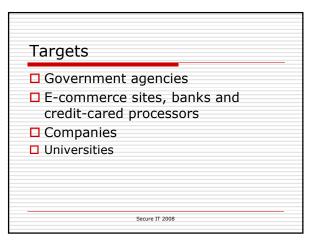
#### NSSA Faculty Involvement in IT Security Auditing at RIT Daryl Johnson and Yin Pan Rochester Institute of Technology

### 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.



Risk Tolerance		
RISK TOTELTHEE		
□ Exposure		
Reputation		
☐ Financial loss		
□ Employment		
□ Freedom		
☐ Injury		
□ Death		
☐ Threat to family		
Secure IT 2008	_	

•	ne Attackers outside threats
	Organized crime
	Sensitive data for identity theft or other fraud
	Terrorists
	<ul> <li>Shut down critical systems, destroy systems or cause potentially life-threatening problem</li> </ul>
	Governments
	Have active interest in the activities of organizations
	Competition
	Hacktivists
	<ul> <li>If your organization does something politically sensitive</li> </ul>
	Hired guns
	■ Hired to stealing information or gaining access
_	Secure IT 2008

#### 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 Secure IT 2008

#### 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? and frameworks in an effort to enforce protection of information, privacy and transparency of information. ensure compliance with information security regulations and industry standards

#### ☐ Regulators create a large set of regulations ☐ We need to manage security risks and □ Audit your system and network periodically! Secure IT 2008

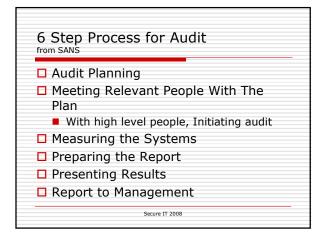
#### Challenges ☐ Where to find the auditors with the IT skills required to meet the rapidly increased needs ☐ Our university, Rochester Institute of Technology (RIT), faces the same challenge. RIT has a team of professional auditors whose expertise lie in financial audits the auditors lack of technical background of IT audits Secure IT 2008

#### 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

	nethodical examination and review measuring something against a
	ndard
	swer the question, "How do you ow?"
□ Exa	ample 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







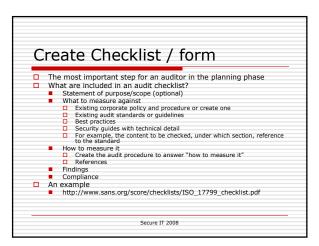
# Determining audit objectives and scope identify responsibility ☐ What is our audit goal? ☐ Policies for compliance? ☐ What should we audit? ☐ What is the time period for auditing?



### 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.nist.gov/ 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

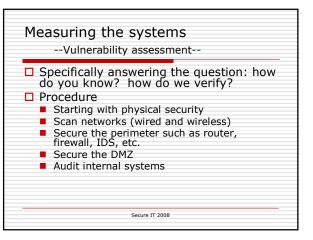
#### Phase I and Phase II Phase I Campus wide modem security audits Require system administration to provide answers to the checklist Phase II Campus wide modem security audits Conduct servers and networks auditing by IT auditors



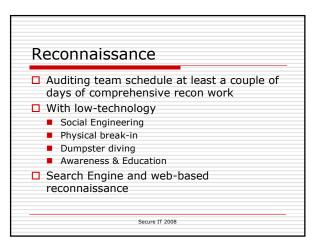
#### Creating checklists ☐ Faculty and auditors studied the given standards and industrial best practice ☐ Meet the chief security officer to discuss the standards ☐ clarify, modify, enhance the server and network security standards ☐ Create IACA network checklist and IACA Server checklist

# Lay out the strategies ☐ How to provide the team with the confidential information (network diagram, routing configurations) in a secure manner?

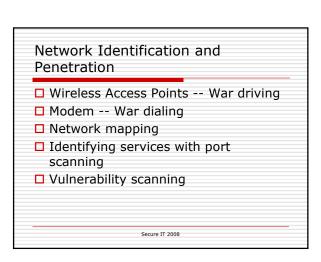
#### Measure the systems First, we will discuss the overall approach Secondly, what we have done for our phase I



# Methodologies for measuring systems Different phases of an audit Discovery methods Reconnaissance Network Identification and Penetration Scanning Systems Auditing Servers and Network perimeters auditing



### 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



#### 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

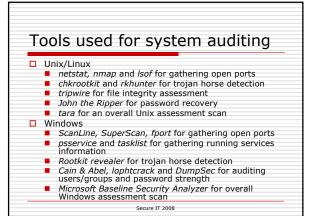
DNS, DHCP, SMB, FTP, SMTP, SNMP, SSH, VPN auditing basics

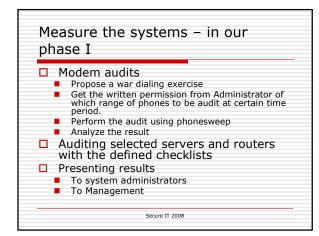
Web server and database auditing basics

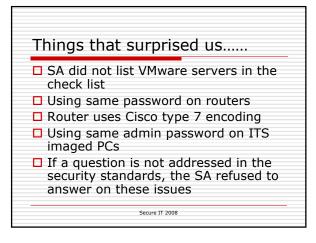
Web server and application audit

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



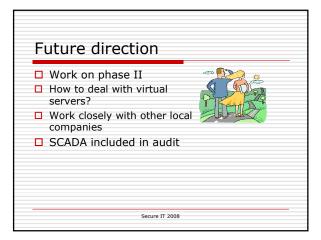




# Other issues How to securely deliver sensitive data such as router config to auditing team to audit? PGP How to work with SAs?

В	enefits
	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



### What did we miss? Suggestions and Questions? Contacts Daryl Johnson daryl.johnson@rit.edu Yin Pan yin.pan@rit.edu