SecureWorks

DATA SHEET

Security Design Architecture

Server Hardening

The Challenge

Most commonly available servers operate on a general-purpose operating system (OS) with standard services, commercial-off-the-shelf (COTS) applications and network protocols that are pre-configured. Because manufacturers cannot account for the unique needs of each organization's security policies, reconfiguration of new and existing server policies and controls is required. To compound this, the techniques for securing different OSs vary greatly depending on a multitude of factors that can create a very challenging task to match them with security requirements and the needs of the business.

Solving the Challenge

Properly hardening servers is unique to every organization. There is no standard checklist that can be widely applied to all organizations that will optimally reduce the surface of vulnerability. That's why SecureWorks emphasizes the importance of first understanding your in-scope environment's business function, placement, configuration, operational/maintenance activities and objectives before ever starting a technical examination. Once completed, SecureWorks consultants will then conduct a technical analysis, utilizing a mixture of the most relevant standards and frameworks, including the Center for Internet Security (CIS) Benchmark program. These industry standards, applied and interpreted through SecureWorks' knowledge of your environment, will be used to provide an Assessment Report. The report will rank findings and prioritize discovered areas of concern to provide clear direction for remediation.

Solution at a Glance

	Server Hardening
Will account for	• Interview/elicitation sessions onsite • Operating System Hardening Assessments • COTS Application Hardening Assessments
Objective	Enhance server security through a variety of means, resulting in a much more secure server operating environment
Can be performed on-premises	✓
Can be performed remotely	✓
Schedule for on-site work	M-F 8am – 6pm Local Time
Schedule for remote work	M-F 8am – 8pm EST
Typical time to complete	3-5 days per server or application
Deliverable timing	Within 3 weeks of engagement completion

	Server Hardening		
Sample operating systems and applications	**Operating Systems: Servers** • Amazon Linux • CentOS • Debian Linux Server • Distribution Independent Linux • FreeBSD Server • HP-UX Server • IBM AIX Server • Microsoft Windows Server • Novell Netware • Oracle Linux • Oracle Solaris Server • Red Hat Linux Server • Slackware Linux Server • SUSE Linux Server • Ubuntu LTS Server **Productivity Software** • Microsoft Office **Virtualization Platforms** • VMware Server • Xen Server • Agnostic VM Server	**Web Servers** • Apache HTTP Server • Apache Tomcat Server • Microsoft IIS Server **Authentication Servers** • Free RADIUS • MIT Kerberos **Database Platforms** • IBM DB2 Server • Microsoft SQL Server • MySQL Database Server • Oracle Database Server	**Directory Servers** • Novell eDirectory • OpenLDAP Server **DNS Servers** • Bind DNS Server **Mail Servers** • Microsoft Exchange **Operating Systems: Desktop** • Apple Desktop • Microsoft Windows
Additional considerations	If any IP addresses, hosts, facilities or devices within scope are owned or hosted with a service provider or other third party, it will be necessary for you to obtain permission from that party in writing or through email before SecureWorks will perform services.		
Out of scope	• Locations, devices or personnel that are not specifically listed as being in scope are out of scope. • Tuning, refining or otherwise altering in any way the logical configuration of any customer device • Standards-based risk analysis or risk assessment • Penetration testing • Implementation of recommendations • Logical configuration changes		

What Does Server Hardening Help Me Answer?

- Are my servers susceptible to attack?
- Are my current policies taking into account business function and security safeguards?
- Are my current configurations sufficiently protecting me?
- Are my servers providing the appropriate level of access?
- Are there software or services running on my server that increase my risk?

Benefits to You

- Reduce attack surface vulnerabilities
- Properly configure OS user authentication and resource controls
- Removal of unnecessary services, applications and network protocols
- Improve patching prioritization and cadence
- Reduce memory and hard drive consumption

Methodology

1 Pre-Engagement

- Goals and objectives established
- Review scope and methodology for engagement
- Define personnel, roles and responsibilities
- Exchange of relevant information (network and application flow diagrams, device configuration dumps, etc.)
- Timelines established

2 Phase 1

- Conduct interviews to gather knowledge of existing environment that shapes the backdrop for the assessment
  - Business purpose and function of device
  - Placement
  - Configuration
  - Operational and maintenance activities

3 Phase 2

- Utilize outcomes of Phase 1 to inform technical analysis portion of the assessment
- Technical analysis using CIS Security benchmarks applied and interpreted through SecureWorks's knowledge of client environment
- Analysis draws on items in the table below as deemed relevant and informed through customer business requirements
- Final report and presentation to key personnel and stakeholders

Note: This is merely to provide an example of some operating systems analysis; menu is not inclusive of applications or all operating systems.

Operating System	Microsoft Windows Server 2008 & 2012	Microsoft IIS	Microsoft Windows 7	Linux
Technical Analysis Snapshot	• Account Policies • Local Policies • Event Log • Restricted Groups • System Services • File System • Wired Network Policies • Windows Firewall with Advanced Security • Wireless Network Policies • Public Key Policies • Software Restriction Policies • Network Access Protection Client Configuration • Application Control Policies • IP Security Policies • Advanced Audit Policy Configuration • Administrative Templates	• Basic Configurations • Authentication Configuration • ASP.NET Configuration • Request Filtering and Restrictions • Logging • FTP Requests	• Drive Encryption • AutoPlay Policies • Event Log • Windows Remote Shell • Windows Explorer • Windows Update • Credential User Interface • Remote Desktop Services • HomeGroup • Power Management • Internet Communication Management • Remote Procedure Call • Remote Assistance • Group Policy • Local Policies • Advanced Audit Policy Configuration • Windows Firewall with Advanced Security • Account Policies • Administrative Templates	• Disablement of unnecessary services • Security settings on key files • Password policy enforcement • Limiting root access • Limiting access to cron • Remote access and ssh settings • inetd.conf and xinetd configuration • System logging • System patching • Host protection with iptables • Applicability of Selinux • File sharing mechanisms

Who Needs Server Hardening?

- Have high value servers that operate significant business functions
- Need an assessment of a "gold" image
- Review for compliance or adherence to security frameworks
- Installing new operating systems on servers
- Deploying a new server or server environment
- Currently utilizing default configurations (software, usernames, logins and services)
- Currently running default or "free" software or applications without proper patching schedule
- Lack of established server hardening policies
- Need to minimize unnecessary software running on server

What to Expect in Your Report

SecureWorks will create an Assessment Report that prioritizes discovered areas of concern and ranks findings. Recommendation and reasoning are listed with each ranked finding to justify the finding and to provide direction for remediation.

Executive Summary
This section summarizes assessment findings and lists the main areas of concern, providing a quick, executive-level synopsis of the engagement in clear and concise language.

The Core Report
Detailed findings of the assessment in technical detail supported by reasoned recommendations for remediation or mitigation of the same. Commentary on technology feature gap or overlap, scalability, degree of automation, and administrative overhead will be presented. The Core Report includes an ordered matrix that categorizes remediation sentiment rated as green/amber/red. The Core Report will be colored in by the analyst and cross-referenced with SecureWorks Counter Threat Unit™ with juxtaposition of how well the client's in-scope infrastructure is configured to ward off such threats.

The Appendices
One or more appendices will be written and included with the Server Hardening Assessment Report, providing additional technical detail and recommendations that back up the findings in the main report.

Why SecureWorks

Our Security Consultants
SecureWorks hires only the best and brightest. From our in-depth technical hiring process to our continued investment in our consultants through generous training programs, we seek to find and cultivate security design excellence. Our consultants can be found speaking at industry conferences and releasing cutting-edge security research that becomes industry standard best practices.

SecureWorks Global Threat Intelligence
Threat intelligence is the fuel that powers the engine of the security solutions we provide. With more than 65 of the world's most highly regarded security researchers, SecureWorks' distinguished CTU research team is what sets us apart. Our researchers analyze threat data across our global client base and actively monitor the cyber threat landscape to provide a globalized view of emerging threats, which provides a basis for the design and architecture decisions we provide.

Proven Methodology
SecureWorks has performed thousands of consulting engagements for a wide array of companies, from small business to Fortune 500. Our server hardening methodology is based on the Center for Internet Security (CIS) benchmarks. This industry standard, applied and interpreted through SecureWorks' knowledge of our clients' environments, provides the information used to create the Assessment Report.

Complimentary Services:

- **Network Security Testing such as Penetration Testing**
- **Application Security Testing**
- **Log Monitoring and Retention**
- **Vulnerability Management**
- **Governance, Risk and Compliance Services**

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com