Consolidated Assessment

Consolidated Risk Report

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: 2020/01/18

Prepared for: Your Company

Prepared by: The IT Guys I/O

2021/02/03

Table of Contents

Consolidated Risk Report Overview

The Consolidated Risk Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a Consolidated Risk Score and a high-level overview of the health and security of the network.

The report details the scan tasks undertaken to discover security issues. In addition to the overall Consolidated Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security, Exchange, SQL Server) and compliance assessments (HIPAA and PCI) performed on the network environment. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis.

At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Consolidated Discovery Tasks

The following discovery tasks were performed.

	TASK	DESCRIPTION
Network		
✓	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 Accounts	Detects local accounts on computer endpoints.
✓	Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
✓	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.
✓	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.
Security		

	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.

Consolidated Risk Score

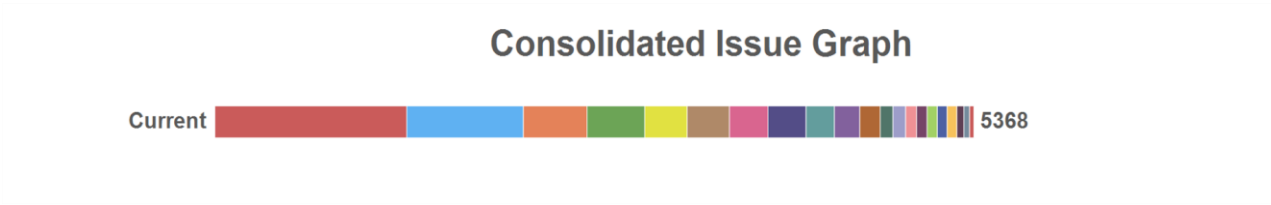
The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.

Several critical issues were identified. Identified issues should be investigated and addressed according to the Consolidated Risk Report.

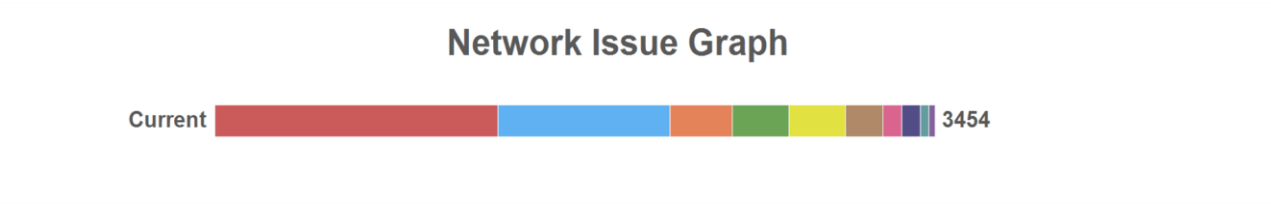
Module	Risk Score
Network	
Security	

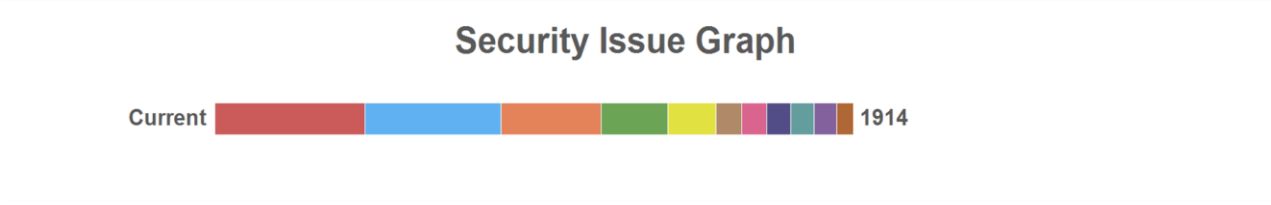
Consolidated Issue Graph

This section contains a summary of issues detected during the Consolidated 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 (%)





Consolidated Issue Summary

Network Issue Summary

1358 **Unsupported operating systems (97 pts each)**

Current Score: 97 pts x 14 = 1358: 39.32%

Issue: Computers 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.

825 **Few Security patches missing on computers. (75 pts each)**

Current Score: 75 pts x 11 = 825: 23.89%

Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches.

Recommendation: Address patching on computers missing 1-3 security patches.

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

Current Score: 13 pts x 23 = 299: 8.66%

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.

272 **Potential disk space issue (68 pts each)**

Current Score: 68 pts x 4 = 272: 7.87%

Issue: 4 computers were found with significantly low free disk space.

Recommendation: Free or add additional disk space for the specified drives.

270 Insecure listening ports (10 pts each)

Current Score: 10 pts x 27 = 270: 7.82%

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. See Listening Ports sheets in Excel Export for details.

180 User password set to never expire (30 pts each)

Current Score: 30 pts x 6 = 180: 5.21%

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.

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

Current Score: 90 pts x 1 = 90: 2.61%

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.

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

Current Score: 90 pts x 1 = 90: 2.61%

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.

40 Operating system in Extended Support (20 pts each)

Current Score: 20 pts x 2 = 40: 1.16%

Issue: Computers are 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.

30 Inactive computers (15 pts each)

Current Score: 15 pts x 2 = 30: 0.87%

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.

Security Issue Summary

450 Medium External Vulnerabilities Detected (75 pts each)

Current Score: 75 pts x 6 = 450: 23.51%

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 remediate all external vulnerabilities as prescribed.

408 Screen lock time is > 15 minutes (68 pts each)

Current Score: 68 pts x 6 = 408: 21.32%

Issue: Even though screen lockout has been activated, extensive lockout times may lead to authorized access when users leave their computers.

Recommendation: Reduce screen lockout to 15 minutes or less on the specified computers.

300 Password complexity not enabled (75 pts each)

Current Score: 75 pts x 4 = 300: 15.67%

Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.

Recommendation: Enable password complexity to assure that network user account passwords are secure.

200 Compromised Passwords found on the Dark Web (50 pts each)

Current Score: 50 pts x 4 = 200: 10.45%

Issue: A scan of the Dark Web revealed one or more compromised passwords from your domain. The most recent compromise occurred in 2019.

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. Only the first 5 per domain are listed here.

144 Automatic screen lock not turned on (72 pts each)

Current Score: 72 pts x 2 = 144: 7.52%

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.

77 Account lockout disabled (77 pts each)

Current Score: 77 pts x 1 = 77: 4.02%

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.

75 Passwords less than 8 characters allowed (75 pts each)

Current Score: 75 pts x 1 = 75: 3.92%

Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to more than 8 characters.

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

Current Score: 72 pts x 1 = 72: 3.76%

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.

70 Maximum password age greater than 90 days (70 pts each)

Current Score: 70 pts x 1 = 70: 3.66%

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.

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

Current Score: 68 pts x 1 = 68: 3.55%

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.

50 Open or insecure Wi-Fi protocols available (50 pts each)

Current Score: 50 pts x 1 = 50: 2.61%

Issue: Open or insecure Wi-Fi protocols may allow an attacker access to the company's network and resources.

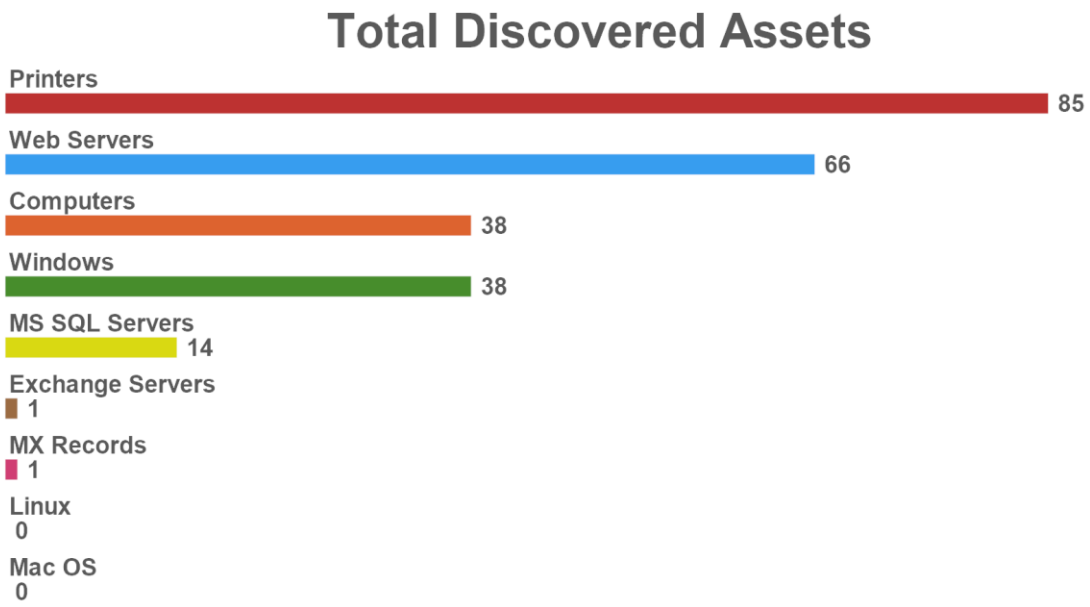
Recommendation: Ensure company's Wi-Fi is secure and discourage the use of any open Wi-Fi connections.

Internet Speed Test Results

Download Speed: **76.17 Mb/s**

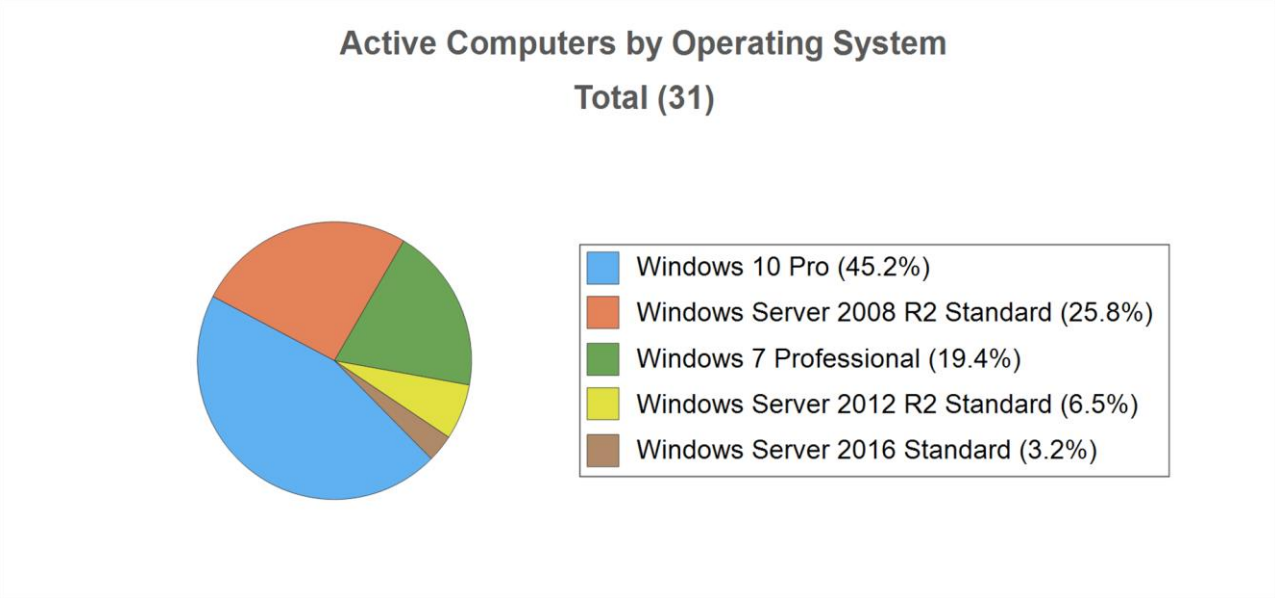
Upload Speed: **78.19 Mb/s**

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 (TOP FIVE)	TOTAL	PERCENT
Windows 10 Pro	14	45.2%
Windows Server 2008 R2 Standard	8	25.8%
Windows 7 Professional	6	19.4%
Windows Server 2012 R2 Standard	2	6.5%
Windows Server 2016 Standard	1	3.2%
Total - Top Five	**31**	**100%**

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	**0**	**0%**

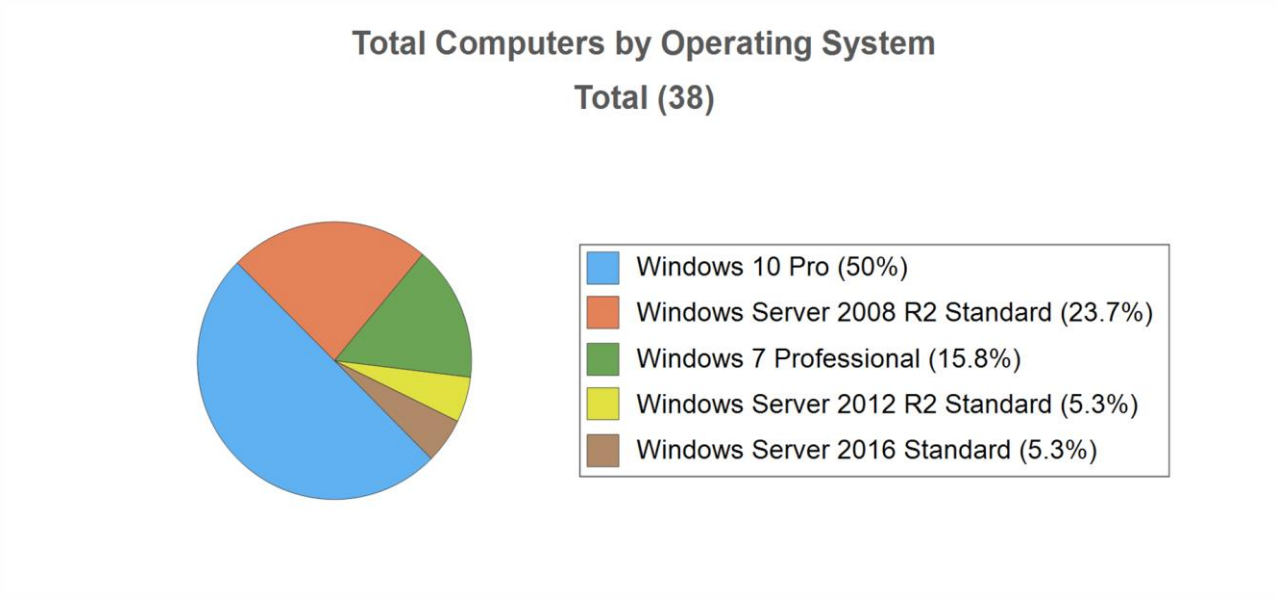
OVERALL TOTAL	31	100%

Operating System Support


Supported
15
Unsupported
14
Extended Support
2
Unknown
0

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).



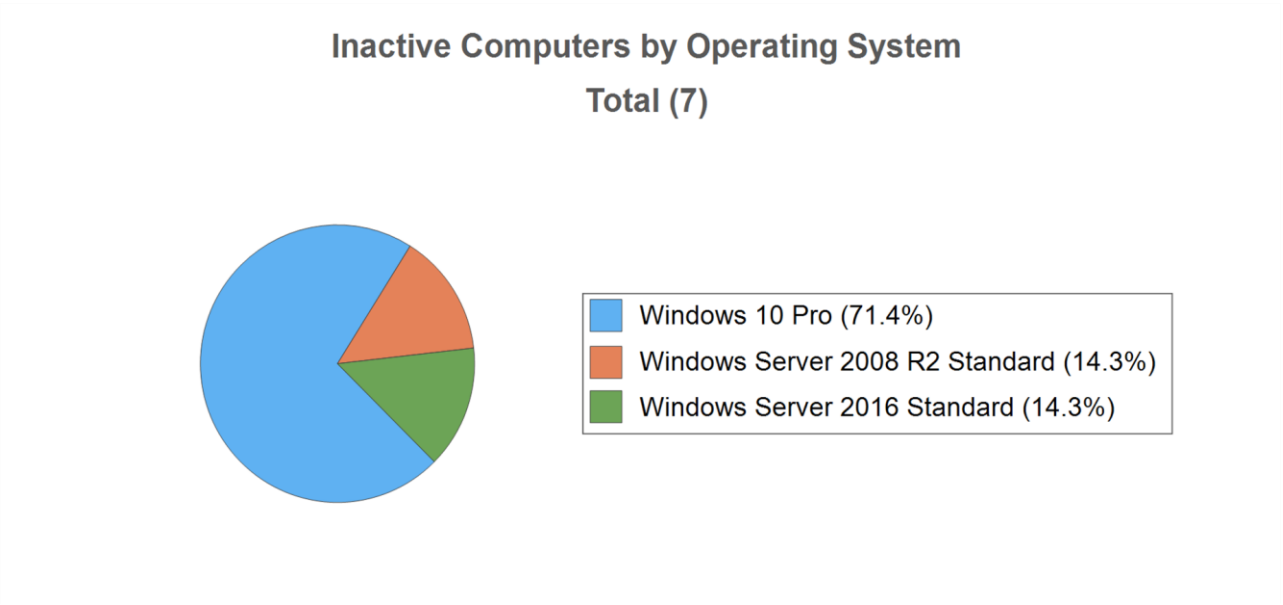
OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
Windows 10 Pro	19	50%
Windows Server 2008 R2 Standard	9	23.7%
Windows 7 Professional	6	15.8%
Windows Server 2012 R2 Standard	2	5.3%
Windows Server 2016 Standard	2	5.3%
Total - Top Five	**38**	**100%**

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	**0**	**0%**

OVERALL TOTAL	38	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.



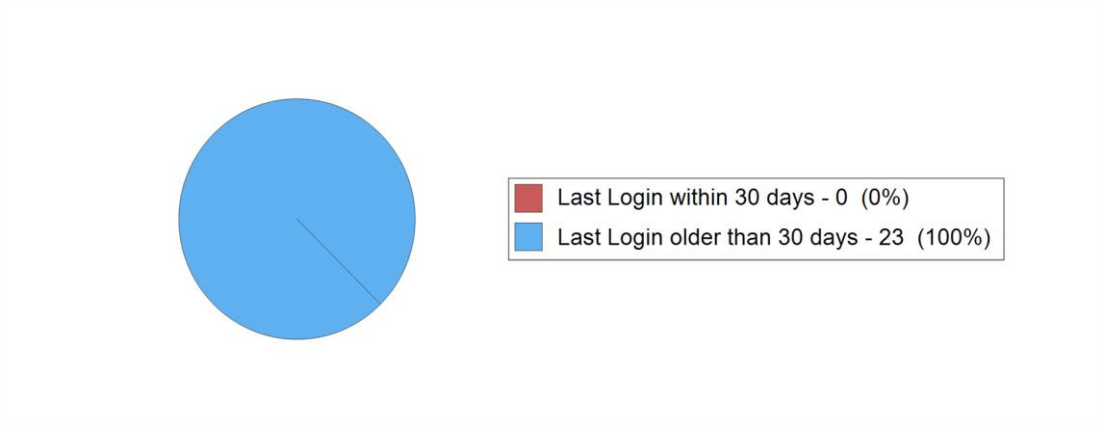
OPERATING SYSTEM (TOP FIVE)	TOTAL	PERCENT
Windows 10 Pro	5	71.4%
Windows Server 2008 R2 Standard	1	14.3%
Windows Server 2016 Standard	1	14.3%
Total - Top Five	**7**	**100%**

OPERATING SYSTEM (OTHER)	TOTAL	PERCENT
Total - Other	**0**	**0%**

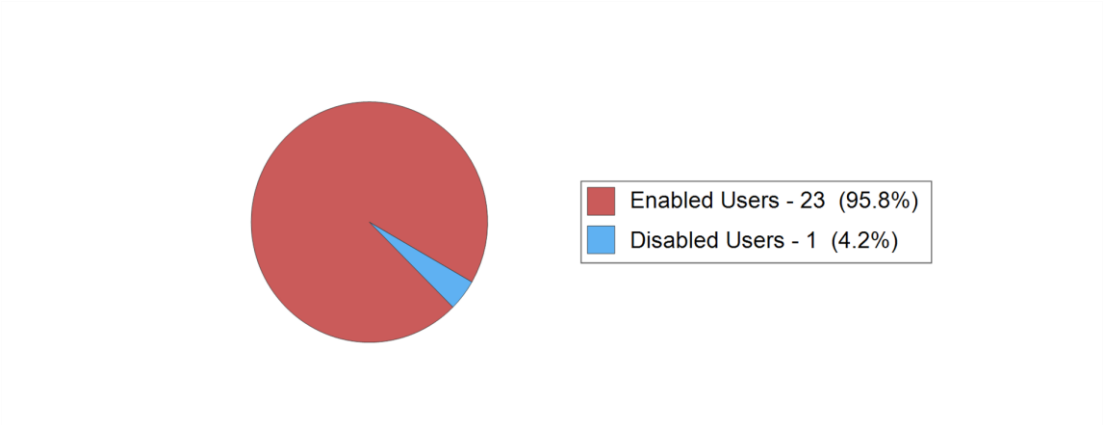
OVERALL TOTAL	7	100%

Asset Summary: Users

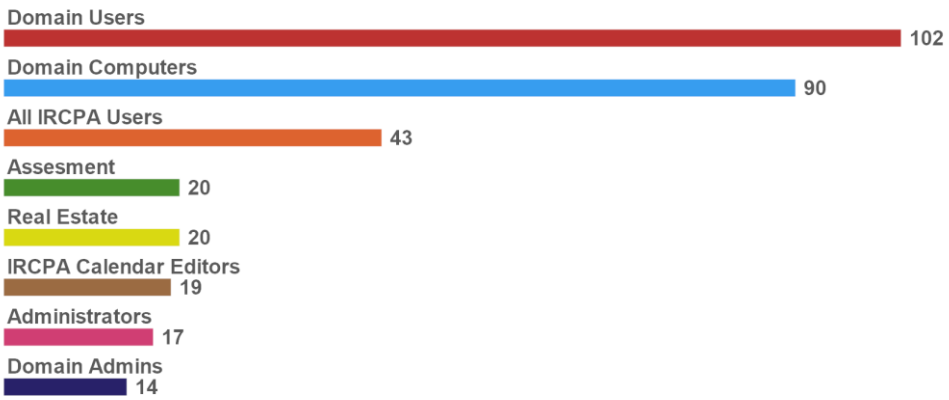
Users Logged in



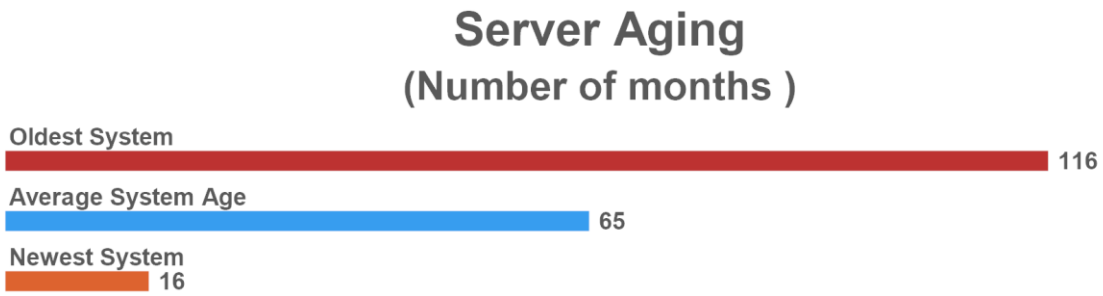
Total Users



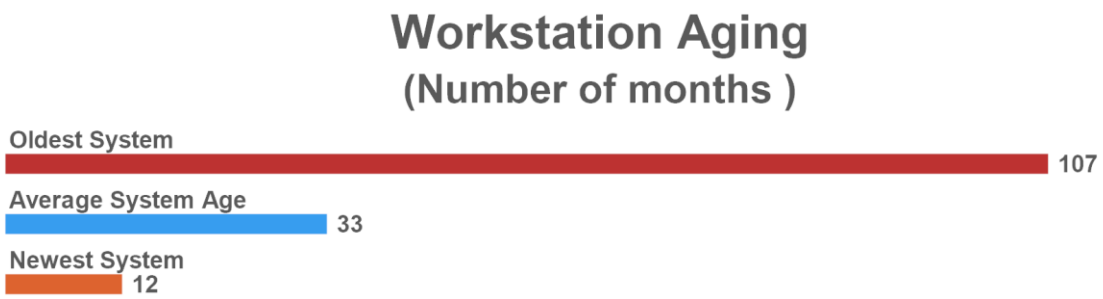
Security Group Distribution (Admin Groups + Top 5 Non-Admin Groups)



Server Aging

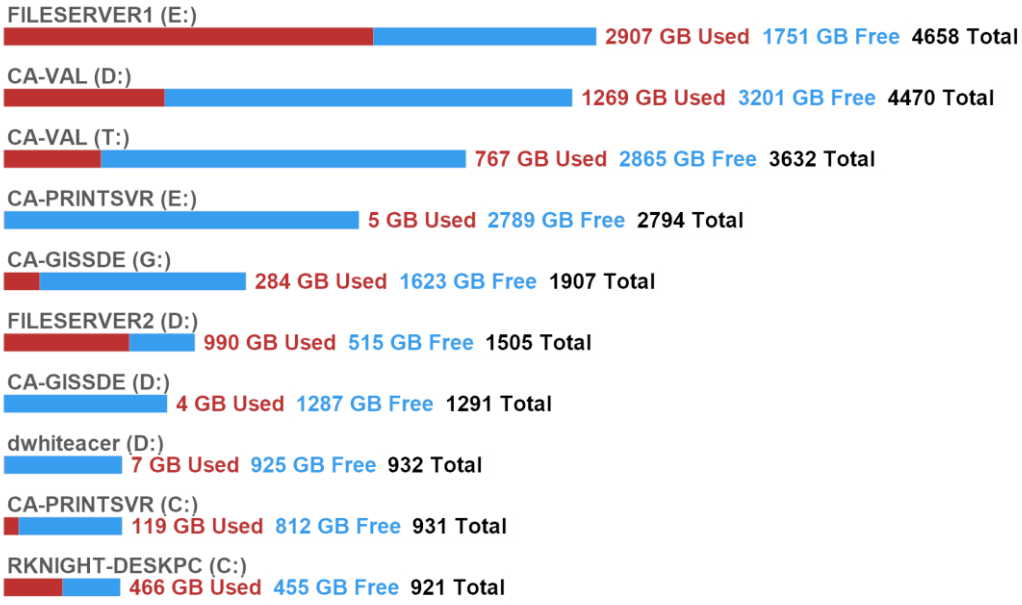


Workstation Aging

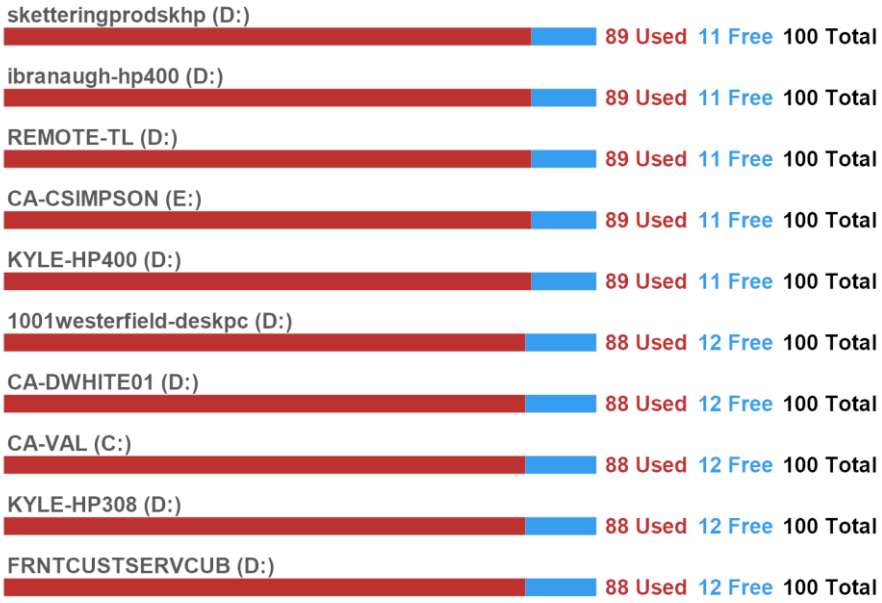


Asset Summary: Storage

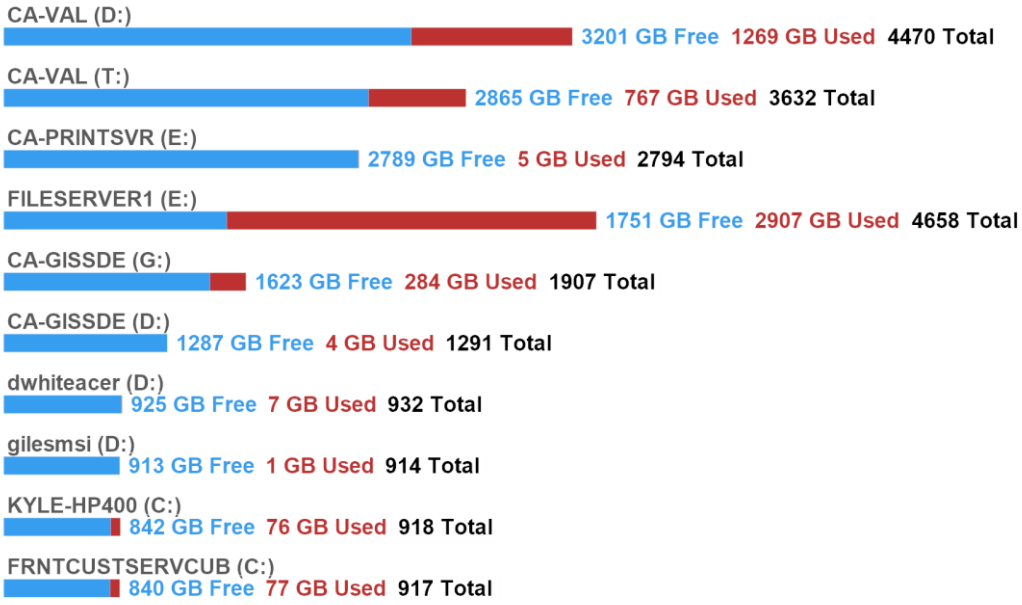
Top 10 Drive Capacity



Top 10 Drive % Used



Top 10 Drive Free Space



External Vulnerabilities

High (0) | Medium (6) | Low (1)

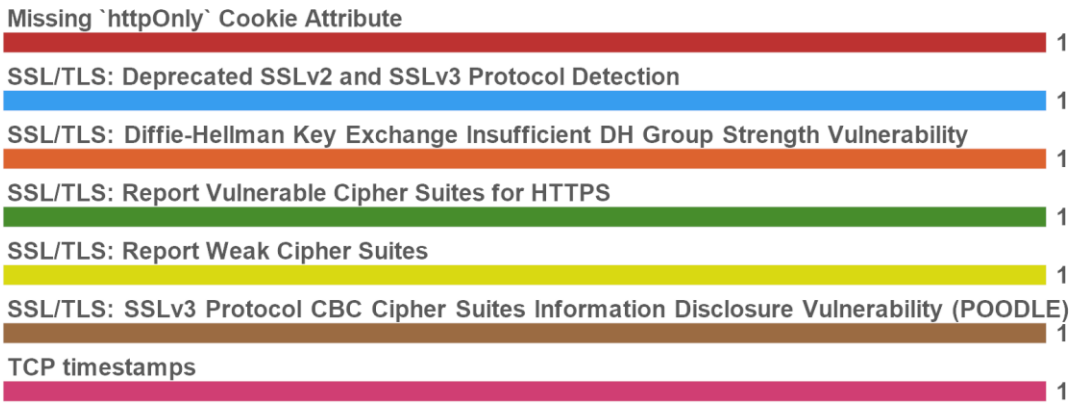
Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	FALSE	HIGHEST CVSS
209.215.109.60 (60.32.109.215.209.in-addr.arpa)	0	0	0	0	0	0.0
66.11.8.80 (66-11-8-80.orf.contbb.net)	3	0	6	1	0	5.0
Total: 2	3	0	6	1	0	5.0

Top Highest Risk (By CVSS Score)

Detected Operating Systems

Issues by NVT



ISSUE	COUNT
TCP timestamps	1
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	1

ISSUE	COUNT
SSL/TLS: Report Weak Cipher Suites	1
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	1
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1
Missing `httpOnly` Cookie Attribute	1

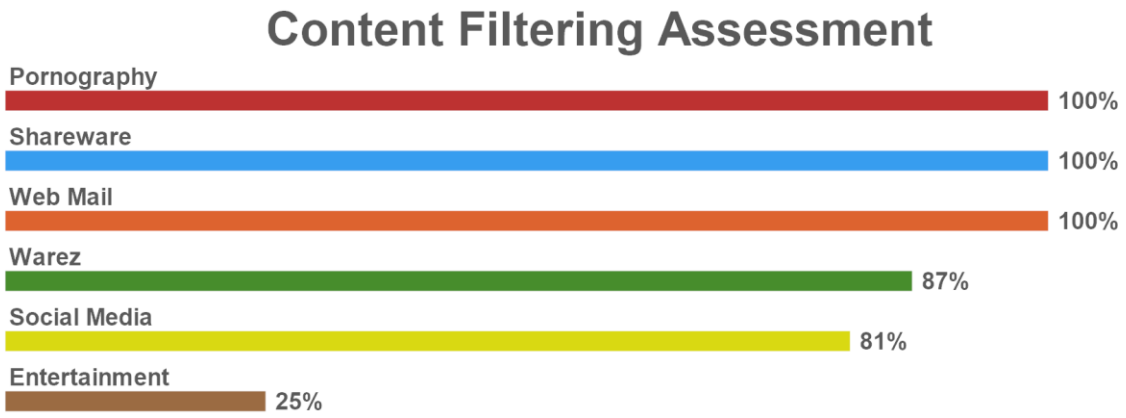
Internal Vulnerabilities

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

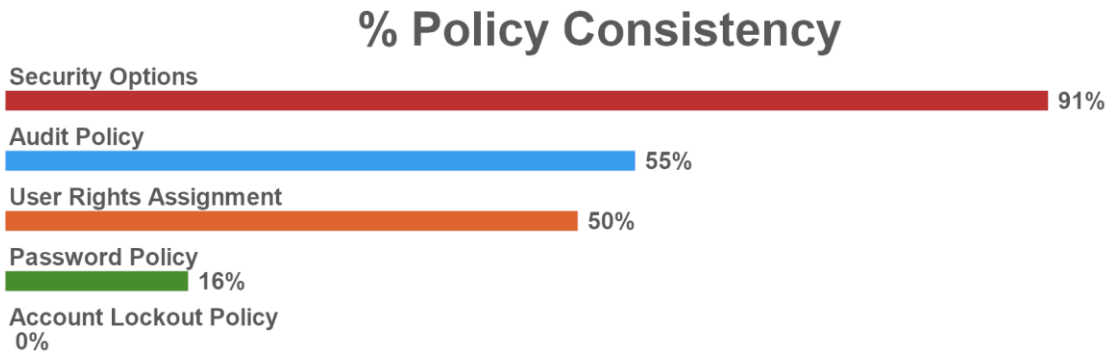
Host Issue Summary

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 using ID Agent (www.idagent.com).

Only the first 5 per domain are listed here.

EMAIL	PASSWORD/SHA1	COMPROMISE DATE	SOURCE
dstaar@ircpa.org	jord**********	2019/10/02 10:15:00 AM	file-upload
lchavis@ircpa.org	chie**********	2019/10/02 10:12:00 AM	file-upload
mstrickland@ircpa.org	mont**********	2019/10/02 10:15:00 AM	file-upload
nneill@ircpa.org	vero**********	2019/10/02 10:14:00 AM	file-upload