DATA SHEET

Foundstone Host Security Configuration Assessment

Identify vulnerabilities that other network assessments miss

Host Security Configuration Assessments are critical because they allow us to identify vulnerabilities that cannot be detected through network assessments. These assessments are the most efficient mechanism to comprehensively assess the security of network components.

The Foundstone® Services Host Security Configuration Assessment—part of the McAfee® product and services offering—evaluates the security of your company's critical servers and the backbone of your technology infrastructure. We analyze the operating system and application-level security issues of your company's operating environments. Foundstone consultants check administrative and technical controls, identify potential and actual weaknesses, and recommend specific countermeasures. We understand that the hosts within scope for configuration assessment will be based on a risk profile created during the engagement. Accordingly, we provide per-host pricing.

Benefits

- Evaluate the security of your company's critical servers.
- Analyze the operating system and application-level security of your operating environments.
- Check administrative and technical controls, identify potential and actual weaknesses, and get recommended countermeasures.

Leverage a Comprehensive Set of Audit Points

Our consultants perform Host Security Configuration Assessments for Microsoft Windows 2000/XP and UNIX environments, including important applications such as IIS, SQL Server, and Apache, as well as routers. Having performed hundreds of Host Security Configuration Assessments for systems in production environments—ranging from ecommerce web servers and financial databases to Internet-facing bastion hosts—we've compiled a comprehensive set of audit points based on our experience with penetration testing. Because our knowledge base stays current with emerging technology, you'll be assured that our Host Security Configuration Assessments check for the latest security patches and configuration methods for the latest applications. Our experienced consultants accurately determine where the highest-risk problems occur and how to address those issues at a policy level. Finally, our techniques use customized scripts that can be run by your administrators to collect data for assessment.

Methodology

Our methodology is created from established public guidelines and our consultants' experience. We've developed tools to automate the collection of data, and use these scripts to help identify high-risk misconfigurations or omissions in your company's server builds. Drawing from our experience, we test the overall risk of the host rather than just check a list of specific vendor-recommended points. As a result, we are able to identify the controls that need the most improvement to reduce the risk faced by the host.

During each engagement we thoroughly check the adequacy of security controls on the features and functions listed for numerous operating systems and devices including:

- Microsoft Windows 2000/XP, Unix (including Solaris, Linux, Tru-64, and AIX), and Novell.
- Specific applications such as IIS, SQL Server, and Apache.
- Router and switch hosts.

Microsoft Windows 2000/XP, UNIX, and Linux Hosts

Each host is measured against the security practices from our methodology. We create a measurement of risk that is comparable between different operating systems and applications.

Account Management and Security

- Password storage mechanisms for adequate restrictions.
- Password generation and management controls.
- Users' accounts have appropriate permissions.
- All users have unique accounts.
- Identify domain or server account policies for password rules, login time restrictions, and intruder detection and lockout.
- Test password policy using password crackers such as LOphtcrack or John the Ripper.

File Management and Security

- Permissions are correct for system, application, data, and user files.
- Shares do not expose unnecessary data.
- Shares are restricted to appropriate users and groups.
- File integrity is monitored (Tripwire, md5 checksums, etc.).
- Antivirus software is installed, up to date, and functioning.

Patch Level

- An environment and procedure exists for testing patches before deploying to production systems.
- Security-related patches for the operating system have been applied.
- Security-related patches for applications have been applied.

Deliverables

- Host Security Configuration Assessment Technical Report
- Host Security Configuration Assessment Executive Summary
- Next-step Recommendations
- Half-day workshop with Host Security Assessment Presentation

Network Security

- No unnecessary protocols are enabled.
- Only business-related services are running.
- Common services have been adequately secured (FTP, HTTP, NFS, RPC services, X Windows).
- Host-level firewall or other network access-control mechanism is enabled, where appropriate.
- Modem security follows established policy.

Logging and Auditing

- Default operating system auditing has been augmented.
- Applications are configured to generate log data and log files are backed up.
- Logs are periodically assessed for suspicious activity.
- System times are synchronized with a central server.

General Security Management

- Ensure that applications are executed with a least-privilege concept.
- Check potential for startup executables and scripts that may provide a back-door vulnerability based on insecure permissions or implementation.
- Identify extent and type of trust relationships between domains.
- Identify extent and type of trust relationships between individual systems.

Detection of Previous Intrusion

- Look for the presence of common Trojans and back doors.
- Check suspicious file permissions.
- Check suspicious user accounts, such as an account with a blank password, excessive rights, not audited.
- External controls (where applicable).
- Physical security.
- Back-up strategy.
- UPS.
- Fire suppressions.
- Environment (AC, humidity).

Host Application Assessment—IIS, SQL Server, Apache

Foundstone also assesses the installation and configuration of major applications such as Microsoft IIS and SQL Server. These applications often represent a high risk to the network because of their history of vulnerabilities and their Internet connectivity.

- Secure configuration.
- Separation of privileges.
- Recommended practices.
- Logging and auditing.

Related Foundstone Services

- Policies and Process Health Check
- Policies and Process Program Development
- Foundstone Training
- Comprehensive Network and Infrastructure Security Assessment

Results

Our methodology not only points out specific points that should be addressed to reduce a host's risk exposure, it also provides recommendations for how to bring up the baseline for deploying servers. These risk-reduction recommendations protect the system from known vulnerabilities and often eliminate exposure to zero-day exploits which reduces the scope of a compromise.

Router and Switch Host Assessment

These assessments begin with the methodology previously described to assess the configuration of the underlying host. Additional checks are performed to assess the particular function of the router and switch. The methodology targets high-level concepts by tracking specific, detailed points:

- Access control lists that restrict packet flow.
- Configurations to prevent or minimize spoofing attacks.
- Filtering rules that restrict traffic destined for the router or firewall.
- Check authentication methods for remote and local access and determine the adequacy of these controls.
- Determine whether per-port security is enabled to eliminate unauthorized spanning, where applicable (Cisco switches).
- Examine authentication mechanisms for routing table updates.
- Examine routes, especially static ones, for security concerns.
- Examine the adequacy and security of logging configurations.
- Ensure installation of recent software updates.
- Examine hosts for unnecessary services and examine services configuration for appropriate security controls.

Discounted Retesting

Foundstone partners with your organization in attaining its strategic security goals. At the conclusion of this engagement, we list all discovered vulnerabilities based upon a ranking of high, medium, and low. At a discounted rate, we perform a retest of each of the discovered vulnerabilities within three months of the completion of your engagement. This allows you to validate that your security remediation efforts resolved all discovered vulnerabilities.

The Foundstone Difference

All Foundstone projects are managed using our proven Security Engagement Process (SEP) for project management. This process ensures continual communication with your organization to ensure the success of all your consulting engagements.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the Intel Security global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about integrating our services. You can get more information at **www.foundstone.com**.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com