

# IT Security Auditing for University

---

Daryl Johnson and Yin Pan

Rochester Institute of Technology

Secure IT 2008

# Agenda

---

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

---

Secure IT 2008

## 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.

---

Secure IT 2008

Why security is important?

Why it is critical to the business?

Network and operating system optimized for convenience and doesn't make security easy.

Linux: either powerless user or powerful root. Suid root

The ability to use/develop tools to thoroughly investigate disk drives, file systems, files, etc

The knowledge about log and history files generated by different OSs and Apps

How to find hidden files

How to read email headers and track the history of email messages

## Targets

---

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

---

Secure IT 2008

By average, every 20 minutes, one unpatched machine is compromised  
Once a patch is announced, an exploit will be available in 2-3 days

Network and operating system optimized for convenience and doesn't make security easy.  
Linux: either powerless user or powerful root. Suid root

Government agencies

Customized trojan horse designed to pilfer sensitive government secrets

Companies

Source code, coca-cola recipe? Game?

## How security is compromised --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
  - The competition
  - Hacktivists
    - If your organization does something politically sensitive
  - Hired guns
    - Hired by other clients to stealing information or gaining access
- 

Secure IT 2008

1) If your organization handles money, critical infrastructure

## How security is compromised

### --Insiders ...

---

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

Secure IT 2008

Vendors are often given full access to systems for remote diagnostics, system upgrades, and administration. The software running on your systems. A developer could have planted a backdoor or deliberately inserted a security flaw

What is at risk

## 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

---

Secure IT 2008

By learning about and properly defending against these most powerful attacks, you will go a long way in securing your system against other related rootkit attacks

## 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

---

Secure IT 2008

## What is "Auditing"

---

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

---

Secure IT 2008

Examples: Financial audit, security audit, ...

You are on the right track. You have defined the policy and scope. The next step is to define a procedure to measure how well employees are in compliance with this policy. What kind of control/tools will you implement to measure the compliance? The key question is how do you know? You need to convince me that you have enough evidence to support your answers.

You may search for the existing best practice on the procedures / checklist for a password policy. Finally, you need to provide a checklist for measuring the policy compliance.

Check my slides on "A case study", "policy and procedure", "checklist" and "audit planning".

I. You need to work with your company to define the audit scope and identify your responsibilities. That may include the follows.

- 1) What should we audit? For example, in terms of users, does the audit affect every user in the company or only one department? In terms of IPs, what are the IP ranges you are supposed to cover?
- 2) The duration of this audit? For example, Audit once or one month or three month, ..., etc.
- 3) What does the company want us to check for? For example, if you are asked for auditing the password strength, do you only check the password policies in AD or you also need to check for the local log in password?

II. The audit checklist involves the step by step audit procedure which includes

## 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
- 

Secure IT 2008

Objectives of our auditor is a tool used by management to measure and valuated risk to the organization. You are referee!

Raise awareness management bout risk thereby increasing security.

Your action of auditing require good skill of politician

## 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

---

Secure IT 2008

An attack only need one weak link to get in

## What to be compliant with?

---

- Policies provided by the campus security office to follow
  - Server security standard
  - Network standard
  - Industrial best practice
  - Web Standards

## 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

---

Secure IT 2008

VMware

# 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

## 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

---

Secure IT 2008

## Lay out the strategies

---

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

---

Secure IT 2008

i.e. getting router configuration files to check with nikto

## 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

---

Secure IT 2008

Password cracking exercise

# Methodologies for measuring systems

---

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

---

Secure IT 2008

## Discovery methods

Security Scans

Social Engineering

Information you can possibly obtain, google, ...

inspection of employees physical environment

care of data storage devices

connections to modem and other communication devices

## 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

---

Secure IT 2008

Example of a bank robber. Visit the bank for physical security reconnaissance. Record the times that security guards enter and leave, the location of security cameras, alarm systems and the leave gate.

The auditor may try these method to find out whether the employees of the company are well educated.

## 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](http://www.internic.net/whois.html)
    - Outside of USA at [www.Uwhois.com](http://www.Uwhois.com)
- Nslookup or dig for DNS information
- Range of IP addresses
  - American Registry for Internet Numbers --Arin [www.arin.net](http://www.arin.net)

---

Secure IT 2008

## 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
- ❑ Aircrack-ng and WEPCrack
  - Brute forces WEP/RC4 keys

---

Secure IT 2008

Extended Service Set ID

## War Dialing Approach

---

- ❑ Dial a sequence of telephone numbers attempting to locate modem carriers
- ❑ 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

---

Secure IT 2008

War games released in 1983, the main character was using a war dialing to break into a game computer company.

The banner sometimes gives out information of a particular brand of modem. By searching the manual, you may find out the default password.

Voicemail, busy/disconnected line, ISDN, data modem, fax modem, fax machine

## 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 dial some known situation

# War Dialing tools

---

## Tools

- THC Scan 2.0 (The Hacker's Choice)
    - Runs on Windows
  - PhoneSweep from SandStorm Enterprises (commercial)
  - Phone Tag
  - ModemScan
  - Rausers
  - TBA –use a Palm OS
  - Microsoft's Hyper Terminal -- connect to modems
- 

Secure IT 2008

THC, the hack's choice

THC-Scan relies on the attacker to go through the logs and recognize the types of system running at target numbers

With a single machine and a single modem, we typically dial 100 to 125 lines per hour.

Once you found a bunch of modems, what do you do with them?

connect to each discovered modem. Some times, you will find a system without a password (PCAnywhere for a clueless user; old, neglected machine still on the network, router). If there is a userID/password, guess it.

THC has released a powerful scripting language for hacking login prompts: Login Hacker (<http://thc.inferno.tusculum.edu/>)

## War Dialing Results

---

- What to be found
  - A list of the phone numbers with 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?

---

Secure IT 2008

## 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
    - It may help attackers identify the software or hardware being used
- 

Secure IT 2008

Find your unprotected modems before the attackers do

Every three to six months

Buy a digital-to-analog converter for only \$100 to a VoIP line

## 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

---

Secure IT 2008

No extraneous services on these hosts.

You can query for specific ports and get Nessus to work only on the specific vulnerability plugins.

## Scan directions

---

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

---

Secure IT 2008

If we've secured the network from the outside, why inside?

Insider threat is more harmful!

Make sure that there are no vulnerabilities through the insider threat.

Internal vulnerabilities can be there even without go through the firewall

## Tools used in network scanning and vulnerability assessment

---

- 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, Cain & Abel
    - Auditing rule base – hping2, nmap
- 

Secure IT 2008

Passwords not the same

Default passwords

## Servers 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

---

Secure IT 2008

## Systems Auditing

---

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

---

Secure IT 2008

## Tools used for system auditing

---

- Unix/Linux
    - *netstat*, *nmap* and *Isof* 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*, *ophtcrack* and *DumpSec* for auditing users/groups and password strength
    - *Microsoft Baseline Security Analyzer* for overall Windows assessment scan
- 

Secure IT 2008

## Measure the systems – in our phase I

---

- Modem audit
  - 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
  - Report and analyze the result
- Auditing selected servers and routers with the defined checklists

# Report

---

- Presenting results
  - To system administrators
  - To Management

## 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

---

Secure IT 2008

## 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

---

Secure IT 2008

One of the auditing assignment is planning.

## Future direction

---

- ❑ Work on phase II
- ❑ How to deal with virtual servers?
- ❑ Work closely with other local companies



## What did we miss?

---

Suggestions?

Questions?