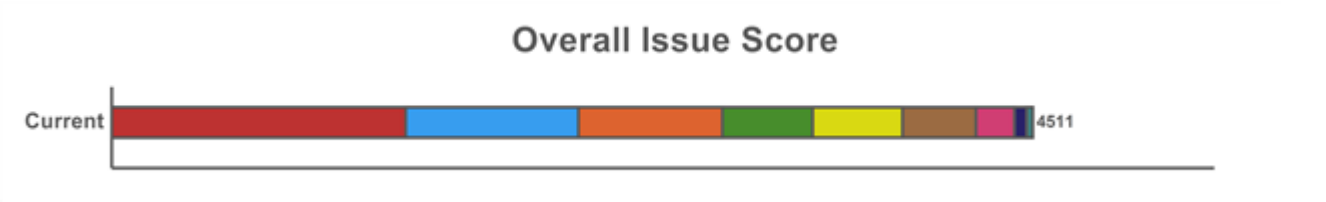
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.



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

Issues Summary

This section contains a summary of issues detected during the Network Assessment process, and is based on industry-wide best practices for network health, performance, and security. 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.



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

	User password set to never expire (80 pts each)
1440	***Current Score:*** 80 pts x 18 = 1440: 31.92%
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.
	Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

	Anti-spyware not installed (94 pts each)
846	***Current Score:*** 94 pts x 9 = 846: 18.75%
	Issue: Anti-spyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend assuring anti-spyware is deployed to all possible endpoints.

	Inactive Computers (15 pts each)
705	***Current Score:*** 15 pts x 47 = 705: 15.63%
	Issue: 47 computers were found as having not checked in during the past 30 days.
	Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, or powered on.

	User has not logged in in 30 days (13 pts each)
442	***Current Score:*** 13 pts x 34 = 442: 9.8%
	Issue: 34 Users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed.

	Recommendation: Disable or remove user accounts for users that have not logged in in 30 days.

	Operating System in Extended Support (20 pts each)
440	***Current Score:*** 20 pts x 22 = 440: 9.75%
	Issue: 22 computers were found using an operating system that is in extended supported. Extended support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.
	Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

	LOTS of Security patches missing on computers (90 pts each)
360	***Current Score:*** 90 pts x 4 = 360: 7.98%
	Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Lots is defined as missing 3 or more patches.
	Recommendation: Address patching on computers with missing security patches.

	Anti-virus not installed (94 pts each)
188	***Current Score:*** 94 pts x 2 = 188: 4.17%
	Issue: Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend assuring anti-virus is deployed to all possible endpoints.

	Insecure Listening Ports (10 pts each)
60	***Current Score:*** 10 pts x 6 = 60: 1.33%
	Issue: 6 computers were found to be using potentially insecure protocols.
	Recommendation: There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they typically lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security.

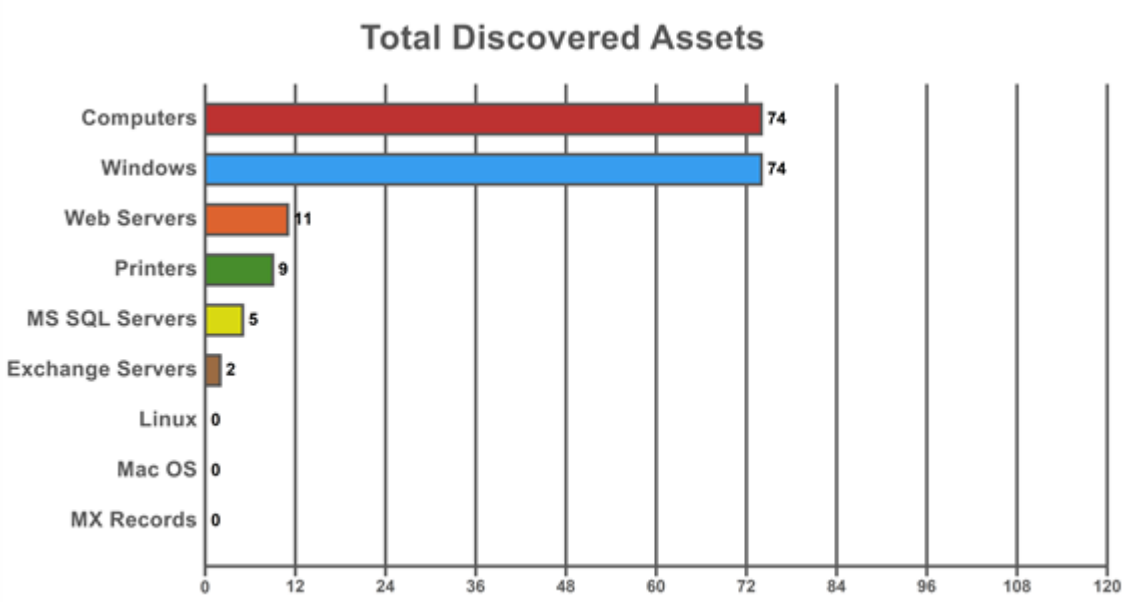
	Un-populated Organization Units (10 pts each)
30	***Current Score:*** 10 pts x 3 = 30: 0.67%
	Issue: Empty Organizational Units (OU) were found in Active Directory. They may not be needed and should be removed to prevent misconfiguration.
	Recommendation: Remove or populate empty Organizational Units.

Internet Speed Test Results

Download Speed: **50.78 Mb/s**

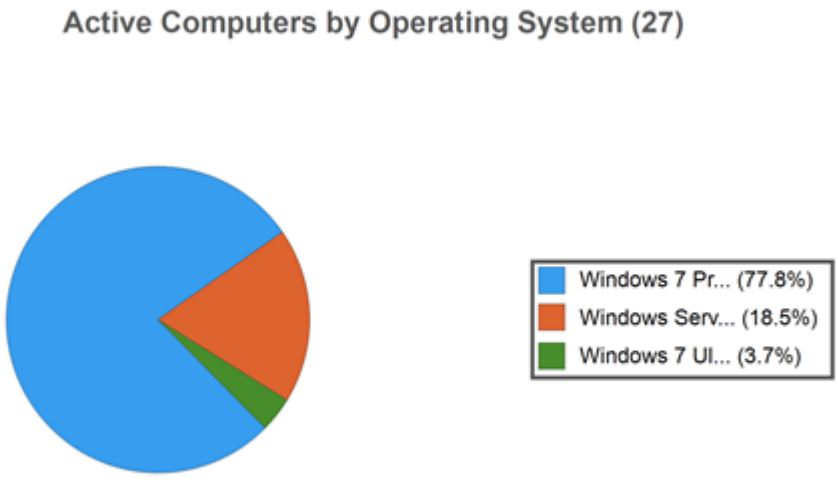
Upload Speed: **12.22 Mb/s**

Asset Summary: Total Discovered Assets

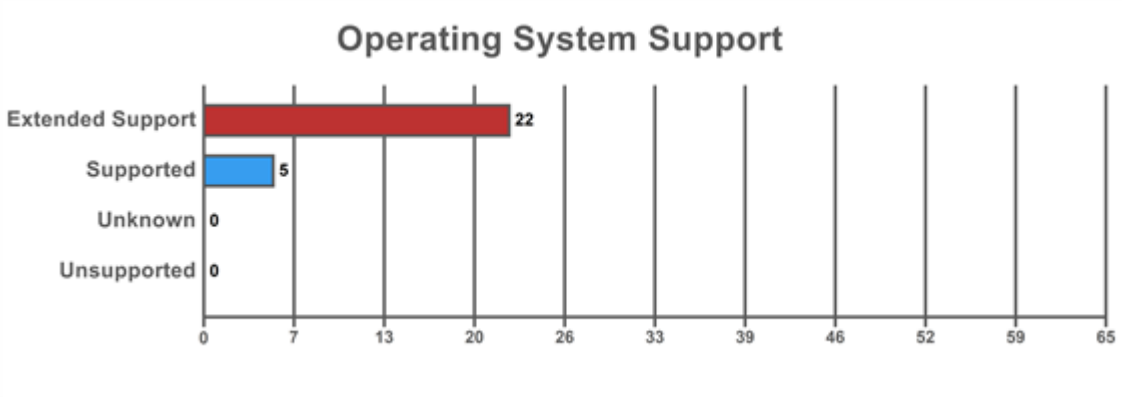


Asset Summary: Active Computers

Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory within the past 30 days.

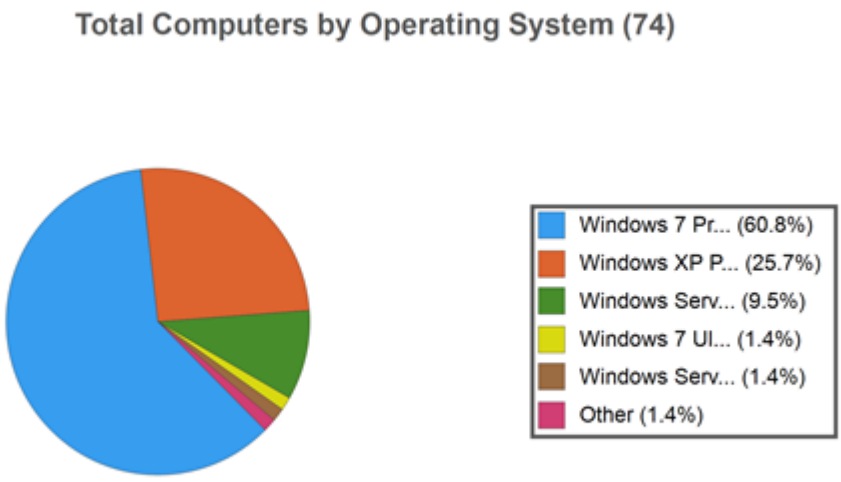


Operating System	Total	Percent
Top Five		
Windows 7 Professional	21	77.8%
Windows Server 2012 R2 Standard	5	18.5%
Windows 7 Ultimate	1	3.7%
Total - Top Five	**27**	**100%**
Other		
Total - Other	**0**	**0%**
Overall Total	**27**	**100%**


Operating System Support
Extended Support
22
Supported
5
Unknown
0
Unsupported
0
0
7
13
20
26
33
39
46
52
59
65

Asset Summary: All Computers

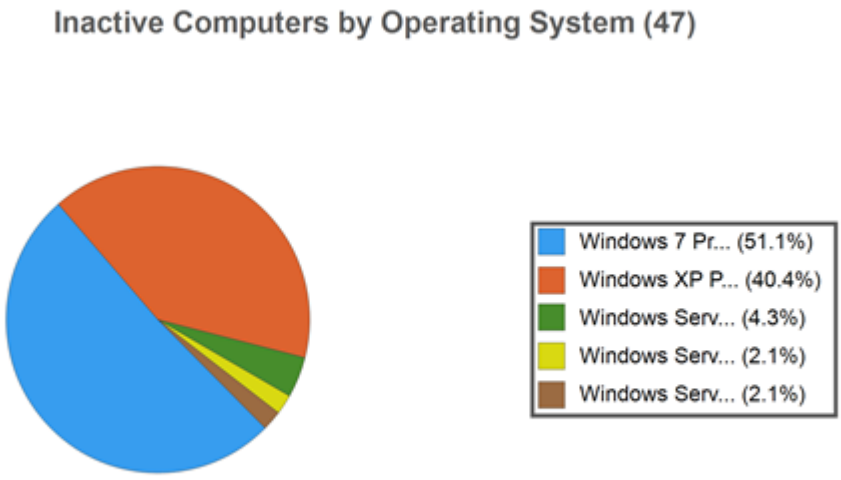
The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a Domain environment).



Operating System	Total	Percent
Top Five		
Windows 7 Professional	45	60.8%
Windows XP Professional	19	25.7%
Windows Server 2012 R2 Standard	7	9.5%
Windows 7 Ultimate	1	1.4%
Windows Server 2003	1	1.4%
Total - Top Five	**73**	**98.6%**
Other		
Windows Server 2008 R2 Standard	1	1.4%
Total - Other	**1**	**1.4%**
Overall Total	**74**	**100%**

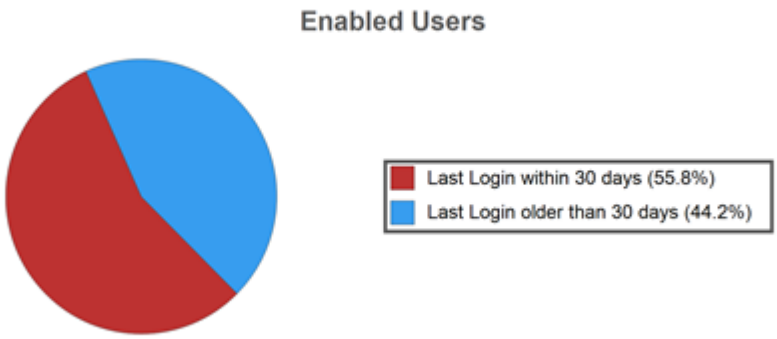
Asset Summary: Inactive Computers

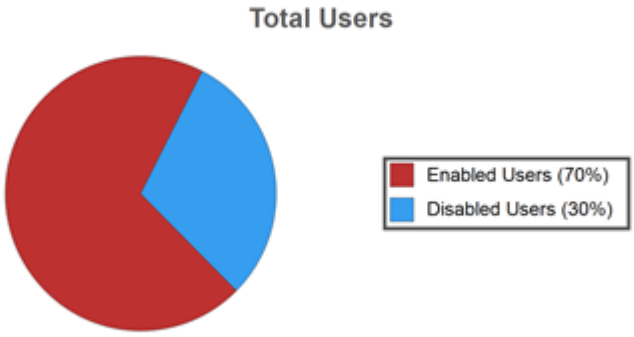
Inactive Computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

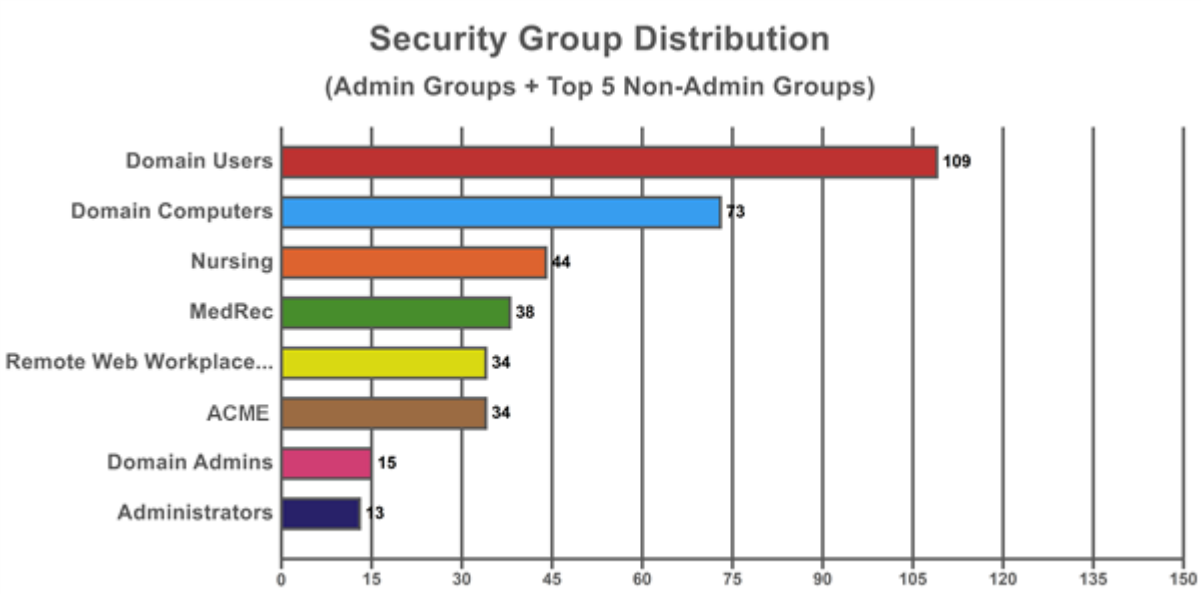


Operating System	Total	Percent
Top Five		
Windows 7 Professional	24	51.1%
Windows XP Professional	19	40.4%
Windows Server 2012 R2 Standard	2	4.3%
Windows Server 2003	1	2.1%
Windows Server 2008 R2 Standard	1	2.1%
Total - Top Five	**47**	**100%**
Other		
Total - Other	**0**	**0%**
Overall Total	**47**	**100%**

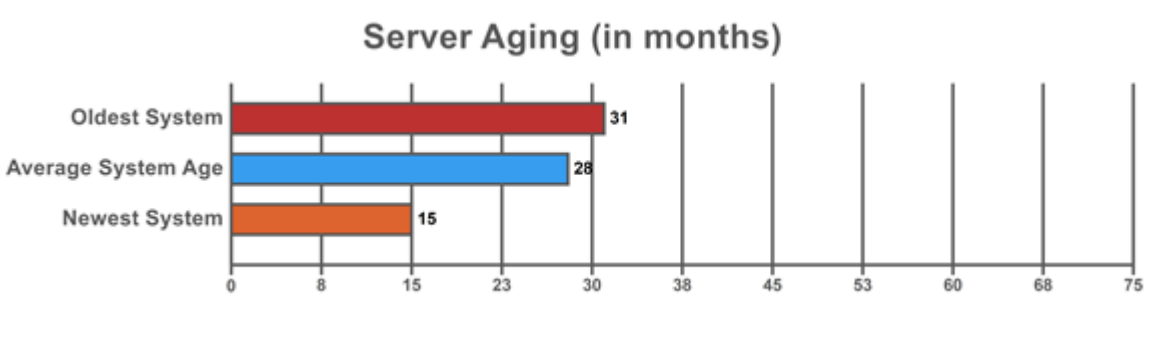
Asset Summary: Users



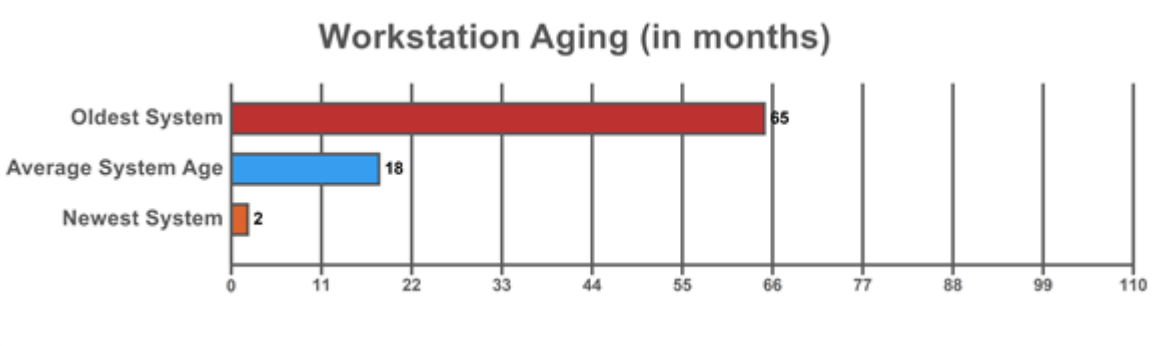



Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)
Domain Users
109
Domain Computers
73
Nursing
44
MedRec
38
Remote Web Workplace...
34
ACME
34
Domain Admins
15
Administrators
13
0
15
30
45
60
75
90
105
120
135
150

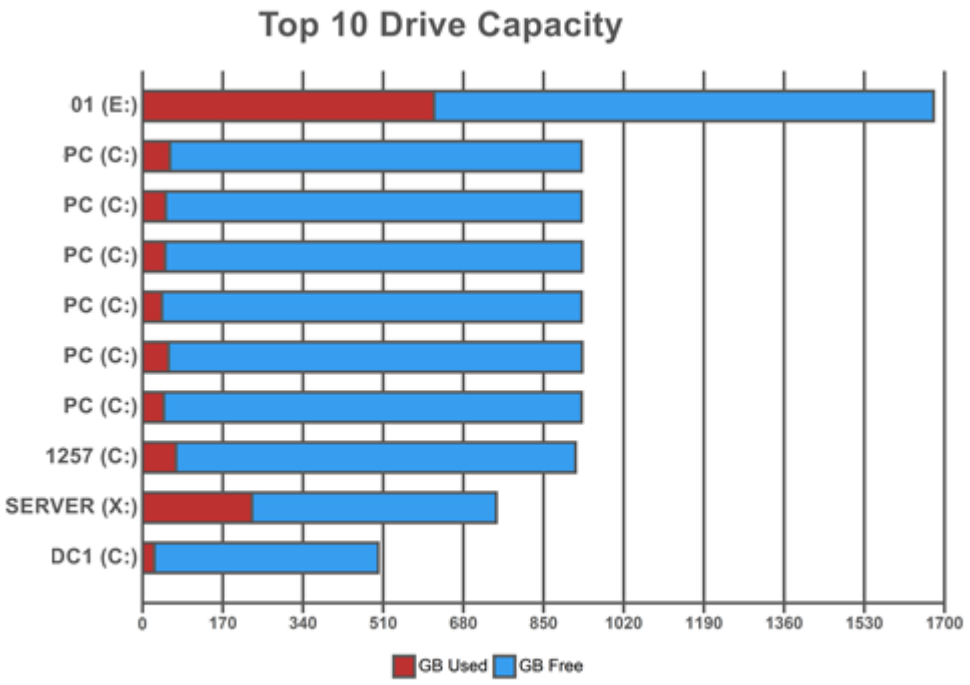
Server Aging

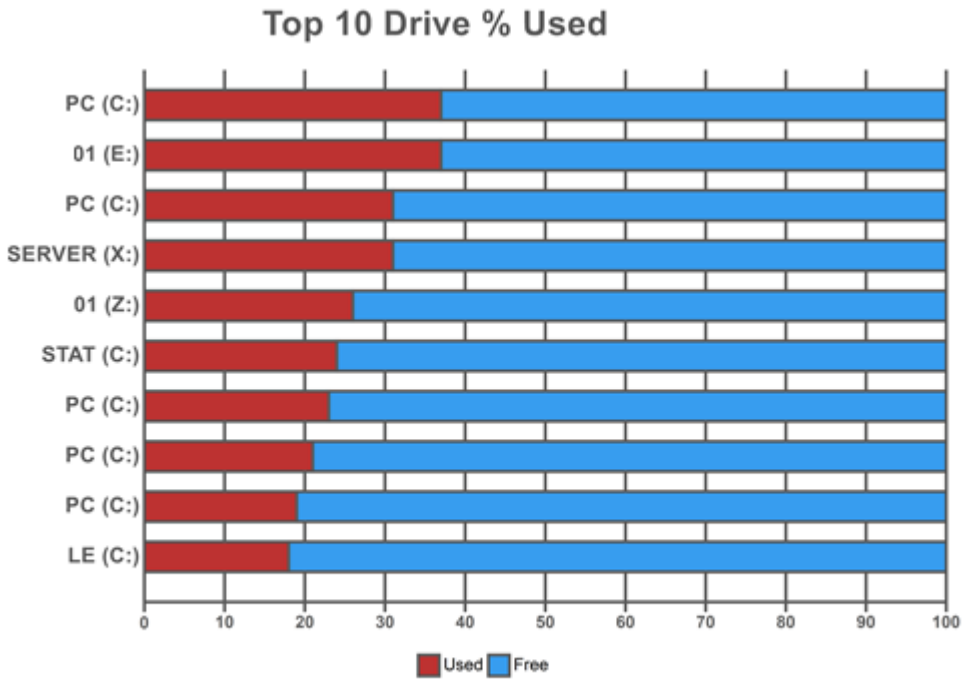


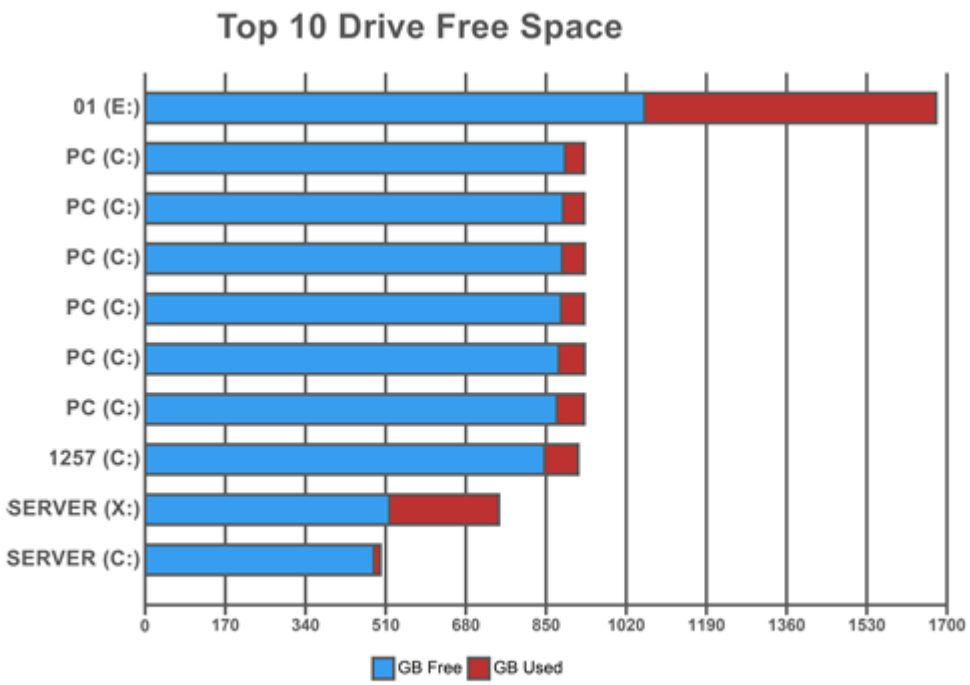
Workstation Aging



Asset Summary: Storage






Top 10 Drive Free Space
01 (E:)
PC (C:)
PC (C:)
PC (C:)
PC (C:)
PC (C:)
PC (C:)
1257 (C:)
SERVER (X:)
SERVER (C:)
0
170
340
510
680
850
1020
1190
1360
1530
1700
GB Free
GB Used

Security Assessment

Security Risk Report

Scan Date: 9/13/2016

Prepared for:
ACME COMPANY
Prepared by:
Sean Gaines

9/13/2016

Table of Contents

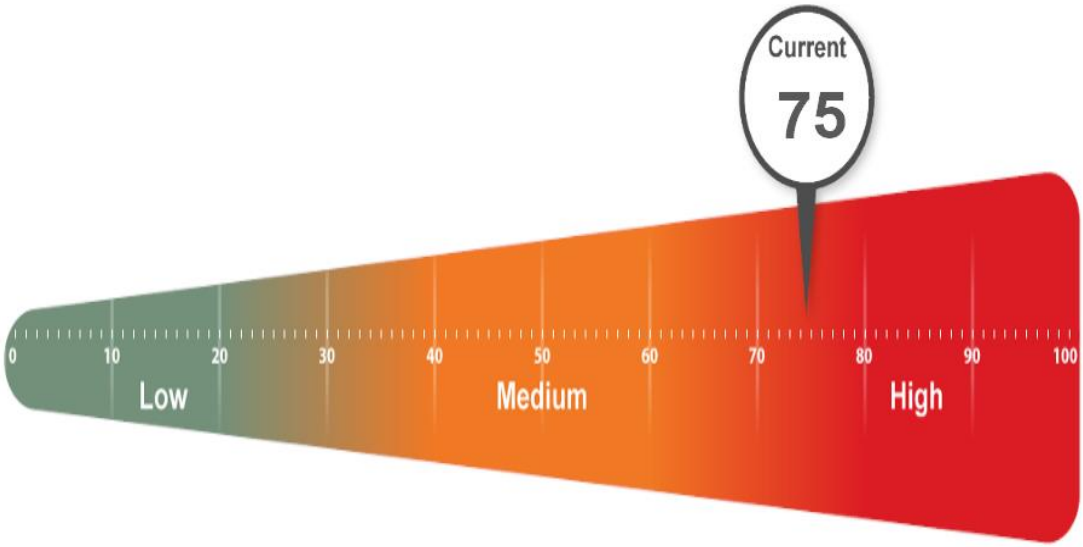
Task

The following discovery tasks were performed:

	Local Security Policy Consistency	Local Security Policy Consistency
✓	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

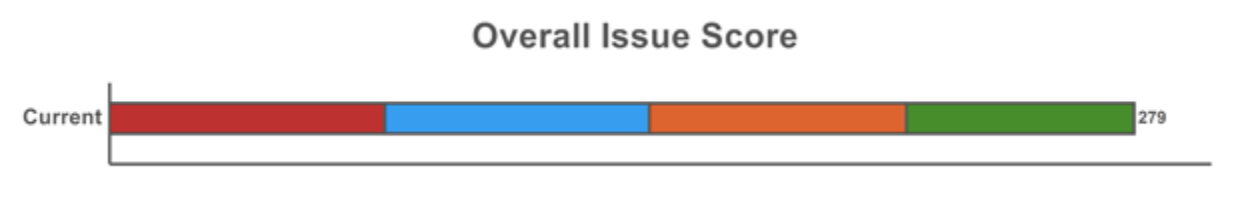
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues.



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

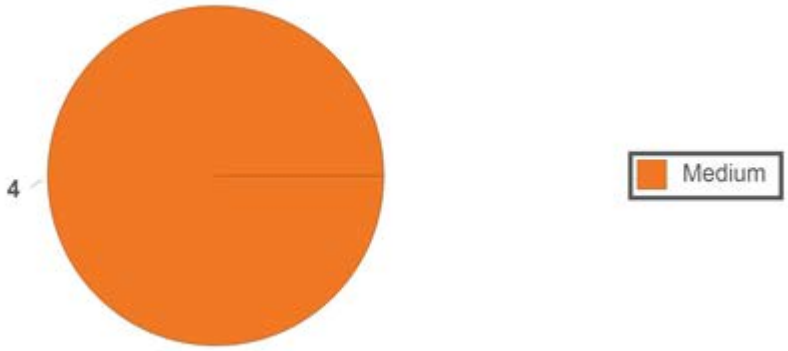
	Medium Severity External Vulnerabilities Detected (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 26.88%
	Issue: External vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential 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.

	Automatic screen lock not turned on. (72 pts each)
72	***Current Score:*** 72 pts x 1 = 72: 25.81%
	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.

	Maximum password age greater than 90 days (70 pts each)
70	***Current Score:*** 70 pts x 1 = 70: 25.09%
	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.

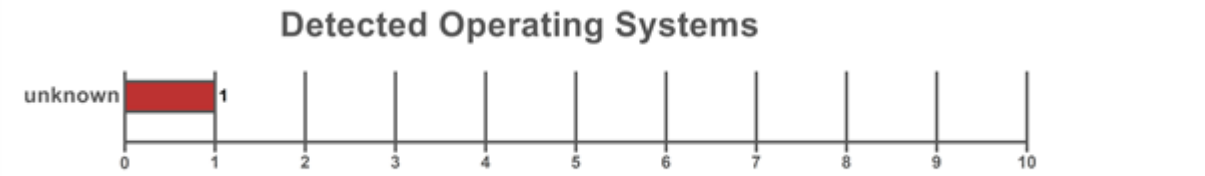
	Lack of Web Filtering (62 pts each)
62	***Current Score:*** 62 pts x 1 = 62: 22.22%
	Issue: Access to all websites appears to be unrestricted. This issue does not imply that any particular user is currently accessing restricted sites, but rather that they can. Controlling access to the Internet and websites 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: We propose putting in place access controls to block websites that violate the company's Internet use policy.

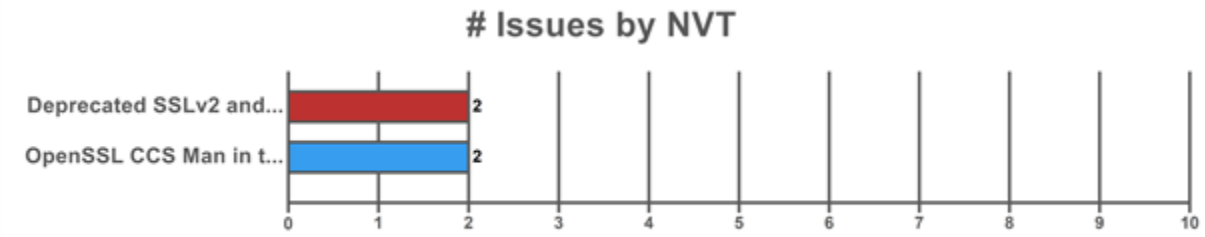
External Vulnerabilities



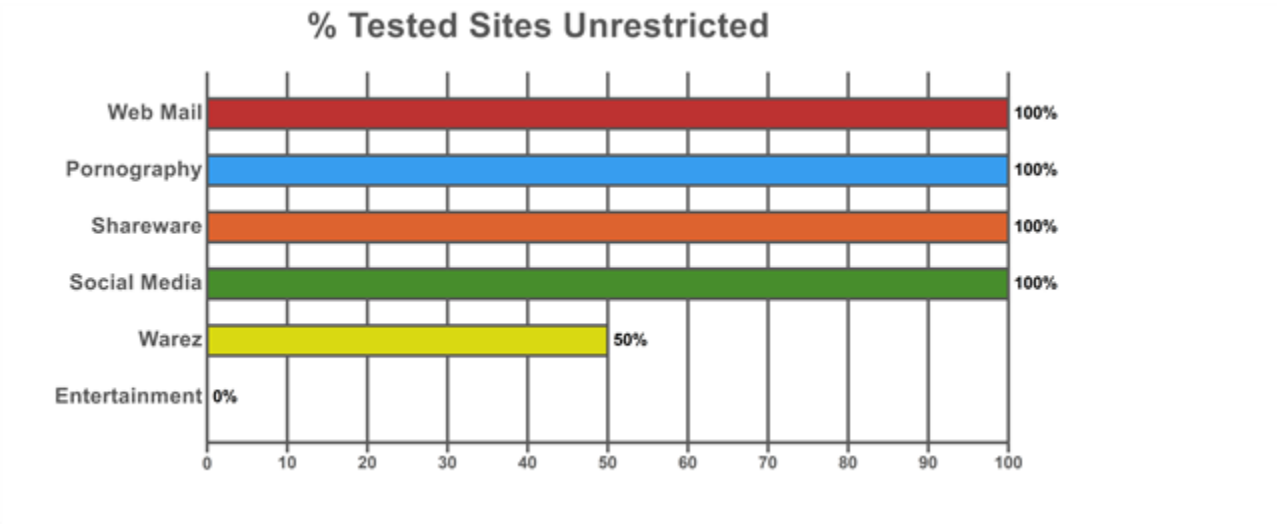
Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
99.99.999.999	3	0	4	0	0	6.8
Total: 1	3	0	4	0	0	6.8





Internal Vulnerabilities



Local Security Policy Consistency