12.1.10 Web Server Countermeasures Facts

Web servers are an open door to the public. As such, they bring a whole new level of complexity to network security. It is critically important to implement countermeasures to safeguard web servers.

This lesson covers the following topics:

- Security settings and configurations
- Web server security tools
- Web server penetration testing
- Web server penetration testing tools

Security Settings and Configurations

The most common and accessible method for determining potential problems is a vulnerability scanner. These scanners can provide insight about where you should make improvements to your network accessibility and configuration. The following table describes areas of vulnerability that you should check for.

Vulnerability	Description
Misconfiguration	The very best security measures can be rendered useless by a simple misconfiguration error. Missing a setting or forgetting to check a box can create a vulnerability. To prevent this type of error, be sure that the server implementation is well thought out. Plan your configuration, accounts, permissions, restrictions, and policies. Test your configurations both before and after implementation.
Patches	As with most security countermeasures, patches and updates play a critical role in network security. A patch is designed to fix known vulnerabilities, eliminate bugs, and, sometimes, improve a system's overall performance. Updates are a collection of these patches. You can manage patches using patch management tools that come with the operating system. Before applying any patch or update, verify the source of the fix to ensure its validity; research relevant documentation to see how, and if, it will apply to your network; and make sure your system is backed up. Not all patches and updates are critical to your infrastructure, so they should be applied on an as-needed basis.
Ports and protocols	Block all unused ports and protocols. Audit the used ports on a regular basis to verify that there are no unsecure services active on the server. If you use protocols that are not secure (Telnet, FTP, SMTP, or POP3), be sure to use protocols such as IPSec to create a secure authentication and communication process. Use tunneling and encryption protocols for remote access.
Files and directories	Remove any unneeded files from .jar files. Monitor all service logs, website access logs, and database server logs. Disable saving specific file types. Remove non-web files, including backup files, text files, header files, and archive files.
User accounts, applications, and modules	Remove unused applications, modules, and user accounts, including default accounts created by the operating system installation. Run all processes using the least privileged account. Use secure web permissions and access control mechanisms.
Website changes	Use a website change detection system to discover hacking attempts on web servers. Do this by running a script that detects files added to the web server or changes made to any existing files. Many website change detection systems also compare the file hash values with the master value to detect possible changes. If any changes are detected on the server, the administrator is notified.

Web Server Security Tools

The following table describes tools you can use to configure security settings.

Tool	Description
MBSA	Microsoft Baseline Security Analyzer is a patch management tool that checks for updates to the operating system, database components, and SQL server. It also scans for any errors or vulnerabilities in the configuration settings.
Syhunt Dynamic	Syhunt Dynamic can automate security testing and can help to guard web infrastructure against known security threats.
Wikto	Wikto is a security scanner for Windows web servers. It checks for errors in code and monitors HTTP requests and responses.
Hackalert	Hackalert is a service that detects hidden malware in websites and advertisements.

Web Server Penetration Testing

Penetration testing is done to check a web server's security. Penetration testing targets the server with various types of attacks in an attempt to find weaknesses in the server environment. The following table identifies steps in penetration testing.

Step	Description
Identify the target	Collect as much information as possible about the target including physical location, operations, contact information, and human resources. Whois query tools can be used to obtain information about a target including the domain name, DNS server, IP address, and registered contact information. Be sure to document all findings.
Fingerprint the web server	Use fingerprinting techniques and tools to collect information about the server, including the server name, operating system, and any applications that may be running on the server.
Crawl the website	Use manual and automated methods to crawl the website and collect information about the target, such as contact information, hours of operation, and employee hierarchy.
Enumerate web directories	Use tools to enumerate a web server's directories to collect information, including login forms and web functions.
Perform a directory traversal attack	Perform a directory traversal attack to gain access to restricted directories and command options outside of the server's root directory.
Perform a man-in-the-middle attack	Intercept and alter communications between a user and the web server in an attempt to obtain sensitive information.
Perform web application penetration testing	Complete penetration testing on web applications. This process is detailed in the web application countermeasures lesson.
Examine web server logs	Examine all web server logs. Although this task can be done manually, it can be difficult to interpret the data. It is also very time-consuming. Tools are available to make this task much easier.
Exploit frameworks	Use various tools to exploit the web server's frameworks.

Web Server Penetration Testing Tools

The following table lists tools you can use for penetration testing:

Tool	Description
COREImpact Pro	COREImpact Pro is a penetration testing tool that checks for vulnerabilities in web applications, network systems, wireless networks, mobile devices, and defense systems, such as IDS or IPS.
Immunity CANVAS	Immunity CANVAS provides an exploit development framework for penetration testers.
Arachni	Arachni is an open-source tool that helps penetration testers evaluate the security of web applications.