Project Documentation

Overview

1
- **Report Components**
  - Comparison of Security Assessments
  - The Report Criteria

2
- **Report Results Matrix**
  - Classification Scoring
  - Report Delivery

3
- **Recommendations**
  - Executive Summary
  - Technical Report

Additional Items

- Code Of Ethics
- NDA
- Project Proposal
- Types Of Assessments
- Questions To Ask The Client
- Legal Documentation
- Defining The Deliverables
- Service Agreement And Authorization

The Report

All Reports should include as little “techno-babble” as possible.

Any vulnerability found should be accompanied with a detailed explanation and possible countermeasures

The delivery of the Final Report should be a formal meeting including all interested parties.

Printed copies for each member of the meeting should be provided

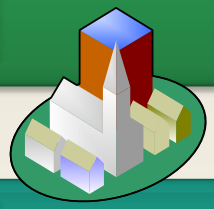
A secure mechanism to provide an electronic copy of the report should also be available

Do not email

Report Criteria: Supporting Documentation

Throughout the penetration test, *all* actions should be logged, recorded and verified.

Text outputs from tools, screenshots and screen video captures all aid this logging.



Opinions do not cut it, proof is imperative!

Is *your* supporting documentation in a format suitable for the recipient client (Executive or Technical)

Analyzing Risk

What is Risk?

- The possibility that something could damage, destroy, or disclose data is known as risk.
- *Managing risk is therefore an element of sustaining a secure environment*.
- The process by which risk management is achieved is known as risk analysis.
- Risk analysis involves analyzing an environment for risks, evaluating each risk as to its likelihood of occurring, and estimating potential loss if the threat occurred.

Analyzing Risk

SANS Top 7 Management Errors

- Number Five: Fail to realize how much money their information and organizational reputations are worth.

How should you evaluate Risk? (This is very involved)

- Asset Valuation
- Threat Identification

Quantitative Risk Analysis – Concrete Numbers

- Placing a dollar figure on each asset and threat.

Qualitative Risk Analysis

- You rank threats on a scale.

How is Risk Reported?

Report Results Matrix

The findings matrix will allow you to easily rate each finding, it will also allow the customer to read and digest the information.

If the customer is regulated (FIDC, etc), then the standard matrix for that regulation should be used.

- **Risk = The level of damage a vulnerability can cause if exploited.**
- **Threat Probability = The likelihood of that vulnerability being exploited.**
- **Impact = Risk + Threat Probability**

Findings Matrix

- For each finding, enter a mark in Risk and Threat boxes.
- Calculate the Impact Score.

	Risk	Threat Probability	Impact
High (3)			
Medium (2)			
Low (1)			

- Impact: 1-2 = Low / 3-4 = Medium / 5-6 = High

Findings Matrix

- **Finding:**
  - **Internet facing servers returning banners.**
    - **SMTP / IIS / FTP, etc**

	Risk	Threat Probability	Impact
High (3)			
Medium (2)			
Low (1)			

- **Impact Score: 1-2 = Low / 3-4 = Medium / 5-6 = High**

Findings Matrix

- **Finding:**
  - **Patch Management not up to date**

	Risk	Threat Probability	Impact
High (3)			
Medium (2)			
Low (1)			

- **Impact Score: 1-2 = Low / 3-4 = Medium / 5-6 = High**

Findings Matrix

- **Finding:**
  - **Input Manipulation associated with a code flaw.**

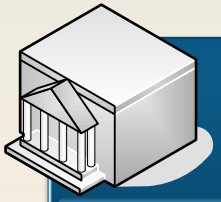
	Risk	Threat Probability	Impact
High (3)			
Medium (2)			
Low (1)			

- **Impact Score: 1-2 = Low / 3-4 = Medium / 5-6 = High**

Delivering The Report

You would complete a findings matrix for *every* finding you have collected during your penetration test.

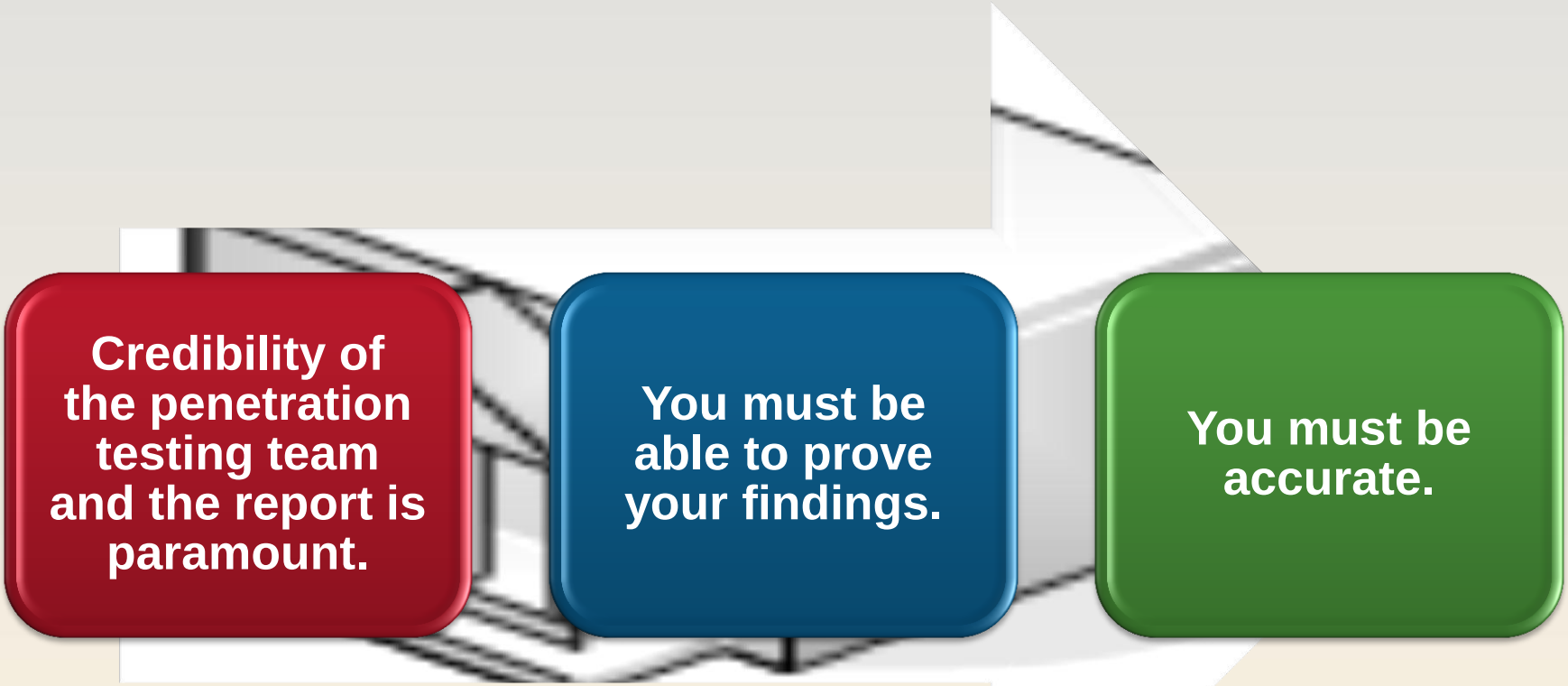
Be careful about destroying a customer with regard to their security posture.



Try to deliver the report in a positive manner.

Maybe approach the IT staff prior to delivering the report to the C level management to resolve the higher risk issues.

Delivering The Report



Stating Fact

When writing the report, you must focus primarily on stating factual data, avoid stating your opinions.

Any statements you make must also be supported by evidence.

- **"The wireless segments of the tested networks were vulnerable by attacking the encryption keys and due to the logical location of the wireless clients, The recovered WPA key was found to be an easily guessed string – "skywalker". Once the WPA key was calculated, an attacker would then have full access to the internal network."**

The report might include recommendations, but those are clearly labeled as such, and are not the focus of the report.

Recommendations

You have been contracted to aid the customer in securing their network.

Therefore you must make recommendat-ions to resolve any issues you have found.

Vulnerability scanners have good information about resolving issues.

Never give an opinion, only facts.

Recommendations

Customers have the choice of the following for all findings.

Accept the risk.

Put up with the problem.

Reduce the risk.

Install Security Controls, Improve Procedures or Carry out security awareness training as examples.

Transfer the risk.

Outsource, Buy Insurance

Eradicate the risk.

Remove all wireless networks from the corporate network.

Executive Summary

The executive summary must be usable to the C level management.

- It must be free of technical jargon.
- Should be short and direct

A clear and concise summary of the vulnerabilities and recommendations is required.

- Graphs and charts also work well to quickly communicate data.
- Finish on a positive note!

Technical Report

Delivered to the people responsible for rectifying the security issues.

Must be complete with all relevant data regarding vulnerabilities, exploits, and attacks.

You cannot put enough information about the attacks, weaknesses, and resolutions here.

Report Table Of Contents

Summary Of Security Weaknesses Identified

Summary of Security Weaknesses Identified

The security weaknesses identified are summarised in the following table (please see Section 4 - Detailed Findings for further information):

Weakness	Description	Overall Risk Rating	Identified From
Finding 1 Compromise of [redacted].57 and [redacted].58 servers.	This was a [redacted] not a [redacted] International target. However, this led to a full compromise of [redacted] and [redacted] must work together to address this. SNMP open to the outside world with the community sting of public. Also username and password of root on development boxes.	High	External

Scope of Testing

Scope of Testing

The first phase was focused on the assessment of all servers and network devices accessible from the internet including servers, routers and firewalls. Each appliance was thoroughly tested using a variety of open source and commercial tools. Denial of Service testing was done between 2am-4am [redacted] time to minimise customer impact. This assessment was undertaken externally from the M2IA testing laboratory.

The following were undertaken:

Summary Recommendations

Summary Recommendations

The following risk ratings and benchmarks are based on observations made during the course of this engagement and are for management information purposes only and do not constitute an opinion or provide any assurance.

Industry Rankings

M2IA has compiled the results of the network security activities and has produced benchmarks for comparison purposes.

Industry Standard Leading Practice Comparison – This is a measure of practices (in the respective assessment area) as they compare to other Victorian financial organisations. This is also a subjective evaluation based upon vulnerability assessment test results and observations.

A 1-to-4 rating was used for each benchmark:

1 Indicates that only very few (or no) industry preferred security practices are employed in the respective benchmark.

2 Indicates that some industry preferred security practices are employed and evident in the respective benchmark.

3 Indicates that most industry preferred security practices are employed and evident for the respective benchmark.

4 Indicates that all (or nearly all) preferred security practices are employed and evident for the respective benchmark.

The following benchmarks were selected because they are considered the most critical components to an enterprise security program. These benchmarks are not meant to be all-inclusive, but the best areas for comparison.

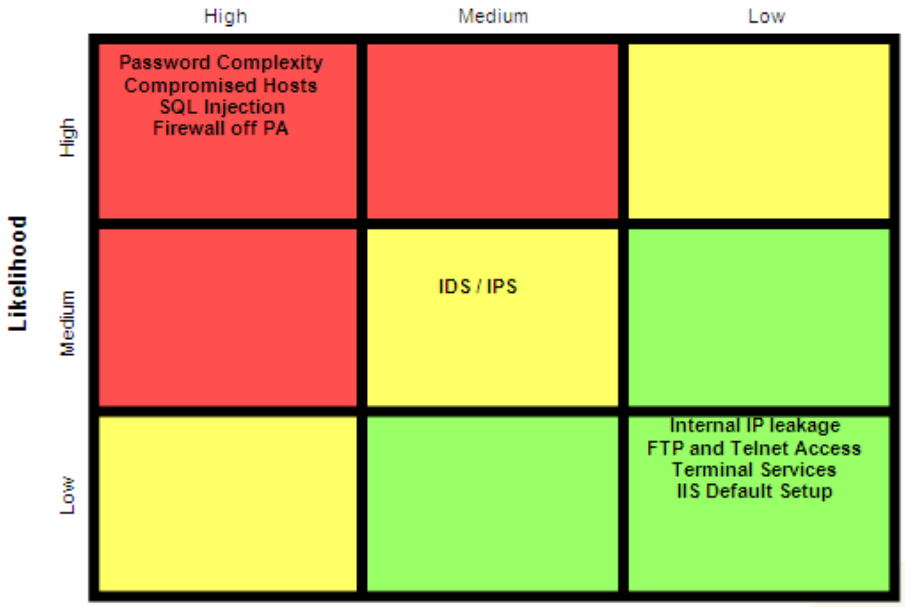
Please note that these benchmarks are provided for management informational purposes only and do not constitute an opinion or provide any assurance.

Summary Observations

Summary Observations

The following table graphically represents the security weaknesses identified as compared to the systems assessed. This table is provided to assist LDSI management in identifying the systems that have produced the most serious security issues in order to best prioritize remediation activities.

System Risk Matrix



The above risk ratings are based on observations made during the course of this engagement and are for management information purposes only and do not constitute an opinion or provide any assurance.

Detailed Findings

Detailed Findings

- These observations and recommendations were developed from the security testing undertaken.

These detailed findings include:

- the observations we made
- the root cause we perceived to be the trigger for the observations
- tactical recommendations that can be rapidly deployed to reduce risk
- strategic recommendations that require a long term commitment to reducing risk

The following risk ratings are based on observations made during the course of this engagement and are for management information purposes only and do not constitute an opinion or provide any assurance.

Detailed Findings

1.1.1 1. Compromise of [redacted]8 servers

Overall Risk Rating	High		
Impact Rating	High	Likelihood Rating	High

Root Cause

The servers [redacted] and [redacted] were compromised due to weak password configuration and SNMP leakage.

Observation

During routine testing M2IA discovered the following services had weak default passwords. Even though these servers were not part of the [redacted]etwork it gave Mile2 the ability to access the [redacted]nternal network. Mile connected to the servers using the password and username of root. The two servers in question are IBM AIX servers.

Impact

An external attacker could penetrate this server beyond the firewall and then attack the other DMZ servers and internal network without firewall protection. This includes sniffing customer traffic using Ethereal and Denial of Service attacks on other servers. This would lead to a FULL compromise of every server within the DMZ and internal network.

Tactical Recommendation

Remediation steps that can be taken immediately to reduce risk are:

- [redacted] must change the passwords on the affected servers
- [redacted] must undergo Penetration Testing just as [redacted]ad done
- Firewall the [redacted] if feasible to prevent further attacks

Strategic and Tactical Directives

5. Strategic and Tactical Directives

The following strategic and tactical directives will ensure [redacted] prevent any High or Medium Risk Vulnerabilities in future security assessments.

[redacted] Internal Penetration Test

[redacted]as had the risk that it has been exposed to Hackers in the past because of vulnerabilities. [redacted] also appeared to have security controls not working effectively such as IDS monitoring, and weak passwords on hosts.

CIS Security Standards

Security Standards will guarantee servers have been configured to the highest level of security before they are deployed. CIS have security standards for Microsoft platforms including Exchange, Domain Controllers and IIS servers. They also have standards for Solaris operating systems, Cisco routers and Apache Web Server.
The Centre for Internet Security (CIS) is a non-profit enterprise whose mission is to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS members develop and encourage the widespread use of security configuration benchmarks through a global consensus process involving participants from the public and private sectors.

Statement of Responsibility / Appendices

6. Statement of Responsibility

This report is prepared on the basis of the limitations set out below:

M2IA
Enterprise Risk Services
January 2008

The security vulnerability assessment performed in this agreement by M2IA does not const
consequently no assurance is expressed.

Where M2IA have provided advice or recommendations in this report, they are not respon
manner in which, suggested improvements, recommendations or opportunities a
management of [redacted] or their nominees, will need to consider carefully the full implica
suggested improvements, recommendations or opportunities, including any adverse eff
requirements, and make such decisions, as they consider appropriate.

This report and all deliverables have been prepared solely for the use of [redacted] and should
or in part without our prior written consent. No responsibility to any third party is accepte
been prepared, and is not intended, for any other purpose.

The matters detailed in our report are only those which came to our attention during the co
procedures and do not necessarily constitute a comprehensive statement of all the wea
exist or actions that might be taken. Accordingly, management should not rely on o
weaknesses and issue
the context of the sco
controls.

7. Appendices

The appendix material that follows contains useful terms, reference materials, vendor web sites and penetration testing tools. Detailed testing results may be found in the Testing Addendum that accompanies this document.

Glossary of Terms

ASP – For business users, ASP refers to Application Service Provider or an outsourcer of applications. The outsourcer generally will purchase the application, hardware and Telco connectivity for the customer, run the corresponding hardware and software and charge the customer a fee (e.g., lease) for use of the service.

Review

1
- **Report Components**
  - Comparison of Security Assessments
  - The Report Criteria

2
- **Report Results Matrix**
  - Classification Scoring
  - Report Delivery

3
- **Recommendations**
  - Executive Summary
  - Technical Report