



Link Mountain, LLC PO Box 182 Port Sanilac Michigan, 48469

Date:
Author:

Link Mountain, LLC
PO Box 182
Port Sanilac, MI 48469
www.LinkMountain.com

External Penetration Test Report

For

[ClientName]

CONFIDENTIAL-SENSITIVE

Page 1

This document contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of Link Mountain, LLC or the Client named above is strictly prohibited.

Contents

Executive Summary	2
Recommendations	3
Scope of Testing	3
Testing Details	3
Network Discovery	3
Tools Used in Network Discovery	3
Summary Table – Network Discovery	3
Passive Discovery – Whois, NsLookup, TraceRoute, Zone Transfer requests	3
ICMP – Echo, Timestamp, Netmask	4
Port Scanning – TCP Syn Scan	4
Port Scanning – UDP Ports	4
Port Scanning – TCP Ack Scan – Stateful Firewall Tests	4
Port Scanning – Source Port	4
Vulnerability Scanning	4
Scanners Used	4
Summary of Scanning Results	5
Penetration Testing	5
Objectives	5
Tools Used in Penetration Testing	5
Test Coverage: Passive Recon	5
Test Coverage: Information Disclosure – Robots.txt, Hidden HTML fields, Comments, etc	5
Test Coverage: Session Handling	5
Test Coverage: Encryption	5
Test Coverage: Authentication – Logon Logic, Password Recovery, Account Creation	6
Test Coverage: Access Controls – Logical Faults, Path Traversal, Predictability, etc	6
Test Coverage: Reflection Issues – XSS, Response Splitting, etc	6
Test Coverage: Input Validation Issues – SQL Injection, Command Injection, etc	6
Test Coverage: Error Handling	6
Test Coverage: Configuration Issues – Directory Enumeration, Open Admin Interfaces, etc	6
Finding Details	7
Item 1: Short Description	7
Item 2: Short Description	7
Item 3: Short Description	7
Item 4: Short Description	7
Item 5: Short Description	7

Executive Summary

The first objective of this external penetration test was to fully examine the internet facing [CLIENTNAME] systems to identify vulnerabilities that could allow an attacker to compromise the confidentiality, integrity or availability of those systems. Our second objective was to safeguard the stability of the [CLIENTNAME] systems under test. Our third objective was to prove exploitability by pursuing vulnerabilities to the point of compromise. The priority of these objectives dictated that

vulnerabilities were not necessarily pursued to the point of full exploitation and compromise. Full exploitation was not pursued if the vulnerability appeared to be systemic, or if remediation was mandatory for PCI compliance, or if exploitation would have jeopardized either full test coverage or the stability of the systems under test.

Full details of our findings are found in the Testing Details section of the report; the following is an executive level summary of issues found:

Finding Summary here...

Recommendations

Link Mountain recommends that all of the vulnerabilities be remediated, and a follow up test be conducted to verify remediation. If the test is conducted for PCI-DSS compliance, a remediation test is required (PCI-DSS 11.3.a: Verify that noted vulnerabilities were corrected and testing repeated.).

Further recommendations here...

Scope of Testing

The following [CLIENTNAME] hosts were in scope and included in this penetration test:

Scope statement here...

Testing Details

Network Discovery

Tools Used in Network Discovery

NMap and Wireshark were used for all port scanning and packet capture. Manual inspection was also conducted using NSLookup, Whois Queries, Trace Route and DNS Zone transfer requests. The following table summarizes the results.

Summary Table – Network Discovery

IP Address	Description	Discovery Method							
		ICMP Echo	ICMP Timestamp	ICMP Netmask	80/TCP ACK	TCP SYN	Source Port 20*	Source Port 53*	UDP Scan

Passive Discovery – Whois, Nslookup, Traceroute, Zone Transfer requests

Manual Whois, NSlookup and Traceroute requests were conducted to learn as much as possible about the target network. DNS Zone transfer requests were issued to any discovered name servers.

Finding Summary here...

CONFIDENTIAL-SENSITIVE

ICMP – Echo, Timestamp, Netmask

The firewall was tested by sending ICMP Echo (commonly known as PING) requests to each host. In addition to Echo, the less commonly known ICMP Timestamp and ICMP Netmask address requests were also sent to each host. Any of these ICMP packet types can be used to gather information about a host, and should be blocked at the firewall.

Finding Summary here...

Port Scanning – TCP Syn Scan

The target hosts were scanned for open ports with NMap. The open ports discovered are noted in the table above.

Finding Summary here...

Port Scanning – UDP Ports

The target hosts were scanned for open UDP ports using NMap. Ports that responded are noted in the table above.

Finding Summary here...

Port Scanning – TCP Ack Scan – Stateful Firewall Tests

The TCP protocol includes 'flag bits' that are used to facilitate the TCP handshake and other aspects of the TCP protocol. Commonly used flag bit combinations are SYN, ACK, PSH, RST, and FIN. Abnormal flag bit combinations can sometimes be used to bypass firewalls or gather additional information about a host.

A firewall that is not capable of stateful inspection, such as a simple packet filtering firewall, will block SYN packets from reaching a port that is disallowed, thereby blocking the normal three way handshake, but can allow other flag combinations to pass. A well configured stateful firewall should drop any packet that is not part of an established TCP session or normal handshake sequence to an allowed port. A stateless or poorly configured stateful firewall can allow these abnormal packets through, and the hosts will respond with a RST flag, to reset the session (because the target host has no knowledge of an established session with the originator).

The target hosts were scanned with requests to TCP port 80, with the flag bits set to ACK. This is an abnormal request, since there was no existing TCP session with the targets.

Finding Summary here...

Port Scanning – Source Port

The target hosts were scanned using a source port used by the FTP data channel (20), and DNS queries (53). Poorly configured firewalls sometimes allow this traffic to pass.

Finding Summary here...

Vulnerability Scanning

Scanners Used

Nessus, Nikto and Link Mountain custom scanners were used to scan the target hosts for known vulnerabilities.

Summary of Scanning Results

Full details of the vulnerability scan are in the attached report. The following summary describes the major items that were of importance to the penetration test or that require remediation for PCI-DSS compliance:

Finding Summary here...

Penetration Testing

Objectives

The first objective was maximum test coverage; the second objective was safeguarding the stability of the systems under test, and the last objective was proof of exploitability. The priority of these objectives dictated that vulnerabilities were not necessarily pursued to the point of full exploitation and compromise. Full exploitation was not pursued if the vulnerability appeared to be systemic, or if remediation was mandatory for PCI compliance, or if exploitation would have jeopardized either full test coverage or the stability of the systems under test.

Tools Used in Penetration Testing

Web Scarab was used to spider web applications, conduct selected tests and document test coverage, Nikto was used to test for common directories, resources and configuration issues, and custom perl scripts were used for automated fuzzing of application parameters. In addition, extensive manual inspection and manipulation was used.

Test Coverage: Passive Recon

A brief passive reconnaissance was conducted using Whois queries, Search engines and other web resources to determine the breadth and depth of information available about the target network, with particular emphasis on harvesting of potential user names and information that could aid in dictionary attacks, phishing and social engineering attacks.

Finding Summary here...

Test Coverage: Information Disclosure – Robots.txt, Hidden HTML fields, Comments, etc

Web servers and web application roots were tested for the existence of Robots.txt files, and if found, were examined for sensitive data. All pages served by web applications were examined for sensitive information disclosed in HTML comments. Pages were inspected for 'hidden' fields to determine if sensitive information was disclosed.

Finding Summary here...

Test Coverage: Session Handling

Session tokens were evaluated for predictability. GET requests were examined to ensure that session tokens were not passed in query strings. Applications were inspected for mixed use of encrypted and unencrypted transport, to insure that cookies containing session tokens are not sent over clear text channels.

Finding Summary here...

Test Coverage: Encryption

Testing included verifying the enforcement of appropriate transport encryption, either SSLv3 or TLSv1. Cookies were examined for sensitive information encrypted with weak encryption or encoding schemes.

CONFIDENTIAL-SENSITIVE

Page 5

This document contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of Link Mountain, LLC or the Client named above is strictly prohibited.

Finding Summary here...

Test Coverage: Authentication – Logon Logic, Password Recovery, Account Creation

Logon logic was assessed to determine if authentication was enforced for access to all functionality and files, and that authentication could not be successfully bypassed. Testing also included verification of account lockout functionality, and examined password recovery and account creation logic for errors or weakness or disclosure of user accounts.

Finding Summary here...

Test Coverage: Access Controls – Logical Faults, Path Traversal, Predictability, etc

Web servers and applications were extensively tested for the existence of common directory names that might have been missed in access control logic or have listable content. Traversal techniques were used to determine if web server or operating system faults could be used to bypass application access controls. Access control logic was tested by requesting resources from unexpected application states, particularly after error states were encountered, and manipulation of parameters and parameter names, host header and referrer values.

Finding Summary here...

Test Coverage: Reflection Issues – XSS, Response Splitting, etc

Web applications were extensively 'fuzzed', and the results were inspected for evidence of unsanitized values reflected back to the client. Header values and cookies were manually manipulated in a similar manner to test for reflection.

Finding Summary here...

Test Coverage: Input Validation Issues – SQL Injection, Command Injection, etc

Web applications were extensively 'fuzzed', and the results were inspected for evidence of unsanitized input values reaching application or other server side code. Header values, parameter names and cookies were manually manipulated in a similar manner to test for input validation.

Finding Summary here...

Test Coverage: Error Handling

All responses received from web servers and applications during testing were inspected for evidence of improper error handling at the application, database and web server layers.

Finding Summary here...

Test Coverage: Configuration Issues – Directory Enumeration, Open Admin Interfaces, etc

Nikto was used to find listable directories, common administrative interfaces and configuration errors. Information gained from HTML comments, error messages, Robots.txt files and other sources was manually examined for any information that could help identify code libraries in use. Default interfaces for web servers and any identified third party components were tested for secure configuration and patch levels.

Finding Summary here...

CONFIDENTIAL-SENSITIVE

Finding Details

Item 1: Short Description

Full Description:

Severity:

Remediation:

Testing Notes:

Item 2: Short Description

Full Description:

Severity:

Remediation:

Testing Notes:

Item 3: Short Description

Full Description:

Severity:

Remediation:

Testing Notes:

Item 4: Short Description

Full Description:

Severity:

Remediation:

Testing Notes:

Item 5: Short Description

CONFIDENTIAL-SENSITIVE

This document contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of Link Mountain, LLC or the Client named above is strictly prohibited.



Link Mountain, LLC PO Box 182 Port Sanilac Michigan, 48469

Full Description:

Severity:

Remediation:

Testing Notes:

CONFIDENTIAL-SENSITIVE

Page 8

This document contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of Link Mountain, LLC or the Client named above is strictly prohibited.