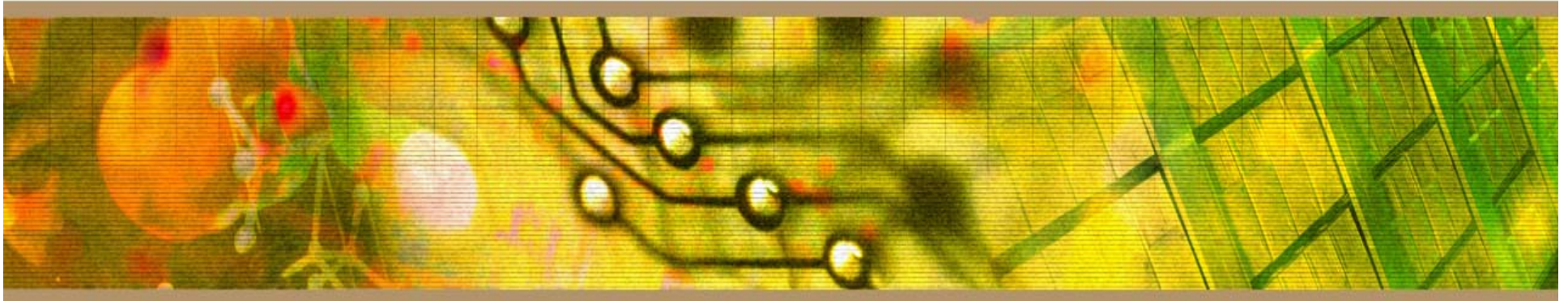


Host Hardening



Presented by

Douglas Couch & Nathan Heck
Security Analysts for ITaP

PURDUE **Background**

UNIVERSITY

- National Institute of Standards and Technology
 - Draft Guide to General Server Security SP800-123
- Server – A host that provides services for other hosts as a primary function
 - Web, Database, DNS, Mail, File Server, etc...
- Server Vulnerabilities, Threats, and Environments
 - Defining threats can help mitigate them

- Security Categorization of Information and Systems
 - 3 objectives of Security
 - » CIA = Confidentiality, Integrity, and Availability
 - FIPS Publication 199 defines 3 security categories
 - » Low, moderate, and high based on impact
 - Security controls
 - » Fixing vulnerabilities
 - » Applying the least privilege needed to complete a task
 - » Balance security and usability
 - » Layer security

- **Basic Server Security Steps**
 1. Plan the installation
 2. Install, configure, and secure the OS
 3. Install, configure, and secure the server software
 4. Test the security
 5. Add network defenses
 6. Monitor and Maintain

PURDUE **Background**

UNIVERSITY

- Server security principles:

Simplicity

Complete Mediation

Separation of Privilege

Psychological Acceptability

Compromise Recording

Fail-Safe

Open Design

Least Privilege

Work Factor

Defense-in-Depth

- The Five P's
- Identify
 - The purpose of the server
 - The services provided on the server
 - Network service software client and server
 - The users or types of users of the server

- Determine
 - Privileges for user and categories of users
 - How the server will be managed
 - Decide if and how users will authenticate
 - How appropriate access will be enforced
 - Which server applications meet the requirements
 - » cost, compatibility, functionality, and prior knowledge

- Work closely with manufacturers during the planning stage
- Choose the OS with provides the following:
 - Ability to restrict admin access
 - Granular control of data access
 - Ability to disable services
 - Ability to control executables
 - Ability to log activities
 - Host based firewall provisioning
 - Support for strong authentication and encryption

- Availability of trained, experienced staff
- Physical Security
 - Protection mechanisms
 - Environmental controls
 - Backup power source
 - Fire containment
 - Redundant network connections
 - Location hardened against local natural disasters

- Basic steps to follow after planning installation and deployment of the OS
 - Patch and update the OS
 - Harden and configure the OS
 - Install and configure additional security controls
 - Test the security of the OS

- Create a process
- Identify vulnerabilities
- Mitigate if necessary and patch when available
- Patch servers in isolation
- Test patches before applying

- Disable or remove unnecessary services or applications
 - Single purpose servers
 - Remove rather than disable to prevent re-enabling
 - Additional services increases the attack vector
 - More services can increase host load and decrease performance
 - Reducing services reduces logs and makes detection of intrusion easier

- Configure user authentication
 - Remove or disable unnecessary accounts
 - Change names and passwords for default accounts
 - Disable non-interactive accounts
 - Assign rights to groups not user
 - Don't permit shared accounts if possible
 - Configure time sync
 - Enforce appropriate password policy
 - Configure to prevent password guessing
 - Use 2-factor authentication when necessary
 - **Always use encrypted authentication**

- Configure resource controls
 - Deny read to protect confidentiality
 - Deny write to maintain integrity
 - Limit execution to prevent reduction of security
 - Use an isolated virtual environment
 - » chroot, sandbox, or jails
 - Control access to:
 - » System software and configuration files
 - » Security files – password hashes, cryptographic keys
 - » OS logs

- Install and Configure Additional Security Controls
 - Anti-malware
 - Host-based IDPS
 - » File integrity tools
 - Host-based firewalls
 - Patch management software
 - Disk encryption
 - Return-to-state software
 - Secure deletion tools
 - Secure remote tools

- Install and patch the Server Software
 - In a secure location
- Clean the installation
 - Remove anything you don't need
- Harden and Configure
 - Apply templates
 - Remove banners
 - Change ports and/or locations

- Control access to:
 - Application software and configuration files
 - Security files
 - Server logs
 - System software and configuration files
 - Application content and uploads

- Run the server with limited privileges
 - Not root or administrator
 - Limit write permission
 - No access to server temp files

- Prevent DOS attacks. Limit resources
 - Install content on a different drive
 - Limit upload space and file size
 - Store log files separately
 - Limit processes
 - Limit memory
 - Limit connection time

- User Access Restrictions
 - Grant individual accounts and access
 - Encrypt authentication
 - IP restrict

- Security maintenance is continual and includes:
 - Logging, backups, testing, patching
- Logging provides:
 - Alerts
 - Tracking
 - Information
 - Evidence

- Identify capabilities and requirements
 - Determine available logs and types
 - Log from other applications
 - Synchronize using NTP
- Review and retain
 - Reviewing can be time consuming
 - Use automated tools
 - Create an archiving policy

- Create a backup policy that fits:
 - Legal requirements
 - Mission requirements
 - Organizational policy
- Create baseline "image"
- Encrypt or securely store backups

- Use identical hardware and software
 - Or consider virtualization
- Can be used for:
 - Testing patches
 - Developing new content and applications
 - Testing configuration changes
 - More risky behavior
 - » Compilers, remote access, additional tools

- **REPORT THE INCIDENT TO ABUSE@PURDUE.EDU**
- Isolate the system or contain the attack
- Consult as appropriate, management, legal counsel, or law enforcement
- Investigate similar hosts for possible compromise
- Analyze the intrusion:
 - current system state including memory, network connections, time stamps and logged in users
 - modifications to the system
 - modifications to the data
 - tools left behind
 - system, ID, and firewall logs

- Restore
 - Use a clean install
 - Disable additional services
 - Apply patches
 - Change all passwords
 - Reconfigure network for additional security and notification
- Test
- Reconnect
- Monitor
- Document

- Use automated vulnerability scanning weekly or monthly
- Use manual Penetration testing annually
- Factors when testing a production server or QA:
 - Possible impact - DOS or data corruption
 - Possible data disclosure
 - Similarity of QA and Production
- Secure Computing Baselines - CIS Benchmarks

- Vulnerability scanning can:
 - Identify hosts on a network
 - Identify active services and which are vulnerable
 - Identify applications and banners
 - Identify OSs
 - Enumerate vulnerabilities in discovered services or OSs
 - Test compliance with policies

- Penetration testing
 - Tests with the same tools as an attacker
 - Verifies vulnerabilities
 - Demonstrates exploits
 - Provides realism
 - Allows for testing of social engineering

- Use strong authentication
- Use strong encryption
- Restrict access
- Enforce least privilege
- No access from the internet
- Remove or change default accounts

- **Recommendations of the National Institute of Standards and Technology (excerpts)**
 - <http://csrc.nist.gov/publications/drafts/800-123/Draft-SP800-123.pdf>
- **Useful tools, guidelines, and best practices:**
 - <http://www.purdue.edu/securepurdue>
- **Questions?**