

CS470 Term Project

System Vulnerability Assessment and Penetration Testing

Due Date:

THE SCENARIO

ACME, Inc. is a fortune 500 company specializing in international commodity trading. The annual gross revenue of the company exceeds \$2 billion. It is located in the middle of the SOHO district in New York City and employs 1350 people. Its physical infrastructure security mechanism, which is very well planned and executed, is administered by an outside contractor: SecureMeTight, LLC. However, the CEO, Ms. Shome D Money, is not quite confident about the security of the company's IT infrastructure. In as much as the company has grown more and more dependent on its IT systems for its online presence, Ms. Money decided that something drastic must be done to ensure that IT operations remain robust. She called the company CIO, Mr. Lowen Behold, and directed him to immediately start a cost and feasibility study on this pressing matter.

Mr. Behold rose from the ranks in the company and became its CIO after several attempts by Ms Money to fill-in the position with outsiders. Ms. Money just would not pay enough! Now, Mr. Behold is in his 70's and does not care much about the situation. Thus, he decided to hire your enterprising group, The AnotherByteAnotherPenny Group, to put together a vulnerability assessment prospectus that he can present to the CEO. To supplement the prospectus, he also asked your group to perform penetration testing of three servers running on different operating systems and to write a detailed report of the activities that were performed. This report will be used as a proof-of-concept artifact which will characterize the current state of ACME's IT infrastructure security. In summary, your group needs to produce two written reports: a vulnerability assessment prospectus and a penetration testing report.

THE VULNERABILITY ASSESSMENT PROSPECTUS

The prospectus is a document whose main purpose is to justify the need for the vulnerability assessment (VA) process. Furthermore, it should be able to convince the management team that your group is capable of executing the VA process and could recommend the necessary measures to correct the perceived system flaws. This document will ultimately be the basis for future legal contracts between AnotherByteAnotherPenny Group and ACME, Inc. The prospectus should include the following:

- 1) Project Title
- 2) Project Manager(s)
- 3) Executive Summary
- 4) Customer Profile
- 5) Project Justification
- 6) Project Scope and Goals
- 7) Methodology*
- 8) Project Timeline
- 9) Project Deliverables

THE PENETRATION TESTING

The Executive Report

The executive report, which is generally free of technical jargons, must be concise and comprehensive. It should provide an overview, a description of the methodology, the results of the assessment process, and the recommended steps or procedures that need to be done to take care of the exposed vulnerabilities. Because the managers and executives are very busy people, they would very much appreciate visual aids or charts to accompany this report. A sample visual aid is attached.

The Technical Report

The technical report includes detailed penetration tests for each system, analysis of vulnerabilities that were detected, the description of the method(s) used to take advantage of each of the vulnerabilities if possible, and the recommended solution for each. The report should, in essence, be a summary of each vulnerability threat which should, at the very least, include the following:

1. a description of the threats, which should include, but not limited to, all of the following web vulnerabilities:
 - a) SQL injection,
 - b) cross-site scripting,
 - c) parameter manipulation,
 - d) session hijacking, and
 - e) LDAP Injection
2. the impact of the threats on the compromised system; and
3. the recommended solution to foil each threat.

Just like the executive report, it is required that you present additional visual aids which summarize the results of your technical investigative efforts.

*The methodology of penetration testing should include at least the Nessus tool and the Metasploit Framework. You may also use SARA, the SiteDigger tools, or Google Hacking Tools and Techniques to broaden your penetration test range. Additional tools that you may need are password crackers, OS detectors, network sniffers, NetBIOS scanners, and web server security checkers. You need to refer to the course notes for the sources of these tools on the Internet. A typical penetration test methodology may consist all or a combination of the following:

- a) Network mapping;
- b) System footprint analysis;
- c) Enumeration of information;
- d) Obtaining access;
- e) Escalation of privilege;
- f) Additional password/information gathering;
- g) Installation of backdoors; and
- h) Abusing the compromised system

REPORT GUIDELINES

Requirements

- The two reports must be bound together. Each report should start with a cover page. Use a single-space paragraph format.
- Refer to the *MLA Guide in Writing Research Papers* for more hints and pointers.
- The conclusion section should include your personal views/comments/recommendations about the study. Future extensions or additions to the completed work may also be included in this section.

Evaluation

The grade will be based on: (a) **technical content (50%)**, (b) **extent of vulnerability assessment coverage (20%)**, (c) **recommendations and analyses (20%)**, and (d) **documentation and style (10%)**.

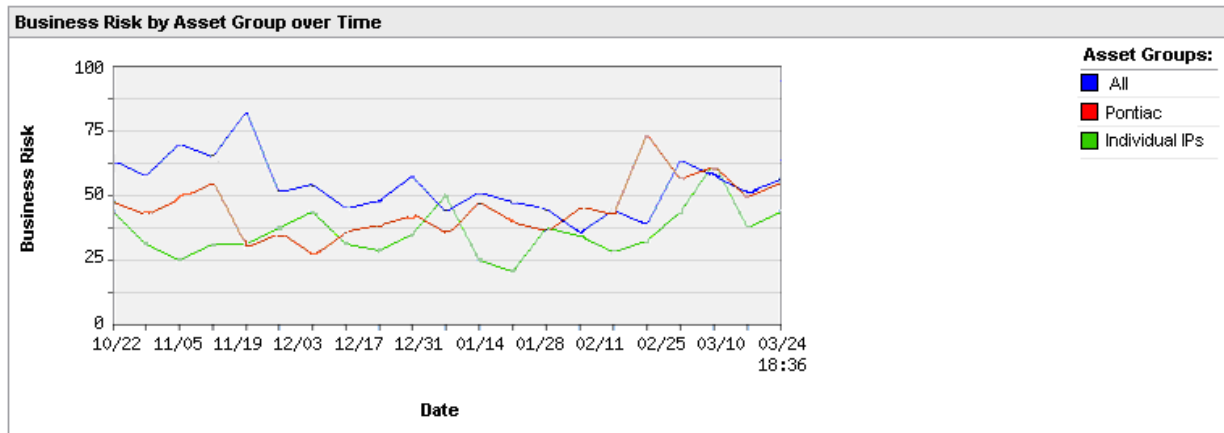
Report Summary	
Company:	[REDACTED]
User:	[REDACTED]
Template Title:	Executive Report
IPs Scanned:	45
Date Range:	10/21/2003 - 03/24/2004
Filters:	Vulnerability Checks: Potential V
Asset Groups/IPs:	All , Pontiac , 64.41.134.59-64.41

BUSINESS RISK ASSESSMENT

[REDACTED] enables users to accurately assess business risk – an advanced method for instantly measuring threats to the critical assets within your organization. Business risk not only takes into account the severity of the vulnerabilities detected but also the criticality of the hosts as defined by the business impact level you assign to your various asset groups.

Summary of Vulnerabilities

Vulnerabilities Total	950 (-247)	Average Security Risk	<div style="display: inline-block; width: 20px; height: 20px; background-color: red; border: 1px solid black;"></div> 2.7	Business Risk	<div style="display: inline-block; width: 20px; height: 20px; background: linear-gradient(to right, green, yellow, orange, red); border: 1px solid black;"></div> 55/100
-----------------------	------------	-----------------------	---	---------------	--



PokeMeAHole LLC

EXECUTIVE AND TECHNICAL REPORTS

Customizable reports support flexible, on demand reporting by business unit for executives and managers. The "Executive" report gives a high level overview by comparing the scan results over the previous 8 weeks, showing the total vulnerabilities by severity and the vulnerability trend over time. The "Technical" report includes detailed host results, sorted by host, based on the most recent saved scan data. The "High Severity" report shows all severity level 4 and 5 vulnerabilities. You can run these reports or customize them to suit your organization's needs.

Executive Report

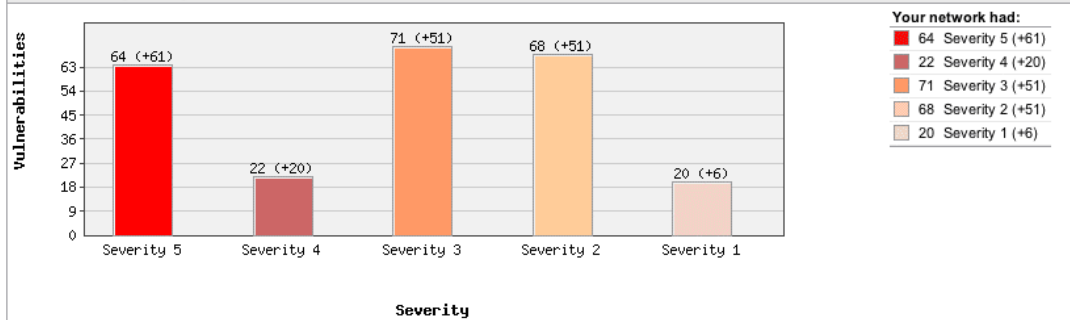
Summary of Vulnerabilities

Vulnerabilities Total	245 (+189)	Average Security Risk	■ ■ ■ ■ ■ 2.6	Business Risk	■ ■ ■ 29/100		
by Status		by Severity			5 Biggest Categories		
Status	Vulnerabilities	Severity	Vulnerabilities	Trend	Category	Vulnerabilities	Trend
New	3	5	64	(+61)	General remote services	33	(+19)
Active	235	4	22	(+20)	Hardware	1	(+1)
Re-Opened	7	3	71	(+51)	TCP/IP	31	(+18)
Fixed	28	2	68	(+51)	SNMP	3	(+1)
Changed	38	1	20	(+6)	Firewall	3	(+3)

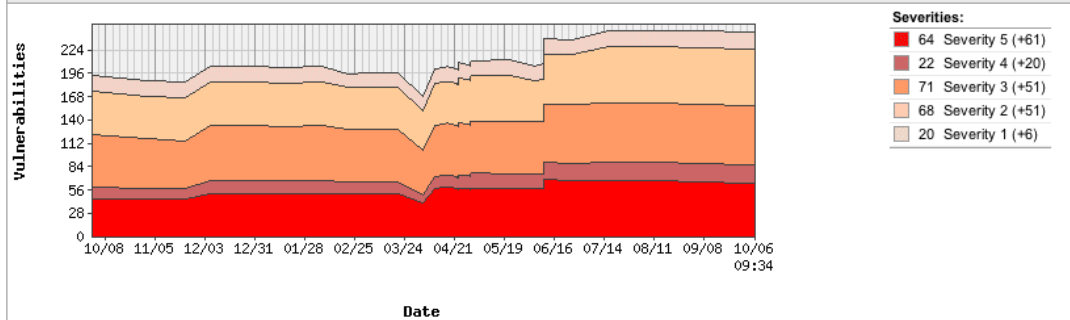
Vulnerabilities by Status



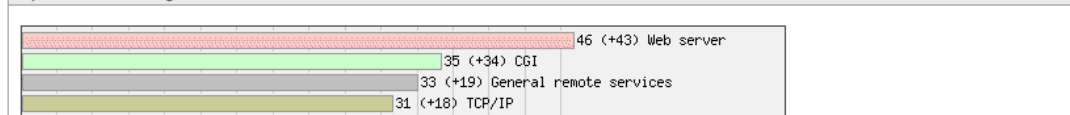
Vulnerabilities by Severity



Vulnerabilities by Severity over Time



Top 5 Vulnerable Categories



PokeMeAHole LLC

VERIFY THE ELIMINATION OF THREATS

provides fully secure audit trails that track vulnerability status for all detected vulnerabilities. As follow up audits occur, vulnerability status levels -- new, active, fixed, and re-opened -- are updated automatically and identified in trend reports, giving users access to the most up-to-date security status.

Critical Asset Verification Report

Summary of Vulnerabilities

Vulnerabilities Total: 245 (+189) | Average Security Risk: 2.6 | Business Risk: 22/100

Vulnerabilities by Status



192.168.100.3 (hackme.jsu.edu) Windows 2000 Server

Vulnerabilities Total: 9 (+7) | Security Risk: 2.3

by Status		by Severity			5 Biggest Categories		
Status	Vulnerabilities	Severity	Vulnerabilities	Trend	Category	Vulnerabilities	Trend
New	0	5	0	(0) -	General remote services	11	(+2)
Active	9	4	2	(0) -	CGI	4	(+4)
Re-Opened	0	3	3	(+1)	TCP/IP	3	(0) -
Fixed	10	2	0	(-1)	Web server	2	(0) -
Changed	10	1	3	(0) -	Information gathering	1	(0) -

Vulnerabilities (9)

4	SSL Server Uses Weak Encryption Vulnerability	port 443/tcp	Active	🔴
4	SSH Protocol Version 1 Supported	port 22/tcp	Active	🔴
3	Webalizer Web Usage Statistics Accessible	port 80/tcp	Active	🔴
3	Webalizer Web Usage Statistics Accessible	port 443/tcp	Active	🔴
3	Netscape/OpenSSL Cipher Forcing Bug	port 443/tcp	Active	🔴
3	OpenSSH Key-Based Source IP Access Control Bypass Vulnerability	port 22/tcp	Active	🔴
1	Expose_php Set to On in php.ini	port 80/tcp	Active	🔴
1	Expose_php Set to On in php.ini	port 443/tcp	Active	🔴
1	ICMP Timestamp Request		Active	🔴
4	PHP4 Multiple Vulnerabilities	port 80/tcp	Fixed	🟢
4	PHP4 Multiple Vulnerabilities	port 443/tcp	Fixed	🟢
3	Smurf Attack (ICMP Amplifier)		Fixed	🟢
3	OpenSSH Remote Root Authentication Timing Side-Channel Weakness	port 22	Fixed	🟢
3	OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability	port 22	Fixed	🟢
3	Web Server Stopped Responding	port 443/tcp	Fixed	🟢
2	Web Server Brute Force Discovery of Unix Account Names Vulnerability	port 80/tcp	Fixed	🟢
1	SSL Certificate - Will Expire Soon	port 443/tcp	Fixed	🟢
1	Apache Web Server ETag Header Information Disclosure Weakness	port 443/tcp	Fixed	🟢
1	Apache Web Server ETag Header Information Disclosure Weakness	port 80/tcp	Fixed	🟢