ACME, Inc.

Blackbox Penetration Test

Monday, June 9, 2008

Table of Contents

Executive Summary

ACME Inc. engaged Rapid7 Professional Services to perform a Blackbox Penetration Test of their corporate network. The objective of this engagement is to provide ACME Inc. with an independent assessment of their information security posture from an external attacker’s standpoint. This document contains the results of these findings.

Customer Information					
Company Name:	ACME Inc., Inc.				
Primary Contact Name:	Michael Bolton	Title:	Manager		
Telephone:		E-mail:	Michael@ACMEInc..com		
Business Address:	2100 Rockefeller Boulevard Suite 19B Mailstop 6				
City:	Beverly Hills	State/Province:	CA	ZIP:	90210
URL:	http://www.ACME Inc.com				

Auditor Information					
Company Name:	Rapid7, LLC.				
Contact Name:					
Telephone:					
Business Address:	545 Boylston St				
City:	Boston	State/Province:	MA	ZIP:	02116
URL:	http://www.Rapid7.com				

Business Description

Founded in 2006, ACME Inc. has production and research facilities across the globe.

Scope and Methodology

The security audit was performed in 3 phases. Each phase is intended to build upon the preceding phases.

Rapid7 Phased Methodology

External Reconnaissance	This is the process of refining the target list produced during the passive reconnaissance phase by using more intrusive methods such as port scanning, service and OS fingerprinting, and vulnerability scanning. ***Objective***: To enumerate the target organization's "Internet Footprint", which represents the sum of all active IP addresses and listening services and to identity potential vulnerabilities
External Vulnerability Assessment	Start with no information from the client. Use "passive" methods to enumerate potential target systems and networks. Passive methods by definition are nonintrusive and would not normally trigger intrusion detection systems. ***Objective***: Demonstrate what information about an organization and their network can be gathered using publicly available sources such as DNS and Search Engines.
External Penetration Testing	The final phase of the external assessment is to attempt to exploit vulnerabilities identified in order to bypass security controls or gain remote access to a target system or network. **Objective**: To test the Internet facing security controls and see of the perimeter security can be breached from the Internet.

Understanding the Results

Rather than report each missing patch as a "vulnerability", this report described risk and findings. A finding is a logical grouping of one or more security issue having a common cause and/or a common resolution. In addition to identifying the underlying cause of each vulnerability, each finding also contains hyperlinked references to resources and provides detailed remediation information. The findings matrix provided summarizes the overall findings and can be used as a workflow plan that can be tracked within the security organization. This plan is intended to assist the remediation team in prioritizing and tracking the remediation effort. Each finding has been categorized according to its relative risk level and also contains a rating as to the amount of work and resources required in order to address the finding. It is important to reiterate that this report represents an "snapshot" of the security posture of the environment at a point in time.

Overall Findings

ACME Inc.'s external security posture is relatively good, with the external perimeter being reasonably well locked down. However, our analysis of the ACME Inc. website revealed the presence of vulnerabilities including blind SQL injection, cross site scripting, and encryption flaws. Through the implementation of a real-time vulnerability assessment tool, ACME Inc. can effectively mitigate vulnerabilities moving forward which will demonstrate measurable improvement in the organization's overall security posture.

External Assessment

ACME Inc. has taken significant steps to harden their perimeter by reducing their overall surface that is accessible from the Internet. There are few open ports exposed to the internet and an IDS/IPS is in place to block automated scanning, which makes discovery and enumeration of those few ports even more difficult. However, Rapid7 was able to identify HTTP/HTTPS vulnerabilities that could provide a hacker with an additional attack vector into your organization.

External Testing Methodology

The engagement began as a black box penetration test. Rapid 7 was provided no information about ACME Inc. or their network in advance. The goal of reconnaissance is to use public sources of information to construct a target list of IP addresses and networks that will be assessed during the later phases.

The methodology of the reconnaissance was to first research the company using public sources. Information was gathered from Google searches, Wikipedia, Netcraft.com, and the corporate website in order to identify business units, partners, customers, domain names, and subdomains.

All of the identified domains are run through a rigorous process of network and host enumeration using the WHOIS and DNS databases. This process produced a final target list of networks and IP addresses that should be included in the vulnerability assessment phase.

External Vulnerability Assessment

Based on the results of the reconnaissance, ACME Inc. provided Rapid7 with a final confirmed IP range of 1.2.3.4 that would be the final scope for the vulnerability assessment and penetration testing.

Rapid7 was able to identify the following active devices within the confirmed scope of this penetration test:

IP ADDRESS	OPEN PORTS	SERVICES ENABLED	PLATFORM
X.Y.Z	80 / 23	Telnet & HTTPD	Cisco IOS
X.Y.Z	10,000	TCPWrapped	Unknown
X.Y.Z	80/23	HTTP / Telnet	Unknown
X.Y.Z	80/443	HTTP / SSL	Unknown
X.Y.Z	80	HTTP	Windows
X.Y.Z	80/3389	HTTP/RDP	Windows
X.Y.Z	80/3389	HTTP/RDP	Windows
X.Y.Z	21	FTP	Windows
X.Y.Z	80	HTTP	Windows
X.Y.Z	80	HTTP	Windows
X.Y.Z	21/22	FTP/SSH	Linux
X.Y.Z	25	SMTP	Windows
X.Y.Z	53	DNS	Windows
X.Y.Z	80	HTTP	Windows
X.Y.Z	80/443	HTTP / SSL	Unknown
X.Y.Z	80/443	HTTP / SSL	Unknown
X.Y.Z	23	Telnet	Cisco IOS
X.Y.Z	443/10,000	SSL / TCPWrapped	Unknown

The first step of vulnerability assessment is to identify potential services on the target devices. Once the services are enumerated and identified, the next step is to determine whether a vulnerability exists either due to a program flaw (such as a buffer overflow) or a misconfiguration (such as a vendor default password). The service identification was performed by using the port scanner, Nmap. Nmap scans all of the target IP addresses for open ports and fingerprint the service protocol and service version.

The next step of vulnerability assessment is to map the services identified to potential vulnerabilities. This is accomplished using a vulnerability scanner. For this component of the engagement, the consultant used both Rapid7 NeXpose and Nessus for the vulnerability assessment.

External Website Assessment

In order to discover the most likely attack vector to be exploited during an actual attack, Rapid7 has performed a high-level website analysis using the ISO 27002 Best Practice Control Objectives as a framework.

External Penetration Testing

The final phase of the external assessment is to attempt to exploit the vulnerabilities identified during the Vulnerability Assessment phase. Exploitation is performed using publicly available exploits from resources such as www.milw0rm.com. In addition an exploitation framework, Metasploit, was used to launch exploits against vulnerabilities identified. If during the penetration testing a vulnerability exploit results in system access then that access is leveraged in order to exploit any trust relationships to further penetrate the target network.

Findings and Recommendations

Rapid7 has identified a number of areas where security could be improved, and recommendations have been provided for consideration. This section of the report describes the details of Rapid7's observations, the impact associated with the vulnerabilities identified, and recommendations for resolving these vulnerabilities. To assist in prioritizing these findings, Rapid7 has categorized the observations with risk rankings based on the DREAD model.

DREAD Scoring Criteria

Damage Criteria		Damage Description	Critical (Score: 10)	High (Score: 7)	Medium (Score : 4)	Low (Score :1)
D	Damage Potential	The level of damage and exposure that could be cased if a vulnerability were exploited	An attacker can gain full access to the system; execute commands as root/administrator	An attacker can gain non-privileged user access; leaking extremely sensitive information	Sensitive information leak; Denial of Service	Leaking trivial information
R	Reproducibility	The level of difficulty in reproducing an attack	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced most of the time.	The attack can be reproduced, but only with a timing window.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	The ease to which the attack could be launched	No programming skills are needed; automated exploit tools exist	A novice hacker/programmer could execute the attack in a short time.	A skilled programmer could create the attack, and a novice could repeat the steps.	The attack required a skilled person and in-depth knowledge every time to exploit.
A	Affected Users	The volume of users and assets that are affected in a successful attack scenario	All users, default configuration, key customers	Most users; common configuration	Some users; non-standard configuration	Very small percentage of users; obscure features; affects anonymous users
D	Discoverability	The level of difficulty involved in enumerating the vulnerability	Vulnerability can be found using automated scanning tools.	Published information explains the attack. The vulnerability is found in the most com-monly used feature.	The vulnerability is in a seldom-used part of the product, and few users would come across it.	The vulnerability is obscure and it is unlikely that it would be discovered.

DREAD Composite Risk Categories

Each vulnerability or finding is assigned a composite Risk Score, calculated by adding each of the DREAD components producing a number between 5 and 50.

Risk Rating	DREAD Score	Risk Description
CRITICAL	40-50	A critical finding or vulnerability should be considered immediately for review and resolution. Exploitation of critical vulnerabilities is relatively easy and can lead directly to an attacker gaining privileged access (root or administrator) to the system. Findings with this risk rating, if not quickly addressed, may pose risks that could negatively impact business operations or business continuity.
SEVERE	25-39	A severe finding or vulnerability should be considered for review and resolution within a short time frame. These vulnerabilities can lead to an attacker gaining non-privileged access (standard user) to a system, or the vulnerability can be leveraged to gain elevated level of access.
MODERATE	11-24	Moderate risk finding or vulnerabilities should be considered once the high critical and severe risks have been addressed. These vulnerabilities may leak sensitive data that an attacker can use to assist in the exploitation of other vulnerabilities. Moderate findings do not pose a substantial threat to business operations.

Remediation Effort Level

EFFORT RATING	EFFORT DESCRIPTION
LOW	Less than a day requiring only a minimal amount of resources.
MODERATE	One to several days requiring moderate amounts of resources.
HIGH	**Significant multi-resource effort that may span over a considerable amount of time. Required a significant network architecture change or the purchase of additional security products.**

FINDINGS MATRIX

This table summarizes the findings documented in this report. The findings are ordered based on a weighed score of the severity of the risk and the effort of remediation.

FINDING	DREAD SCORE	REMEDIATION EFFORT
CRITICAL EXTERNAL FINDINGS		
OPENSSH BUFFER MANAGEMENT HEAP OVERFLOW	***CRITICAL***	**LOW**
OPENSSH CHALLENGE-RESPONSE BUFFER OVERFLOW	***CRITICAL***	**LOW**
OPENSSH KERBEROS AFS BUFFER OVERFLOW	***CRITICAL***	**LOW**
SEVERE EXTERNAL FINDINGS		
MICROSOFT IIS AUTHENTICATION METHOD DISCLOSURE	**SEVERE**	**LOW**
SECUREID PASSCODE REQUEST	**SEVERE**	**LOW**
APPLICATION ACCELERATOR	**SEVERE**	**LOW**
RDP AVAILABILITY	**SEVERE**	**LOW**

OPENSSH BUFFER MANAGEMENT HEAP OVERFLOW

DREAD Score Summary **STATUS: EXPLOIT SUCCESSFUL**

Risk Rating	CRITICAL
Category	SSH
Affects	1.2.3.4
References	CVE-2003-0693

Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
9	9	7	9	10	44	**LOW**

Findings Summary

During the vulnerability assessment phase, Rapid7 determined that a heap overflow in the 'buffer_append_space' memory management function for the device referenced above may exist. Successful exploitation of this device can yield root access to an attacker.

Remediation

For detailed remediation instructions, please visit:
http://www.rapid7.com/vulndb/lookup/ssh-openssh-buffer-heap-overflow

OPENSSH CHALLENGE-RESPONSE BUFFER OVERFLOW

DREAD Score Summary **STATUS: EXPLOIT SUCCESSFUL**

Risk Rating	CRITICAL
Category	SSH
Affects	1.2.3.4
References	CVE-2002-0640

Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
9	8	8	9	10	44	**LOW**

Findings Summary

Rapid7 has found multiple buffer overflows in the OpenSSH daemon during the challenge-response handshake when compiled with BSD_AUTH or SKEY support. Authentication is not required, and successful exploitation of this vulnerability can yield root access.

Remediation

For detailed remediation instructions, please visit:
http://www.rapid7.com/vulndb/lookup/ ssh-openssh-0010

OPENSSH KERBEROS AFS BUFFER OVERFLOW

DREAD Score Summary **STATUS: EXPLOIT SUCCESSFUL**

Risk Rating	CRITICAL					
Category	SSH					
Affects	1.2.3.4					
References	CVE-2002-0640					
Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
9	9	7	9	10	44	**LOW**

Findings Summary

Rapid7 has found multiple buffer overflows in the OpenSSH daemon during the challenge-response handshake when compiled with BSD_AUTH or SKEY support. Authentication is not required, and successful exploitation of this vulnerability can yield root access.

Remediation

For detailed remediation instructions, please visit:
http://www.rapid7.com/vulndb/lookup/ssh-openssh-0009

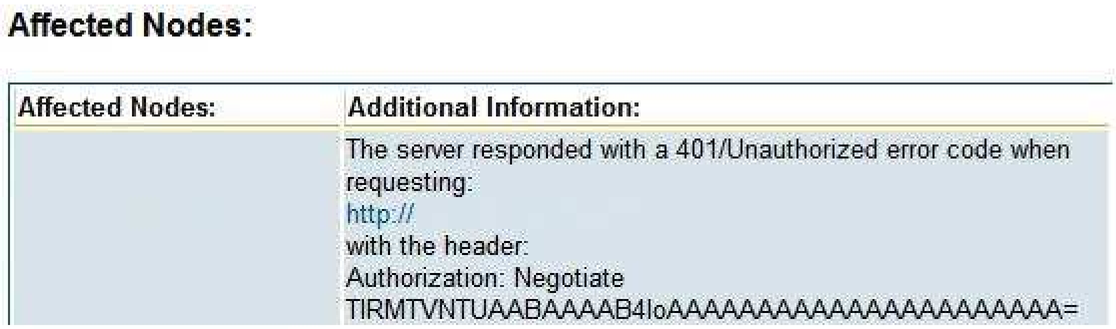
MICROSOFT IIS AUTHENTICATION METHOD DISCLOSURE

DREAD Score Summary **STATUS: EXPLOIT SUCCESSFUL**

Risk Rating	SEVERE					
Category	Best					
Affects	1.2.3.4					
References	CVE-2002-0419					
Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
6	5	5	6	8	30	**LOW**

Findings Summary

Rapid7 has determined that the authentication methods supported by the server can be revealed to an attacker through the inspection of returned error messages, even when anonymous access is also granted. The consultant found that when a valid authentication request is submitted for either message with an invalid username and password, an error message will be returned. This happens even if anonymous access to the requested resource is allowed. An attacker may be able to use this information to launch further intelligent attacks against the server, or to launch a brute force password attack against a known user name.



Affected Nodes:

Affected Nodes:	Additional Information:
	The server responded with a 401/Unauthorized error code when requesting: http:// with the header: Authorization: Negotiate TlRMTVNTUAABAAAAB4IoAAAAAAAAAAAAAAAAAAAAAAA=

NOTE: The image above has been included as proof of concept

Remediation

For detailed remediation instructions, please visit:
http://www.rapid7.com/vulndb/lookup/ http-iis-auth-method-disclosure

SECUREID PASSCODE REQUEST

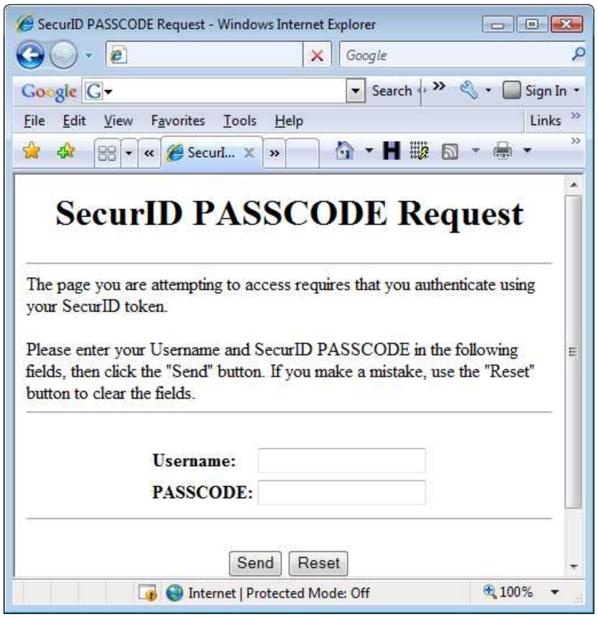
DREAD Score Summary **STATUS: INFORMATION LEAKAGE**

Risk Rating	SEVERE
Category	Best Practice
Affects	1.2.3.4
References	ISO27002 Best Practice Control Objectives

Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
6	6	5	6	8	26	**LOW**

Findings Summary

During the reconnaissance phase of this penetration test, Rapid7 has found the following target revealing the presence of an RSA SecurID platform:


SecurID PASSCODE Request - Windows Internet Explorer
Google
Search
Sign In
File
Edit
View
Favorites
Tools
Help
Links
SecurI...
Internet | Protected Mode: Off
100%

SecurID PASSCODE Request

The page you are attempting to access requires that you authenticate using your SecurID token.

Please enter your Username and SecurID PASSCODE in the following fields, then click the "Send" button. If you make a mistake, use the "Reset" button to clear the fields.

Username:

PASSCODE:

Send Reset

Further Analysis

Rapid7 recommends that ACME Inc. enable the HTTPS protocol on the server. Change the "action" URL of the form tag to use the HTTPS protocol ("https://...") instead of just the HTTP protocol ("http://..."). All sensitive data should be sent over HTTPS instead of over HTTP. If this device is no longer in use, Rapid7 recommends that ACME Inc. disable this server.

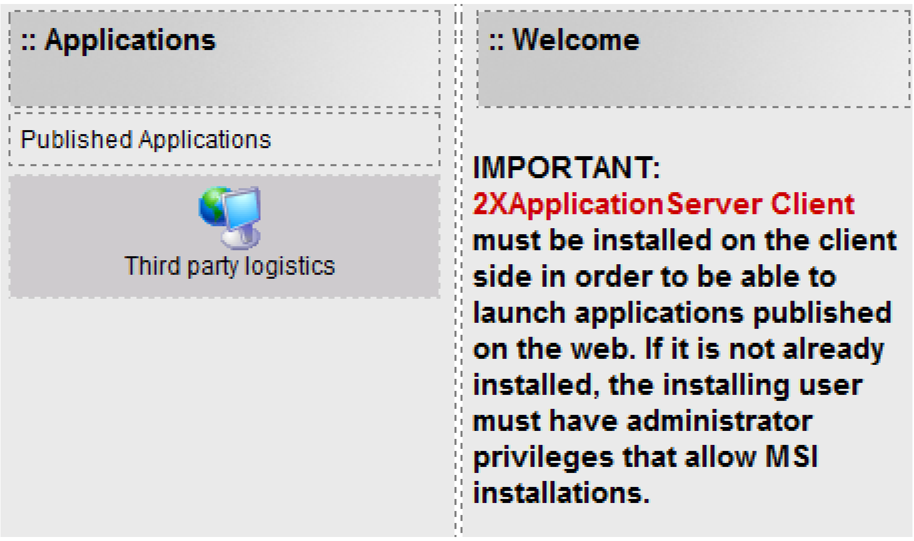
APPLICATION ACCELERATOR

DREAD Score Summary **STATUS: INFORMATION LEAKAGE**

Risk Rating	SEVERE					
Category	Best Practice					
Affects	1.2.3.4					
References	ISO27002 Best Practice Control Objectives					
Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
6	5	5	6	7	25	**LOW**

Findings Summary

During the reconnaissance phase of this penetration test, Rapid7 has found the following target revealing the presence of an application acceleration application:



IMPORTANT:
2XApplicationServer Client must be installed on the client side in order to be able to launch applications published on the web. If it is not already installed, the installing user must have administrator privileges that allow MSI installations.

Further Analysis

The presence of this application via HTTP on the ACME Inc website provides attackers with additional information that can be used by an attacker to map various attack vectors. In addition, the credentials being transmitted via HTTP are subject to eavesdropping.

Remediation

If this application is not currently in production, Rapid7 recommends that ACME Inc. disable this functionality.

REMOTE DESKTOP ROUTABLE THROUGH FIREWALL

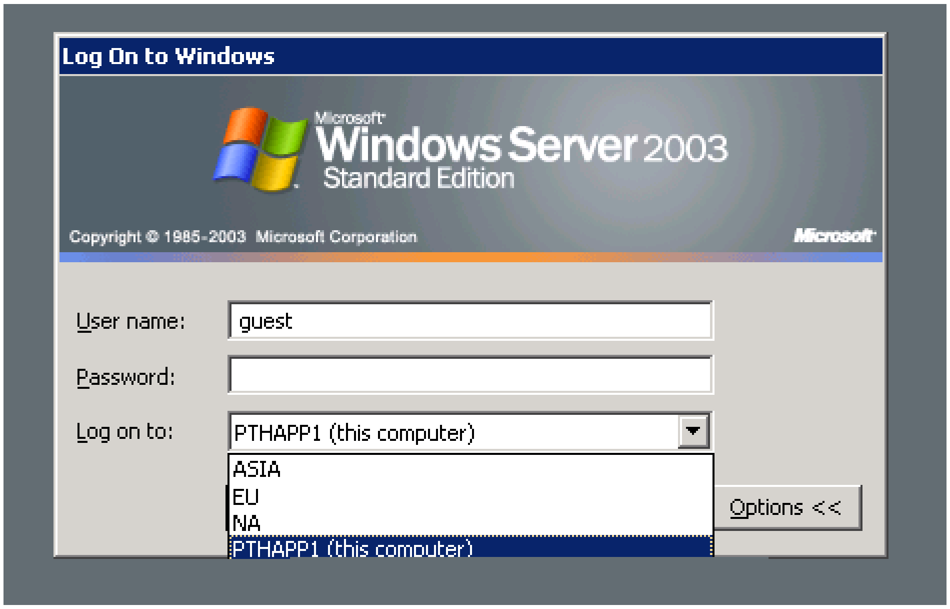
DREAD Score Summary **STATUS: INFORMATION LEAKAGE**

Risk Rating	SEVERE
Category	Best Practice
Affects	1.2.3.4
References	ISO27002 Best Practice Control Objectives

Damage Potential	Reproducibility	Exploitability	Affected Users	Discoverability	Total	Remediation Effort
6	5	5	6	7	25	**LOW**

Findings Summary

During the reconnaissance phase of this penetration test, Rapid7 has found that Remote Desktop access is externally routable through the firewall on port 3389.



User name: guest

Password:

Log on to: PTHAPP1 (this computer)

ASIA
EU
NA
PTHAPP1 (this computer)

Further Analysis

Rapid7 recommends that ACME Inc. disable port 3389 at the firewall, and require all external users to authenticate via VPN. In addition to information leakage, this configuration is susceptible to brute-force attacks.