DOMINANT SYSTEMS CORPORATION
3850 VARSITY DR.
ANN ARBOR, MI 48108

Computer Network Security Assessment

Performed for
ABC, Inc.

By Jesse Roberts and William D. Ritchie

1/1/2017

Contains CONFIDENTIAL analysis and recommendations regarding the security procedures and policies related to the computer network owned by ABC, Inc. Ann Arbor, MI.

Computer Network Security Assessment
Executive Summary

January 1, 2017
Prepared for ABC, Inc.
12345 ABC Drive
Ann Arbor, MI 48108

By Jesse Roberts and William D. Ritchie
Dominant Systems Corporation
3850 Varsity Dr.
Ann Arbor, MI 48108
+1.734.971.1210

Introduction

Dominant Systems Corporation (DSC) was hired by ABC, Inc. (ABC) to analyze and prepare an assessment of external vulnerabilities related to the security systems and procedures of ABC's computer networks. DSC started scanning your networks on December 25th and continued through December 29th of 2017. These scans performed a number of tests and analyses with the goal of uncovering any computer network related security issues that could allow ABC's network to be infiltrated via the internet. While we cannot guarantee that our work has discovered all of the security vulnerabilities that exist within the systems used by ABC, we have analyzed the most critical systems and based on our tests and analyses, we respectfully submit our findings and recommendations below.

Methodology

In our analysis we ran several network security penetration tools including OpenVAS, Nmap, and Metasploit. These programs were used to gather information on internet-facing software programs as well as the currently installed version(s) of those programs. The issues and vulnerabilities in this report that we are concerned with are Medium (4.0-6.9 on the CVSS scale) or higher.

Results

1. HTTP TRACE XSS vulnerability

You have two systems that were found to be vulnerable to cross-site scripting attacks due to the debugging functions on the HTTP server(s) being enabled. The TRACK and TRACE methods are enabled. This is a diagnostic method that returns in the response body the entire HTTP request.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Disable the TRACK and TRACE methods or turn off the debugging functions on this server if they are not needed.*

2. DNS Amplification Attacks

Your DNS server was found to be misconfigured and is subject to being used for a DNS Amplification Attack. It is possible to use your DNS server to forge return IP addresses which allows an attacker to perform a Denial of Service attack on remote targets.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Disable recursion on your DNS server or at least do not allow recursion from outside networks.*

3. Weak SSL Ciphers

You have several servers that were found to have weak SSL ciphers. Weak SSL ciphers allow for the decryption of transmitted data.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Cease the support of these weak SSL ciphers. See the raw report for a list of ciphers that were found to be weak.*

4. SSL Certification expiration

You have several servers that are using an old, default SSL certificate which expired in July of 2013.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Generate and use a new SSL certificate for these servers.*

5. SSH Weak Encryption Algorithms Supported

You have two systems that support weak SSH encryption algorithms.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Disable the weak encryption algorithms. You may also want to consider turning off all SSH access from the outside if it is not absolutely necessary. See the raw report for a list of weak algorithms we found were being used.*

6. Missing httpOnly Cookie Attribute

There is an application running on several servers that has cookies that are missing the 'http0nly' attribute. This could allow a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Set the 'http0nly' attribute for any session cookies.*

7. IIS Service Packs

It appears that you have IIS versions that are old and/or not up to the latest service pack. As IIS service packs contain many security fixes it stands to reason that your systems may be vulnerable if this is the case. While we can't confirm your versions either way because our external scanning tools rely on certain values within the IIS Server's 404 error message; we felt this was something we should mention to you as a precautionary measure so you could verify this on your side.

Systems affected - 255.255.255.255

Recommendation – **MEDIUM PRIORITY** – *Ensure that all IIS servers are running the latest service packs or consider using a newer version of IIS. In addition, our scans also indicated that you were running Windows Server 2003. If this is true, then you should consider moving to a newer operating system as Windows Server 2003 is no longer supported and is likely to be increasingly vulnerable in the future.*

8. SSL Diffie-Hellman Key Exchange

Several of your systems use Diffie-Hellman groups with insufficient strength. Any key size of less than 2048 is considered insufficient.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY –** *Use a 2048-bit or stronger Diffie-Hellman group.*

9. SSL versions

It was possible to detect deprecated SSLv2 and/or SSLv3 protocol(s) on some systems. An attacker can use known cryptographic flaws to eavesdrop the connection between clients and the service, thus obtaining sensitive data transferred within the secured connection.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY –** *You should disable the SSLv2 and/or SSLv3 protocol(s) in favor of the TLSv1.1+ protocols.*

10. SCTP Vulnerability (Potential DoS)

One of your systems is potentially vulnerable to an ICMP Denial of Service attack. Linux Kernels older than 2.6.13 contain a bug that could allow an attacker to send malformed ICMP packets and cause a kernel panic. We were unable to confirm the veracity of this as we did not want to take your system down, however, it is something you should take a look at as a precautionary measure.

Systems affected – 255.255.255.255

Recommendation – **HIGH PRIORITY –** *Update to Linux 2.6.13 or later and/or disable SCTP support.*

11. HTTP 1.1 header overflow

One of your systems is potentially vulnerable to an HTTP attack. By sending an invalid request with a long HTTP 1.1 header an attacker might be able to bring down your web server. We were unable to confirm this as we did not want to bring the web server down, but it is something you should look at.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY –** *Upgrade your software or protect it with a filtering reverse proxy.*

12. TFTP software vulnerability

One of your systems is potentially vulnerable to a software Denial of Service attack. This attack is only for the Hillstone Software TFTP Server. The scan indicated that you were running this software, but we could not verify this or if the server was vulnerable as we did not want to bring your server down. We just wanted to mention this as a precautionary measure.

Systems affected – 255.255.255.255

Recommendation – **MEDIUM PRIORITY –** *If you are using this software, then upgrade to the latest version or contact Hillstone for a fix. If you are not using this software, then you can safely ignore this.*

Executive Summary

Based on our analysis of ABC's network from an external perspective, we find that your network has a number of external vulnerabilities that need to be addressed. Many of these vulnerabilities can be addressed by simply patching systems/services up to the latest versions or making minor configuration changes. It is important to note that you only had one potential "High" priority item this year and no critical items. A majority of the items we found were to be of a "Medium" priority based on the CVSS scale. Overall, we are of the opinion that your network is more secure than it was a year ago.

It should be noted that we did not attempt to fully exploit all of the vulnerabilities stated in this report. This is due to potential impact upon your live production systems that would cause direct harm to the business.

As stated elsewhere in this document, no network can be made 100% free from vulnerabilities, and over time vulnerabilities can crop up where they did not exist before. In addition, we only tested for vulnerabilities that can be found externally, potentially missing other security exploits that can come from inside the network. Therefore, besides rectifying the problems detailed in this report, we recommend that you have a Comprehensive Network Security Assessment performed at least once a year. This type of Assessment would include analysis of your software update services, network documentation, personnel cross-training, intrusion detection systems, network access and segmentation, wireless networks, potentially illegal activity, password security, infiltration from both internal and external sources, acceptable use policies, virus, spyware and malware defenses, physical access, hardware / software fault-tolerance, data backup and archiving, and disaster recovery.

Respectfully submitted,

Jesse Roberts and William D. Ritchie

Dominant Systems Corporation.
3850 Varsity Dr.
Ann Arbor, MI 48108
http://www.domsys.com
+1.734.971.1210
+1.734.677.3321 fax

COMPUTER NETWORK SECURITY REPORT CARD

ABC, Inc.
January 1, 2017

Focus Areas	Grade
1) Infiltration from External Sources	B
2) Infiltration from Internal Sources	N/A
3) Wireless Threats	N/A
4) Physical Access	N/A
5) Intrusion Detection	N/A
6) Password Security	N/A
7) Virus/Spyware/Malware Detection and Removal	N/A
8) Acceptable Use Policies	N/A
9) Backup and Archiving	N/A
10) Hardware and Software Fault-Tolerance	N/A
11) Software Update Services	N/A
12) Potentially Illegal Activity	N/A
13) Network Documentation	N/A
14) Network Access and Segmentation	N/A
15) Personnel Cross-Training and Backup	N/A

Overall Grade	N/A