|  |  |  |
| --- | --- | --- |
| Image | |  |
| Penetration Test Report for Contoso Inc. | | |
| Adataum Security, Llc.  01/01/2020  John Smith |  | |

# Confidentiality Statement

This document contains confidential and privileged information from Contoso Inc. (henceforth known as Contoso). The information contained in this document is confidential and may constitute inside or non-public information under international, federal or state laws. Unauthorized forwarding, printing, copying, distribution or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

# Contact Information

|  |  |
| --- | --- |
| **Company Name** | Adatum Security, Llc. |
| **Contact Name** | John Smith |
| **Contact Title** | Senior Penetration Tester |
| **Contact Phone** | 913.555.1234 |
| **Contact Email** | j.smith@adatum.com |
| **Qualifications** | GIAC Certified Penetration Tester  License #12345  5 Years’ experience working within highly secured computing environments. |

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Comments** |
| 001 | 10/01/2016 | J. Smith |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

In accordance with Contoso’s policies, Adatum Security, Llc (Henceforth known as Adatum) conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of the engagement was to assess the networks’ and systems’ security and identify potential security flaws in them by utilizing industry accepted testing methodology and best practices. The project was conducted on a number of systems on Contoso’s network segments by Adatum during June of 2016.

For the testing, Adatum focused on the following:

* Attempt to determine what system level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
* Attempt to determine what Web Application vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
* Attempt to exploit vulnerabilities found and access confidential information that may be stored on systems.
* Document and report on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers.

This document contains the results of that assessment.

# Executive Summary

## Project Information

The primary goal of this assessment was to provide an analysis of security flaws present in Contoso’s web applications, networks and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on remediating the vulnerabilities to provide a greater level of security for the environment.

Adatum used its proven vulnerability testing methodology to assess all relevant web applications, networks and systems in scope.

## Penetration Testing Methodology

### Identification of Vulnerabilities and Services

Adatum used custom, private and public tools such as Putty, Metasploit, Kali Linux, AppSpider, BurpSuite, Nmap and Nexpose to gain perspective of the network security from a hacker’s point of view. These methods provide Contoso with an understanding of the risks that threaten its information, and also the strengths and weaknesses of its current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system level vulnerabilities, attempting to discover unexpected hosts within the environment and eliminating false positives that might have arisen from scanning.

### Vulnerability Exploitation

Adatum’s normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Adatum was unsuccessful in exploiting any potential vulnerabilities during the penetration test. Network segmentation testing confirmed the accuracy of configurations detailed in the provided network diagram and firewall rulesets. Therefore, the overall result of the penetration test is a **Pass.**

### Main Exposures

Adatum’s evaluation of Contoso’s web applications, internal, and external networks found no direct exploitable vulnerabilities of any impact to the systems or Contoso’s customers.

### Re-testing

Having a passing result of the penetration tests, penetration testing of the assets defined in this document will not be necessary until the next period of testing as defined by Contoso’s policies and procedures or until after a change has been made to the configuration of the assets defined in this scope including systems, networks, and any web applications hosted by Contoso.

## Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose on the business processes implemented by the application, based on the following criteria:

**Critical**: Immediate threat to key business processes.

**High**: Indirect threat to key business processes/threat to secondary business processes.

**Medium**: Indirect/partial threat to business processes.

**Low**: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.

**Pass:** Exploit unavailable or unsuccessful

**Fail**: Exploit able to gain privileges and/or disclose information

Note: “Unique” is defined as the number of different exploitable vulnerabilities found within that risk level. For example, if five High level exploits were found, but three are Unique, then some of the exploitable vulnerabilities are present on more than one host.

## Summary of Findings - External

No Vulnerabilities were discovered. Therefore, the overall result of the penetration test is a **Pass**.

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Severity** | **Test Result** |
| No vulnerabilities were discovered |  | **Pass** |

The summary tables below represent an overview of the assessment findings for the external penetration test.

|  |  |
| --- | --- |
| **Scan Type** | **Total** |
| Hosts | 19 |
| Ports | TCP, UDP 1-65535 |

|  |  |
| --- | --- |
| **Exploitation Risk** | **Total** |
| **High** | 0 (Unique:0) |
| **Medium** | 0 (Unique:0) |
| **Low** | 0 (Unique:0) |

## Summary of Findings – WebApp Penetration Testing Results

After extensive testing of each web application, there were no vulnerabilities discovered. Therefore, the overall result of the penetration test is a **Pass**.

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Severity** | **Test Result** |
| No vulnerabilities were discovered |  | **Pass** |

The summary tables below represent an overview of the assessment findings for the WebApp penetration test.

|  |  |
| --- | --- |
| **Scan Type** | **Total** |
| Hosts | 9 |
| Forms | 149 |

|  |  |
| --- | --- |
| **Exploitation Risk** | **Total** |
| **High** | 0 (Unique:0) |
| **Medium** | 0 (Unique:0) |
| **Low** | 0 (Unique:0) |

## Summary of Findings - Internal

No Vulnerabilities were discovered. Therefore, the overall result of the penetration test is a **Pass**.

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Severity** | **Test Result** |
| No vulnerabilities were discovered |  | **Pass** |

The summary tables below represent an overview of the assessment findings for the internal penetration test.

|  |  |
| --- | --- |
| **Scan Type** | **Total** |
| Hosts | 3 |
| Ports | TCP, UDP 1-65535 |

|  |  |
| --- | --- |
| **Exploitation Risk** | **Total** |
| **High** | 0 (Unique:0) |
| **Medium** | 0 (Unique:0) |
| **Low** | 0 (Unique:0) |

# External Facing Assets

Adatum utilized a document containing all public facing websites, web forms, and IP ranges within the Contoso production and corporate environments. The items tested against are as follows:

## Public Facing IP Ranges:

192.0.2.0/24

198.51.100.0/24

203.0.113.0/24

## **Public Facing Websites**

https://adventure-works.com

https://alpineskihouse.com  
https://cohowinery.com  
https://contoso.com  
https://contoso.net  
https://contosohotel.com  
https://fabrikam.com  
https://northwindtraders.com  
https://treyresearch.net

## Public Facing WebForms

http://203.0.113.15:80/ATLAS/Default.aspx

http://203.0.113.15:80/atlas/WebResource.axd

http://203.0.113.15:80/redreports/Default.aspx

http://203.0.113.15:80/redreports/WebResource.axd

https://203.0.113.15:443/ATLAS/Default.aspx

https://203.0.113.15:443/atlas/WebResource.axd

https://203.0.113.15:443/redreports/Default.aspx

https://203.0.113.15:443/redreports/WebResource.axd

http://contoso.com:80/Account/ForgotPassword

http://contoso.com:80/Account/Login

http://contoso.com:80/Account/Register

http://contoso.com:80/Card

http://contoso.com:80/Error

http://contoso.com:80/Home/SetCulture

http://contoso.com:80/Promotion/RedeemCode

http://contoso.com:80/css/account-login

http://contoso.com:80/css/card-index

http://contoso.com:80/css/index

http://contoso.com:80/css/site

http://contoso.com:80/js/account-register

http://contoso.com:80/js/card-index

http://contoso.com:80/js/forgot-password

http://contoso.com:80/js/jqueryval

http://contoso.com:80/js/modernizr

http://contoso.com:80/js/site

http://adventure-works.com:80/Account/ForgotPassword

http://adventure-works.com:80/Account/Login

http://adventure-works.com:80/Account/Register

http://adventure-works.com:80/Card

http://adventure-works.com:80/Error

http://adventure-works.com:80/Home/SetCulture

http://adventure-works.com:80/css/account-login

http://adventure-works.com:80/css/card-index

http://adventure-works.com:80/css/index

http://adventure-works.com:80/css/site

http://adventure-works.com:80/js/account-register

http://adventure-works.com:80/js/card-index

http://adventure-works.com:80/js/forgot-password

http://adventure-works.com:80/js/jqueryval

http://adventure-works.com:80/js/modernizr

http://adventure-works.com:80/js/site

http://cohowinery.com:80/Account/ForgotPassword

http://cohowinery.com:80/Account/Login

http://cohowinery.com:80/Account/Register

http://cohowinery.com:80/Card

http://cohowinery.com:80/Error

http://cohowinery.com:80/Home/SetCulture

http://cohowinery.com:80/css/account-login

http://cohowinery.com:80/css/card-index

http://cohowinery.com:80/css/index

http://cohowinery.com:80/css/site

http://cohowinery.com:80/js/card-index

http://cohowinery.com:80/js/jqueryval

http://cohowinery.com:80/js/modernizr

http://cohowinery.com:80/js/site

http://iisadmin.contoso.net:80/ATLAS/Default.aspx

http://iisadmin.contoso.net:80/atlas/WebResource.axd

http://iisadmin.contoso.net:80/redreports/Default.aspx

http://iisadmin.contoso.net:80/redreports/WebResource.axd

https://iisadmin.contoso.net:443/ATLAS/Default.aspx

https://iisadmin.contoso.net:443/atlas/WebResource.axd

https://iisadmin.contoso.net:443/redreports/Default.aspx

https://iisadmin.contoso.net:443/redreports/WebResource.axd

http://info.contoso.net:80/Default.aspx

http://info.contoso.net:80/WebResource.axd

https://info.contoso.net:443/Default.aspx

https://info.contoso.net:443/WebResource.axd

http://contosohotel.com:80/Account/ForgotPassword

http://contosohotel.com:80/Account/Login

http://contosohotel.com:80/Account/Register

http://contosohotel.com:80/Card

http://contosohotel.com:80/Error

http://contosohotel.com:80/css/account-login

http://contosohotel.com:80/css/card-index

http://contosohotel.com:80/css/index

http://contosohotel.com:80/css/site

http://contosohotel.com:80/js/account-register

http://contosohotel.com:80/js/card-index

http://contosohotel.com:80/js/forgot-password

http://contosohotel.com:80/js/jqueryval

http://contosohotel.com:80/js/modernizr

http://contosohotel.com:80/js/site

http://www.fabrikam.com:80/Account/ForgotPassword

http://www.fabrikam.com:80/Account/Login

http://www.fabrikam.com:80/Account/Register

http://www.fabrikam.com:80/Card

http://www.fabrikam.com:80/Error

http://www.fabrikam.com:80/Home/SetCulture

http://www.fabrikam.com:80/css/account-login

http://www.fabrikam.com:80/css/site

http://www.fabrikam.com:80/js/account-register

http://www.fabrikam.com:80/js/forgot-password

http://www.fabrikam.com:80/js/jqueryval

http://www.fabrikam.com:80/js/modernizr

http://www.fabrikam.com:80/js/site

http://www.northwindtraders.com:80/Account/ForgotPassword

http://www.northwindtraders.com:80/Account/Login

http://www.northwindtraders.com:80/Account/Register

http://www.northwindtraders.com:80/Card

http://www.northwindtraders.com:80/Error

http://www.northwindtraders.com:80/css/account-login

http://www.northwindtraders.com:80/css/card-index

http://www.northwindtraders.com:80/css/index

http://www.northwindtraders.com:80/css/site

http://www.northwindtraders.com:80/js/account-register

http://www.northwindtraders.com:80/js/card-index

http://www.northwindtraders.com:80/js/forgot-password

http://www.northwindtraders.com:80/js/jqueryval

http://www.northwindtraders.com:80/js/modernizr

http://www.northwindtraders.com:80/js/site

http://www.treyresearch.net:80/Account/ForgotPassword

http://www.treyresearch.net:80/Account/Login

http://www.treyresearch.net:80/Account/Register

http://www.treyresearch.net:80/Card

http://www.treyresearch.net:80/Error

http://www.treyresearch.net:80/css/account-login

http://www.treyresearch.net:80/css/card-index

http://www.treyresearch.net:80/css/index

http://www.treyresearch.net:80/css/site

http://www.treyresearch.net:80/js/account-register

http://www.treyresearch.net:80/js/card-index

http://www.treyresearch.net:80/js/forgot-password

http://www.treyresearch.net:80/js/index

http://www.treyresearch.net:80/js/jqueryval

http://www.treyresearch.net:80/js/modernizr

http://www.treyresearch.net:80/js/site

# External Penetration Testing Results

## Scope

CONTOSO provided Adatum with the publicly accessible IP address range for the production environment (203.0.113.0/24). These public IPs correspond to the scope of subnets that were chosen for the internal penetration test. The IPs were scanned to determine open ports and services running prior to the penetration testing.

| **IP Address** | **Hostname** | **Ports** |
| --- | --- | --- |
| 203.0.113.1-19 | No Live Host Identified |  |
| 203.0.113.20 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.21 | No Live Host Identified |  |
| 203.0.113.15 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.23 | 203-0-113-20.isp.contoso.com | TCP/443 Open |
| 203.0.113.24 | No Live Host Identified |  |
| 203.0.113.25 | 203-0-113-20.isp.contoso.com | TCP/80 Open |
| 203.0.113.26 | No Live Host Identified |  |
| 203.0.113.27 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.28-45 | No Live Host Identified |  |
| 203.0.113.46 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.47-49 | No Live Host Identified |  |
| 203.0.113.50 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.51 | No Live Host Identified |  |
| 203.0.113.52 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.53-129 | No Live Host Identified |  |
| 203.0.113.130 | 203-0-113-20.isp.contoso.com | TCP/443 Open |
| 203.0.113.131 | No Live Host Identified |  |
| 203.0.113.132 | 203-0-113-20.isp.contoso.com | TCP/443 Open |
| 203.0.113.133-188 | No Live Host Identified |  |
| 203.0.113.189 | 203-0-113-20.isp.contoso.com | No open ports found |
| 203.0.113.190-196 | No Live Host Identified |  |
| 203.0.113.197 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.198 | No Live Host Identified |  |
| 203.0.113.199 | 203-0-113-20.isp.contoso.com | TCP/443 Open |
| 203.0.113.200 | 203-0-113-20.isp.contoso.com | TCP/443 Open |
| 203.0.113.201 | No Live Host Identified |  |
| 203.0.113.202 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.203 | No Live Host Identified |  |
| 203.0.113.204 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.205 | 203-0-113-20.isp.contoso.com | TCP/443 Open |
| 203.0.113.206 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.207 | No Live Host Identified |  |
| 203.0.113.208 | 203-0-113-20.isp.contoso.com | TCP/80 Open TCP/443 Open |
| 203.0.113.209-254 | No Live Host Identified |  |

# WebApp Penetration Testing Results

## Scope

CONTOSO provided Adatum with the publicly accessible web applications for the production environment (203.0.113.0/24). These WebApps correspond to the scope of subnets that were chosen for the external penetration test. The WebApps were scanned to identify existence of Coding, logic, or configuration flaws resulting in a vulnerability.

|  |  |
| --- | --- |
| **URL** | **WebSocket** |
| contoso.com | http(80) , https(443) |
| backoffice.contoso.net | http(80) , https(443) |
| cardfront.contoso.net | http(80) , https(443) |
| cardspot.contoso.net | http(80) , https(443) |
| adventure-works.com | http(80) , https(443) |
| dashboard.contoso.net | http(80) , https(443) |
| contosohotel.com | http(80) , https(443) |
| storelink.contoso.net | http(80) , https(443) |
| webservices.contoso.net | http(80) , https(443) |
| whitelabel-ecommerce.contoso.net | http(80) , https(443) |
| whitelabel.contoso.net | http(80) , https(443) |
| www.fabrikam.com | http(80) , https(443) |
| www.northwindtraders.com | http(80) , https(443) |

# Internal Penetration Testing Results

## Scope

The following networks were determined to be in scope for the internal network penetration test.

|  |  |  |
| --- | --- | --- |
| **VLAN** | **IP Address** | **Ports** |
| VLAN\_101 | 10.1.1.0/24 | PRIMARY DC |
| VLAN\_102 | 10.1.2.0/24 | PRIMARY DC |
| VLAN\_103 | 10.1.3.0/24 | PRIMARY DC |
| VLAN\_104 | 10.1.4.0/24 | PRIMARY DC |
| VLAN\_105 | 10.1.5.0/24 | PRIMARY DC |
| VLAN\_106 | 10.1.6.0/24 | PRIMARY DC |
| VLAN\_107 | 10.1.7.0/24 | PRIMARY DC |
| VLAN\_108 | 10.1.8.0/24 | PRIMARY DC |
| VLAN\_109 | 10.1.9.0/24 | PRIMARY DC |
| VLAN\_110 | 10.1.10.0/24 | PRIMARY DC |
| VLAN\_111 | 10.1.11.0/24 | PRIMARY DC |
| VLAN\_112 | 10.1.12.0/24 | PRIMARY DC |
| VLAN\_113 | 10.1.13.0/24 | PRIMARY DC |
| VLAN\_114 | 10.1.14.0/24 | PRIMARY DC |
| VLAN\_115 | 10.1.15.0/24 | PRIMARY DC |
| VLAN\_116 | 10.1.16.0/24 | PRIMARY DC |
| VLAN\_117 | 10.1.17.0/24 | PRIMARY DC |
| VLAN\_118 | 10.1.18.0/24 | PRIMARY DC |
| VLAN\_119 | 10.1.19.0/24 | PRIMARY DC |
| VLAN\_120 | 10.1.20.0/24 | PRIMARY DC |
| VLAN\_121 | 10.1.21.0/24 | PRIMARY DC |
| VLAN\_122 | 10.1.22.0/24 | PRIMARY DC |
| VLAN\_123 | 10.1.23.0/24 | PRIMARY DC |
| VLAN\_124 | 10.1.24.0/24 | PRIMARY DC |
| VLAN\_125 | 10.1.25.0/24 | PRIMARY DC |
| VLAN\_126 | 10.1.26.0/24 | PRIMARY DC |
| VLAN\_127 | 10.1.27.0/24 | PRIMARY DC |
| VLAN\_128 | 10.1.28.0/24 | PRIMARY DC |
| VLAN\_129 | 10.1.29.0/24 | PRIMARY DC |
| VLAN\_130 | 10.1.30.0/24 | PRIMARY DC |
| VLAN\_201 | 10.2.1.0/24 | BACKUP DC |
| VLAN\_202 | 10.2.2.0/24 | BACKUP DC |
| VLAN\_203 | 10.2.3.0/24 | BACKUP DC |
| VLAN\_204 | 10.2.4.0/24 | BACKUP DC |
| VLAN\_205 | 10.2.5.0/24 | BACKUP DC |
| VLAN\_206 | 10.2.6.0/24 | BACKUP DC |
| VLAN\_207 | 10.2.7.0/24 | BACKUP DC |
| VLAN\_208 | 10.2.8.0/24 | BACKUP DC |
| VLAN\_209 | 10.2.9.0/24 | BACKUP DC |
| VLAN\_210 | 10.2.10.0/24 | BACKUP DC |
| VLAN\_211 | 10.2.11.0/24 | BACKUP DC |
| VLAN\_212 | 10.2.12.0/24 | BACKUP DC |
| VLAN\_213 | 10.2.13.0/24 | BACKUP DC |
| VLAN\_214 | 10.2.14.0/24 | BACKUP DC |
| VLAN\_215 | 10.2.15.0/24 | BACKUP DC |
| VLAN\_216 | 10.2.16.0/24 | BACKUP DC |
| VLAN\_217 | 10.2.17.0/24 | BACKUP DC |
| VLAN\_218 | 10.2.18.0/24 | BACKUP DC |
| VLAN\_219 | 10.2.19.0/24 | BACKUP DC |
| VLAN\_220 | 10.2.20.0/24 | BACKUP DC |
| VLAN\_221 | 10.2.21.0/24 | BACKUP DC |
| VLAN\_222 | 10.2.22.0/24 | BACKUP DC |
| VLAN\_223 | 10.2.23.0/24 | BACKUP DC |
| VLAN\_224 | 10.2.24.0/24 | BACKUP DC |
| VLAN\_225 | 10.2.25.0/24 | BACKUP DC |
| VLAN\_226 | 10.2.26.0/24 | BACKUP DC |
| VLAN\_227 | 10.2.27.0/24 | BACKUP DC |
| VLAN\_228 | 10.2.28.0/24 | BACKUP DC |
| VLAN\_229 | 10.2.29.0/24 | BACKUP DC |
| VLAN\_230 | 10.2.30.0/24 | BACKUP DC |
| Guest Vlan | 192.168.1.0./24 | WHQ Office |
| Internal Data Vlan | 192.168.2.0./24 | WHQ Office |
| Third Floor | 192.168.3.0./24 | WHQ Office |
| Fourth Floor | 192.168.4.0./24 | WHQ Office |

The networks were scanned to identify live hosts and any running services.

|  |  |  |
| --- | --- | --- |
| **Host Name** | **IP Address** | **Port(s)** |
| 192.168.8.5 | Mgmt..contoso.net | TCP 22 |
| 192.168.7.4 | Diskstation.contoso.net | TCP 22 |
| 192.168.7.4 | Diskstation.contoso.net | TCP 443 |

## Additional Testing

Adatum attempted to log into the Synology DiskStation Administration web page using default and common credentials at https://diskstation.contoso.net and was denied access.

A screenshot of a cell phone

Description automatically generated

Adatum attempted to log into the corporate management server using default and common credentials at mgmt.contoso.net and was denied access.

A screenshot of a cell phone

Description automatically generated

Adatum attempted to log into the Synology Diskstation server using default and common credentials at diskstation.contoso.net and we were denied network level access.

A screenshot of a cell phone

Description automatically generated