Module 3

Information Security Management

Monitor systems and apply controls - security assessment using automated tools

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 (weakness) 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

Types

- Non-Intrusive
  1. Security Audit
  2. Risk Assessment
  3. Risk Analysis
- Intrusive
  1. Vulnerability Scan
  2. Penetration Testing / Ethical Hacking
- All have the goal of identifying 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.[1]
- Features
  - Formal Process
  - Paper Oriented
    - Review Policies for Compliance and Best Practices
  - Review System Configurations
    - Questionnaire, or console based
  - Automated Scanning
  - Checklists

1 http://www.atis.org/tg2k/_security_audit.html

Security Assessment: Non-Intrusive Types

2. Risk Assessment

- **Risk Assessment** (Vulnerability Assessment) is:
  - 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

How to choose

- Security audit, risk assessment and risk analysis have similar goals.

Security Assessment

Assessment vs. Analysis vs. Audit

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

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 process
  - Fast and cheap
- 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 (Ethical Hacking)
  - 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:

- Avoiding the risk
  - by changing requirements for security or other system characteristics
- Transferring the risk
  - by allocating the risk to other systems, people, organizations assets or by buying insurance
- Assuming 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 (of IT staff, 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

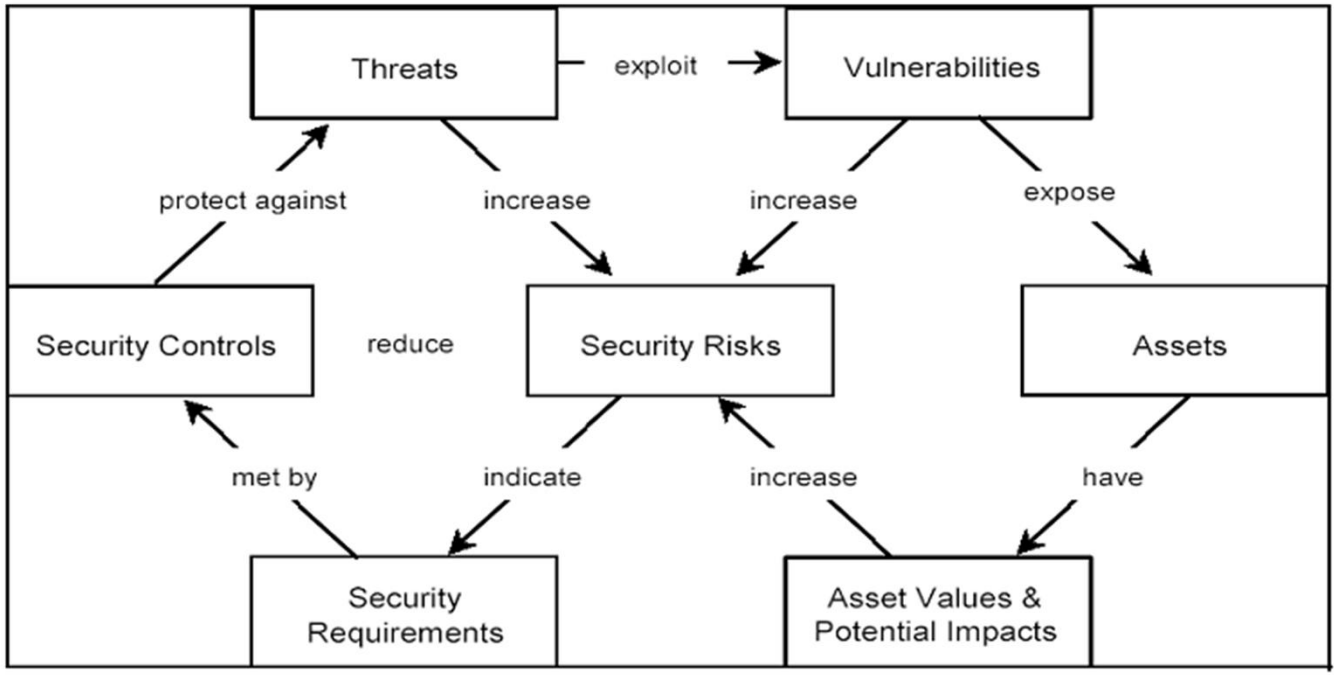
What is Security Assessment?

Case

- Scenario to identify the suitable method for application to the scenario

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.

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*.[1] 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*.

1 http://www.oit.nsw.gov/au/pdf/4.4.16.IS1.pdf

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 Cont'd

- 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

Sources 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

Physical Asset Risks

- Physical Asset Risks
  - Relating to items with physical and tangible items that have an associated financial value

Risk Analysis

Mission Risks

- Mission Risks
  - Relating to functions, jobs or tasks that need to be performed

Risk Analysis

Security Risks

- Security Risks
  - Integrates with both asset and mission risks

Risk Analysis: Definitions and Nomenclature

Question 1

1) From the concept map, fill in the blanks:

Vulnerabilities are exploited by_____.

_____ are used to diminish risk from threats.

To determine _____ it is necessary to know the values of assets as well as the _____ to threats.

Knowledge of security _____ is necessary before deciding on controls to implement.

Risk Analysis: Definitions and Nomenclature

Question 2

2) Match the type of asset to the potential threat

Organization	Stolen Credit Card Numbers
Operational	Air Traffic Radar Failure
Data	Loss of Orders
Legal	System Administrator's Death
Personnel	Loss of Reputation
Infrastructure	Denial of Service

Risk Analysis: Definitions and Nomenclature

Question 3

3) Threat or Vulnerability ? Place a T next to an example of a threat and a V next to an example of a vulnerability

_____ Misconfigured firewall

_____ Denial of Service

_____ Unpatched operating system

_____ Theft

_____ Hard Drive Failure

_____ Unauthorized access to data

_____ Code within IE which allows for an attacker to execute malicious program

_____ Unlocked door

_____ Code Red Worm

_____ Weak passwords

Risk Analysis: Define Objectives

Standards

- ISO 17799
  - Title: Information technology -- Code of practice for information security management
  - Starting point for developing policies
  - http://www.iso.ch/iso/en/prods-services/popstds/.../en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35
- ISO 13335
  - Title: Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security
  - Assists with developing baseline security.
  - http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21733&ICS1=35

- NIST SP 800-xx
  - Different standards for various applications
  - http://csrc.nist.gov/publications/nistpubs/
- Center for Internet Security
  - Configuration Standards (benchmarks)
  - http://www.cisecurity.org/

Risk Analysis: Tools and Usage

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

Source: http://techrepublic.com.com/5100-6262-5060605-2.html

Risk Analysis: Tools and Usage

Asset inventory

Source: http://techrepublic.com.com/5100-6262-5060605-2.html

- 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.
- Autodiscovery 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: Tools and Usage

Asset Inventory Tools

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 Management	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

Tools

Asset Inventory Tools, cont'd.

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: Tools and Usage

Software Usage

- 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

Risk Analysis: Tools and Usage

Software Usage Tools

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: Tools and Usage

Vulnerability Assessment

- 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: Tools and Usage

Vulnerability Assessment (Host or Network Based)

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.

Source: http://www.nwfusion.com/news/2004/0405specialfocus.html

Risk Analysis: Tools and Usage

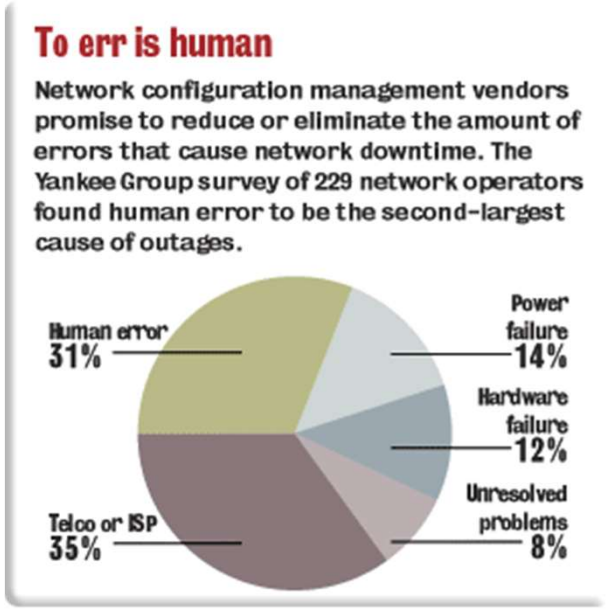
Vulnerability Assessment

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	This is 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: Tools and Usage

Configuration Validation

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



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

Source: http://nww1.com/news/2004/0216specialfocus.html

Risk Analysis: Tools and Usage

Configuration Validation

- 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: Tools and Usage

Configuration Validation

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: Tools and Usage

Penetration Testing

- 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

Source: http://www.penetration-testing.com

Risk Analysis: Tools and Usage

Penetration Testing

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: Tools and Usage

Password Auditing

- 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 6 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: Tools and Usage

Password Auditing

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: Tools and Usage

Documentation

- 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