



Network Assessment

Risk Report

Prepared for: A Example

Prepared by: Lost in I.T

04-Mar-2020

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: 02-Mar-2020

Table of Contents

- 1 - [Discovery Tasks](#)
- 2 - [Risk Score](#)
- 3 - [Issues Summary](#)
- 4 - [Internet Speed Test](#)
- 5 - [Assessment Summary](#)
- 6 - [Server Aging](#)
- 7 - [Workstation Aging](#)

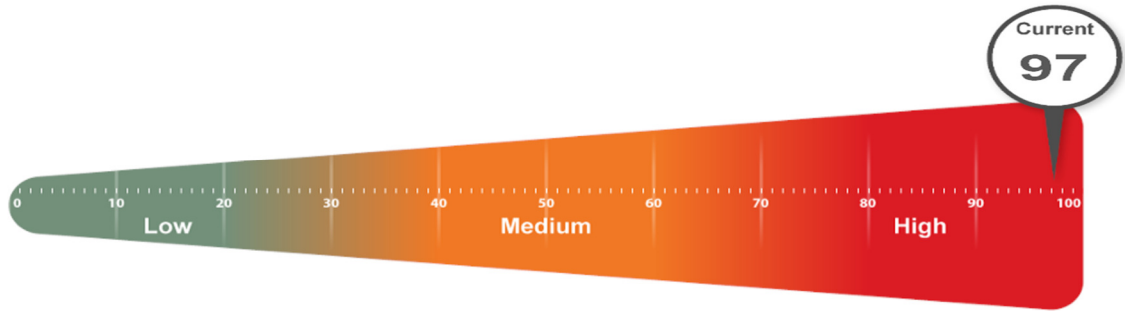
Discovery Tasks

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	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓ Detect Local Mail Servers	Detects mail server(s) on the network.
✓ Detect Time Servers	Detects server(s) on the network.
✓ Discover Network Shares	Discovers the network shares by server.
✓ Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓ Detailed Domain Controller Event Log Analysis	Lists the 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	Lists the web servers and type.
✓ Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓ Internet Access and Speed Test	Tests Internet access and performance.
✓ SQL Server Analysis	Lists the SQL Servers and associated database(s).
✓ Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
✓ Missing Security Updates	Identifies computers missing security updates.
✓ System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
✗ External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.

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 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.

Overall Issue Score



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

Unsupported operating systems (97 pts each)

2716 **Current Score:** 97 pts x 28 = 2716: 34.56%

Issue: found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

Recommendation: Upgrade or replace computers with operating systems that are no longer supported.

User password set to never expire (30 pts each)

2430 **Current Score:** 30 pts x 81 = 2430: 30.92%

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.

User has not logged on to domain in 30 days (13 pts each)

962	Current Score: 13 pts x 74 = 962: 12.24%
	Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.
	Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

Inactive computers (15 pts each)

765	Current Score: 15 pts x 51 = 765: 9.73%
	Issue: Computers have 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, logged into by authorized users, or powered on.

Anti-spyware not turned on (92 pts each)

368	Current Score: 92 pts x 4 = 368: 4.68%
	Issue: We were unable to determine if anti-spyware software is enabled and running on some computers.
	Recommendation: Determine if anti-spyware is enabled properly.

Anti-spyware not up to date (90 pts each)

180	Current Score: 90 pts x 2 = 180: 2.29%
	Issue: Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.
	Recommendation: Ensure anti-spyware definitions are up to date on specified computers.

Anti-virus not up to date (90 pts each)

180	Current Score: 90 pts x 2 = 180: 2.29%
-----	---

Issue: Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.

Recommendation: Ensure anti-virus definitions are up to date on specified computers.

Anti-spyware not installed (94 pts each)

94 **Current Score:** 94 pts x 1 = 94: 1.2%

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: Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues.

Anti-virus not installed (94 pts each)

94 **Current Score:** 94 pts x 1 = 94: 1.2%

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 ensuring that anti-virus is deployed to all possible endpoints.

Insecure listening ports (10 pts each)

40 **Current Score:** 10 pts x 4 = 40: 0.51%

Issue: Computers are 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 often 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	<p>Current Score: 10 pts x 3 = 30: 0.38%</p> <p>Issue: Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.</p> <p>Recommendation: Remove or populate empty organizational units.</p>

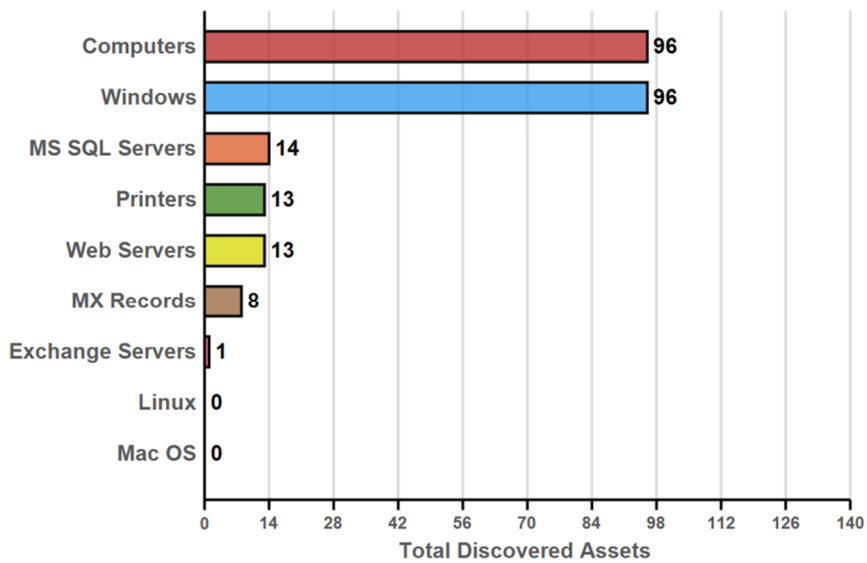
Internet Speed Test Results

Download Speed: **79.9 Mb/s**

Upload Speed: **51.2 Mb/s**



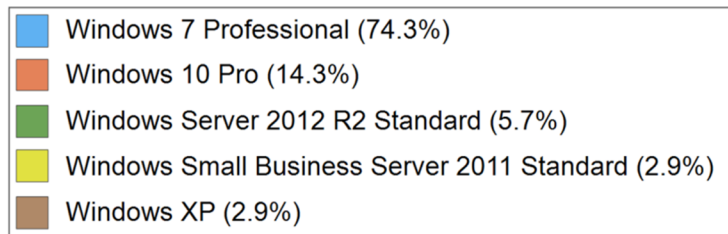
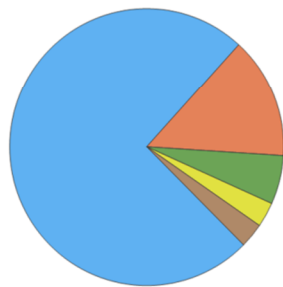
Asset Summary: Total Discovered Assets



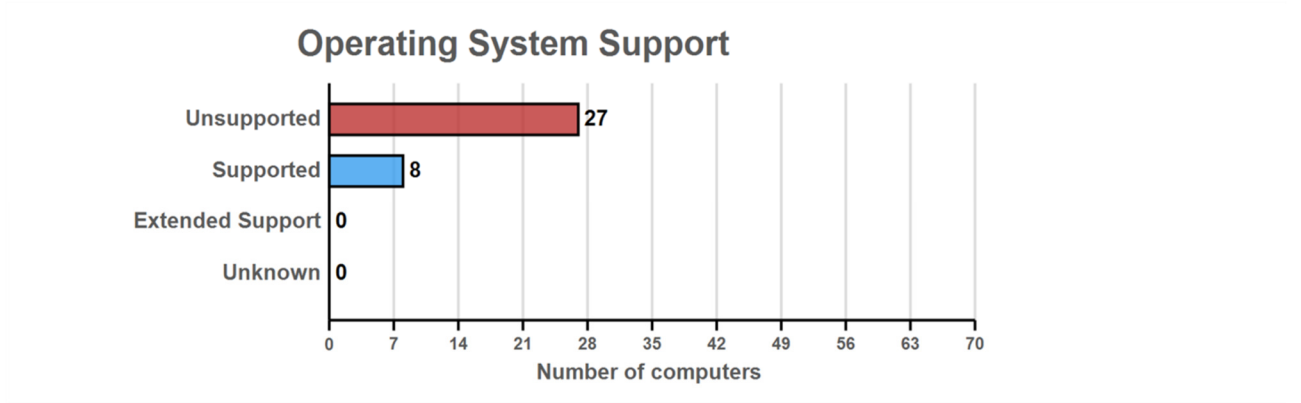
Asset Summary: Active Computers

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.

Active Computers by Operating System
Total (35)



Operating System	Total	Percent
Top Five		
■ Windows 7 Professional	26	74.3%
■ Windows 10 Pro	5	14.3%
■ Windows Server 2012 R2 Standard	2	5.7%
■ Windows Small Business Server 2011 Standard	1	2.9%
■ Windows XP	1	2.9%
Total - Top Five	35	100%
Other		
Total - Other	0	0%
Overall Total	35	100%

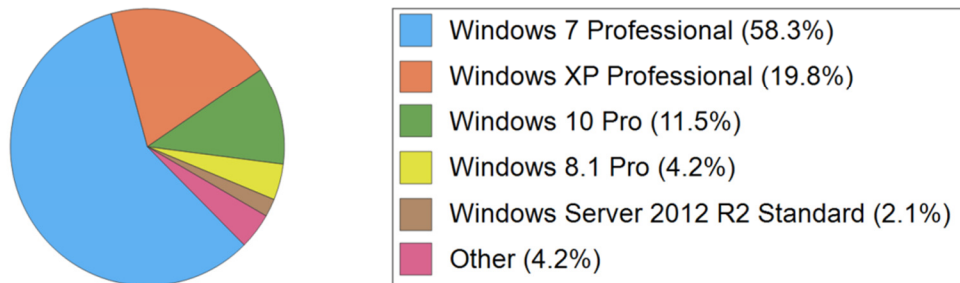


Asset Summary: All Computers

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

Total Computers by Operating System

Total (96)



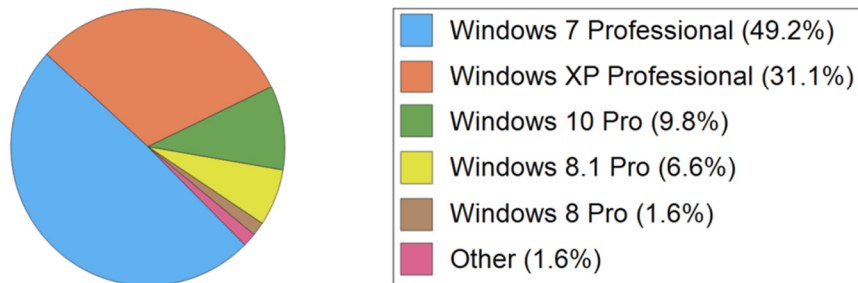
Operating System	Total	Percent
Top Five		
Windows 7 Professional	56	58.3%
Windows XP Professional	19	19.8%
Windows 10 Pro	11	11.5%
Windows 8.1 Pro	4	4.2%
Windows Server 2012 R2 Standard	2	2.1%
Total - Top Five	92	95.8%
Other		
Windows 8 Pro	1	1%
Windows Server 2012 Standard	1	1%
Windows Small Business Server 2011 Standard	1	1%

Operating System	Total	Percent
Windows XP	1	1%
Total - Other	4	4.2%
Overall Total	96	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.

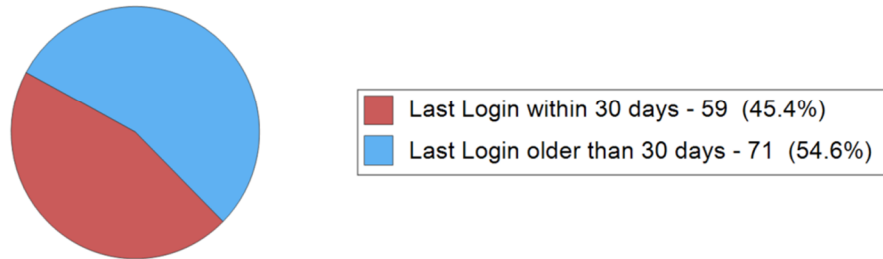
Inactive Computers by Operating System
Total (61)



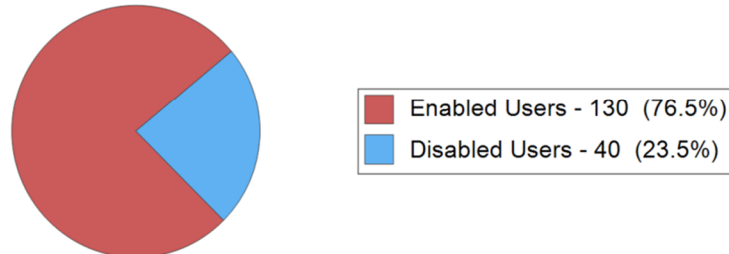
Operating System	Total	Percent
Top Five		
Windows 7 Professional	30	49.2%
Windows XP Professional	19	31.1%
Windows 10 Pro	6	9.8%
Windows 8.1 Pro	4	6.6%
Windows 8 Pro	1	1.6%
Total - Top Five	60	98.4%
Other		
Windows Server 2012 Standard	1	1.6%
Total - Other	1	1.6%
Overall Total	61	100%

Asset Summary: Users

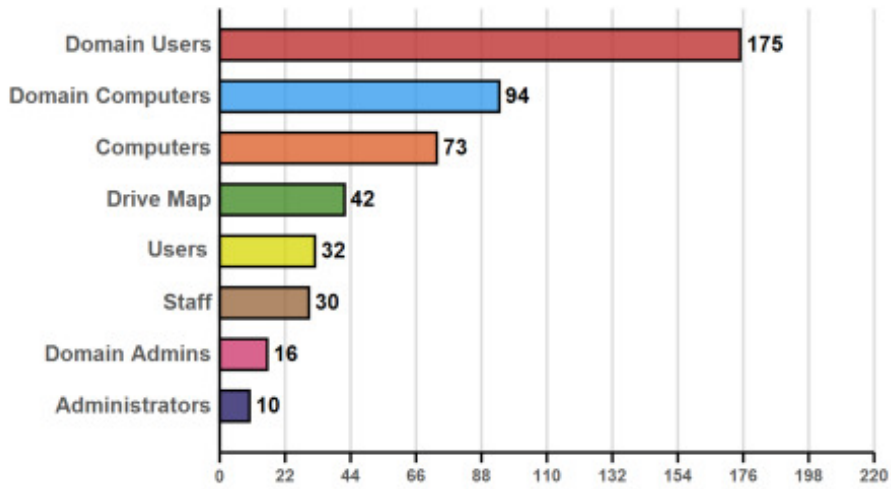
Users Logged in



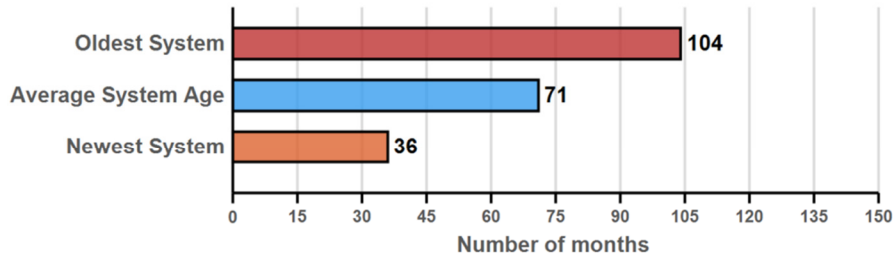
Total Users



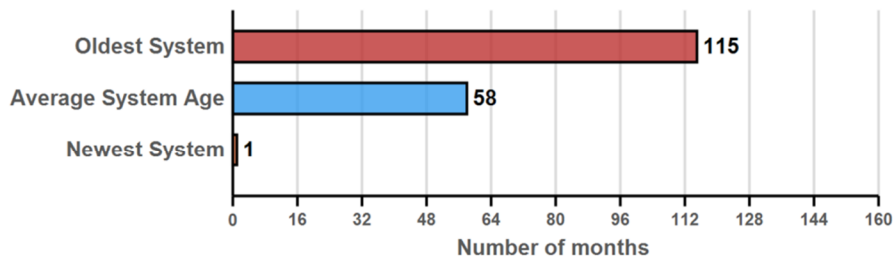
Security Group Distribution (Admin Groups + Top 5 Non-Admin Groups)



Server Aging



Workstation Aging



Asset Summary: Storage

