



IT Security Auditing

September 13, 2016

Nate Robb, CISA, IT Auditor



Agenda



- Department of Revenue – Security of Taxpayer Information Report
 - Background
 - Findings
- IT Security Audit Approach
 - Penetration Testing
 - Social Engineering
 - Security Program Review
- IT Security Auditing w/ More Resources

Arizona Department of Revenue



- Department processes large volumes of sensitive taxpayer data
 - 5.7 million tax documents in fiscal year 2015
- Data used to perform core business functions:
 - Processing taxes
 - Auditing taxpayers
 - Performing economic analyses



Potential Target for Attack



- Sensitive data maintained makes the Department a likely target
- 420 data breaches of government organizations / educational institutions between 2011 and 2014
- Breaches worldwide increased 23 percent from 2013 to 2014

Recent Breaches



- Utah Department of Health – 780,000 records
 - \$2.75 million
- South Carolina Department of Revenue – 3.6 Million records
 - \$20.1 million
- U.S. Internal Revenue Service – 100,000 records

IT Security Audit Approach



- Penetration Testing
- Social Engineering
- Security Program Review (Policies and Procedures)

Penetration Testing

1. Information Gathering – Reconnaissance
2. IT System Scanning – Port Scanning
3. Exploitation
4. Repeat

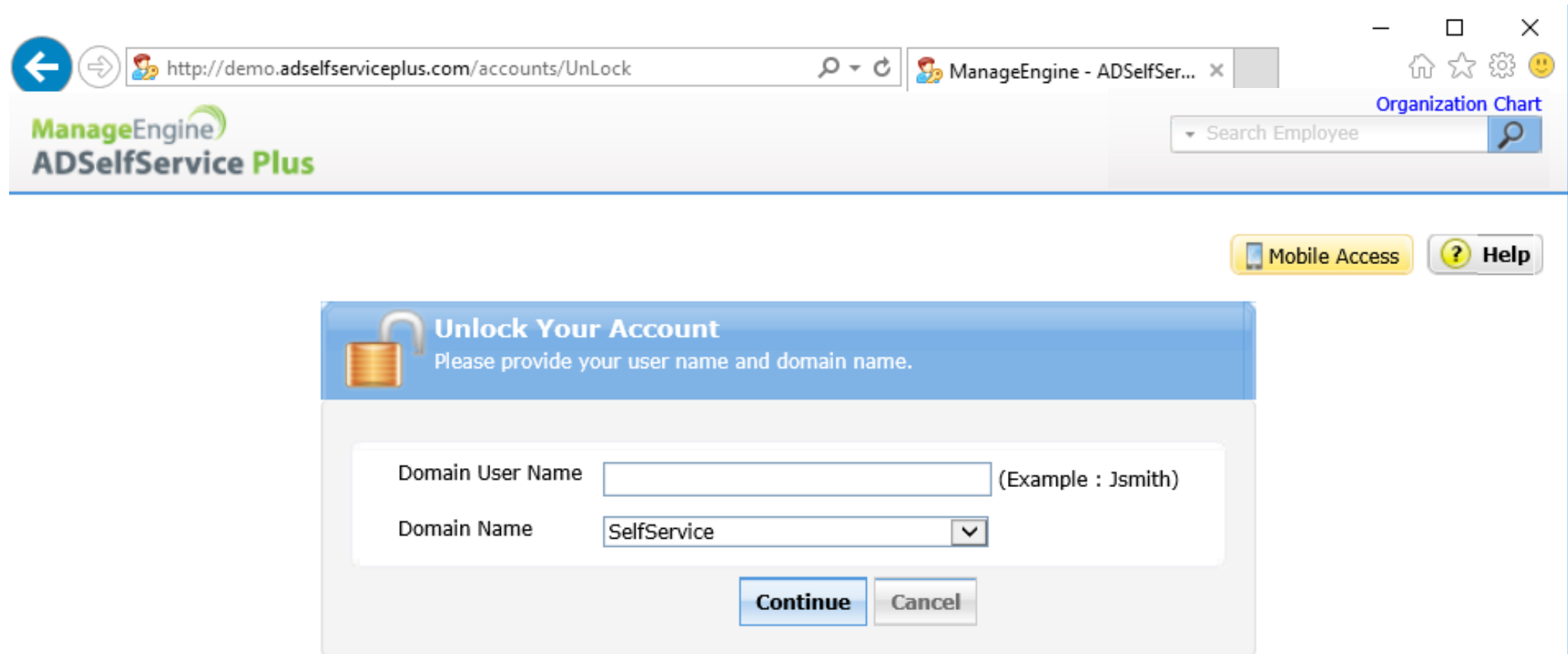


Penetration Testing – Information Gathering

- Gathering as much information about an entity as possible using public resources
 - Google
 - Shodan
 - Netcraft

The Google logo, consisting of the word "Google" in its characteristic multi-colored font.The Shodan logo, featuring three red circles of varying sizes to the left of the word "SHODAN" in a bold, black, sans-serif font.The Netcraft logo, featuring the word "NETCRAFT" in a bold, black, sans-serif font with a colorful, brush-stroke-like underline.

Information Gathering Example



Browser address bar: <http://demo.adselfserviceplus.com/accounts/UnLock>

Page Header: ManageEngine ADSelfService Plus

Page Header: Organization Chart

Page Header: Search Employee

Page Header: Mobile Access Help

Unlock Your Account
Please provide your user name and domain name.

Domain User Name (Example : Jsmith)

Domain Name


Information Gathering Example



Organization Chart for Domain: [adselfservice](#) [\[Change\]](#) [Mobile Access](#) [Help](#)

adselfservice

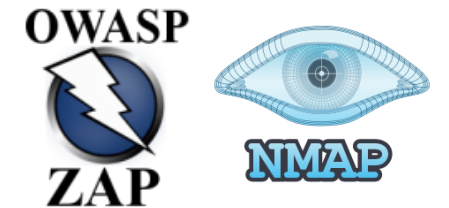
- Un-Managed Users
 - Administrator
 - Guest
 - adssp
 - sysadm
 - krbtgt
 - parthiban
 - umarajeshwaran
 - sspadmin**
 - DemoUser1
 - DemoUser2
 - selfuser1
 - selfuser100
 - testuser1
 - Jsmith



Description	Hans Meiser	Telephone number	+27748456470
Full name	sspadmin	Department	-
E-mail	-		

Penetration Testing – System Scanning

- Identify security weaknesses that could allow unauthorized access using
 - Port Scanning
 - Web Application Scanning
 - External (internet facing) / Internal (network)



System Scanning Example



System Scanning Example



CRITICAL

MS12-054: Vulnerabilities in Windows Networking Comp... >

Description

The remote Windows host is potentially affected by the following vulnerabilities :

- A denial of service vulnerability exists in Windows networking components. The vulnerability is due to the service not properly handling specially crafted RAP requests. (CVE-2012-1850)
- A remote code execution vulnerability exists in the Windows Print Spooler service that can allow a remote, unauthenticated attacker to execute arbitrary code on an affected system. (CVE-2012-1851)
- A remote code execution vulnerability exists in the way that Windows networking components handle specially crafted RAP responses. (CVE-2012-1852, CVE-2012-1853)

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 :

<http://technet.microsoft.com/en-us/security/bulletin/ms12-054>

Plugin Details

Severity:	Critical
ID:	61529
Version:	\$Revision: 1.6 \$
Type:	local
Family:	Windows : Microsoft Bulletins
Published:	2012/08/15
Modified:	2013/06/03

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector:
CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3
IAVM Severity: I

Penetration Testing – Exploitation



- Acquiring unauthorized access using identified security weaknesses
 - Unpatched software
 - Security misconfigurations
 - Flaws in access process (login forms, user registration, passwords)

Exploitation Example

The screenshot shows a web browser window with the URL <http://demo.testfire.net/bank/login.aspx>. The page features the Altoro Mutual logo and a navigation menu with links for [Sign Off](#), [Contact Us](#), and [Feedback](#). A search bar is also present. The main content area is titled "Online Banking Login" and displays a red error message: "Login Failed: We're sorry, but this username was not found in our system. Please try again." Below the message are input fields for "Username:" (containing "jdoe") and "Password:", and a "Login" button. A left sidebar contains a "MY ACCOUNT" section with sub-sections for PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL, each with a list of service links. A "DEMO SITE ONLY" banner is visible in the top right of the page content.

Exploitation Example

The screenshot shows a web browser window with the URL `http://demo.testfire.net/bank/login.aspx`. The page title is "Altoro Mutual: Online Bank...". The browser's address bar and navigation icons are visible. The page content includes the Altoro Mutual logo, navigation links for "Sign Off", "Contact Us", and "Feedback", and a search bar. A banner image shows a woman and a man, with a red "DEMO SITE ONLY" overlay. The main navigation menu has four tabs: "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "PERSONAL" tab is selected, and the page title is "Online Banking Login". The main content area displays a red error message: "Login Failed: Your password appears to be invalid. Please re-enter your password carefully." Below the message are input fields for "Username:" (containing "admin") and "Password:", and a "Login" button. The left sidebar contains a "MY ACCOUNT" section with a lock icon and a list of links under "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL".

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search

Altoro Mutual

DEMO SITE ONLY

[MY ACCOUNT](#) | [PERSONAL](#) | [SMALL BUSINESS](#) | [INSIDE ALTORO MUTUAL](#)

Online Banking Login

Login Failed: Your password appears to be invalid. Please re-enter your password carefully.

Username:

Password:

MY ACCOUNT

PERSONAL

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

INSIDE ALTORO MUTUAL

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)

Exploitation Example

The screenshot shows a web browser window with the URL `http://demo.testfire.net/bank/main.aspx`. The page features the Altoro Mutual logo and navigation links: [Sign Off](#), [Contact Us](#), [Feedback](#), and a search bar with a [Go](#) button. A banner image displays a woman, hands typing, and a group of people, with a red **DEMO SITE ONLY** overlay. The main navigation bar includes [MY ACCOUNT](#), [PERSONAL](#), [SMALL BUSINESS](#), and [INSIDE ALTORO MUTUAL](#). The **MY ACCOUNT** sidebar lists options under "I WANT TO ..." (View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, Customize Site Language) and "ADMINISTRATION" (View Application Values, Edit Users). The main content area displays "Hello Admin User" and "Welcome to Altoro Mutual Online." Below this is a "View Account Details:" section with a dropdown menu and a [GO](#) button. The footer contains [Privacy Policy](#), [Security Statement](#), and copyright information: © 2016 Altoro Mutual, Inc.

Social Engineering



- Attempt to persuade an entity's employees to provide information about, or direct access to, the entity's network or systems
 - Email phishing
 - Phone phishing
 - Physical social engineering

Social Engineering Example



https://youtu.be/bjYhmX_OUQQ?t=1m38s

Security Program Review



- Analysis of agency-wide written plan that encompasses security policies and procedures
 - Data classification
 - Risk Assessment
 - Information security awareness education and training
 - Incident response

Security of Taxpayer Information - Finding 1

- Department needs to improve its IT security
 - Sensitive information and systems exposed because of IT security weaknesses
 - Improvements needed to Department's IT security processes
 - Inadequate process for restricting access to only authorized users
 - Insufficient IT system log monitoring

Security of Taxpayer Information - Finding 2

- Department should continue developing its information security program
 - Information security officer's authority strengthened
 - Department has begun enhancing its existing security policies by developing information security program
 - Department should continue to establish information security program in four key areas
 - Department should create action plan to complete development of its information security program

Security of Taxpayer Information - Recommendations

- Department should develop and implement written policies and procedures for:
 - Vulnerability assessments
 - Updating and maintaining IT software and systems
 - Securely configuring systems
 - Log monitoring
- Improve management of access controls across IT systems

Security of Taxpayer Information - Recommendations

- Ensure that Information Security Officer monitors Department-wide compliance
- Continue to develop and implement information security program
- Develop and implement an action plan for completing the development of the information security program

Arizona Auditor General Audit Reports



- Report No. 15-116: Arizona Department of Revenue - Security of Taxpayer Information
- Found on AZ OAG website: <http://www.azauditor.gov>

Auditing IT Security with less resources

- Foundation up approach
- Requirements – Standards, Laws, Regulations, Policies
 - Auditing policies, procedures
- Oversight
- Processes to ensure requirements met
 - Test work – identification of inappropriate users
- IT audit support
 - Technical assistance
 - Tools / scripts to audit IT

Auditing IT Security with more resources

- Tools
 - Kali Linux
- Training
 - SANS
 - Offensive Security
- Techniques / Frameworks
 - OWASP – Open Web Application Security Project
 - PTES – Penetration Testing Execution Standard

Information



Nate Robb, CISA, IT Audit Senior
Office of the Auditor General Arizona
(602) 553-9809
nrobb@azauditor.gov