NSSA Faculty Involvement in IT Security Auditing at RIT

Daryl Johnson and Yin Pan

Rochester Institute of Technology

Agenda

- Motivation
- challenges
- A special IT security auditing team
- Auditing Procedures
- Techniques and Tools
- Benefits and our experience
- Improvements

Why think about security?

With our great reliance on computers and the Internet, plus the numerous flaws found in most systems, today is the Golden Age of Hacking.

Targets

- Government agencies
- E-commerce sites, banks and credit-cared processors
- Companies
- Universities

Risk Tolerance

- Exposure
- Reputation
- Financial loss
- Employment
- Freedom
- Injury
- Death
- Threat to family

The Attackers --outside threats

- Organized crime
  - Sensitive data for identity theft or other fraud
- Terrorists
  - Shut down critical systems, destroy systems or cause potentially life-threatening problem
- Governments
  - Have active interest in the activities of organizations
- Competition
- Hacktivists
  - If your organization does something politically sensitive
- Hired guns
  - Hired to stealing information or gaining access

The Attackers --Insiders …

- Disgruntled employees
- Clueless employees
- Customers
  - Attacking suppliers in an attempt to gain sensitive information about other customers or alter prices
- Suppliers/ Vendors
  - Attack customers
- Contractors and consultants

The Challenge

- Those in the security arena understand these threats.
- The challenge is to impart some sense of vulnerability to those outside.
- Everyone is a target of opportunity
- Some are a High Valued Target
- Which are you?

How to fight back in this battle?

- Regulators create a large set of regulations and frameworks
  - in an effort to enforce protection of information, privacy and transparency of information.
- We need to manage security risks and ensure compliance with information security regulations and industry standards
- Audit your system and network periodically!

Challenges

- Where to find the auditors with the IT skills required to meet the rapidly increased needs
- Our university, Rochester Institute of Technology (RIT), faces the same challenge.
  - RIT has a team of professional auditors whose expertise lie in financial audits
  - the auditors lack of technical background of IT audits

Our solution

- Utilizing faculty's auditing and computer security expertise
- RIT formed an auditing team that was composed of
  - the RIT faculty
  - the auditors
  - the campus security officers
- Auditing campus wide servers and networks, and systems

What is "Auditing"

- A methodical examination and review of measuring something against a standard
- Answer the question, "How do you know?"
- Example of audits

Objective of Auditing

- To measure and report on risks
  - Against existing policy within the organization
  - Against existing standards or guidelines, best practices
- Raise awareness and reduce risks

How do we start?

- **Preparation for the auditing**
  - Faculty signs confidentiality agreement.
- **Follow the six-step Process for Audit from SANS**

6 Step Process for Audit
from SANS

- Audit Planning
- Meeting Relevant People With The Plan
  - With high level people, Initiating audit
- Measuring the Systems
- Preparing the Report
- Presenting Results
- Report to Management

Audit Planning
by faculty and the campus auditors

- Determining audit objectives and scope identify responsibility
- Research vulnerabilities and risks
- Creating checklist
- Lay out the strategies

Determining audit objectives and scope identify responsibility

- What is our audit goal?
- Policies for compliance?
- What should we audit?
- What is the time period for auditing?

Our goal

- To secure every possible path into our critical systems
- To prevent the leaking of sensitive data out

What to be compliant with?

- Policies provided by the campus security office to follow
  - Server security standard
    - http://security.rit.edu/articles/serverstandard.pdf
  - Network standard
    - http://security.rit.edu/articles/networkstandard.pdf
  - Industrial best practice
    - Center for Internet Security
    - NIST: http://www.nist.gov/
    - NSA: http://www.nsa.gov/snac/
    - SANs:www.san.org
  - Web Standards
    - OWASP: www.owasp.org

What should we audit?

- Reviewing the RIT System Inventory and RIT Logical Network diagram provided by campus Information Technology Support Team
- Randomly select 5-10 systems, 5-10 servers and 5-10 routers for auditing
- Audit campus wide modem systems

Time period audited

Phase I and Phase II

- Phase I
  - Campus wide modem security audits
  - Require system administration to provide answers to the checklist
- Phase II
  - Campus wide modem security audits
  - Conduct servers and networks auditing by IT auditors

Create Checklist / form

- The most important step for an auditor in the planning phase
- What are included in an audit checklist?
  - Statement of purpose/scope (optional)
  - What to measure against
    - Existing corporate policy and procedure or create one
    - Existing audit standards or guidelines
    - Best practices
    - Security guides with technical detail
    - For example, the content to be checked, under which section, reference to the standard
  - How to measure it
    - Create the audit procedure to answer "how to measure it"
    - References
  - Findings
  - Compliance
- An example
  - http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

Creating checklists

- Faculty and auditors studied the given standards and industrial best practice
- Meet the chief security officer to discuss the standards
  - clarify, modify, enhance the server and network security standards
- Create IACA network checklist and IACA Server checklist

Lay out the strategies

- How to provide the team with the confidential information (network diagram, routing configurations) in a secure manner?

Measure the systems

- First, we will discuss the overall approach
- Secondly, what we have done for our phase I

Measuring the systems

--Vulnerability assessment--

- Specifically answering the question: how do you know? how do we verify?
- Procedure
  - Starting with physical security
  - Scan networks (wired and wireless)
  - Secure the perimeter such as router, firewall, IDS, etc.
  - Secure the DMZ
  - Audit internal systems

Methodologies for measuring systems

- Different phases of an audit
  - Discovery methods
    - Reconnaissance
  - Network Identification and Penetration
    - Scanning
  - Systems Auditing
  - Servers and Network perimeters auditing

Reconnaissance

- Auditing team schedule at least a couple of days of comprehensive recon work
- With low-technology
  - Social Engineering
  - Physical break-in
  - Dumpster diving
  - Awareness & Education
- Search Engine and web-based reconnaissance

Tools for Reconnaissance

- Google
- Sam Spade: A general purpose reconnaissance client tool
- Whois databases
  - To find out a registrar for organization based on its domain name
    - InterNIC at www.internic.net/whois.html
    - Outside of USA at www.Uwhois.com
- Nslookup or dig for DNS information
- Range of IP addresses
  - American Registry for Internet Numbers --Arin www.arin.net

Network Identification and Penetration

- Wireless Access Points -- War driving
- Modem -- War dialing
- Network mapping
- Identifying services with port scanning
- Vulnerability scanning

War driving tools

- Identifying wireless access points and determining their ESSIDs
- Wireless side techniques include
  - Active scanning-- NetStumbler
  - Passive scanning -- Wellenreiter and Kismet
  - Forcing de-authentication -- ESSID-Jack
- Wired side audit
  - Nessus-- plugin 11026, Access point detection
- Airsnort and WEPCrack
  - Brute forces WEP/RC4 keys

War Dialing Approach

- Dial a collection of telephone numbers attempting to locate modem carriers, etc.
- Why are we still talking about war dialing?
  - Clueless users connect a modem to their desktop computer in order to access it from home through *PC Anywhere* for example
  - Give modem access to vendors and service providers to troubleshoot devices remotely via phone when the existing IP network goes down
  - Abandoned and forgotten routers and servers still connect to modems
  - Malicious act – purposeful unauthorized access
  - Rogue fax machines

War Dialing

- How to prepare for the audit?
  - Get permission – the difference between a hacker and auditor
  - Define the range to dial (remove emergency numbers)
  - When to dial?
  - How often?
  - Test the audit by dialing some known numbers

War Dialing tools

Tools

- ToneLoc
- THC Scan 2.0 (The Hacker's Choice)
  - Runs on platforms w/PC emulation
- PhoneSweep from SandStorm Enterprises (commercial)
- Phone Tag
- ModemScan
- TBA –use a Palm OS

War Dialing Results

- What can be found
  - Modems
  - Secondary dial tones
  - Fax machines
  - Logs warning banner or login prompt for revealing platform information
- Level of penetration
- Once you found a bunch of modems, what do you do with them?

War Dialing Audit

- Strong modem and dial-up line policy and procedure
  - Modems identified should be authorized for business use only
- Scan all telephone lines for authentication and authorization
  - PBX or direct lines from the phone company
  - digital PBX lines
  - VoIP connections
- perform war dialing periodically
  - Conduct a baseline of the modems within your environment
  - audit the changes to the baseline over time
- Audit the dial-up banner information

Network Audit

- Secure the DMZ
- Map the hosts in the DMZ
- Audit goal:
  - Make sure there are no extra ports open on the DMZ hosts
  - Once you find out the open ports/services, use vulnerability tools to find any possible vulnerabilities associated with these services

Network scan directions

- From outside to eliminate externally accessible vulnerabilities
- Form inside to eliminate internally accessible vulnerabilities

Tools used in network scanning and vulnerability accessment

- Nmap, scanline, superscan
- Netstat, fport
- Nessus
- Firewalk
- cheops-ng

Perimeter Devices Audit

- Company policy/procedure review and interviews
- Perimeter configuration
- Rule validation and perimeter penetration test
  - From outside
  - From inside
- Tools
  - Auditing router configuration file -- RAT, SDM
  - Password recovery -- Cain & Abel
  - Auditing rule base -- hping2, nmap

Services Auditing

- DNS, DHCP, SMB, FTP, SMTP, SNMP, SSH, VPN auditing basics
- Web server and database auditing basics

Web server and application audit

- Web server audit
  - Apache
  - Windows IIS
- Web applications audit
- Commercial/free tools
  - AppScan from Firewatch
  - Hailstorm from Cenzic
  - Nikto
  - Brutus

Systems Auditing

- System information
- logging information
- Files and permissions
- data integrity
- Users, groups, and passwords
- services and processes
- Hidden data and rootkits detection

Tools used for system auditing

- Unix/Linux
  - *netstat, nmap* and *lsof* for gathering open ports
  - *chkrootkit* and *rkhunter* for trojan horse detection
  - *tripwire* for file integrity assessment
  - *John the Ripper* for password recovery
  - *tara* for an overall Unix assessment scan
- Windows
  - *ScanLine, SuperScan, fport* for gathering open ports
  - *psservice* and *tasklist* for gathering running services information
  - *Rootkit revealer* for trojan horse detection
  - *Cain & Abel, lophtcrack* and *DumpSec* for auditing users/groups and password strength
  - *Microsoft Baseline Security Analyzer* for overall Windows assessment scan

Measure the systems – in our phase I

- Modem audits
  - Propose a war dialing exercise
  - Get the written permission from Administrator of which range of phones to be audit at certain time period.
  - Perform the audit using phonesweep
  - Analyze the result
- Auditing selected servers and routers with the defined checklists
- Presenting results
  - To system administrators
  - To Management

Things that surprised us……

- SA did not list VMware servers in the check list
- Using same password on routers
- Router uses Cisco type 7 encoding
- Using same admin password on ITS imaged PCs
- If a question is not addressed in the security standards, the SA refused to answer on these issues

Other issues

- How to securely deliver sensitive data such as router config to auditing team to audit?
  - PGP
- How to work with SAs?

Benefits

- Through this audit, the professional auditor learned IT auditing technologies
  - Auditor sits in auditing class
- Faculty members gain real auditing experiences
- Benefit to college
  - Utilize the existing resources, save cost
- Security Officer
  - Enhance the security standard

Benefits (Con't)

- Benefit to students
  - Faculty members were able to bring their real auditing experience to the auditing and security courses.
  - The auditing procedures and auditing experience will be added to the auditing course material
  - Invite auditor to the auditing class

Future direction

- Work on phase II
- How to deal with virtual servers?
- Work closely with other local companies
- SCADA included in audit

What did we miss?

- Suggestions and Questions?
- Contacts
  - Daryl Johnson
    - daryl.johnson@rit.edu
  - Yin Pan
    - yin.pan@rit.edu