Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Overview of Threat and Risk Assessment

The purpose of this document is to provide an overview of the process involved in performing a threat and risk assessment. There are many methodologies that exist today on how to perform a risk and threat assessment. There are some that are "open-source" and those that are proprietary; however, they all try to answer the following questions. 1) What needs to be protected? 2) Who/What are the threats and vulnerabilities? 3) What are the implications if they were damaged or lost? 4) What is the value to the organization?...

Copyright SANS Institute
Author Retains Full Rights

AD

James Bayne
Version 1.2f

An Overview of Threat and Risk Assessment

The purpose of this document is to provide an overview of the process involved in performing a threat and risk assessment. There are many methodologies that exist today on how to perform a risk and threat assessment. There are some that are "open-source" and those that are proprietary; however, they all try to answer the following questions.

- What needs to be protected?
- Who/What are the threats and vulnerabilities?
- What are the implications if they were damaged or lost?
- What is the value to the organization?
- What can be done to minimize exposure to the loss or damage?

The outcome or objective of a threat and risk assessment is to provide recommendations that maximize the protection of confidentiality, integrity and availability while still providing functionality and usability. In order to best determine the answers to these questions a company or organization can perform a threat and risk assessment. This can be accomplished using either internal or external resources. It is important that the risk assessment be a collaborative process, without the involvement of the various organizational levels the assessment can lead to a costly and ineffective security measure.

The choice between using internal or external resources will depend on the situation at the time. The urgency of the assessment will also help in determining whether to outsource or use internal resources. The external resource should not have a vested interest in the organization and "be free from personal and external constraints which may impair his or her independence."[1]

The core areas in a risk assessment are:

- Scope
- Data Collection
- Analysis of Policies and Procedures
- Threat Analysis
- Vulnerability Analysis
- Correlation and assessment of Risk Acceptability

Scope

Identifying the scope is probably the most important step in the process. The scope provides the analyst with what is covered and what is not covered in the assessment. It identifies what needs to be protected, the sensitivity of what is being protected and to

[1] Canadian Handbook on Information Technology Security, pg 9-9

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

what level and detail. The scope will also identify what systems and applications are included in the assessment. When investigating and determining the scope keep in mind the intended audience of the final recommendations (i.e. senior management, IT department or certifying authority). The scope should indicate the perspective from which the analysis will take place, whether it is from an internal or external perspective or both. The level of detail is directly related to the intended recipient of the final analysis.

Collecting data

This step involves collecting all policies and procedures currently in place and identifying those that are missing or undocumented. Interviews with key personnel can be conducted using questionnaires or surveys to assist in identifying assets and missing or out-of-date documentation. The systems or applications identified in the scope are enumerated and all relevant information gathered on the current state of those systems.

- Service pack levels
- Services running
- Operating system type
- Network applications running
- Physical location of the systems
- Access control permissions.
- Port scanning
- Wireless leakage
- Intrusion detection testing
- Phone systems testing
- Firewall testing
- Network Surveying

Information on vulnerabilities and threats against the specific systems and services identified can be gathered from various resources.

- Security Focus (www.securityfocus.com) - searchable databases of vulnerabilities and relevant news groups.
- Incidents.org (www.incidents.org) - information on current threat activities.
- Packet Storm (packetstormsecurity.org)
- InfoSysSec (www.infosyssec.com)
- SANS (www.sans.org)

Analyze the policies and procedures

The review and analysis of the existing policies and procedures is done to gauge the compliance level within the organization. Sources for policy compliance that can be used as a base line are:

- ISO 17799
- BSI 7799
- Common Criteria – ISO 15504

It is important to identify the portions that are deemed not to be in compliance with respect to the specific industry and organization. Care must be taken not to determine

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

non-compliance when it is not necessary for the specific organization/region or application.

> Because so many security standards exist, it is often difficult to determine which best applies to the organization. Generic standards offer the most comprehensive view, but these often require security measures that are inappropriate in one or another industry. They fail to take into account the context.[2]

Vulnerability Analysis

The purpose of vulnerability analysis is to take what was identified in the gathering of information and test to determine the current exposure, whether current safe guards are sufficient in terms of confidentiality, integrity or availability. It will also give an indication as to whether the proposed safe guards will be sufficient. Various tools can be used to identify specific vulnerabilities in systems.

- Nessus
- SAINT
- Whisker
- Sara

The problem faced within many organizations is the ability to effectively filter out the false positives inherent in assessment applications. The result of the various tools must be verified in order to accurately determine the reliability of the tools in use and to avoid protecting an area that in reality does not exist. False positive results can be mitigated by ensuring that the assessment applications are up to date with the latest stable signatures and patches.

The vulnerability analysis phase also includes penetration testing with the objective of obtaining something of value, such as a text file, password file, classified document etc. It is important to note that this should be pre-determined with senior management. There are two classifications of penetration testing, testing with knowledge and testing with zero-knowledge. Zero-knowledge testing is usually conducted as an external penetration test, where the tester has no knowledge of the systems involved or network architecture, in effect simulating an external attack and compromise. In a knowledge penetration test the analyst assumes the role of an employee with basic rights and privileges and has access to basic knowledge regarding systems and network topology.

The specific vulnerabilities can be graded according to the level of risk that they pose to the organization, both internally and externally. A low rating can be applied to those vulnerabilities that are low in severity and low in exposure. Vulnerabilities would receive

[2] Security Assessment Methodology – Vigilinx, pg5.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

a high rating if the severity was high and the exposure was high. The following tables from the Threat and Risk Assessment Working guide illustrate this grading system.

Severity	Rating	Exposure
Minor severity: Vulnerability requires significant resources to exploit, with little potential for loss.	1	**Minor exposure:** Effects of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited.
Moderate severity: Vulnerability requires significant resources to exploit, with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.	2	**Moderate exposure:** Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.
High severity: Vulnerability requires few resources to exploit, with significant potential for loss.	3	**High exposure:** Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.

Table 1 – Vulnerability Severity and Exposure Ratings[3]

Severity Rating	**Exposure Rating**		
	1	**2**	**3**
1	1	2	3
2	2	3	4
3	3	4	5

Table 2 – Vulnerability Rating Combinations[4]

Rating	**Description**
1	Minor exposure, minor severity.
2	Minor exposure, moderate severity; or moderate exposure, minor severity.
3	Highly exposed, minor severity; or minor exposure, high severity; or moderate exposure, moderate severity
4	Highly exposed, moderate severity; or, moderate exposure, high severity.
5	Highly exposed, high severity.

Table 3 – Overall Vulnerability Ratings[5]

[3, 4, 5] Threat and Risk Assessment Working Guide, pg 41

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Threat Analysis

Threats are described as anything that would contribute to the tampering, destruction or interruption of any service or item of value. The analysis will look at every element of risk that could conceivably happen. These threats can be split into Human and Non-human elements. For example:

Human	Non-Human
• Hackers • Theft (electronically and physically) • Non-technical staff (financial/accounting) • Accidental • Inadequately trained IT staff • Backup operators • Technicians, Electricians	• Floods • Lightning strikes • Plumbing • Viruses • Fire • Electrical • Air (dust) • Heat control

Threats that are identified must be looked at in relation to the business environment and what affect they will have on the organization. Threats go hand in hand with vulnerabilities and can be graded in a similar manner, measured in terms of motivation and capability. For example, the internal non-technical staff may have low motivation to do something malicious; however, they have a high level of capability due to their level of access on certain systems. A hacker, on the other hand, would have a high motivation for malicious intent and could have a high level of capability to damage or interrupt the business. It is important to note that motivation does not play a part in natural occurring phenomena. A low rating can be given where the threat has little or no capability or motivation. A high rating can be given for those threats that are highly capable and highly motivated.

The use of a grading system will assist greatly in the quantification of risk. The difficulty has always been in justifying the protection of assets. Management is better able to understand the implications of the threat and vulnerabilities when they are quantifiable and measurable.

Analysis of acceptable risks

One of the final tasks is to assess whether or not the existing policies, procedures and protection items in place are adequate. If there are no safeguards in place providing adequate protection, it can be assumed that there are vulnerabilities. A review of the existing and planned safeguards should be performed to determine if the previously known and discovered risks and threats have been mitigated.

It is not the job of the analyst to determine what an acceptable risk is to an organization. The analyst's role is to use the findings from the vulnerability and risk assessment to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

assist in determining, along with the parties involved, what level of risk is acceptable to the organization. The results are the basis for selecting appropriate security measures to be put in place or to remove those that are ineffective. Over-protection can introduce unnecessary costs and overhead. The level of protection required and maintainable will be different for every organization. Depending on the size of the IT department they may or may not be able to maintain the recommended safeguards. This needs to be taken into account in order to effectively recommend a product or procedure.

Conclusion

In summary the threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of the infrastructure.

Organizations that do not perform a threat and risk analysis are leaving themselves open to situations that could disrupt, damage or destroy their ability to conduct business. Therefore the importance of performing a threat and risk analysis must be realized by both the staff supporting the infrastructure and those that rely upon it for their business.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Bibliography:

Stephanou, Tony, "Assessing and Exploiting the Internal Security of an Organization", March 13 2001, http://rr.sans.org/audit/internal_sec.php (January 02 2002)

Vigilinx, "Security Assessment Methodology". 2001, http://www.vigilinx.com/pdf/50722_White_Paper-SAM.pdf (January 02 2002)

Raytheon, "Risk Management and Security, Analysis of the Risk Assessment Process", http://www.silentrunner.com/files/whitepaperriskassess.pdf (January 02 2002)

Naidu, Krishni, "How to Check Compliance with your security policy", January 30, 2001, http://rr.sans.org/policy/compliance.php (January 02 2002)

Kaye, Krysta, "Vulnerability Assessment of a University Computing Environment" May 28 2001, http://rr.sans.org/casestudies/univ_comp.php (January 02 2002)

Symantec, "Vulnerability Assessment Guide", http://enterprisesecurity.symantec.com/PDF/167100088_SymVAGuide_WP.pdf (January 02 2002)

Canadian Communications Security Establishment, "Threat and Risk Assessment Working Guide", November 18 1999, http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/ITSG-04e.pdf (January 02 2002).

Canadian Communications Security Establishment, "Canadian Handbook on Information Technology Security", May 15 1998, http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/mg9e.pdf (January 02 2002)

Herzog, Pete, "Open-Source Security Testing Methodology Manual", Version 1.5, May 5 2001, http://uk.osstmm.org/osstmm.pdf (January 02 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**