BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani
Pilani Campus

SSZG681: Cyber Security
Lecture No: 08

Risk Analysis

Agenda

- What is a Security Assessment?
- Risk Analysis: Definitions and Nomenclature
- Risk Analysis: Methodology and Objectives
- Risk Analysis: Deliverables and Work Plan
- Risk Analysis: Tools and Usage
- Risk Analysis: Dealing with Risk

Content Courtesy (First 5 Topics): Mr Sanjay Goel, University at Albany, SUNY

Security Assessment

Security Assessment Outline

- What is security assessment?
- What are the non-intrusive types?
- How do you choose between these types?
- What are the intrusive types?
- What are the types of risk reduction?
- What is effective security?
- What are the limitations to security assessment?

Security Assessment Overview

- Definition
  - Security assessment identifies existing IT vulnerabilities and recommends countermeasures for mitigating potential risks
- Goal
  - Make the infrastructure more secure
  - Identify risks and reduce them
- Consequences of Failure
  - Loss of services
  - Financial loss
  - Loss of reputation
  - Legal consequences

Security Assessment Type

- Non-Intrusive
  - Security Audit
  - Risk Assessment
  - Risk Analysis
- Intrusive
  - Vulnerability Scan
  - Penetration Testing / Ethical Hacking
- Goal is to identify vulnerabilities and improving security
  - Differ in rules of engagement and limited purpose of the specific engagement (what is allowed, legal liability, purpose of analysis, etc.)

Security Assessment: Non-Intrusive Types

1. Security Audit

- **Security Audit:** Independent review and examination of system records & activities to determine adequacy of system controls, ensure compliance of security policy & operational procedures, detect breaches in security, and recommend changes in these processes.
- Features
  - Formal Process
  - **Paper Oriented:** Review of policies for compliance and best practices
  - **Review System Configurations:** Questionnaire, or console based
  - Automated Scanning
  - Checklists

Security Assessment: Non-Intrusive Types

2. Risk Assessment

- **Risk Assessment** (Vulnerability Assessment):
  - determination of state of risk associated with a system based upon thorough analysis.
  - includes recommendations to support subsequent security controls/decisions.
  - takes into account business as well as legal constraints.
- Involves more testing than traditional paper audit
- Primarily required to identify weaknesses in the information system
- Steps
  - Identify security holes in the infrastructure
  - Look but not intrude into the systems
  - Focus on best practices (company policy is secondary)

Security Assessment: Non-Intrusive Types

3. Risk Analysis

- **Risk Analysis** is the identification or study of:
  - an organization’s assets
  - threats to these assets
  - system’s vulnerability to the threats
- Risk Analysis is done in order to determine *exposure* and potential *loss*
- Computationally intensive and requires data to
  - Compute probabilities of attack
  - Valuation of assets
  - Efficacy of the controls
- More cumbersome than *audit* or *assessment* and usually requires an analytically trained person

Security Assessment

Audit v/s Assessment v/s Analysis

	Audit	Assessment	Analysis
Objective	Measure against a Standard	Baseline	Determine Exposure and Potential Loss
Method	Audit Program/ Checklist	Various (including use of tools)	Various (including use of tools)
Deliverables	Audit Report	Gaps and Recommendations	Identification of Assets, Threats & Vulnerabilities
Performed by	Auditors	Internal or External	Internal or External
Value	Compliance	Focused Improvement	Preparation for Assessment

Security Assessment: Intrusive Types

1. Vulnerability Scan

- **Definition:** Scan the network using automated tools to identify security holes in the network
- Usually a highly automated, fast and cheap process
- Limitations
  - False findings
  - System disruptions (due to improperly run tools)
- Differences in regular scans can often identify new vulnerabilities

Security Assessment: Intrusive Types

2. Penetration Testing

- **Definition:** Penetration Testing (Ethical Hacking) is a simulated attacks on computer networks to identify weaknesses in the network.
- Steps
  - Find a vulnerability
  - Exploit the vulnerability to get deeper access
  - Explore the potential damage that the hacker can cause
- Example
  - Scan web server: Exploit buffer overflow to get an account
  - Scan database (from web server)
  - Find weakness in database: Retrieve password
  - Use password to compromise firewall

Security Assessment: Risk Reduction

There are three strategies for risk reduction:

- **Avoid the risk:** by changing requirements for security or other system characteristics
- **Transfer the risk:** by allocating the risk to other systems, people, organizations assets or by buying insurance
- **Assume the risk:** by accepting it, controlling it with available resources

Security Assessment: Effective Security

- Effective security relies on several factors
  - Security Assessments
  - Policies & Procedures
  - Education (IT team, users & managers)
  - Configuration Standards/Guidelines
    - OS Hardening
    - Network Design
    - Firewall Configuration
    - Router Configuration
    - Web Server Configuration
  - Security Coding Practices

Security Assessment: Limitations

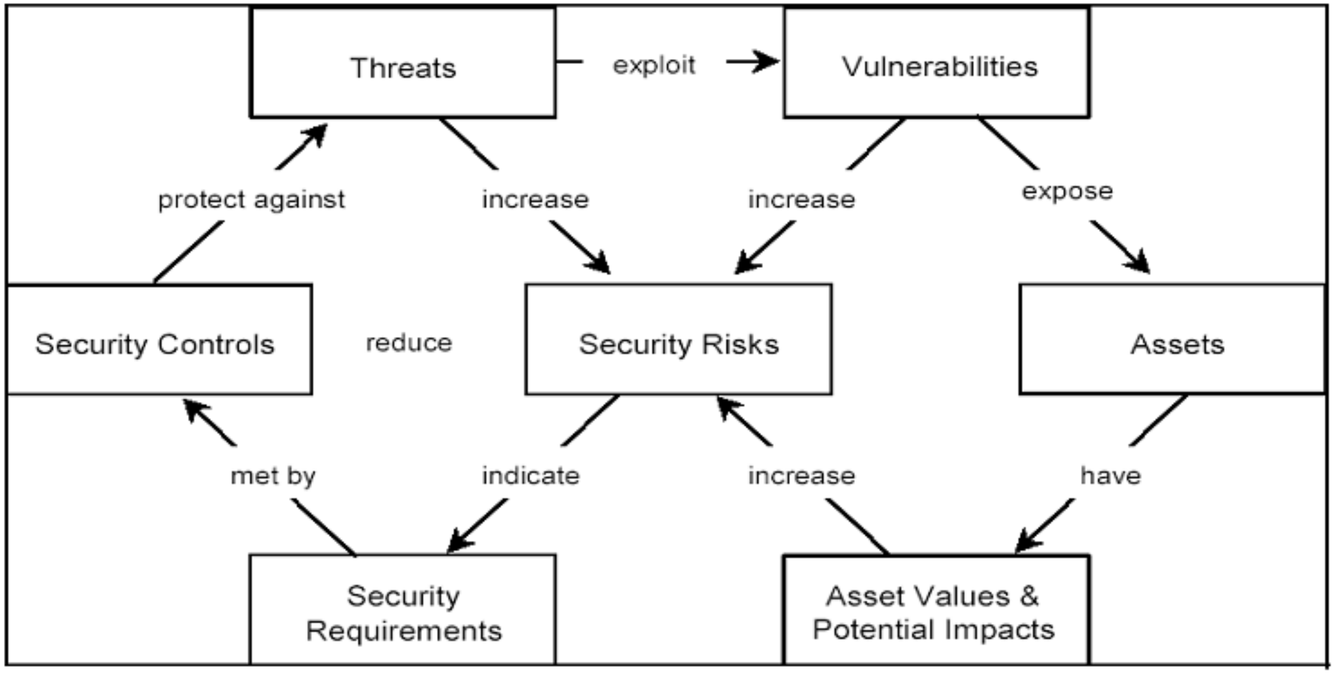
- Often locates previously known issues
  - Provides false sense of security
- Just the first step
  - Needs due diligence in applying the recommendation of the assessment
- Becomes obsolete rapidly
  - Needs to be repeated periodically

Risk Analysis: Definitions and Nomenclature

Risk Analysis: Outline

- What is risk analysis?
- What terms are needed in risk analysis?
- What are assets?
- What are vulnerabilities?
- What are threats?
- What types of risk exist?
    - Security Risk
    - Physical Asset Risks
    - Mission Risks
    - Security Risks

Risk Analysis: Concept Map



- Threats exploit system vulnerabilities which expose system assets.
- Security controls protect against threats by meeting security requirements established on the basis of asset values.

Source: Australian Standard Handbook of Information Security Risk Management – HB231-2000

Risk Analysis: Basic Definitions

- **Assets:** Something that the agency values and has to protect. Assets include all information and supporting items that an agency requires to conduct business.
- **Vulnerability:** A weak characteristic of an information *asset* or group of assets which can be exploited by a t*hreat*. Consequence of weaknesses in *controls*.
- **Threat:** Potential cause of an unwanted event that may result in harm to the agency and its *assets.*[1] A threat is a manifestation of *vulnerability.*
- **Security Risk:** is the probability that a specific *threat* will successfully exploit a *vulnerability* causing a *loss*.
- **Security Controls:** Implementations to reduce overall *risk* and *vulnerability*.

Risk Analysis: Assets

- **Assets:** Something that the agency values and has to protect. Assets include all information and supporting items that an agency requires to conduct business.
- **Data**
  - Breach of confidentiality
  - Loss of data integrity
  - Denial of service
  - Corruption of Applications
  - Disclosure of Data
- Organization
  - Loss of trust
  - Embarrassment
  - Management failure
- Personnel
  - Injury and death
  - Sickness
  - Loss of morale

Risk Analysis: Assets…

- Infrastructure
  - Electrical grid failure
  - Loss of power
  - Chemical leaks
  - Facilities & equipment
  - Communications
- Legal
  - Use or acceptance of unlicensed software
  - Disclosure of Client Secrets
- Operational
  - Interruption of services
  - Loss/Delay in Orders
  - Delay in Shipments

Risk Analysis: Vulnerabilities

- Vulnerabilities are flaws within an asset, such as an operating system, router, network, or application, which allows the asset to be exploited by a threat.
- Examples
  - Software design flaws
  - Software implementation errors
  - System misconfiguration (e.g. misconfigured firewalls)
  - Inadequate security policies
  - Poor system management
  - Lack of physical protections
  - Lack of employee training (e.g. passwords on post-it notes in drawers or under keyboards)

Risk Analysis: Threats

- Threats are potential causes of events which have a negative impact.
- Threats exploit vulnerabilities causing impact to assets
- Examples
  - Denial of Service (DOS) Attacks
  - Spoofing and Masquerading
  - Malicious Code
  - Human Error
  - Insider Attacks
  - Intrusion

Risk Analysis: Source of Threats

Source	Examples of Reasons
External Hackers with Malicious Intent	• Espionage • Intent to cause damage • Terrorism
External Hackers Seeking Thrill	• Popularity
Insiders with Malicious Intent	• Anger at company • Competition with co-worker(s)
Accidental Deletion of Files and Data	• User errors
Environmental Damage	• Floods • Earthquakes • Fires
Equipment and Hardware Failure	• Hard disk crashes

Risk Analysis: Security Risk

- Risk is the probability that a specific *threat* will successfully exploit a *vulnerability* causing a *loss*.
- Risks of an organization are evaluated by three distinguishing characteristics:
  - loss associated with an event, e.g., disclosure of confidential data, lost time, and lost revenues.
  - likelihood that event will occur, i.e. probability of event occurrence
  - Degree that risk outcome can be influenced, i.e. controls that will influence the event
- Various forms of threats exist
- Different stakeholders have various perception of risk
- Several sources of threats exist simultaneously

Risk Analysis: Risk Exposure

- Risk Exposure = Probability of Risk * Risk Impact
- Example:
  - Likelihood (Probability of Risk) of a virus attack is 0.30 and cost of cleanup (Risk Impact) after virus attack is 10000 then Risk Exposure is 3000
  - Cost of an antivirus is 500 which reduces the likelihood to 0.05, revised Risk Exposure is 1000 (500 + 0.05*10000)
  - Thus investment in antivirus is worth it

Risk Analysis: Risk Leverage

- Cost associated with risk occurrence = Risk Impact
- Cost associated with risk control = Risk Reduction
- **Risk Leverage is amount of benefit per unit spent**

$$\textbf{Risk Leverage} = \frac{\text{Risk Exposure (before Reduction – after Reduction)}}{\text{Cost of Risk Reduction}}$$

Example: Risk Leverage = (3000 – 1000) / 500

= 4 : 1

Risk Analysis: Risk Types

- **Physical Asset Risks:** Relating to physical and tangible items that have an associated financial value
- **Mission Risks:** Relating to functions, jobs or tasks that need to be performed
- **Security Risks:** Integrates with both asset and mission risks

Risk Analysis: Methodology

Risk Analysis: Methodology Outline

- What are the key steps in risk analysis?
- When should risk analysis be performed?
- How to determine breadth and depth?
- How to determine a baseline?
- How to determine the scope?
  - Strategic Context
  - Organizational Context
  - Risk Management Context
- What criteria should be used for risk evaluation?
- What standards should be considered?

Risk Analysis: Methodology Steps

1. Define objectives
2. Define deliverables
3. Establish a work plan
4. Determine tools to assist with process

Risk Assessment: Define Periodicity

- **Periodically**
  - Often event-driven
  - Typically year-over-year comparison
  - Generally labor-intensive
  - Most organizations start with periodic assessments
- **Continuously**
  - Part of the normal workflow
  - Provides “real-time” risk view
  - Often supported by technology and analysis tools
  - Integrated with other IT/business processes

Risk Analysis: Define Objectives

- **Breadth**
  - Organizational
  - People
  - Processes
  - Technology
  - Physical
- **Depth of Analysis**
  - Comprehensive vs. Sampling
  - Key Components vs. Individual Elements

Risk Analysis: Define Baseline

- Baseline
  - Where is the organization today?
  - What controls are in place?
- Evaluation of security control effectiveness
  - Where should the security of the organization be?
  - Where are the gaps?
  - What are opportunities for improvement?
- Establish awareness of threats & vulnerabilities
- Lay foundation for development of security improvement plan

Risk Analysis: Define Scope

- Defining the scope will set the framework for the risks to be managed and will provide guidance for future decisions. This avoids unnecessary work and improves the quality of risk analysis.
- Components
  - Establish strategic context
  - Establish organizational context
  - Establish risk management context
  - Develop risk evaluation criteria

Risk Analysis: Define Standards

- ISO 17799
  - Information technology (Code of practice for information security management)
  - Starting point for developing policies
- ISO 13335
  - Information technology (Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security)
  - Assists with developing baseline security.
- NIST SP 800-xx
  - Different standards for various applications
- Center for Internet Security
  - Configuration Standards (benchmarks)

Risk Analysis: Define Strategic Context

- This is based on the environment in which the agency operates.
- The agency should understand:
  - Strengths, weaknesses, opportunities, & threats
  - Internal and external stakeholders (objectives and perceptions)
  - Financial, operational, competitive, political, social, client, cultural and legal aspects of agency's functions.
- Risk analysis should be related to agency's mission or strategic objectives
- Cross-organizational issues should be taken into consideration when applicable

Source: Information Security Guidelines for NSW Government
Agencies Part 1 Information Security Risk Management

Risk Analysis: Define Organizational Context

- Organizational Context requires
  - Understanding of agency
  - How it is organized
  - Capabilities, goals, objectives, and strategies
  - Knowledge of assets and values

- This assists in:
  - Defining criteria to determine risk acceptability
  - Forms the basis of controls and risk treatment options

Source: Information Security Guidelines for NSW Government
Agencies Part 1 Information Security Risk Management

Risk Analysis: Define Risk Management Context

- Define review project and establish goals and objectives
  - Will review cover whole organization or just a single project, individual assets or groups of assets?

- Define timeframe and location of review
  - What is budgeted time for review?
  - Where will the review take place? (one site or group of sites)

Source: Information Security Guidelines for NSW Government Agencies Part 1 Information Security Risk Management

Risk Analysis: Define Risk Management Context…

- Identify resources required to conduct review
  - Use to identify sources of risk, common vulnerabilities, threat types and areas of impact
  - Is assessment done internally or through an outside consultant?
  - How many people will be involved?
  - Who are the best people to involve?
  - What tools are going to be used?
- Define extent of risk analysis
  - What are the functions of the parts of organization participating in managing risk?
  - What is the relationship between the risk assessment and other projects within other parts of the agency?

Source: Information Security Guidelines for NSW Government
Agencies Part 1 Information Security Risk Management

Risk Analysis: Define Risk Evaluation Criteria

- Qualitative or Quantitative methods
- Level of acceptable risk should be considered
- Baseline
  - a collection of policies, *standards*, processes and technologies that establish a defined security level.
- Risk criteria is influenced by:
  - Agency's internal policy, goals and objectives
  - Expectations of stakeholders and customers
  - Legal requirements

Risk Analysis: Deliverables and Work Plan

Risk Analysis: Deliverables and Work Plan Outline

- Who is the intended audience for risk analysis?
- Who should take part in risk analysis?
- How is a work plan created?
  - Planning
  - Preparation
  - Threat Assessment
  - Risk Assessment
  - Recommendations

Risk Analysis: Target Audiences

- Executives
  - Upward communication
  - Brief and concise
- Operational
  - What needs to be done for implementation of controls
- Internal Employees
  - Awareness
  - Training
- External Parties

Risk Analysis: Work Plan Team Composition

- **Business**
  - **Security Officer:** planning, budgeting and management of security staff
  - **Security Manager:** policy negotiation, data classification, risk assessment, role analysis
- **Technical**
  - **Security Operations:** vulnerability assessment, patch management, intrusion detection, scanning, forensics, response management, security technology research
  - **Security Architect:** technology implementation, implementation options
  - **Security Administrator:** user administration, server security configuration, desktop security
  - **Resource Owner:** own any residual risk after controls are implemented
  - **Resource Custodian:** implements/monitors controls
- **Communications**
  - **Security Communications:** marketing, awareness

Source: CSCIC & Meta Group, Inc.

Risk Analysis: Work Plan Creation

1. Planning Stage
   - Aim and scope
   - Identification of security baselines
   - Schedule and methodology
   - Acknowledgement of responsibility
2. Preparation
   - Asset and value listings
3. Threat Assessment
   - Threats, sources, and impact
4. Risk Assessment
   - Evaluation of existing controls
   - Vulnerabilities and exploit probability
   - Analysis of risk
5. Recommendations
   - Addition of new controls
   - Modification of existing controls
   - Removal of obsolete/inadequate controls

Risk Analysis: Tools and Usage

Risk Analysis: Tools and Usage Outline

- What are asset inventory tools?
- What are software usage tools?
- What are vulnerability assessment tools?
- What are configuration validation tools?
- What are penetration testing tools?
- What are password auditing tools?
- What are documentation tools?

Risk Analysis: Tool Types

- Tools can speed up the security assessment and help in automation of the risk analysis process.
- Several categories of tools exist:
  - Asset Inventory
  - Software Usage
  - Vulnerability Assessment
  - Configuration Validation
  - Penetration Testing
  - Password Auditing
  - Documentation

Risk Analysis: Assets & Tools Inventory

- Inventory process includes physical inventory and automated tools
- Physical inventory of IT assets that are not attached to the network
  - e.g. in storage closets or locally attached and that are thus not discoverable.
- Auto-discovery tools collect physical data on an enterprise's IT assets and record history of changes made to the asset from the last scan
  - e.g. memory, processor, and software version
- Inventory tools can either:
  - install an agent on the hardware device, which lets the inventory run even if the device is not attached to the network,
  - or be agentless, which can send information only when it is attached to the network.
- In environments with mobile set of assets that are sporadically connected (e.g. once a month), agentless technology requires alternatives way to capture the inventory
  - e.g. such as an e-mail that kicks off the scan.
- The assets that need to be discovered include
  - PDAs, PCs, networking equipment, and servers.

Risk Analysis: Assets & Tools Inventory

Name	Description
Asset Tracker for Networks	Inventory software tool intended to audit software and hardware components installed on computers over a network. It collects network inventory information, provides detailed comprehensive reports and allows export of assets details to external storages, such as SQL database or web site. http://www.alchemy-lab.com/products/atn/
Asset Center	Peregrine Autodiscovery/inventory tool which maintains “an evolving snapshot of IT infrastructure” and provides: what hardware and software is available, asset connection to other assets, location of assets, access to assets, as well as financial and contractual information on assets. http://www.peregrine.com/products/assetcenter.asp
Unicenter Access Managem ent	Computer Associates International asset management tool. It features: “automated discovery, hardware inventory, network inventory, software inventory, configuration management, software usage monitoring, license management and extensive cross-platform reporting.” http://www3.ca.com/Solutions/Product.asp?ID=194

Risk Analysis: Assets & Tools Inventory

Name	Description
Tally Systems	Tally Systems offers three tools which can be used for IT asset inventory. These are: TS Census Asset Inventory, WebCensus and PowerCensus. These products provide unparalleled IT asset inventory and tracking, hosted PC inventory and reporting, and enhanced inventory for Microsoft SMS respectively. http://www.tallysystems.com/products/itassettracking.html
Isogon	Isogon offers multiple tools. SoftAudit gathers software inventory and usage data from your z/OS, OS/390, or UNIX server. Asset insight offers PC, PDA, & network device auto-discovery software & captures data. Vista manages and organizes details from contracts, contract addenda/attachments, and maintenance agreements. http://www.isogon.com/SAM%20Solutions.htm

Risk Analysis: Software Usage

- Tools monitor the use of software applications in an organization
- Several uses of such tools
  - Track usage patterns and report on trends to assist with server load balancing and license negotiation to prevent costly overbuying or risk-laden under buying.
  - Used to monitor and control the use of unauthorized applications (for example, video games and screen savers).
  - Important for vendor auditing the customers especially for monitoring clients for subscription-based pricing

Name	Description
Software Audit Tool (GASP)	Designed to help detect and identify pirated software through tracking licenses. It is a suite of tools used by the Business Software Alliance and is freely available at: http://global.bsa.org/uk/antipiracy/tools/gasp.phtml

Risk Analysis: Vulnerability Assessment Tools

- Vulnerability Assessment helps determine vulnerabilities in computer networks at any specific moment in time.
- Deliverables:
  - List of exploits and threats to which systems and networks are vulnerable. (Ranked according to risk levels)
  - Specific information about exploits and threats listed. (name of exploit or threat, how the threat/exploit works)
  - Recommendations for mitigating risk from these threats and exploits.
- Tools used can be:
  - Commercial or open source (decide based on staff skills)
  - Perform analysis such as Host-based or network-based

Risk Analysis: Vulnerability Assessment Tools

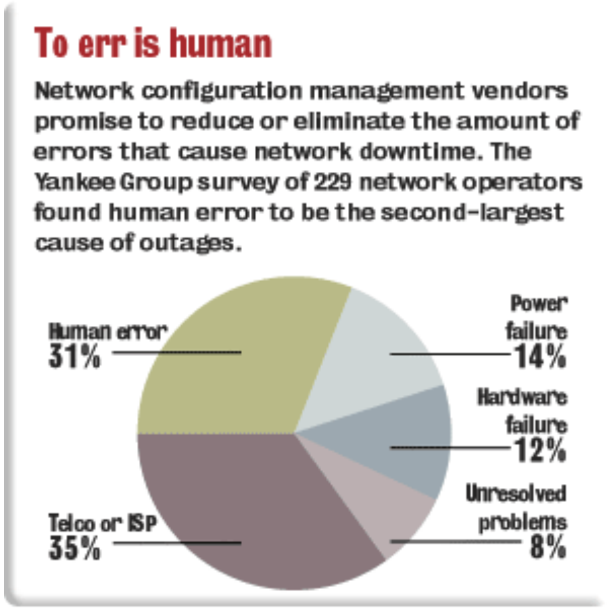
Host-based Tools	Network-Based Tools
Pros	Pros
Can provide rich security information, such as by checking user access logs.	Once deployed, have limited impact on network traffic.
Can give a quick look at what weaknesses hackers and worms can exploit.	Available as software, appliances and managed services.
Cons	Cons
Costs can add up when deploying agents across many desktops and servers.	Deployment can be time-consuming.
Requires careful planning to avoid conflict with security systems.	Generates considerable network traffic.

Risk Analysis: Vulnerability Assessment Tools

Name	Description
Cerberus Internet Scanner	Windows web server vulnerability tester designed to help administrators locate and fix security holes in their computer systems http://www.cerberus-infosec.co.uk/cis.shtml
Cgichk	A web vulnerability scanner which searches interesting directories and files on a site. Looks for interesting and hidden directories such as logs, scripts, restricted code, etc. http://sourceforge.net/projects/cgichk/
Nessus	Server and client software vulnerability assessment tool which provides remote and local security checking. http://www.nessus.org/download.html
SAINT	SAINT (Security Administrator's Integrated Network Tool) is a security assessment tool. It scans through a firewall updated security checks from CERT & CIAC bulletins. Also, it features 4 levels of severity (red, yellow, brown, & green) through an HTML interface. Based on SATAN model. http://www.saintcorporation.com/products/saint_engine.html
SARA	SARA (Security Auditor's Research Assistant) Third generation UNIX-based security analysis tool. It contains: SANS/ISTS Certified, CVE standards support, an enterprise search module, standalone or daemon mode, user extension support and is based on the SATAN model http://www.www-arc.com/sara/
Nikto	A web server scanner which performs comprehensive tests against web servers for multiple items, including over 2200 potentially dangerous files/CGIs, versions on over 140 servers, and problems on over 210 servers http://www.cirt.net/code/nikto.shtml

Risk Analysis: Configuration Validation Tools

- Configuration Validation
  - is the process in which the current configuration of a specific system, software, or hardware tool is tested against configuration guidelines.



To err is human

Network configuration management vendors promise to reduce or eliminate the amount of errors that cause network downtime. The Yankee Group survey of 229 network operators found human error to be the second-largest cause of outages.

- Human error is shown to be the 2nd largest reason for network downtime.
- Using configuration validation tools will help correct for human error

Risk Analysis: Configuration Validation Tools

- Depending on focus, especially with network and OS configurations, configuration validation can utilize the same tools as vulnerability assessment & penetration testing
- However, there are more specialized tools for validating specific software applications and hardware.

Risk Analysis: Configuration Validation Tools

Name	Description
Microsoft Baseline Security Analyzer	Method of identifying common security misconfigurations among Microsoft Windows NT 4.0, 2000, XP, 2003, IIS, SQL Server, Exchange Server, Media Player, Data Access Components (MDAC), Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, Host Integration Server & Office. http://www.microsoft.com/technet/security/tools/mbsahome.mspx
CISCO Router and Security Device Manager	This offers advanced configuration support for LAN and WAN interfaces, NAT, Stateful Firewall Policy, Inline Intrusion Prevention and IPSec virtual private network (VPN) features. It also provides a 1-click router lockdown and ability to check and recommend changes to router configuration based on ICSA Labs, and Cisco TAC recommendations." http://www.cisco.com/en/US/products/sw/secursw/ps5318/
Linux Configuration and Diagnostic Tools	This site provides a listing of various Linux configuration tools for system and network configuration, X configuration, library and kernel dependency management, and general diagnostics. http://www.comptechdoc.org/os/linux/usersguide/linux_ugdiag.html

Risk Analysis: Penetration Testing Tools

- Penetration Testing is the evaluation of a system for weaknesses through attempting to exploit vulnerabilities.
- Can be done in-house or by a neutral 3rd party
- “Black-box” (no knowledge) or “White-box” (complete knowledge)
- Steps
  - Define scope (*External*: servers, infrastructure, underlying software; *Internal*: network access points; *Application*: proprietary applications and/or systems; *Wireless/Remote Access*; *Telephone/Voice Technologies*; *Social Engineering*)
  - Find correct tools (freeware or commercial software)
  - Properly configure tools to specific system
  - Gather information/data to narrow focus (“white-box”)
  - Scan using proper tools
- Penetration Testing tools can include:
  - Network exploration (ping, port scanning, OS fingerprinting)
  - Password cracking
  - IDS, Firewall, Router, Trusted System, DOS, Containment Measures Testing
  - Application Testing and Code Review

Risk Analysis: Penetration Testing Tools

Name	Description
Whois	Domain name lookup to find administrative, technical, and billing contacts. It also provides name servers for the domain. http://www.allwhois.com
Nmap	Utility for network exploration or security auditing. Can scan large networks or single hosts. It uses raw IP packets to determine hosts available on network, services those hosts are running, OS and OS version they are running, type of packet filters/firewalls being used, etc. http://www.insecure.org/nmap/nmap_download.html
MingSweeper	Network Reconnaissance Tool. Supports various TCP port & filter scans, UDP scans, OS detection (NMAP and ICMP style), Banner grabbing etc. http://www.hoobie.net/mingsweeper/
Cheops	Network mapping tool with graphical user interface (GUI). http://www.marko.net/cheops/
QueSO	Remote OS detector. Sends obscure TCP packets to determine remote OS. http://www.antiserver.it/Unix/scanner/Unix-Scanner/

Risk Analysis: Password Auditing Tools

- Used for testing passwords for weaknesses which lead to vulnerable systems
- Reasons for password weakness
  - Poor encryption
  - Social engineering (e.g. password is spouse's, pet's or child's name)
  - Passwords less than 8 characters
  - Passwords do not contain special characters and numbers in addition to lower and uppercase letters.
  - Passwords from any dictionary
- Software tools might perform these tasks:
  - Extracting hashed passwords / encrypted passwords
  - Dictionary attack (cracks passwords by trying entries in a pre-installed dictionary)
  - Brute force attack (cracks passwords by trying all possible combinations of characters)
- Deliverables
  - Recommendations for future password policies

Risk Analysis: Password Auditing Tools

Name	Description	OS
John the Ripper	Detects weak UNIX passwords. "Uses highly optimized modules to decrypt different ciphertext formats and architectures" Can be modified to crack LM hashes in Windows. http://www.openwall.com/john/	All platforms
Brutus	Remote password cracker. http://www.hoobie.net/brutus/	Windows
Magic Key	Audits the AppleTalk users file for weak passwords using brute force methods. http://freaky.staticusers.net/security/auditing/MK3.2.3a.sit	Macintosh
L0phtcrack	Assesses, recovers, and remediates Windows and Unix account passwords from multiple domains and systems. http://www.atstake.com/products/lc/	Windows & UNIX
SAMInside	Extracts information about users from SAM-files and performs brute force attack of Windows NT/2000/XP. Breaks defense of Syskey. http://www.topshareware.com/SAMInside-download-5188.htm	Windows
GetPass!	Cracks weakly encrypted Cisco IOS type 7 passwords once encrypted password file is obtained. http://www.networkingfiles.com/Network/downloads/bosongetpassdownload.htm	Cisco Router IOS
wwwhack	Brute force utility that will try to crack web authentication. Can use a word file or try all possible combinations, and by trial-and-error, will attempt to find a correct username/password combination. http://www.securityfocus.com/tools/1785	Windows

Risk Analysis: Documentation Tools

- Documentation contains data from the risk analysis
- These documents should contain deliverables from other parts of the process (asset inventory, vulnerability assessment etc.).
  - These can be provided automatically from specialized software or through compiled reports.
- Documentation critical for legal cases where it can be used as evidence to justify expense on controls.
- Documentation might include:
  - Focus of analysis
  - Current system vulnerabilities
  - Cost benefit analysis
  - Recommended controls

Risk Analysis: Dealing With Risks

Dealing With Risks: Dealing with Natural Disasters

- Flood
  - Redundant assets like servers, data storage etc
  - Mechanisms to save machines from water like plastic waterproof bags to cover computing machines
  - Store backup at safe and separate location
- Fire
  - Plan to shutdown system in orderly manner
  - Windowless fire-resistant facility especially for critical assets like servers, data backup etc
  - Regular fire drills to assess readiness
- Other natural disasters: Storms, Earthquakes, Volcanoes etc
  - Develop contingency plans so that people know how to react
  - Take insurance cover for physical assets
  - Preserve sensitive data by maintaining physical/digital copy at separate location

Dealing With Risks: Dealing with Power Loss

- Uninterrupted power supply
- Surge suppressors

Dealing With Risks: Human Vandals

- Disgruntled employee, Saboteur, Bored operator, People seeking excitement, Unwitting bumblers
  - Physical security
- Unauthorized access and use
  - Intercept access, access by authorization only
- Theft: portable reports or PDAs
  - Prevent access & portability of assets, Detect at exit

Dealing With Risks: Preventing Access

- **Physical guards:** record of each person entering/exiting the facility
- **Lock control:** Mechanical or digital. Piggy-backing is a challenge
- Magnetic strip cards, RFID cards, smart cards with electronic chips

Dealing With Risks: Preventing Portability

- Pad connected with fixed cables
- Large lockable cabinets for computing devices
- Movement activated alarms

Dealing With Risks: Detecting Theft

- Marking with special labels which can be detected at exit: libraries use it
- Security tags like to one used by retails stores
- GPS enabled tags to show location of asset
- Radio enabled tags

Dealing With Risks: Interception of Sensitive Information

- Shredding
- Overwriting magnetic data: data can be reconstrcuted
- Degaussing: usage powerful magnetic force to realign magnetic particles
- Protecting against emanation: radio signals emitted by devise (screens, disk drives, printers) can be read and data reconstructed.
    - Tempest: US govt program to certify a device as emission free

Dealing With Risks: Contingency Planning - Backup

- Backup: enables recovery from loss or failure of comuting devices
  - Complete or incremental
  - All assets or selected assets
  - Revolving backup
  - Completeness of backups
  - Restorability of backups
  - Cost of backup
- Individuals often fail to backup their data
- Off-site backup: Purpose of backup is to protect against disaster thus disaster should not destroy backup.

Dealing With Risks: Contingency Planning - Backup

- Network storage: Provided by private players, Good for critical data
- Cloud backup: Google Docs, Amazon S3, Dropbox, Apple etc
  - Cloud provider may go out of business
  - Data privacy/secrecy issues
- **Cold or Shell site**: A facility with power and cooling available where computing machines can be installed to immediately start limited or full operations. Normally operations can start within a week.
- **Hot site**: Facility with installed and ready to run computing systems. To start operations, team needs to load software and data only.
  - Self owned hot site
  - Third party owned hot site (shared)

Security Assessment: Summary

- Security Assessment is critical to build a measured defense against intrusions
- Risk Analysis involves:
  - Asset Valuation
  - Vulnerability Analysis
  - Threat Identification
  - Evaluation and Recommendation of Controls
- Several levels of risk analysis can be performed:
  - Audit (checklists and rules)
  - Non-Intrusive Vulnerability Assessment
  - Penetration Testing

Thank You