

Security Policy Fundamentals

Principles, Policies, Best Practices

Tools of the Trade

Hands-on Security Exercises

Kerry Steele – CISSP, GCWN, MCSE, MVP (Security)

Chief Technology Officer – SecurePointe



Overview

- Security Basics
 - Firewall, Anti-Virus, IDS, Vulnerability Scanning, etc.
- Security Fundamentals
 - Vulnerability Management (VM) = PM + CM + UM + NS
 - Patch Management + Configuration Management
 - + User Management + Network Segmentation
- Attack Analysis
 - Tools of the Trade
- Business Case
 - Problem, Solutions, Statistics, and Case Studies (80/90 rule)
- Guidance for in-house non-security IT personnel
- Hands-On Exercises – Security Lockdown Basics



Shameless Plug: About Kerry Steele

- Co-Founder and CTO – Secure Pointe
- Microsoft MVP – Security
- CISSP, GCWN, MCSE (NT4, 2000)
- Chair – SANS GCWN Advisory Board
- CIS Windows Security Scoring Tool Lead Developer
- CIS IIS Gold Standard Project Leader
- Windows Gold Standard Consensus Team Member

Questions for the Audience

- Are you responsible for implementing, defining, or auditing security policy? Are you “the computer guy”?
- Size of organization? <10, 10-100, 101-1000, >1000
- What operating system? 95, 98, Me, NT, 2000, XP?
- Are you running with Administrative Privileges?
- Do you have a dedicated IT staff (or systems administrator)?
- Do you have a dedicated security administrator (staff)?
- Have you used a vulnerability assessment tool?

Definitions

- Vulnerability
 - A point where a network, system, device or application is susceptible to an attack
- Vulnerability Scanner / Assessment Tool
 - A tool that scans devices to identify existing vulnerabilities (Retina, Nessus, ISS Internet Scanner, Harris STAT Scanner, Foundscan, CIS tools, etc.)
- Vulnerability Remediation
 - Effective removal, neutralization, and prevention of existing and potential vulnerabilities

The Risk Equation

- $RISK = (THREATS) \times (ASSETS) \times (VULNERABILITIES)$
- If THREATS and ASSETS remain relatively constant then the primary factor we control is VULNERABILITIES
- Consequently, we can reduce RISK by *mitigating* VULNERABILITIES

Categories of Vulnerabilities

- Software Defects
 - Patches, patches, patches, and more patches...
- Insecure Accounts and Passwords
 - Weak Password, Blank Password, No Expiration, Excessive number of Admins, No Account Lockout...
- Misconfigurations
 - Null sessions, Anti-Virus not up-to-date, unnecessary services enabled and active, etc.

Vulnerability Breakdown

Software Defects	70% +
Insecure User Accounts and Passwords	15%
Misconfigurations	15%

System Hardening/Lockdown

- Enable security settings (often not enabled by default)
- Disable unnecessary services (often enabled by default)
- Group computers by roles (workstation, server, DC, etc.)
- Develop baselines for each role
- Baselines designed based on authoritative guidance
 - SANS Step-By-Step Guides – SANS Press – sans.org
 - CIS Security Benchmarks – www.cisecurity.org
 - Microsoft Prescriptive Security Guidance
 - Microsoft Threats and Countermeasures Guide

Firewalls (1)

- Packet-Filtering
- Stateful Packet-Filtering
- Proxy Firewalls – Application layer
 - Higher in the TCP/IP stack so can provide additional protection as traffic is terminated at the proxy firewall, shielding the client machine's true identity and allowing for additional decoding of the traffic being transmitted.
- Application-Layer Intelligence

Firewalls (2)

- > Commercial Firewalls:
 - CheckPoint – www.checkpoint.com
 - NetScreen – www.netscreen.com
 - Cisco PIX – www.cisco.com
 - ISA Server – www.microsoft.com/isaserver
 - Sonicwall – www.sonicwall.com
 - Symantec Gateway Security – www.symantec.com
 - Lucent – www.lucent.com
- > Consumer end:
 - Linksys – www.linksys.com
 - Netgear – www.netgear.com

Virus Protection

- > Deploy at:
 - Mail Gateway
 - Desktop/Laptops
 - Servers
 - Application Proxy Firewalls
- > VIA products will be scanned by Windows XP SP 2
- > microsoft.com/technet/security/topics/virus/via.mspx

Virus Information Alliance
Computer Associates
F-secure
Global Hauri
Network Associates
Norman
Panda
Sophos
Sybari
Symantec
Trend Micro

Spyware

- Why are users getting it? Because Joe Six-Pack and others are:
 - Clicking on links they shouldn't be clicking on
 - Opening files they shouldn't be opening
 - Installing or running "questionable" files
- A few tools to detect and remove Spyware installation
 - Update virus definitions and run a full system scan
 - Stinger – download.nai.com/products/mcafee-avert/stinger.exe
 - CWShredder – www.spywareinfo.com/~merijn/downloads.html
 - Ad-aware – www.lavasoftusa.com/software/adaware/
 - Spybot – www.safer-networking.org
- Use a different web browser or email program?
 - Ever tried Eudora or Firefox?

Virtual Private Network (VPN)

- Types of VPN connections:
 - IPSEC
 - PPTP
 - SSL
- Threat of users connecting via VPN connections:
 - Security of connecting device/network may be unknown
 - Many intrusions have occurred as a result of insecure machines connecting via insecure VPN connections
- Emerging Technologies:
 - Microsoft Network Access Quarantine feature of Server 2003
 - Cisco Network Admission Control

Authentication

- Use encrypted protocols – SSH VS. clear-text Telnet
- Smart Cards
- LM vs. NTLM vs. NTLMv2 vs. Kerberos
- LMCompatibilityLevel
 - 0 is the default
 - 1 is most compatible
 - 3 for clients, 5 for servers
- NoLMHash
- RestrictAnonymous
- Password Complexity – Custom Password Filters
- SSL

Vulnerability Assessment

- Most security tools are multi-purpose:
 - Black hats (attackers)
 - White hats (security professionals)
- Variations in assessment tools:
 - Black-box testers (attacker perspective)
 - White-box testers
 - Privileged administrative access
 - Allows for a complete, thorough, accurate assessment

Selecting a Vulnerability Assessment (VA) Tool

- Buyer Beware!
- Use more than one tool. WHY?
 - False Positives False Negatives
- Host-based or Network-based?
 - IT DEPENDS! – each has it's trade-offs
 - Network-based simulate hacker attacks
 - Host-based are more accurate, greater detail
 - CIS Tools are Host-based VA tools

Vulnerability Assessment Tools/Scanners

- Eeye Retina
- Nessus
- ISS Internet Scanner
- Harris STAT Scanner
- Foundstone Foundscan
- Sunbelt Network Security Inspector
- Microsoft Baseline Security Analyzer (MBSA)
- CIS Scoring Tools

Application Vulnerability Scanners

- System VS. Application Vulnerabilities

- WebScarab – www.owasp.org
- VulnXML

- SPI Dynamics WebInspect
- Sanctum AppScan
- Kavado ScanDo
- Nikto

Intrusion Detection Systems (IDS)

- Comparable to a car alarm or a home alarm system
- Network-Based IDS (NIDS) – ISS Real Secure or Cisco Secure IDS
 - Monitors network traffic in real-time
- Host-Based IDS (HIDS)
 - Agent which resides on a host system or device
- IDS Analysis Engines:
 - Rule-Based – (Snort – freeware for Windows and Unix)

 - Statistical-Based/Anomaly-Based
 - Compares traffic to “normal” activity for anomalies after defining what is “normal” for a specific environment
 - Signature-Based
 - Matches traffic with known patterns of attack signatures and intrusions

Intrusion Prevention Systems (IPS)

- Proactive defense mechanisms designed to detect and block intrusions/attacks in real-time
- McAfee, ISS, NetScreen, TippingPoint, and others
- Can *potentially* disrupt normal business transactions!

Penetration Testing

- Custom exploit code
 - "Exploiting Software" – How to Break Code
 - "The Shellcoder's Handbook" – Discovering and Exploiting Security Holes
 - "Smashing The Stack For And For Profit"
 - <http://www.phrack.org/phrack/49/P49-14>
- Or use existing tools
 - PacketStorm – www.packetstormsecurity.com
 - Hacking Exposed – the "Hacker's Bible" – www.hackingexposed.com
- Or use existing code
 - Full-Disclosure – <http://lists.netsys.com/mailman/listinfo/full-disclosure>
 - SecurityFocus mailing lists – vuln-dev, pen-test, bugtraq – securityfocus.com
- Penetration testing "suites"
 - Metasploit 2.0 – www.metasploit.com (freeware)
 - Core IMPACT – www.coresecurity.com (cost varies with size of engagement)
 - Immunitysec CANVAS – immunitysec.com (\$1000 + \$495/qtr maintenance)

3rd Party Access to Resources

- DMZ
- Extranet
- SLA's
- Outsourcing of client's sensitive financial data
 - CPA's responsibility to notify clients that sensitive client data is outsourced?
 - Use as a selling point

Administrative Privileges

- Do you really need to be running with Admin privileges?
- Run day to day tasks with a non-administrative account
- Use the RunAs command or a different mechanism to perform "administrative" tasks
- Protects you from yourself.

Security Fundamentals

- People + Processes + Policies + Technology
- Vulnerability Management (VM) = PM + CM + UM + NS
 - Patch Management + Configuration Management + User Management + Network Segmentation
- No Silver Bullet!
- Principle of Least Principle
- Defense In Depth – Multi-layered Security

People: User Education

- DON'T OPEN THOSE ATTACHMENTS!!!
- IF YOU DON'T RECOGNIZE THE SENDER, DON'T CLICK ON ANY WEB LINKS!!!

- Inform users of existing threats
- Keep end-users informed with new threats
- When an incident occurs, EDUCATE

Security Principles

- CISSP Ten Domains:
 - Access Control Systems & Methodology
 - Telecommunications, Network & Internet Security
 - Security Management Practices
 - Applications & Systems Development
 - Cryptography
 - Security Architecture & Models
 - Operations Security
 - Business Continuity Planning
 - Law, Investigation & Ethics
 - Physical Security

Security Policies

- The SANS Security Policy Project
 - www.sans.org/resources/policies/

Acceptable Encryption Policy	Dial-in Access Policy	Password Protection Policy
Acceptable Use Policy	DMZ Lab Security Policy	Remote Access Policy
Analog/ISDN Line Policy	E-mail Policy	Risk Assessment Policy
Anti-Virus Process	E-mail Retention	Router Security Policy
Application Service Provider Policy	Ethics Policy	Server Security Policy
Application Service Provider Standards	Extranet Policy	Third Party Network Connection Agreement
Acquisition Assessment Policy	Information Sensitivity Policy	VPN Security Policy
Audit Vulnerability Scanning Policy	Internal Lab Security Policy	Wireless Communication Policy
Automatically Forwarded Email Policy	Internet DMZ Equipment Policy	
Database Credentials Coding Policy	Lab Anti-Virus Policy	

Security Best Practices

- SANS Step-By-Step Guides
- SANS GIAC Certifications
- CIS Security Benchmarks
- Microsoft Security Guidance

7 Steps to Implement a Security Process

- Establish a security team or organization
- Perform a security assessment of the current infrastructure (asset identification and baseline assessment)
- Conduct a risk analysis for the assets
- Write an organizational security policy
- Design and implement operations plan and security standards based on best practices
- Implement training and awareness measures for all users
- Perform ongoing security management

Vulnerability Management

- Patch Management
 - Process of inventorying systems, assessing system and application patch levels, installation of necessary patches, auditing, and monitoring for newly released patches and updates
- Configuration Management
 - Establishment of baselines derived from best practices
- User Management
 - Effective Account/Password policy, enforcement, monitoring, and auditing
- Network Segmentation
 - Compartmentalization and isolation of network resources based upon risk associated with asset and business function

Patch Management (1)

- It is almost impossible to keep up with patches, unless you have a patch management program in place.
- Ongoing maintenance is a pain
 - Apply the latest:
 - Service packs
 - Cumulative patches
 - Security patches for the operating system
 - All necessary security patches for all applications installed
- Security Management
 - Oh Patch How I Hate Thee; Let Me Count the Ways:
 - microsoft.com/technet/community/columns/secmgmt/default.mspx

Patch Management (2)

- Develop a Process:
 - Inventory
 - Create criticality matrices for specific server roles
 - Testing
 - Configure test environments to expedite evaluation of updates
 - Installation
 - Manually (Custom scripting solutions or Sneaker-net)
 - Commercial Tools (SUS, SMS, HFNetChk Pro, UpdateExpert, etc.)
 - Prioritize
 - Develop accelerated release-management processes for security-related updates

Patch Management (3)

- Get current security information:
 - <http://microsoft.com/technet/security>
 - <http://microsoft.com/security/it>
 - Vendor mailing lists for EACH product on your network
 - Other mailing lists:
 - SANS – www.sans.org
 - Bugtraq – www.securityfocus.com
 - CERT – www.cert.org
 - Patchmanagement.org

Patch Management (4)

BigFix Enterprise Suite Patch Manager	BigFix	www.bigfix.com
Dynamic Network Administration (DNA)	NetSupport Software	www.netsupport-inc.com
Ecora Patch Manager **	Ecora	www.ecora.com
HFNChkPro *	Shavlik	www.shavlik.com
LANDesk Patch Manager	LANDesk Software	www.landesk.com
LANGuard Network Security Scanner	GFI Software	www.gfi.com
Opsware	Opsware	www.opsware.com
Patch Management Solution	Altiris	www.altiris.com
Patchlink	Patchlink	www.patchlink.com
Security Update Manager	Configuresoft	www.configuresoft.com
Service Pack Manager 2000	Gravity Storm Software	www.securitybastion.com
Systems Management Server 2003 (SMS)	Microsoft	www.microsoft.com/sms
Software Update Services (SUS or WUS)	Microsoft	www.microsoft.com/sus
SysUpdate Policy Compliance and Enforcement	Security Profiling	www.securityprofiling.com
UpdateExpert	St. Bernard Software	www.stbernard.com



** Best Buy * Recommended
(per SC Magazine group product test April 2004)



Patch Management (5)

- When choosing a patch management solution, some of the things to consider are:
 - Architecture – Agent-based or Agentless (scanning-based)?
 - Scalability – How many client systems can be supported per server?
 - Policy-Based Management – can policies be configured to require specific patches on groups or classes of similar devices?
 - Role-based Administration – can machines be categorized into groups, allowing for delegation of patch management of the grouped devices?
 - Customized Reporting – can the reports from the product be customized to tailor individual needs? How robust is the report customization feature?
 - Automatic Alerts – can the product be configured to send alerts when a failure or exception to policy occurs?
 - Integration – can data from the product leverage an existing SQL Server, Oracle, or DB2 database?



Configuration Management

- Enforcement of a uniform policy-based configuration
- Active Directory (Windows 2000 and Windows 2003)
- Commercial Tools
 - Configuresoft
 - Bindview

User Management

- User Account Policies
 - Account Lockout (15 minutes after 5 attempts)
 - Aged/Stale Accounts
 - Excessive Administrative Privileges
- Password Policies
 - Minimum Length (8 characters)
 - Recommend >14 characters for sensitive accounts (admins)
- Two-form authentication
 - Smartcards
 - Biometrics

Network Segmentation (1)

- Ingress Filtering
 - Manages the flow of traffic as it enters a network under your administrative control.
 - Servers are typically the only machines that need to accept inbound connections from the public Internet.
 - In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound connections to machines that provide no public services.
 - Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound connections to non-authorized services.
 - In this fashion, the effectiveness of many intruder scanning techniques can be dramatically reduced.

Network Segmentation (2)

- Egress Filtering
 - Egress filtering manages the flow of traffic as it leaves a network under your administrative control.
 - There is typically limited need for machines providing public services to initiate outbound connections to the Internet.
- Network Isolation
 - Complex networks can benefit by separating data channels and control channels, such as BGP, into different logical or physical networks.
 - Technologies such as VLANs, VPNs, leased links, NAT may all be able to contribute to separating the transmission of control information from the transmission of the data stream.
 - Separation of network devices based upon role

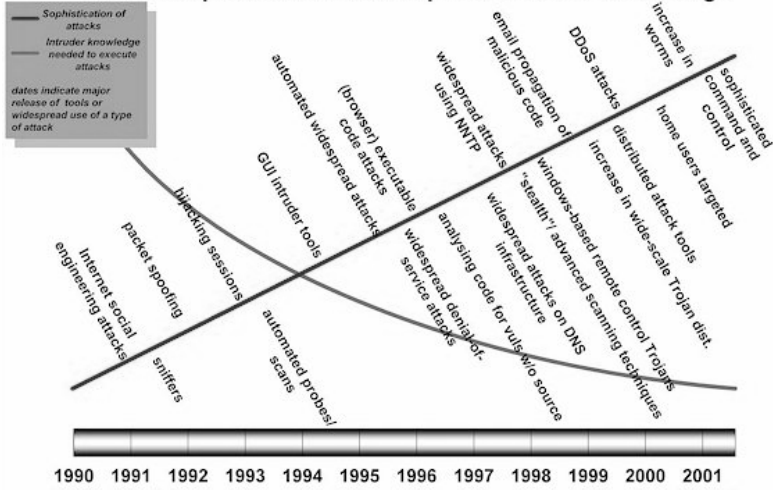
Network Segmentation (3)

- Network Isolation
 - Separation of network devices based upon role:
 - Servers
 - Web, Database, Email, File, Infrastructure, etc.
 - HR applications (sensitive personnel data)
 - Financial applications (critical financial data/transactions)
 - Workstations
 - Job Roles, Departments, Separate Users/Administrators
 - Implementation of Access Control Lists (ACLs)
 - Limit traffic between each isolated network "island"

Attack Analysis

- General Trends
- Reconnaissance
- Discovery, Scanning and Vulnerability Assessment
- Exploiting Vulnerabilities
- Keeping Access
- Covering Tracks
- Defenses

Attack Sophistication vs. Required Intruder Knowledge



GLERT Coordination Center
www.cert.org

Copyright 1999-2001
Carnegie Mellon University



General Trends

- Two types of attackers:
 - Drive by shooters – “script kiddies” or “ankle biters”
 - Advanced Skilled Attackers with dedicated resources
- Hacker Tools – easy to use and widely distributed
- Underground Community – excellent communication
- Homogenization of our computing environments



General Trends – Worms

- Super Worms
- Zero-Day Exploit Worms
- Multiple Exploits
- Multiple Platforms
- Fast Spreading
- Polymorphic

Reconnaissance

- “Casing the joint”
- Google is a hacker’s best friend – “Google Hacks”
 - www.oreilly.com/catalog/googlehks/
 - phonebook:, site:, link:, related:, info:, cache:, filetypes such as .xls or .ppt
- Gathering Information:
 - Search engines, company website searches, job postings (Monster, HotJobs), SEC Edgar searches
- Tools: Sam Spade, others at www.attackportal.net
- *Defenses – limit and control publicly available info*

Discovery, Scanning and Assessment (1)

- War dialers – THC-Scan 2.0
 - *Defenses – Remove modems, Modem Policy*
- War driving (with GPS) – NetStumbler, Wellenreiter
 - *Defenses – Wireless Access Policy, Routine Audits*
- Wireless Sniffers – Kismet, Airopoek, Aircrack-ng
 - *Defenses – SSID, WEP, MAC Filtering, VPN, Policy*
- Port Scanners – NMAP, SuperScan, Cheops-NG
 - *Defenses – System hardening, firewalls, proxies, IDS*

Discovery, Scanning and Assessment (2)

- Passive Scanning – p0f2
 - *Defenses – System hardening, firewalls, proxies, IDS*
- Vulnerability Assessment – Nessus, MBSA, ISS Internet Scanner, Eeye Retina, Foundstone Foundscan, Harris STAT Scanner
 - *Defenses – System hardening, patch management, firewalls, proxies, IDS*
- Application Vulnerability Assessment – SPI Dynamics WebInspect, Sanctum AppScan, Kavado ScanDo, Nikto
 - *Defenses – "Writing Secure Code", by M. Howard*

Exploiting Vulnerabilities (1)

- Spoofing – IP Addresses, Email addresses
- Social Engineering – Highly successful – “Kevin Mitnick”
- Sniffers – Ethereal, tcpdump, windump, Snort, DSniff
- Session Hijacking – Hunt, Ettercap (on switched networks)
- Network swiss-army knife – NetCat
- Steganography – Hydan
- Password Crackers – LC4, Pwdump3, John the Ripper
 - *Defenses – Anti-Spam and content filtering, Network Segmentation, Encryption, System Hardening, Firewalls/Proxies, IDS, IPS, etc.*

Exploiting Vulnerabilities (2)

- Buffer Overflows
 - *Defenses – System hardening, patch management, firewalls, proxies, IDS... Writing Secure Code*
- Polymorphic Buffer Overflows – ADMutate (evades IDS)
- Format String Vulnerabilities
- Penetration Testing Exploit Suites:
 - Metasploit Framework 2.0 (open source freeware)
 - Core IMPACT (commercial software)
 - CANVAS (commercial software)

Keeping Access (1)

- Backdoors:
 - VNC
 - Sub Seven
 - Back Orifice 2000
 - NetBus
 - NetCat
 - Remotely Anywhere
 - *pcAnywhere*

Keeping Access (2)

- Rootkits:
 - Surfaced from the underground in 1993
 - Keep backdoor access
 - Mask installation and system compromise
 - Replace critical system files/binaries with trojan files
 - Keystroke logging and network sniffing
 - Leads to access on other systems and resources
- *Defenses – System Hardening, Patch Management, Firewalls, Proxies, Anti-Virus, IDS, Data Integrity Tools*

Keeping Access (3)

- Kernel Level Rootkits:
 - Hot topic within security researchers
 - Ability to mask and hide:
 - Processes
 - Files and Directories
 - Trojan replacements of critical files
 - Registry data
 - Network activity
- *Defenses – System Hardening, Patch Management, Firewalls, Proxies, Anti-Virus, IDS, Data Integrity Tools*

Covering Tracks

- Hiding Files – Alternate Data Streams
- Editing Log Files – Winzapper
- Steganography
 - Conceal sensitive information within documents, images (.bmp, .jpg)
 - S-Tools, Hydan
- *Defenses – System Hardening, Anti-Virus, IDS, Data Integrity Tools*
- *Detection – FIRE, Knoppix*

Defenses - Summary

- Limit public information
- System Hardening/Lockdown
- Patch Management
- Firewalls/Proxies
- Anti-Virus
- Wireless?
- IDS
- Data Integrity Tools
- *Writing Secure Code*

The Business Case – 10,000 foot overview

- The Problem – People are slow to adopt best practices
- The Solution – Implement basic best practice security policies, audit, maintain, and educate end users.
- Case Studies – Security Benchmarks and Best Practices Effectively Eliminate 80-99% of Vulnerabilities
- Vulnerability Management (VM) = PM + CM + UM + NS
 - Patch Management + Configuration Management + User Management + Network Segmentation

We have met the ENEMY, it is US

“Through 2005, 90 percent of cyber attacks will continue to exploit known security flaws for which a patch is available or a preventive measure known.”

Gartner Group, May 6, 2002

“Many recent cyber attacks could have been avoided if enterprises were more focused on their security efforts, but users seem not to learn from their mistakes.”

Gartner Group, May 6, 2002

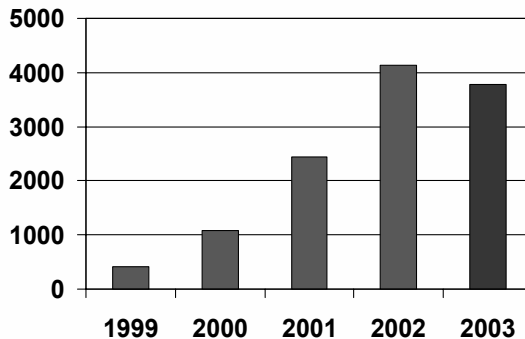
“Treat your password like your underwear, change it often.”



Global Network Security Issues

- Dangerous new network vulnerabilities detected on a daily basis – 4,129 in 2002.
- In 2003 vulnerabilities dropped slightly (3,784), but had the greatest financial losses to date.
- Business impact of not understanding and fixing network security issues is devastating.

New Vulnerabilities Detected



-- Source: CERT Data..



Impact of Exploits (1)

- SQL Slammer/Sapphire – 1/25/03
 - Exploited a buffer overflow in SQL Server and MSDE.
 - The SQL Slammer/Sapphire worm was the fastest computer worm in history.
 - Doubled in size every 8.5 seconds.
 - Infected more than 90 percent of vulnerable hosts within 10 minutes
 - Estimated \$1.2 billion in lost productivity

Impact of Exploits (2)

- Impact to Large North American Bank – Sapphire/Slammer
 - Downtime:
 - Lost an estimated 12.9 million transactions
 - Over 13,000 ATM machines completely disabled
 - Financial Impact:
 - \$1.9 million in lost fees / \$200K est. repair costs
- Impact to Large Airline – Sapphire/Slammer
 - Downtime:
 - Ticketing and kiosk stations down.
 - Revenue generating online ticketing web site was down for most of Sunday
 - Financial Impact:
 - Reservations hotline wait times soared to more than 140 minutes.

Impact of Exploits (3)

- Large University in Texas
 - Student hacked into system
 - Stole over 45,000 student records
 - Including confidential information such as Social Security number, address, etc
- Impact
 - Potential identity theft
 - Escalation to Governors office
 - Re-transformation of security strategy
 - Personnel changes

Cycle of Failure (1)

- “How can I get beyond this cycle of failure?”
 - A break in occurs
 - A well-known vulnerability was exploited
 - Security staff and system administrators argue about who was to blame
 - Senior management sees the process as broken
 - Staff are reorganized
 - Managers are reassigned or fired
 - The new managers hire consultants to conduct a vulnerability assessment and penetration test

Cycle of Failure (2)

- So...The Pointy-Haired Boss
 - Consultant's analysis shows average of 30 vulnerabilities per system
 - Management writes a memo telling system administrators and department heads to fix these vulnerabilities within 4 weeks
 - The work would take several months to complete
 - System administrators don't make all the fixes
 - Not even a small fraction.
 - At the same time new software is installed; new vulnerabilities are created

Cycle of Failure (3)

- And then again...Einstein's Theory of Insanity
 - Another break in occurs
 - A well-known vulnerability was exploited
 - Security staff and system administrators argue again...whose fault is it?
 - Senior management sees the process as broken
 - The MBA's logically go ahead and "move bodies around", as they are trained to do.
 - Senior management are ultimately responsible

Window of Time to Patch is Decreasing

Worm or <i>Attack</i>	Bulletin	Patch Date	Attack Date	Advance Notice
<i>LSASS</i>	04-011	4/13/04	4/14/04	1 Day
<i>ASN.1 DoS</i>	04-007	2/10/04	2/14/04	4 Days
Blaster	03-026	7/16/03	8/11/03	26 Days
SQL Slammer	02-039	7/24/02	1/25/03	185 Days
Code Red	01-033	6/18/01	7/19/01	31 Days
Nimda	00-078	10/17/00	9/18/01	336 Days

MS Blaster Worm – MS03-026

- 26 Days to apply the patch prior to infection
- Response time and keeping informed are crucial

Phase	Date	Time
Vulnerability Report to MS	7/1/03	1 Day
Bulletin & Patch Release	7/16/03	15 Days
Proof of Concept (PoC) Exploit Code Published	7/25/03	9 Days
Worm in the wild	8/11/03	17 Days

Attacks CAN be prevented (1)

- "99% of all attacks come from known vulnerabilities and are preventable."
 - CERT® Coordination Center (CERT/CC)
Carnegie Mellon Software Engineering Institute
- Businesses can virtually eliminate cyberattacks by identifying and resolving network vulnerabilities and implementing a risk-reduction process.

Attacks CAN be prevented (2)

- "95% of all network intrusions could be avoided by keeping systems up-to-date with appropriate patches."
 - CERT® Coordination Center (CERT/CC)
Carnegie Mellon Software Engineering Institute
- Organizations struggle to keep systems current, often neglecting to apply critical patches quickly or correctly.
- Adding to this challenge is the shrinking timeframe between a vulnerability announcement and the release of exploit code.

Vulnerability Management IS Manageable (1)

- Patch Management
 - Microsoft releases patches second Tuesday of each month
 - Numerous freeware and enterprise patch management solutions
- User Account and Password Policy Management
 - Weak passwords account for attacks which can lead to further attacks, back doors, escalation of privilege, etc.
 - Establish an effective password and account policy for both users and administrative accounts, enforce, monitor, and audit.
- Configuration Management
 - Establish a baseline security configuration policy based on CIS/NSA/NIST/SANS/Microsoft settings.
 - Test for compatibility within the enterprise, adjust accordingly

Vulnerability Management IS Manageable (2)

- Consensus security benchmark settings
 - Developed by the CIS teams
 - Eliminate 80-90% of the vulnerabilities that are being exploited by cyber-attackers.
 - Substantial reduction in the risk of unauthorized intrusion
- Research Methodology
 - Scan a system “out of the box” and list identified vulnerabilities
 - Configure the system with the appropriate benchmark or policy
 - Rescan the system and identify the vulnerabilities remaining
 - Conducted by Solutionary, RDA, SecurePointe, NSA, Mitre (CVE), and others.

Case Studies – Validating the Solution

Study	Date	Scanner	System	Level	Low	Med	High	Total
Solutionary		Comm.	W2K Srv	I	74%	89%	100%	85%
NSA	'02	Comm.	W2K Pro	II	50%	90%	96%	91%
Mitre (CVE)	'02	CVE	W2K Pro	II	-	-	-	83%
Kerry Steele	4/03	STAT	W2K Pro	I	74%	91%	92%	81%
Kerry Steele	4/03	ISS	W2K Srv	II	99%	100%	100%	99%
Kerry Steele	4/03	STAT	Redhat	I	100%	89%	73%	88%
Kerry Steele	2/04	Retina	XP Pro	III				??

- Available at <http://www.securepointe.com/studies.html>
- CIS Studies available at <http://www.cisecurity.org>

Business Drivers for Vulnerability Mgmt. (1)

- > Financial Losses
 - . Loss of Revenue
 - . Transaction Downtime
 - . Stolen Intellectual Property (IP)
 - . Exposure of sensitive customer data and other private data
 - . TARNISHED BRAND
 - . Lost Credibility
 - . Negative Public Relations
- > Productivity Losses
 - . System Downtime
 - . Loss of data
 - . Remediation Time

Business Drivers for Vulnerability Mgmt. (2)

- Regulatory requirements:
 - HIPAA
 - Protection of private and sensitive healthcare information
 - Sarbanes Oxley – (SEC 404)
 - Management's duty in the assessment of internal controls
 - Gramm-Leach-Bliley
 - Requires financial companies to institute security programs that safeguard and inform their customer's their rights with regards to their private and sensitive information
 - CB 1386
 - Any breach of security resulting in a CA residents loss of personal information must be publicly disclosed

Business Drivers for Vulnerability Mgmt. (3)

Risk of not having a process in place

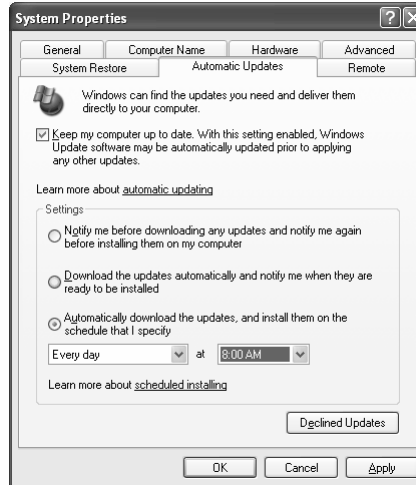
- Research shows that on average a patch was available months before an exploit occurred [Forrester, 2003]
- CERT reports that up to 95% of security breaches exploit vulnerabilities for which a countermeasure exists (often a security patch).

The situation is getting worse, not better

- Factors exacerbating the Patch Management issue within the last five years include:
 - Proliferating numbers of servers in organizations
 - More security threats and higher consequences of not deploying updates
 - Increasing visibility and media coverage of security incidents
 - Increasing audits for regulatory compliance

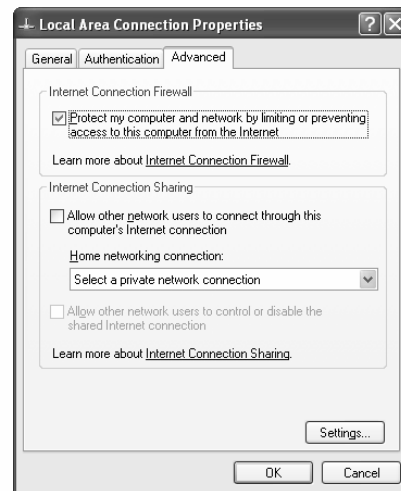
Configure Automatic Updates (WU/SUS)

- Configure to download automatically and either notify or automatically install updates.
- XP: Start -> Control Panel -> System -> Automatic Updates
- 2K: Start -> Settings -> Control Panel -> Automatic Updates



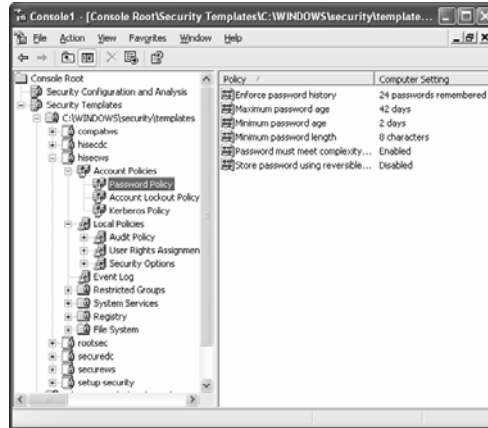
Enable Internet Connection Firewall (ICF)

- XP: Start -> Control Panel -> Network Connections -> Local Area Connection (each connection) -> Advanced
- Can be configured to allow various server functions



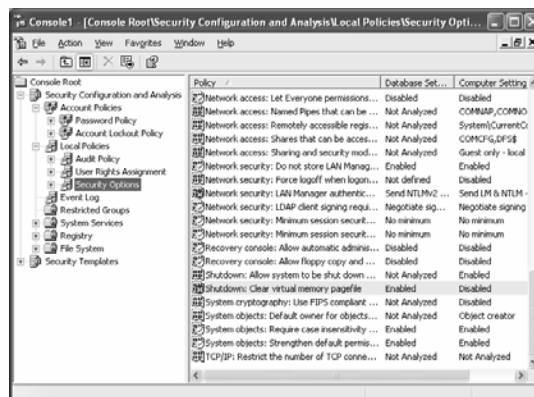
Security Templates

- Start -> Run -> mmc
- File -> Add/Remove Snap-in -> Add -> Security Configuration and Analysis -> Add -> Security Templates -> Add -> Close -> OK
- Security Templates -> Expand hisecws and setup security



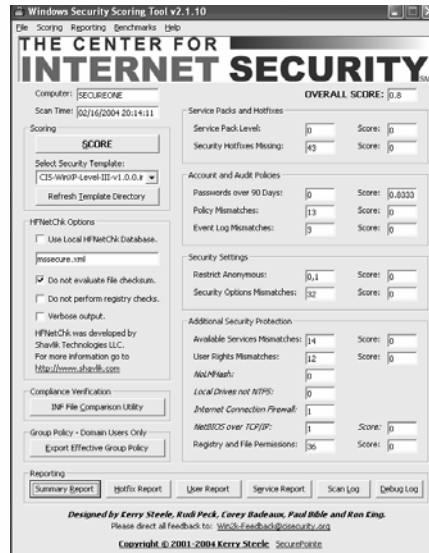
Audit Using a Security Template

- Right-click the Security Configuration and Analysis scope item -> Select Open database -> Enter a name such as aicpatemp -> Select a template such as hisecws.inf -> OK
- Right-click the Security Configuration and Analysis scope item -> Select Analyze Computer Now -> In the dialogue, type the log file path, and then click OK



Audit – CIS Scoring Tool

- Non-invasive, Host-based security scanning tool gives a SCORE indicating compliance with a policy
- Audit local configuration using ANY security template
- 10 may not be usable
- There is NO silver bullet
- Scoring default (shown) installation of XP = 0.8



Security Policy Implementation

1. Review
 - Modify as necessary per local policy
 - Do NOT implement the settings blindly
2. Backup
3. Test
 - Test replicas of production machines on non-production machines in a test lab
 - If no lab is available, backup or Ghost prior to implementation
4. Implement

CAUTION!

- Security may break functionality!
- Constant trade-off: *Usability VS Security*
- All settings should be tested on non-critical systems or in a test lab environment



Potential Problematic Settings

- Enterprise and other applications may require:
 - Administrative Shares (C\$, ADMIN\$)
 - Remote Registry Service
 - Task Scheduler
 - RestrictAnonymous (Null User Sessions)
 - NTFS/Registry Permissions
 - NetBIOS over TCP/IP
 - LM VS. NTLM VS. NTLMv2 Authentication
 - File/Printer Sharing Bindings
 - Workstation Service
 - Server Service

Conclusion

- Google
- Defense In Depth
- Policies Based on Consensus Standards Mitigate 80-99% of Vulnerabilities
- Develop Policies, Regardless of size of organization
- Vulnerability Management IS Manageable
 - Vulnerability Management (VM) = PM + CM + UM + NS
 - Patch Management + Configuration Management
 - + User Management + Network Segmentation
- TEST
- Stay informed!

Resources

- Center for Internet Security (CIS) – www.cisecurity.org
- SANS Institute – www.sans.org
- SANS Press – www.sans.org (Step-By-Step Guides and others)
- GIAC Certification – www.giac.org
- Microsoft Security – www.microsoft.com/technet/security
- CERT – www.cert.org
- CISSP Certification – International Information Systems Security Certification Consortium – www.isc2.org
- Information Systems Audit & Control Association (ISACA) – www.isaca.org
- Information Systems Security Association – ISSA – www.issa.org

CIS Security Benchmarks

- The Center for Internet Security – www.cisecurity.org
- Gold Standard Benchmarks
 - Jointly developed by CIS, SANS, NSA, NIST, DISA, Microsoft, and other industry experts
- Levels of Security
 - Legacy (backwards compatibility for downlevel clients and apps)
 - Enterprise (domain environment where management is key)
 - High (high security environments where security is highest priority)
- Moving to role-based guidance
 - Domain / Standalone / Bastion / Kiosk Home
 - Workstation / Server / Domain Controller

SANS Top X

1. Patch, configure auto-update
2. Enable firewall (or buy one)
3. Strong Password
4. Virus software, configure auto-update
5. No P2P programs installed
6. Disable anonymous connections
7. Disable file-sharing

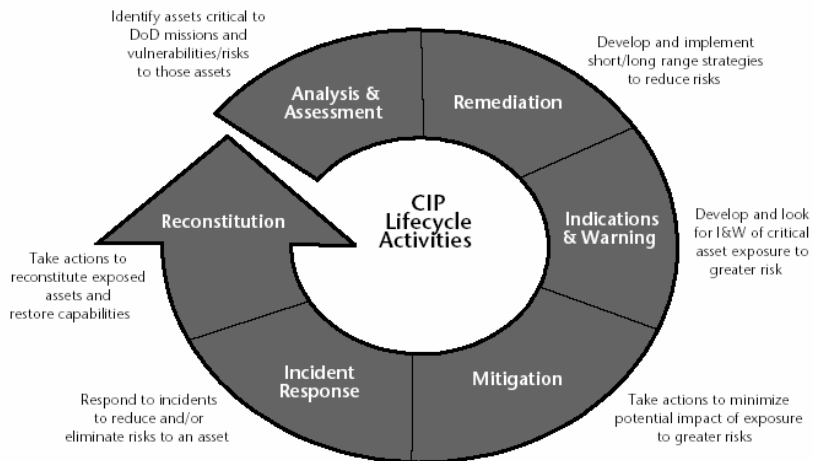
SANS Enhanced Top X

- **Patching**
 - Update Service pack level
 - Query and Install Patches
 - Configure Automatic Update service to download and install patches
- **Firewall**
 - Enable ICF firewall on XP and above
- **Authentication – User Accounts and Passwords**
 - Strong Password
 - No blank passwords
 - Inspect passwords hashes??? (not in the initial release)
 - Limit blank password use to console logon only (XP and above)
 - Passwords < 90 days old are flagged
 - Look for stale user accounts?
 - Account Policies enabled
 - Password Complexity enabled
 - NoLMHash enabled
- **Unnecessary and Rogue Programs**
 - Anti-Virus software installed, up-to-date, and configure auto-update
 - Disable Messenger and Telnet services
 - No P2P programs installed
 - No IRC programs installed or running
- **Windows Networking**
 - Disable anonymous connections (RestrictAnonymous)
 - Disable File and Printer Sharing on each network interface
 - Disable NetBIOS over TCP/IP on each network interface
 - Enable NTLMv2 Authentication when negotiated

Home/Dorm User's Security Checklist

- Articles and guidance are available for:
 - Home users
 - University students
 - Others?
- How is compliance monitored?
- How is it enforced?
- Do they know about this guidance?

CIP Appendix 16 Requirements



DoD CIP lifecycle activities



Additional Tools via SecurePointe

- MSSECCHK – freeware audit tool
- PatchCHK – open-source patch checker
- S.W.A.T. – Secure Windows Audit Tool



Contact Information

Kerry Steele

Secure Pointe Inc.

<http://www.securepointe.com>

ksteele@securepointe.com

ksteele@securitypenetration.com

504.250.3368

