Your Company SITE SECURITY AUDIT

XXXXXXXXXXX

This document contains the final report of the full-site security audit of the Your Company network and associated servers.

Document Version Number: 1.03
Last Modified: February, 18 2017

ATTENTION

This document contains information from xxxxxxxxxthat is considered confidential and privileged. This information is intended for the private use of CompanyXXX. By accepting this document, you agree to keep the contents in confidence and to not copy, disclose, or distribute this document in whole or part without a written request to *and* written confirmation from xxxxxxxxxxx. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document in whole or part is prohibited.

TABLE OF CONTENTS

1.0 Executive Summary

This document details the security audit for the Your Company networks and servers.

The security audit begins with a full assessment of the network's security posture. This is accomplished by using various tools and automated scanners, as well as a manual review of system configurations, in order to find all vulnerabilities and security issues from within the network. These tests are performed using valid credentials created solely for the purpose of the assessment. Following the internal assessment, a penetration test is performed from outside the system. This "pen test" will check to see if the security measures are in place and functioning as expected. The pen test will also examine the responsiveness of any reactionary systems active on the network.

1.1 Acronyms, Abbreviations, and Glossary

Term	Definition
DISA	Defense Information Systems Agency
DRAC	Dell Remote Access Cards
EOL	End Of Life
FIFO	First In, First Out
IDS	Intrusion Detection System
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
Phishing	The act of attempting to acquire personal information via the internet through various deceptive practices.
PII	Personal Health Information
RDS	Remote Desktop Services
SSH	Secure Shell
SSL	Secure Sockets Layer
STIG	Security Technical Information Guides
USB	Universal Serial Bus
VPN	Virtual Private Network

2.0 Scope of Work

The audit [State the systems covered in the audit].

3.0 Summary Findings

Threat Level Description: The scores range from 0 to 10.

7-10	Critical
4-6.9	Major
0-3.9	Minor

(See the Wikipedia article on CVSS at http://en.wikipedia.org/wiki/CVSS for more information.)

OVERALL SECURITY HEALTH LEVEL – '3' (out of 10 with 10 being the most critical and 1 the healthiest)

The Your Company network was found to be in good security posture. In most cases, the findings and recommendations of this report represent additional levels of security that should exist for the system. The VPN profiles for the Your Company network are configured in a manner that would prevent a VPN user from accessing the Your Company networks. The VPN user can only access computers in the colo. With this configuration, the "Insider Threat" by VPN to the Your Company office is halted, as those machines would have no access. This is by design and considered optimal. Other notable issues include:

1. Threat Level 8: With the exception of the OWA server, system updates seem to be sporadic. Not all systems are at the same patch level, and all systems are behind in patching.
2. Threat Level 8: Windows XP will be beyond End of Life in April 2014.
3. Threat Level 8: Windows Server 2003 sp1 is beyond End of Life.
4. Threat Level 6: SSL for the OWA server is accepting SSLv2.
5. Threat Level 5: Server for OWA still has default IIS page.
6. Threat Level 5: Multiple servers in colo are running IIS with default web page available.
7. Threat Level 5: Minimum password length shorter than accepted industry standard.
8. Threat Level 5: No password expiration policy set.

4.0 Summary of Recommendations

- Threat Level 8: Upgrade computers with End of Life operating systems.
- Threat Level 8: Establish a set schedule for system updates (weekly).
- Threat Level 8: Implement a stronger site password policy.
- Threat Level 6: Disable SSLv2 on OWA Server.
- Install a vulnerability management system such as Rapid7's Nexpose.

4.1 User Education and continuing training

The audit and penetration test serves to verify that the technical controls in place on the network are functioning as expected. However, the technical controls can still be rendered ineffective if the users of the network are not sufficiently vigilant in maintaining and understanding basic computer and network security. Most major network intrusions in recent years were not attributed to obscure technical flaws, but to the inadvertent actions of users. Users should be mindful that the following technologies and tactics are the most likely vectors for network intrusions.:

4.1.1 General practices

THREAT (level 9) – Antivirus (not installed or up to date):

In the ever-changing landscape of computer security, it is essential that *all* computers run an anti-virus and anti-malware program. In addition, updates to this program need to be applied regularly and consistently.

PREVENTIVE SOLUTION:

Keep antivirus up to date on pre-determined schedule and along with anti-malware software.

4.1.2 Phishing & Spear phishing

THREAT (level 7) - Phishing:
Often attackers will use "phishing" (a form of social engineering in which individuals use email to masquerade as a legitimate entity) to try and convince a user to open an infected email attachment or click on links that lead to malicious web sites. These emails are formatted and laid-out as to convince the reader that they are from a valid source. They may be personalized and written in such a way that they appear to be coming from people the recipient knows personally, or may to appear to come from a coworker or other reputable source (such as a bank). Once opened, an attachment within the email could then compromise the computer and/or network by giving the attacker access and control of the target computer. Emails containing links to external web pages could be configured to send the user to a web page controlled by an attacker. The attackers could then install malicious software or try to collect the user's credentials (such as username and password) or other personal information (such as credit card data).

PREVENTIVE SOLUTION:
In order to offer protection against these threats, users should be educated to *NEVER* click on links or open attachments in an email unless they are absolutely certain of the origin of the email.

4.1.3 Web sites with malicious code

THREAT (level 6) - Watering Hole:
A new popular web-based threat vector is known as the "Watering Hole" attack. In this attack, a popular website frequented by the target group is infected with malicious code. When the target user browses to this site, vulnerabilities in the user's web browser could be used to gain access to the user's computer or install malicious software on the user's computer.

PREVENTIVE SOLUTION:
Unfortunately, there is no easy way to avoid these attacks. The best defense is to ensure malware detection and prevention software is kept up to date.

4.1.4 USB devices

THREAT (level 4) - USB Offering
Attackers are known to leave USB (Universal Serial Bus) drives lying about a targeted office or offer them to users by stating they contain free demos. Instead of a software demo, these USB keys would contain software capable of compromising any system they are plugged into. They may also contain what is called a "Trojan" in the form of infected executables, documents, or images.

PREVENTIVE SOLUTION:
It is best practice to always scan USB keys and other removable media—such as CDs or DVDs—for viruses and malware before using them. If the source of the device is unknown, any data on the device should be treated with extreme caution.

5.0 Testing Methodology

5.1 White box Versus Black Box

This Your Company Security Audit was based on white box testing methodology. In a white box test, the analyst is given full access to all systems inside and outside of the protection boundaries of the network being tested. The analyst uses that access to determine possible attack vectors by analyzing system security posture and configurations. The tester will then attempt to exploit vulnerabilities found during the assessment to validate any security concerns found. White box testing is a more time-efficient and comprehensive test than the alternative, a black box test. In black box testing, the analyst is given no knowledge of the network and must use the access vectors available to anyone on the Internet to attempt to gain access to the network. While this type of testing may seem to be more realistic, it is significantly less comprehensive.

5.2 Threat Vectors

Trusted Insider Threat

For the purposes of this audit, a trusted insider is considered to be anyone with VPN access to the Your Company networks or a user on the Your Company networks. The basic assumption during this test is that a computer used by an authenticated VPN user or a computer on the Your Company network has been compromised. The attacker at this point would have access to the Your Company network equal to that user's access level.

External Network Threats

The external threat is based on an attacker who has no prior access to the Your Company networks and is attempting to gain access to the Your Company network or its data. Additionally, testing was performed from various points within the Your Company network to validate that firewall rule sets preventing access from the Your Company network to the Registry networks were functioning properly.

6.0 Detailed Findings & Recommendations

6.1 Most systems are missing critical security patches (Threat Level 8)

6.1.1 Explanation

System updates are an essential part of maintaining a secure system. As new vulnerabilities are discovered almost daily, it's important to have the most recent software updates installed in order to minimize the number of vulnerabilities to a system. Ideally, updates are installed as soon as they are available. However, this may not be feasible on production systems. The majority of high and critical vulnerabilities found by the vulnerability scanners are attributed to a lack of updates. (Reference: Nexpose and OpenVAS reports.)

6.1.2 Recommendation

If necessary, a schedule should be established to take the servers down in order to perform system updates. Given that the user base for the network is rather small, it should be feasible to perform updates during low usage times such as late nights or weekends to minimize the impact to users.

6.2 End of Life Operating Systems (Threat Level 7)

6.2.1 Explanation

Operating system vendors as well as hardware vendors limit the amount of time that they provide support for their products. Once a product passes its end of life (EOL), the vendor will no longer provide parts, patches, or security updates for the product. The xxxxxxxx residence has 1 Windows Server 2003 instance. The Windows 2003 sp1 server has already passed Microsoft's EOL in April of 2009.

6.2.2 Recommendation

Plan to upgrade or decommission this machine as soon as possible.

6.3 Minimum password length less than industry standards (Threat Level 5)

6.3.1 Explanation

The National Institute of Standards and Technology (NIST) refers to the Defense Information Systems Agency (DISA) Security Technical Information Guides (STIG). The STIG recommends a password minimum of 14 characters using all four-character classes (upper case, lower case, numbers, and special characters.) See supporting document: RedHat6_STIG.pdf.

6.3.2 Recommendation

Increase required password complexity.

6.4 Most accounts have passwords with no expiration (Threat Level 5)

6.4.1 Explanation

The National Institute of Standards and Technology (NIST) refers to the Defense Information Systems Agency (DISA) Security Technical Information Guides (STIG). The STIG recommends a maximum password age of less than 60 days. The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the passwords. Further, scheduled changing of passwords hinders the ability of unauthorized system users to crack passwords and gain access to a system. See supporting document: Win2k8R2_STIG.xlsx.

6.4.2 Recommendation

Establish a password expiration policy of less than 60 days.

6.5 IIS Default web page found on OWA server and other Windows servers on the network (Threat Level 5)

6.5.1 Explanation

The IIS default installation or "Welcome" page is installed on the OWA server and two other servers in the colo as well as 3 servers in the NY Your Company office. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, IIS is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

6.5.2 Recommendation

If IIS is required, the default page should be removed. If the IIS service is not required, then IIS should be disabled.

6.6 OWA server supports SSLv2 (THreat Level 4)

6.6.1 Explanation

Although the server accepts clients using TLS or SSLv3, it also accepts clients using SSLv2. SSLv2 is an older implementation of the Secure Sockets Layer protocol. It suffers from a number of security flaws allowing attackers to capture and alter information passed between a client and the server, including the following weaknesses:

- No protection from against man-in-the-middle attacks during the handshake.
- Weak MAC construction and MAC relying solely on the MD5 hash function.
- Exportable cipher suites unnecessarily weaken the MACs
- Same cryptographic keys used for message authentication and encryption.
- Vulnerable to truncation attacks by forged TCP FIN packets

SSLv2 has been deprecated and is no longer recommended. Note that neither SSLv2 nor SSLv3 meet the U.S. FIPS 140-2 standard, which governs cryptographic modules for use in federal information systems. Only the newer TLS (Transport Layer Security) protocol meets FIPS 140-2 requirements.

6.6.2 Recommendation

Since all modern browsers support TLS and SSLv3, it should be safe to disable SSLv2 support for the OWA server and require all clients to use either TLS or SSLv3. (Reference: Nexpose Report and OWS-SSL_Labs_Report.pdf.)

6.7 Install a vulnerability management and tracking system such as Rapid7's Nexpose

An enterprise vulnerability management system can proactively find and track security vulnerabilities, misconfigurations, and malware within the network. It can also be used to provide consistent reporting and evaluation of the network over time to help find security trends. Keeping track of the vulnerabilities and validating configurations will help maintain the highest security level for the entire network.

7.0 Supporting Data (Raw Tool outputs and Summaries)

All supporting data is supplied in digital format. The contents are organized in the following directories:

1. **Nmap Scans**: Nmap ("Network Mapper") is utility for network discovery and security auditing. The reports are saved as HTML files and named according to the site contained in the scan.

2. **OpenVAS Scans**: OpenVAS is framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The reports are saved as HTML files and named for the Operating Systems scanned in the report.

3. **Nexpose Reports:** Nexpose by Rapid7 is an Enterprise Vulnerability management suite. (Rapid7 also created and maintains the most popular framework for exploits known as Metaploit.) The reports are saved as PDF files and have been named for the associated site.

4. **Standards:** This directory contains any standards documents referenced by the report.