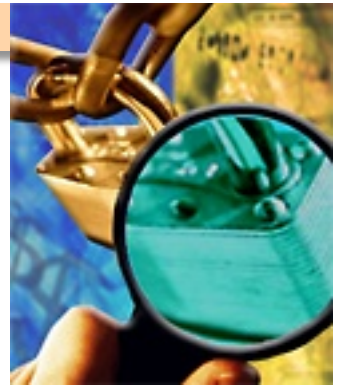
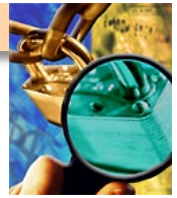


Unix Security

Vulnerability Assessment Course

All materials are licensed under a Creative Commons “Share Alike” license.



- **http://creativecommons.org/licenses/by-sa/3.0/**

You are free:

to Share — to copy, distribute and transmit the work

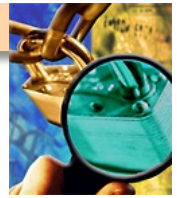
to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

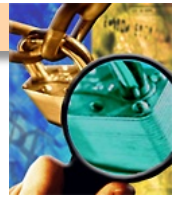
Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Agenda



- Why assess
- Where are we in the process
- What's needed
- Defining vulnerabilities
- NIST 800-53A controls
- Assessment Exercise
- Security Exercise
- Conclusion

Vulnerability Assessment



- Provides the opportunity to address weaknesses before an enemy can exploit them
- Implementation: Scanning tools that identify vulnerabilities in computer hardware, software, networks and operating systems
- Common techniques
  - Multiple tools – one tool may not identify all vulnerabilities
  - Ability to identify backdoors security perimeter, e.g. modems, VPNs, etc. – all potential vulnerabilities need to be assessed
  - Correction verification mechanism – ability to check if vulnerability has been eliminated
- Compliance with OMB, DOD, DHS policy
  - Utilize NIST 800-53 and 800-53A
  - DOD 8500 series

What's Needed

- Unix experience
  - Hands on experience: configuration, managing, building various Unix systems
  - Working knowledge of best practices
- Security Experience
  - Intimate knowledge of how to secure a system
  - Prior experience with CIS Benchmark, DISA STIG/SRR
- Data Collection
  - Network scans from NMAP and Nessus
  - Host output from any data collection tools
- Other Skills
  - Need to work with administrators
  - Put vulnerability in their language
  - Be tedious while looking for vulnerabilities
  - Work well in a team

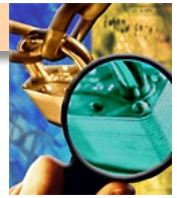
Defining Unix Vulnerability Assessment

- **Defining Unix Vulnerability Assessment**
  - Unix Vulnerability Assessment
  - Unix Security Issues
  - Security Paradigm
  - System Hardening: The CIS Philosophy
  - Network Based Vulnerability Scanning
  - Host (Local) Vulnerability Scanning
  - Remote vs. Local Vulnerability Scanning
  - Common Problems and Issues
  - Mitigation

Unix Vulnerability Assessment

- **Definition**
  - Examining the operating characteristics of a Unix environment remotely and locally in order to accurately assess its security posture (or profile).
- **Methodology**
  - Remote Vulnerability Scanning
  - Local System Checks
- **Mitigation**
  - System Hardening
  - OS Patching
  - System Monitoring

UNIX Security Issues



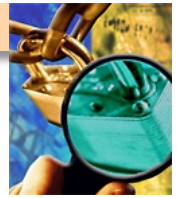
- Remote (Think “Access”)
  - Listening services or programs
  - Routing Capabilities
  - User-initiated remote attacks
- Local (Think “Escalation”)
  - Passwords
  - OS bugs and vulnerabilities
- System (Think “Manipulation”)
  - Permissions
  - File and Kernel Integrity
  - Sniffing
- Poor system configuration and monitoring coupled with the raw utilitarian power of Unix make the Unix operating system ideal to manipulate, continually abuse, and leverage for attackers.

Security Paradigm[1]

1. The hacker who breaks into your system will probably be someone you know
2. Trust no one, or be careful about whom you are required to trust. Don't trust yourself, or verify everything you do.
3. Make would-be intruders believe they will be caught
4. Protect in layers
5. While planning your security strategy, presume the complete failure of any single security layer
6. Make security a part of the initial design
7. Disable unneeded services, packages, and features
8. Before connecting, understand and secure
9. Prepare for the worst

[1] Solaris Security, by Peter H. Gregory, Copyright 2000, pages 11-19

System Hardening: the CIS[2] Philosophy



Recommendations from the CIS's Benchmark documents:

- **Patches and additional software (e.g., OpenSSH, TCP Wrappers)**
- **Minimize Network Services (e.g., inetd, sendmail)**
- **Minimize Boot Services**
- **Kernel Tuning**
- **Enhance Logging**
- **File/Directory Permissions/Access**
- **System Access, Authentication, and Authorization**
- **User Accounts and Environment**

[2] The Center for Internet Security, http://www.cisecurity.org/

System Hardening: Other Philosophy

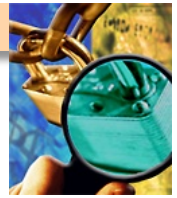
Recommendations from the CIS's Benchmark documents:

- **If its not needed disable, remove, uninstall**
  - **Disable ALL unneeded services and software**
- **If it is still needed patch, secure, audit**
  - **Make sure its current**
  - **Make sure you log all critical aspects (authentication, priv access)**
- **Always use security protocols**
  - **SSLv3, TLS, SSH protocol 2, SNMPv3**
- **Use host based security**
  - **Sudo, RBAC, auditing (authentication and priv access) , BART**
  - **Set proper permissions**
- **Network based security**
  - **IPFILTER, Tune TCP stack, NOT TCP Wrappers!!!**
- **Repeat frequently and use a CM process**

Network Based Vulnerability Scanning

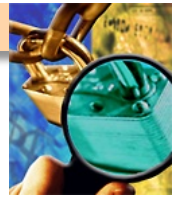
- **Definition**
  - **Using previously gained knowledge of a target network to check specific services and protocols of that network for the existence of vulnerabilities.**
- **Methodology**
  - **Automated Vulnerability Scanners (simple, somewhat reliable, thorough, and FAST!)**
    - **Based on the information gained from network mapping, you can unleash a scanner to discover known vulnerabilities that exist on the target network.**
    - **Ideally, when possible, manual verification of the existence of a vulnerability is recommended to supplement the automated tool.**

Analyzing Network Vulnerability Scans

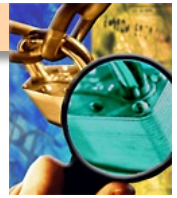


- What vulnerabilities were discovered?
- What is the severity of each of the vulnerabilities discovered?
- Are any of the vulnerabilities false-positives?
  - Manual Banner Grabbing (more reliable, but time consuming)
  - Verification with host output
- Did the vulnerability scanning tool miss anything?
- Ranking the severity of vulnerabilities discovered helps you focus on what needs to be fixed first.
- Consolidate the results from your vulnerability scans to create a report that will help you assess your security posture.

NMAP



- Information & Features
  - Utility for network exploration or security auditing.
  - Most operating systems: Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX
  - Supports dozens of advanced techniques for mapping networks
  - Widely used and accepted by the security community
  - Well documented
  - Easy to use graphical interface
  - Cost: Free



Nessus

- **Information & Features**
  - **Historically an open source utility for automated vulnerability scanning**
  - **Runs on Solaris, Linux, OSX, Windows, and *BSD**
  - **Highly configurable and intelligent**
  - **Easy to use graphical interface**
  - **Widely used and accepted by the security community**

Automated Scanners

- **Use security probing tools from a trusted source to check your system for weaknesses (before someone else does)!**
- **Retina**
- **ISS**
- **http://www.nessus.org**
- **http://www.insecure.org/nmap/**

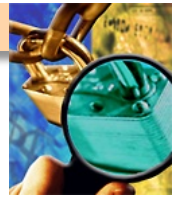
Host (Local) Vulnerability Scanning

- **Definition**
  - Using interactive shell access on a system to identify the vulnerabilities and exposures on a system
- **Methodology**
  - Manual checking of versions and configuration settings for flaws (very time consuming)
  - Collection of local system settings and files with a script
  - Automated vulnerability scanners (simple, somewhat reliable, thorough, and FAST!)
    - Ideally, when possible, manual verification of the existence of a vulnerability is recommended to supplement the automated tool

Analyzing Host Vulnerability Scans

- **Analysis**
  - **What vulnerabilities were discovered?**
  - **What is the severity of each of the vulnerabilities discovered?**
  - **Are any of the vulnerabilities false-positives?**
  - **Ranking the severity of vulnerabilities discovered helps you focus on what needs to be fixed first.**
  - **Consolidate the results from your vulnerability scans to create a report that will help you assess your security posture.**

CISecurity Tools



- Utility for assessing security under multiple variants of *NIX
- Compares system against a defined “Level 1” benchmark
- Released versions on Solaris, Red Hat Linux, HP-UX, FreeBSD, AIX
- Other Unix variants in development.
- Easy to understand and use
- Non-invasive
- Quick and configurable
- Available to Category 1 CIS members

THE CENTER FOR INTERNET SECURITY℠

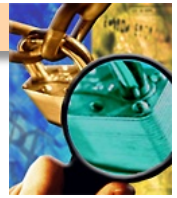
Remote vs. Local Vulnerability Scanning

- Remote
  - Pros:
    - Requires no system access
    - More authentic view of a system to a remote attacker
  - Cons:
    - More likely to cause system disruption
    - False positive and false negatives are more likely
- Local
  - Pros:
    - Usually more accurate
    - More likely to examine overall posture than just individual remote vulnerabilities
  - Cons:
    - Requires system access, installing software

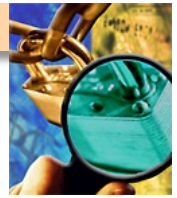
Common Problems and Issues

- Understanding results
  - Findings may be cryptic
  - Mission supplied services declared findings
  - Some findings require authoritative resolution
  - Common misunderstandings
    - Make the findings go away!
    - Perfect score = boat anchor
- Mitigations
  - Shut down unnecessary services
  - Harden mission support services
  - Install only necessary packages and applications
  - Accept residual risks
    - Cost of supplying service
- Only accurate when actively maintained
  - Tools quickly become legacy

Mitigation



- System Hardening Scripts
- OS Patching
  - Sun
    - Sunsolve from Sun
  - Red Hat
    - up2date
- Run patch evaluation tools regularly
  - Re-secure after patching
- Maintain a service contract!
  - Not all patches available without contract
- System Monitoring
- Maintain security profile



- **Questions**

Security Specifics

Accounts Passwords and Shells

- Make sure passwords are required for login to all accounts
- Force passwords to be at least eight (8) characters long depeding on security level
  - /etc/default/passwd (solaris)
- Disable or remove all unnecessary accounts
  - toor, games, nfs
- Assign disabled accounts are an invalid shell
  - /usr/bin/false /sbin/nologin
- Create the file /etc/ftpusers
  - cat /etc/passwd | cut –d “:” –f1 > /etc/ftpusers

Validate Accounts

- Review user accounts for common configuration errors
- Solaris
  - pwck – notes inconsistencies in /etc/passwd file
  - grpck – verifies entries in the /etc/group file

Limiting Privileges

- Disable root login capability
  - Disable Allow Root Login in sshd_config
  - /etc/login.conf and /etc/default/login
- Restrict root's search path
  - Make sure ./ is not in any PATH variables
    - .cshrc .bashrc .profile .login
- Check files sourced by root's login files
- Set root's umask to 077 or 027
  - Translates to root file/directories being 700 or 750
- Use sudo
  - Provides auditing and access control on privileged commands
  - Tightly configure what commands can be run with sudo
  - visudo /etc/sudoers

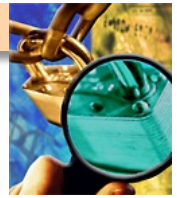
Remote Access Control

- VPN's, SSL VPN, SSH,
- Do
  - Use secure protocols
    - FIPS 140-2 compliant
    - VPN, SSH
  - Use strong multi-factor authentication
  - Establish policy
  - Harden hosts
  - Limit capability to specific tasks
    - Root not allowed but sudo possible
- Don't
  - Enable split tunneling
  - Allow personal machines to participate
  - Forget to audit connections

System Partitioning

- Use privilege separation
  - Solaris 10 Zones / Trusted Solaris
  - Jail / Chroot
- Creates an isolated system within a system
  - Minimal install
  - Limited capability and accessibility
  - Deters “escaping” when compromised
- Critical to implement for:
  - Web severs, shared environments
  - Remote access systems
  - Strict user seperation

Secure Remote Access



- Ensure that secure protocols like SSHv2 and HTTPS are used for remote access
  - FIPS 140-2 Compliant
- Validate that user and administrative functions are separated
  - Web applications
  - Network administration
- Ensure that management is performed with a secondary network interface

Restrict Access

- Disable trusted host capability
  - rhosts shosts logins
- Provide a security warning banner
  - /etc/issue.net
  - /etc/motd
- Set an eeprom password and security mode
  - Prevents un authorized users from access the prom
  - Do NOT forget the prom password

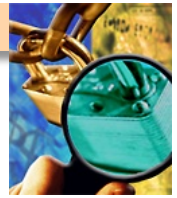
Restrict Access

- Disable IP forwarding and dynamic routing
  - Solaris
    - ndd –set /dev/ip ip_forwarding=0 (realtime)
    - echo “set ip:ip_forwarding=0” >> /etc/system (boot)
  - /etc/norouter
- Install IPFilter
  - Block broadcast packets
  - Block host from responding to broadcast packets
  - Be restrictive with acl’s

System Auditing

- Ensure that proper auditing is configured
  - Enable Syslog
  - Enable Basic Security Module (BSM)
- Consider centralized logging depending on security level

Validate Audit Files

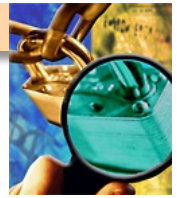


- Restrict access to audit files
  - chown –R root:sysadmin /var/log; var/adm
  - chmod –R 750 /var/log; /var/adm
- Log all su activity
  - /var/log/sulog
- Log incoming connections for all TCP services
  - IPFilter logging
  - Service logging through syslog (stunnel, ssh, http)
- Process accounting
  - See what commands are executed

Time Synchronization

- Validate the use of Network Time Protocol (NTP)
  - Synchronize all devices with multiple internal sources
  - Ensure offset is appropriately configured
  - Check to see if crypto and keys are configured in ntpd.conf

Configuration Management

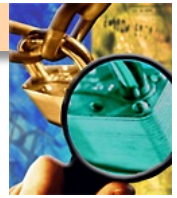


- CM shortfalls
  - Identified by inconsistencies across systems
    - Especially when systems are “mirrored” for backup
  - Out of date patches
    - Kernel version is one quick obvious indicator
  - Old or vulnerable software
    - Revealed in network scans or prior knowledge

Conformance to Baselines

- All systems should conform to the organization's security baselines
  - Many exist for Solaris, Linux and HP-UX
  - Provide consistency in configuration and security
  - Establish a means of validating a system

Minimal Installs



- Install minimum operating system packages
  - Solaris can be built around 90 packages versus 600
    - pkginfo |more – list the current installed packages
    - pkgrm ‘pkgname’ – removes ‘pkgname’
    - pkgchk –l –p <full /path/to/file> -- which package a file belongs to
- Install the current recommended patch cluster
  - Sunsolve.sun.com
    - Sun recommended patch clusters
  - Cvsup / buildworld
    - Update entire source and rebuild

System Startup

- Remove startup scripts for unneeded services
  - Solaris (prior to 10) /etc/rc*.d (rc2.d, rc3.d mainly)
    - Move capital to lowercase
    - mv S70snmp s70snmp
  - Solaris 10
    - Use service manager and xml templates
    - Does not apply to “Legacy Services”

System Services

- Disable all cron jobs except those belonging to root
  - /etc/cron
  - cron.allow cron.deny
  - at.allow at.deny
- Remove unneeded network service entries from /etc/inetd.conf
  - grep –v “^[#]” /etc/inetd.conf
- Disable NFS
- Test all boot file changes by rebooting
  - Look for extraneous processes in ps -elf
  - Odd ports Listening netstat -an
  - Examining the /var/adm/messages

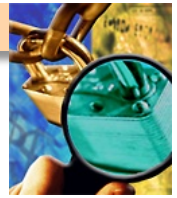
File System Layout

- Separate user/system files
  - Separate mount point for / /tmp /usr /home
  - Add NOSUID and NODEV flags to /tmp
  - Add NOSUID flag to /home (user files)
- Allows for additional security and expansion

File Permissions

- Limit non-root user access to files and file systems
- Remove nouser/group files
  - find / -name xfn -prune -o -nouser -exec ls -la {} \;
- Remove setgid permissions from system files
  - find / -name xfn -prune -o -perm -2 -exec ls -la {} \;
- Prohibit setuid programs from being executed
  - find / -name xfn -prune -o -type f \(-perm -4000 -o -perm -2000 \) -exec ls -la {} \;

Account Anonymity



- Shared accounts
  - Identified by reviewing auth and su logs
    - Accounts that do not have password expiration
    - Vague user id's like admin, monitoring, helpdesk
  - Remove the capability to performing auditing
  - Reduce the effectiveness of holding users accountable

Multi-Factor Authentication

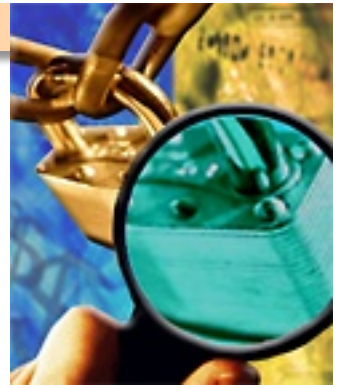
- Recommend using strong authentication
  - Especially for remote access
  - High security
- Implement strong authentication
  - Something a user has (token)
  - Something the user knows (pin, pass, pass phrase)
  - Something the user is (fingerprint, retinal)

Incident Handling

- Is there a plan?
  - Protect
  - Detect
  - Defend
  - Restore

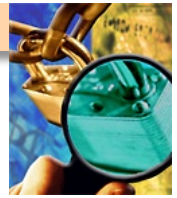
Host-Based Security

- Are HIPS, HIDS, employed?
  - Monitor for malicious connections
  - Audit events
  - Audit system logs
- System integrity checking
  - Tripwire
  - Solaris 10 Basic Auditing and Reporting Tool (BART)



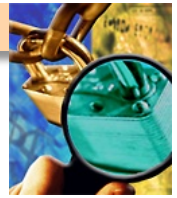
Security Exercise

Solaris X86 VM



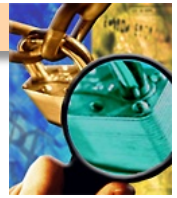
- You have all been provided a Solaris x86 VM that is NOT secure.
  - Authentication root:duckduck
  - Should dhcp an address (do we really want it on the network?)
- Your job is to secure it using the best practices that we have just discussed

Helpful commands



- vi commands
  - Insert mode press “i”
  - Exist insert mode press escape
  - Save changes :w! (press enter)
  - Exit :q (press enter)
  - Save and exit :wq! (press enter)
  - Delete with the “x” key
- Modify system profile
  - svccfg apply /var/svc/profile/generic_open.xml
- List running services
  - svcs –a |more
- Redirect output to a file
  - svcs –a > services.txt

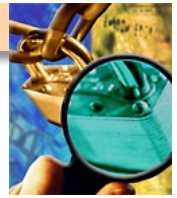
Helpful commands



- Show network information
  - ifconfig –a
  - ifconfig pcn0
  - netstat –an |more
- Restart
  - reboot
  - shutdown –g0 –i0 –y

- IPFilter firewall comments
  - Show current rule base ipfstat –hio
  - Reload rule base ipf –Fa –f /etc/ipf/ipf.conf
  - Show ipf version ipf –V
  - Rules base /etc/ipf/ipf.conf
  - Enable ipfilter - svcadm enable ipfilter
  - Service status svcs -l ipfilter

Physical Security



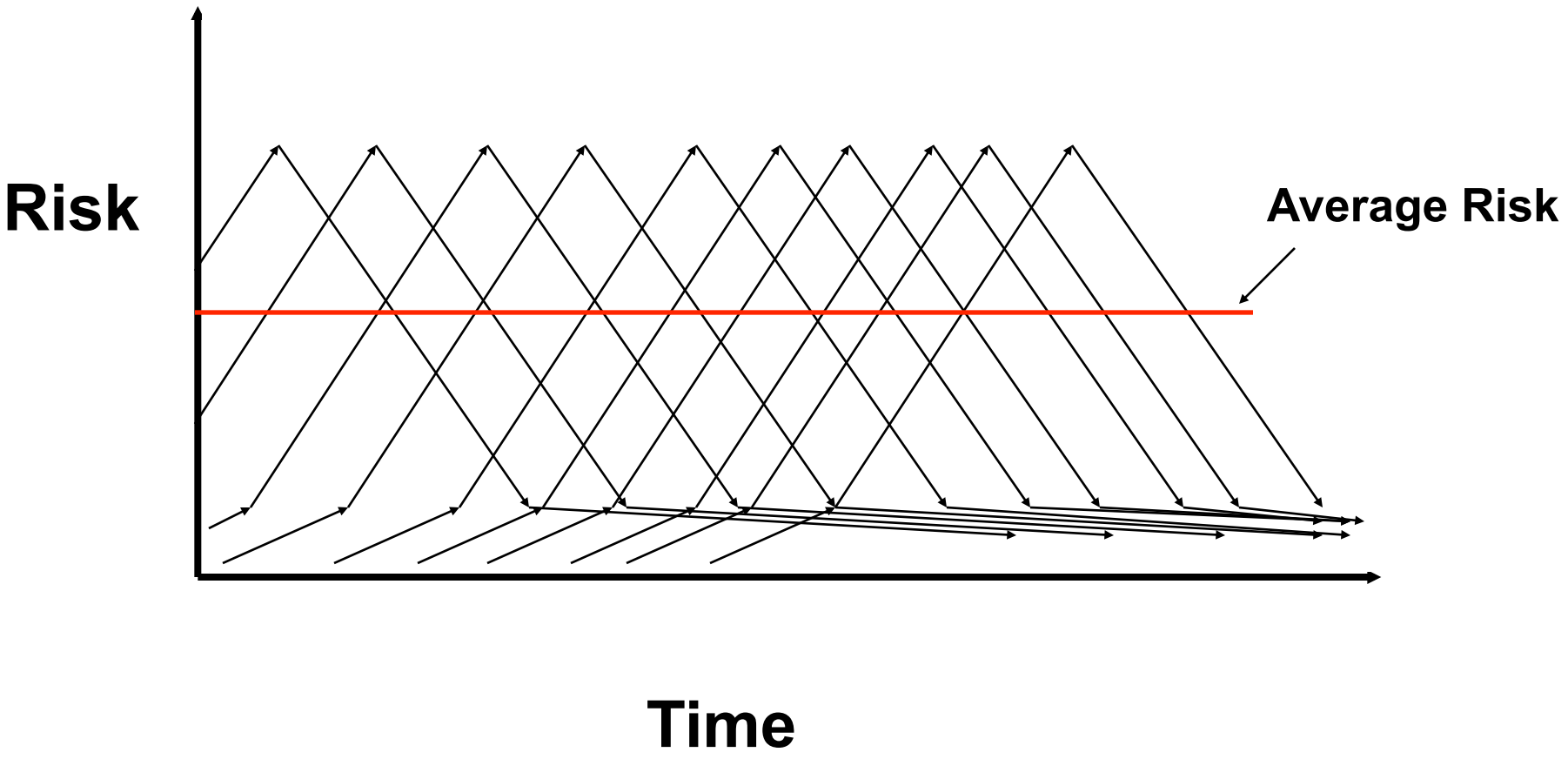
- How much is enough?
  - What's being protected
  - How easy was it to tailgate
  - Are equipment racks locked
  - Comm Closets locked


"The chain is no weaker than its strongest link"
Photo by ToHell, 2003-09-23 in Slagsta, SE

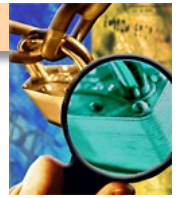
Host Security Challenge

- Host security is highly dependent on specific operating system version and individual configuration
  - A constant “patch and wait” problem
  - Security patches often break other things or operational necessity can make applying patches impractical
  - Often patches are not released until after vulnerabilities are being widely exploited
  - Patches for some applications (i.e. IIS, MS SQL server, IE, etc.) are released at a rate which is unmanageable
- It is easier and more effective to block traffic to most hosts, then secure all internal hosts as time permits

Vulnerability Life Cycle

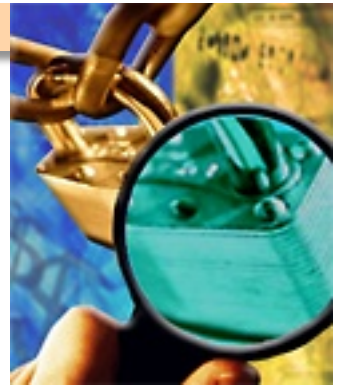


Best Practices



Recommendations from the CIS's Benchmark:

- **Patches and additional software (e.g., OpenSSH, TCP Wrappers)**
- **Minimize Network Services (e.g., inetd, sendmail)**
- **Minimize Boot Services**
- **Kernel Tuning**
- **Enhance Logging**
- **File/Directory Permissions/Access**
- **System Access, Authentication, and Authorization**
- **User Accounts and Environment**



Questions

References

- http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf
- http://www.sage.org/index.html
- http://draenor.org/securebsd/secure.txt
- http://www.spitzner.net/armoring.html
- http://www.sabernet.net/papers/Solaris.html
- http://www.cisecurity.org
- http://wwws.sun.com/software/security/jass/

Books

- *Unix System Administration Handbook, Second Edition*, by Evi Nemeth et al, Prentice Hall, Englewood Cliffs, NJ, Copyright 1995, ISBN 0-13-151051-7.
- *Practical Unix & Internet Security, Second Edition*, by Simson Garfinckel and Gene Spafford, O'Reilly, Sebastopol, CA, Copyright 1996, ISBN 1-565592-148-8.
- *Solaris Security*, by Peter H. Gregory, Sun Microsystems Press, Prentice Hall, Englewood Cliffs, NJ, Copyright 2000, ISBN 0-13-096053-5.
- *Red Hat Linux Security and Optimization*, by Mohammed J. Kabir, Red Hat Press, Hungry Minds Inc., New York, NY, Copyright 2002, ISBN 0-7645-4754-2.

Questions