

When this document is printed, the document needs to be stamped top and bottom with the appropriate classification.

VL05 - Checklist Report

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Checklist: Netscape Instance

Vulnerability Key: V0002224

STIG ID: WA050

Release Number: 3

Status: Active

Short Name: WA050

Long Name: Trained staff are not available to respond to web server or web content problems.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 6.4 Training & Certification

Effective Date: 12 Nov 1999

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: As web sites are available to the user 24 hours per day, 7 days a week, the potential for problems relating to the web server operations to arise at anytime is significant. Operating staff may discover

a problem with the organizations web server operation or the web content. Points of Contact (staff) with the appropriate access and training must be available to respond to immediate operational needs to correct the problem.

Documentable: No

**Documentable
Explanation:**

**Potential
Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.1
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WA050 (Manual)

This check verifies, by discussion with the site staff, that an appropriately trained staff is available to answer questions and take corrective action.

- Site should have an SOP on how this is handled. Staff should be questioned on their knowledge of this aspect of the SOP.
- The staff should be trained to carry out their duties.
- Depending on the sensitivity of the data on the web server and the operational needs of the site, the site may have staff on-hand or on-call.

Reviewer should ensure that local procedures exist and are understood.

Proposed Questions:

Is the SA trained or certified for the operating system being used?
Is the SA or Web Manager trained or certified for the web software being used?
Is needed training scheduled? (This can be a comment, which mitigates the situation.)

If staff is not trained or they are not available when needed, this is a finding.

Vulnerability Key: V0002242

STIG ID: WA060

Release Number: 4

Status: Active

Short Name: WA060

Long Name: A public web server is not isolated in accordance with the DOD Network STIG and DOD Enclave STIG.

IA Controls: EBPW-1 Public WAN Connection

Categories: 14.5 Physical Layer Security

Effective Date: 10 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: To minimize exposure of private assets to unnecessary risk by attackers, Public web servers must be isolated from internal systems. Public web server also refers to web servers that may be located on non-public networks and that contain information that is approved for release to the entire community. Public web servers must not have trusted connections with assets outside the confines of the demilitarized zone (DMZ) or isolated separate public enclave (subnet). This trusted connection is not to be confused with a Microsoft Domain trust. A trusted connection can be an attachment to Microsoft shares, in UNIX as Network File System (NFS) mounts, as well as connections to interior enclave printers. This relationship can also be found with connections from public web servers to interior enclave databases.

Documentable: No**Documentable
Explanation:****Potential
Impacts:****Responsibility:** System Administrator
Information Assurance Officer**References:** ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.4
Network Infrastructure Security Implementation Guide**Checks:** WA060 (Manual)

The reviewer should question the IAO/SA/Webmaster to see where the public web server is logically located on the site's LAN. The reviewer should review the site's Network diagram, available from the NSO, to see how the web server is connected to the LAN. Based on these discussions and the LAN diagram, the reviewer should visually check the web server hardware connections to see if it is in conformance with the site's Network diagram. A public web server must be located in a DMZ. This is normally a subnet isolated from Internal LANs. An improperly located public web server is a potential threat to the entire network.

NOTE: If there is a Network Reviewer available, they should be able to provide much of the information needed to validate this check.

Proposed Questions:

What devices, i.e. router, switch, firewall, lie between the web server and Internet connectivity?
Is the web server on a separate subnet?

Is the web server on a LAN with servers and workstations dedicated to functions not intended for public access?

If the web server is not isolated in accordance with the DoD Enclave and Network Infrastructure STIGs, this is a finding.

Vulnerability Key: V0002243**STIG ID:** WA070**Release Number:** 3**Status:** Active**Short Name:** WA070**Long Name:** A private web server is not located on a separate controlled access subnet.

IA Controls: EBPW-1 Public WAN Connection
Categories: 14.5 Physical Layer Security
Effective Date: 10 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Private web servers, which host sites that serve controlled access data, must also be protected from outside threats in addition to insider threats. Insider threat may be accidental or intentional, but in either case, can cause a disruption in service of your web server. To protect the private web server from these threats, it must be located on a separate controlled access subnet and not part of the public DMZ that houses the public web servers. It also cannot be located inside the enclave as part of the local general population LAN.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE
NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.4

Checks: WA070 (Manual)

This check verifies, through a discussion with the IAO/SA/Web Manager, a check of the sites network diagram, and visual check of the web server, that the private web server is located on a separate controlled access subnet and not part of the public DMZ that houses the public web servers. In addition, the private web server needs to be isolated via a controlled access mechanism from the local general population LAN.

NOTE: If there is a Network Reviewer available, they should be able to provide much of the information needed to validate this check.

Proposed Questions:

What devices, i.e. router, switch, firewall, lie between the web server and Internet connectivity?
 Is the web server on a separate subnet?
 Is the web server on a LAN with servers and workstations dedicated to functions not intended for public access?

If the web server is not located inside the premise router, switch or firewall, and is isolated via a controlled access mechanism from the general population LAN, this is a finding.

Vulnerability Key: V0002253**STIG ID:** WA110**Release Number:** 4**Status:** Active**Short Name:** WA110**Long Name:** Web server access logs are not archived in accordance with the DOD Instruction 8500.2.**IA Controls:** ECRR-1 Audit Record Retention**Categories:** 10.5 Retention**Effective Date:** 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: Audit trails (logs) are required as a minimum to determine accountability, according to DoD Instruction 8500.2. They also provide the accountability functionality of a C2 level trusted requirement. Auditing (logging) provides an investigative tool to detect misuse of the system and has been used as evidence to convict individuals of computer crime. As stated in the DoD Instruction 8500.2: Enclave and Computing Environment Integrity ECRR-1 Audit Record Retention If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.

Documentable: No**Documentable Explanation:****Potential Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.7.1

Checks: WA110 (Manual)

Interview the IAO and Web Manager to determine the retention and storage of the Web Server access logs.

Proposed Questions:

Are you archiving your access / audit logs?
Where are the logs maintained for one year?
Who has access to the logs while they are archived?

If the logs are not being archived IAW policy, this is a finding.

Vulnerability Key: V0002257

STIG ID: WA120

Release Number: 4

Status: Active

Short Name: WA120

Long Name: The Web Manager or Webmaster has not documented the administrative users and groups that have access rights to the web server.

IA Controls: ECPA-1 Privileged Account Control

Categories: 1.3 Identity Management

Effective Date: 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: As noted in section 3.3 of the Web Services STIG, there are typically several individuals and groups which are involved in running a production web site. In most cases we can identify several types of users on a web server. These are the System Administrators (SAs), Web Managers, Auditors, Authors, Developers, and the Clients. Nonetheless, only necessary user and administrative accounts will be allowed on the web server. Accounts will be restricted to those that are necessary to maintain web services, review the server's operation and the operating system. Owing to the sensitivity of web servers, a detailed record of these accounts must be maintained.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Manager
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10

Checks: WA120 - Windows (Manual)

Proposed Questions:

How many user accounts are associated with the Web site operation and maintenance?

Where are these accounts documented?

Using User Manager, User Manager for Domains, or Local Users and Groups examine user accounts to verify the above information.

Query the SA or Web Manager regarding the use of each account and each group.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: As noted in section 3.3 of the Web Services STIG, there are typically several individuals and groups which are involved in running a production web site. In most cases we can identify several types of users on a web server. These are the System Administrators (SAs), Web Managers, Auditors, Authors, Developers, and the Clients. Nonetheless, only necessary user and administrative accounts will be allowed on the web server. Accounts will be restricted to those that are necessary to maintain web services, review the server's operation and the operating system. Owing to the sensitivity of web servers, a detailed record of these accounts must be maintained.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WA120 - Unix (Manual)

Proposed Questions:

How many user accounts are associated with the Web site operation and maintenance?

Where are these accounts documented?

Use the command line utility more /etc/passwd to identify the accounts on the web server.

Query the SA or Web Manager regarding the use of each account and each group.

Vulnerability Key: V0006485

STIG ID: WA140

Release Number: 1**Status:** Active**Short Name:** WA140**Long Name:** Web server content and configuration files are not part of a routine backup program in order to recover from file damage and system failure.**IA Controls:** CODB-1 Data Back-up Procedures
CODB-2 Data Back-up Procedures
CODB-3 Data Back-up Procedures**Categories:** 13.4 Backup & Recovery**Effective Date:** 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: Backing up web server data and web server application software after upgrades or maintenance ensures that recovery can be accomplished up to the current version. It also provides a means to determine and recover from subsequent unauthorized changes to the software and data. A tested and verifiable backup strategy will be implemented for web server software as well as all web server data files. Backup and recovery procedures will be documented and the Web Manager or SA for the specific application will be responsible for the design, test, and implementation of the procedures. The site will have a contingency processing plan/disaster recovery plan that includes web servers. The contingency plan will be periodically tested in accordance with DoDI 8500.2 requirements. The site will identify an off-site storage facility in accordance with DoDI 8500.2 requirements. Off-site backups will be updated on a regular basis and the frequency will be documented in the contingency plan.

Documentable: No**Documentable Explanation:****Potential Impacts:****Responsibility:** System Administrator
Information Assurance Officer
Web Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.7
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)**Checks:** WA140 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine whether or not a tested and verifiable backup strategy has been implemented for web server software as well as all web server data files.

Proposed Questions:

Who maintains the backup and recovery procedures?
 Do you have a copy of the backup and recovery procedures?
 Where is the off-site backup location?
 When was the last time the contingency plan was tested? and is that documented?

If there is not a backup and recovery process for the web server, this is a finding.

NOTE: Backup media containing sensitive data needs to be compliant with DOD Memorandum: "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media", dated 3 Jul 2007.

Vulnerability Key: V0013591

STIG ID: WA155

Release Number: 1

Status: Active

Short Name: WA155

Long Name: Classified web servers are not afforded physical security commensurate with the classification of its content.

IA Controls: PECF-2 Access to Computing Facilities

Categories: 5.9 Device Locations

Effective Date: 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Severity: Category I

Vulnerability Discussion: When data of a classified nature is migrated to a web server, fundamental principles applicable to the safe guarding of classified material must be followed. A classified web server needs to be afforded physical security commensurate with the classification of its content to ensure the protection of the data it houses.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Information Assurance Officer

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9

Checks: WA155 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if a classified web server is afforded physical security commensurate with the classification of its content (i.e., is located in a vault or room approved for classified storage at the highest classification processed on that system).

Proposed Questions:

Ask what the classification of the Web Server is. Based on the classification, evaluate the location of the web server to determine if it is approved for storage of that classification level.

If there is a traditional reviewer available, you can work with them to address specific conditions or questions.

If the web server is not appropriately physically protected based on its classification, this is a finding.

Vulnerability Key: V0013592

STIG ID: WA160

Release Number: 3

Status: Active

Short Name: WA160

Long Name: The server host platform operating system is not utilizing guidance from the appropriate STIGs as well as the Enclave STIG as a method for maintaining a secure configuration.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.9 Documentation

Effective Date: 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Specific policies and requirements that must be followed when implementing a web server. A good plan will address items such as proper hardware selection, software configuration on the server, components to be installed, and security controls to be used. Failure to follow published security guidance will increase the exposure of the host to attack and as a result increase the risk to the applications it is supporting.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3

Checks: WA160 (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the appropriate OS, Technology Specific, and Enclave STIG is being used as a guideline for the secure configuration of the server host platform.

Proposed Questions:

What STIGs are you using to ensure the security of your server?
How do you keep up to date with changes in the STIGs or Checklists?
Ask them to provide evidence to indicate that they are performing self-assessments of the host operating system. This can be via VMS reporting, documented procedures in the SOP, or existence of reports that show the state of vulnerabilities on the system.

If they cannot demonstrate that they are utilizing published security configuration guidance, this is a finding.

Vulnerability Key: V0006487

STIG ID: WA170

Release Number: 6

Status: Active

Short Name: WA170

Long Name: Web server incident response procedures do not exist.

IA Controls: VIIR-1 Incident Response Planning
VIIR-2 Incident Response Planning

Categories: 10.3 Review
13.3 Coop Plans

Effective Date: 29 Jun 2005

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: In the event that an unexpected occurrence disrupts the web server's function, a mechanism will be in place to guide the SA or Web Manager through the process of determining the cause and effect of such an event. This will involve the use of forensic techniques such as log file research as well as file and directory modification analysis.

Documentable: No**Documentable****Explanation:****Potential****Impacts:****Responsibility:** System Administrator
Information Assurance Officer**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4**Checks:** WA170 (Manual)

Query the IAO to determine if a plan or procedures exist to guide the SA or Web Manager through the process of unanticipated event analysis.

In the event that an unexpected occurrence disrupts the web server's function, a mechanism will be in place to guide the SA or Web Manager through the process of determining the cause and effect of such an event. This will involve the use of forensic techniques such as log file research as well as file and directory modification analysis.

If the site does not have procedures or if the SAs are not aware of the procedures, this is a finding.

Vulnerability Key: V0013608**STIG ID:** WA200**Release Number:** 1**Status:** Active**Short Name:** WA200**Long Name:** The site does not have a formal migration plan for removing or upgrading the web server software prior to the date the vendor drops security patch support.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 3.1 Security Patches**Effective Date:** 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II**Vulnerability Discussion:**

The use of unsupported software presents a significant risk to the computing environment. When software is no longer supported by the vendor, patches are no longer supplied for the particular piece of software which can make you vulnerable to attack. Also, unsupported software is normally not included on various vulnerability notices, such as IAVMs and CVEs due to the fact that the vendors are not providing this information since the software is not supported. To prevent the use of unsupported software, the site should have, as part of their

configuration management process, a detail plan for staying up to date with current software versions.

Documentable: No

**Documentable
Explanation:**

**Potential
Impacts:**

Responsibility:

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3

Checks: WA200 (Manual)

Query the IAO to determine if the site has a detail process as part of their configuration management plan to prevent the use of unsupported software.

If the site cannot provide a copy of the migration plan to stay up to date with software versions, this is a finding.

Vulnerability Key: V0013613

STIG ID: WA230

Release Number: 3

Status: Active

Short Name: WA230

Long Name: The site software used with the web server does not have all applicable security patches applied and documented.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 3.1 Security Patches

Effective Date: 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

**Vulnerability
Discussion:**

The IAVM process does not address all patches that have been identified for the host operating system, or in this case, the web server software environment. Many vendors have subscription services available to notify users of known security threats. The site needs to be aware of these fixes and make determinations based on local policy and what software features are installed, if these patches need to be applied. In some cases, patches also apply to middleware and database systems. Maintaining the security of web servers requires frequent reviews of security notices. Many security notices mandate the installation of a software patch to overcome security vulnerabilities. SAs and IAOs should regularly check the OS and application software vendor web sites for information on new security patches that are applicable to their site. All

applicable security patches will be applied to the operating system and web server software. Security patches are deemed applicable if the product is installed, even if it is not used or is disabled.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: Information Assurance Officer

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3

Checks: WA230 - Generic (Manual)

Query the Web Manager to determine if the site has a detailed process as part of their configuration management plan to stay compliant with all security related patches.

Proposed Questions:

How does the SA stay current with vendor patches?

How is the SA notified when a new security patch is issued by the vendor? (Not IAVM)

What is the process followed for applying patches to the web server?

If the site is not in compliance with all applicable security patches, this is a finding.

Vulnerability Key: V0002234

STIG ID: WG040

Release Number: 5

Status: Active

Short Name: WG040

Long Name: A Public Web server has a working connection with a Private asset.

IA Controls: EBPW-1 Public WAN Connection

Categories: 14.5 Physical Layer Security

Effective Date: 08 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion:

This check verifies through checks of the OS and the web server configuration, that the public web server does not have a working connection with a site asset that is not also a public asset. For example, it has been proven that printer rights can be a serious vulnerability to a web server. There are three likely possibilities where a trusted relationship may be established: printers,

directory server or file server. This check does not imply a "Trust" as defined by a Microsoft Domain controller. One way trusts between a database or backup server and the web server are not prohibited by this requirement.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG040 - Windows (Manual)
The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the public web server has a trusted relationship with any systems resource, which is not also accessible to the public.

NOTE: One way trusts between a database or backup server and the web server are not prohibited by this requirement. This check does not imply a "Trust" as defined by a Microsoft Domain Controller.

Navigate to the web server content folders/directories. These directories must not be shared. Right click for Properties of the web server content folder; Select Sharing; all entries must be disabled. If Sharing is selected for any web folder, this is a finding.

Alternative method: from a command prompt type net share and enter. This will provide the available shares.

Also, Check to see if file and printer or file sharing is enabled under the Network icon in the Control Panel. If it is, and a drive, partition, printer or fax device is a shared resource, this is a finding.

Proposed Questions:

Is the public web server a part of the local LAN?

Does the public web server have shares with the local LAN?

If the web server has a trusted relationship with any systems resource, which is not also accessible to the public, then this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability This check verifies through checks of the OS and the web server configuration, that the public

Discussion: web server does not have a working connection with a site asset that is not also a public asset. For example, it has been proven that printer rights can be a serious vulnerability to a web server. There are three likely possibilities where a trusted relationship may be established: printers, directory server or file server. This check does not imply a "Trust" as defined by a Microsoft Domain controller. One way trusts between a database or backup server and the web server are not prohibited by this requirement.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.4
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG040 - Unix (Manual)
Use the command `find / name [filename]` to find such files as: `hosts.equiv`, `.rhosts`, or `.netrc`.

If these files exists and have content, which is in the form of 'hostname username', this implies that a trust relationship exists and this is a finding.

Look for the presence of a print service configuration file by using the command, `find /etc -name hosts.lpd -print`; if this file does not exist, as it will normally be found on older systems, use the command `find /etc -name Systems -print`. The Systems file should be in `/etc/lp`. After finding the configuration file use the more command on it and look for the presence of a '+' character in the first position of a line. For current versions of Solaris this may not matter, but there is no harm in commenting the line out anyway.

If these files exists and have content, this implies that a trust relationship exists and this is a finding.

Vulnerability Key: V0002232

STIG ID: WG050

Release Number: 4

Status: Active

Short Name: WG050

Long Name: The web server password is not entrusted to the SA or Web Manager.

IA Controls: IAAC-1 Account Control

Categories: 1.1 Passwords
1.6 Documentation and Storage

Effective Date: 19 Apr 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server (Target: Netscape Instance 6.1)

Policy: All Policies

MAC /

--	--	--	--

Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
	Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Normally, a service account is established for the web server. This is because a privileged account is not desirable and the server is designed to run for long uninterrupted periods of time. The SA or Web Manager will need password access to the web server to restart the service in the event of an emergency as the web server is not to restart automatically after an unscheduled interruption. Where possible, the account used to run the web server should be a non-privileged account.

Documentable: No**Documentable Explanation:****Potential Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.6
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG050 (Manual)

The reviewer should make a note the name of the account being used for the web service. This information may be needed later in the SRR. There may also be other server services running related to the web server in support of a particular web application. Such services should run as service accounts with a password that is changed annually as well.

Query the SA or Web Manager to determine if they have the web server password(s).

If the web services password(s) are not entrusted to the SA or Web Manager, this is a finding.

NOTE: For IIS installation or other Web Servers that use the LocalSystem account, the password is OS generated, so the SA or Web Manager having an Admin account on the system would meet the intent of this check.

Vulnerability Key: V0002235**STIG ID:** WG060**Release Number:** 3**Status:** Active**Short Name:** WG060**Long Name:** The web server application or system password is not changed at least annually.

IA Controls: IAIA-1 Individual Identification and Authentication
IAIA-2 Individual Identification and Authentication

Categories: 1.1 Passwords**Effective Date:** 08 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	Comments:
--	-----------

☐ Not Reviewed**Condition:** Web Server AND UNIX (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Normally, a service account is established for the web service to run under rather than permitting it to run as system or root. The password on such accounts must be changed at least annually. It is a fundamental tenet of security that passwords are not to be null and not to be set to never expire. Finally, given the nature and proliferation of password cracking tools, the potential for a malicious party to gain access to an atrophied web services account is significant.

Documentable: No**Documentable
Explanation:****Potential
Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran
ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.6

Checks: WG060 (Manual)

This is a query to the IAO and confirmed with the SA and Web Manager or individual in an equivalent role.

Proposed Questions:

What is your policy for service account passwords?
What types of services does this policy apply to?
How often are the service account passwords changed?

If the web services password is not changed at least annually, this is a finding.

NOTE: For IIS or other web server installations that are running as localsystem, the password is changed automatically by the OS every 7 days, so this should be marked as N/A.

☐ Open
☐ Not a Finding
☐ Not Applicable
☐ Not Reviewed

Comments:

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Normally, a service account is established for the web service to run under rather than permitting it to run as system or root. The password on such accounts must be changed at least annually. It is a fundamental tenet of security that passwords are not to be null and not to be set to never expire. Finally, given the nature and proliferation of password cracking tools, the potential for a malicious party to gain access to an atrophied web services account is significant.

Documentable: No**Documentable Explanation:****Potential Impacts:****Responsibility:** System Administrator
Web Administrator

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran
ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE
WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 2.6

Checks: WG060 (Manual)

This is a query to the IAO and confirmed with the SA and Web Manager or individual in an equivalent role.

Proposed Questions:

What is your policy for service account passwords?
What types of services does this policy apply to?
How often are the service account passwords changed?

If the web services password is not changed at least annually, this is a finding.

NOTE: For IIS or other web server installations that are running as localsystem, the password is changed automatically by the OS every 7 days, so this should be marked as N/A.

Vulnerability Key: V0002236**STIG ID:** WG080**Release Number:** 7**Status:** Active**Short Name:** WG080**Long Name:** A compiler will not be installed on a production web server.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 12.4 CM Process**Effective Date:** 08 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition:

Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II**Vulnerability
Discussion:** The presence of a compiler on a production server facilitates the malicious user's task of creating custom versions of programs and installing Trojan Horses or viruses. For example, the attacker's code can be uploaded and compiled on the server under attack. Of particular concern are C compilers.**Documentable:** No**Documentable
Explanation:****Potential
Impacts:****Responsibility:** System Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.3
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)**Checks:** WG080 - Windows (Manual)

Using Windows Explorer, search the system for the existence of known compilers such as msc.exe, msvc.exe, Python.exe, javac.exe, Lcc-win32.exe or equivalent. Look in: all hard drives

Also, query the SA and Web Manager to determine if a compiler is present on the server.

NOTE: This check does not prohibit the use of the .Net Framework. This does not prohibit the use of the java compiler for Oracle.

NOTE: ColdFusion would not be considered a compiler as long as the site is not using the tools for development work.

Any compilers required to be present on the systems need to be restricted to Administrative users only.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II**Vulnerability
Discussion:** The presence of a compiler on a production server facilitates the malicious user's task of creating custom versions of programs and installing Trojan Horses or viruses. For example, the attacker's code can be uploaded and compiled on the server under attack. Of particular concern are C

compilers.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.3
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG080 - Unix (Manual)

UNIX: find / -name gcc -print

find / -name jdk -print

find / -name javac -print

The reviewer may use the command pkginfo -i to determine what applications may have been installed.

Also, query the SA and Web Manager to determine if a compiler is present on the server.

Note: This does not apply to the JDK and Tomcat with Apache using Java Server Pages, the JDK with Netscape or WebObjects, or Oracle and the Visual Studio .Net Framework with .Net server.

NOTE: ColdFusion would not be considered a compiler as long as the site is not using the tools for development work.

Any compilers required to be present on the systems need to be restricted to Administrative users only.

Vulnerability Key: V0002251

STIG ID: WG130

Release Number: 4

Status: Active

Short Name: WG130

Long Name: All utility programs, not necessary for operations, are not removed or disabled.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Effective Date: 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
---------------	-------------------------------------	-------------------------------------	-------------------------------------

Severity: Category III

Vulnerability Discussion: Just as running unneeded services and protocols is a danger to the web server at the lower levels of the OSI model, running unneeded utilities and programs is a danger at the application layer of the OSI model. Office suites, development tools and graphical editors are examples of such programs that are troublesome in two ways. These individual productivity tools have no legitimate place or use on an enterprise, production web server. Such tools are also prone to their own security risks and their existence on a web server adds to the inherent risk of running a web server. Such tools require patch maintenance via a separate track from the web server software and maintaining their patches and hotfixes can expose the web server to additional risks by altering configurations and introducing additional unwanted features and services.

Documentable: No**Documentable Explanation:****Potential Impacts:****Responsibility:** System Administrator
Web Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.3
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)**Checks:** WG130 - WIndows (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the web server is configured with unnecessary software.

The Web Server SA should be questioned to determine if processes other than those that support the web server are loaded and/or run on the web server.

Examples of software that should not be on the web server are all web development tools, office suites, (unless the web server is a private web development server) and compilers, utilities that are not part of the web server suite or the basic operating system.

Check the directory structure of the server and ensure that additional, unintended or unneeded applications are not loaded on the system.

Start >> Programs >> check for programs services such as:

Front Page (as evident by directories which begin _vti)
MS Access
MS Excel
MS Money
MS Word
Third party text editors
Graphics editors

If, after review of the application on the system, the SA cannot provide justification for the requirement of the identified software, this is a finding.

NOTE: If the site requires the use of a particular piece of software, the IAO will need maintain documentation identifying this software as necessary for operations and that the software will be maintained to meet any and all released security patches. In addition, if the software is unsupported, it is not acceptable for use. If this is the case, this should be marked as Not a Finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding	Comments:
---	-----------

☐ Not Applicable

☐ Not Reviewed

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category III

Vulnerability Discussion: Just as running unneeded services and protocols is a danger to the web server at the lower levels of the OSI model, running unneeded utilities and programs is a danger at the application layer of the OSI model. Office suites, development tools and graphical editors are examples of such programs that are troublesome in two ways. These individual productivity tools have no legitimate place or use on an enterprise, production web server. Such tools are also prone to their own security risks and their existence on a web server adds to the inherent risk of running a web server. Such tools require patch maintenance via a separate track from the web server software and maintaining their patches and hotfixes can expose the web server to additional risks by altering configurations and introducing additional unwanted features and services.

Documentable: No

**Documentable
Explanation:**

**Potential
Impacts:**

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.3
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG130 - Unix (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the web server is configured with unnecessary software.

The Web Server SA should be questioned to determine if processes other than those that support the web server are loaded and/or run on the web server.

Examples of software that should not be on the web server are all web development tools, office suites, (unless the web server is a private web development server) and compilers, utilities that are not part of the web server suite or the basic operating system.

Check the directory structure of the server and ensure that additional, unintended or unneeded applications are not loaded on the system.

The command `ps -ef | more` can show what processes (applications) are active on the server. Likely programs may include Open Office, Star Office, Adobe tools or graphics editors.

If, after review of the application on the system, the SA cannot provide justification for the requirement of the identified software, this is a finding.

NOTE: If the site requires the use of a particular piece of software, the IAO will need maintain documentation identifying this software as necessary for operations and that the software will be maintained to meet any and all released security patches. In addition, if the software is unsupported, it is not acceptable for use. In this case, this should be marked as Not a Finding.

Vulnerability Key: V0013617**STIG ID:** WG135**Release Number:** 1**Status:** Active**Short Name:** WG135**Long Name:** Unnecessary services are not disabled on the web server.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 12.4 CM Process**Effective Date:** 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Active services that are not necessary for the operations of the web server will increase the potential attack surface of the web server. These services provide the potential intruder with additional methods of compromising the server and makes the system more vulnerable to attack. Services that are not necessary for the operational mission, will not be active and running on the web server.

Documentable: No**Documentable Explanation:****Potential Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4**Checks:** WG135 - Windows (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the web server is configured with unnecessary services.

Web Server SA should be questioned to determine if services / processes other than those that support the operation of the web server running. This is not limited to the FTP service, you will need to review the active services on the system and question the SA regarding the operational need for anything that may not appear to be required based on the operation purpose of the server.

Examples would be if an HTTP server is running the FTP service when it is not providing that functionality. In this case the FTP should not be running.

From the Services option in Administrative Tools, review the active services for things such as FT, eMail services, collaboration tools, etc.

"Start > Control Panel > Administrative Tools > Services"

If, after review of the application on the system, the SA cannot provide justification for the requirement of the identified service, this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Active services that are not necessary for the operations of the web server will increase the potential attack surface of the web server. These services provide the potential intruder with additional methods of compromising the server and makes the system more vulnerable to attack. Services that are not necessary for the operational mission, will not be active and running on the web server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.4

Checks: WG135 - Unix (Manual)

The reviewer should query the Information Assurance Officer (IAO) SA, Web Manager, Webmaster or developers as necessary to determine if the web server is configured with unnecessary services.

Web Server SA should be questioned to determine if services / processes other than those that support the operation of the web server running. This is not limited to the FTP service, you will need to review the active services on the system and question the SA regarding the operational need for anything that may not appear to be required based on the operation purpose of the server.

Examples would be if an HTTP server is running the FTP service when it is not providing that functionality. In this case the FTP should not be running.

You can do a "ps -ef" to get a list of the active processes on the system. Review these to determine if unnecessary services are running.

If, after review of the application on the system, the SA cannot provide justification for the requirement of the identified service, this is a finding.

Vulnerability Key: V0002246**STIG ID:** WG190**Release Number:** 5**Status:** Active**Short Name:** WG190**Long Name:** The web server is not using a vendor-supported version of the web server software.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 12.4 CM Process**Effective Date:** 10 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Many vulnerabilities are associated with old versions of web server software. As hot fixes and patches are issued, these solutions are included in the next version of the server software. Maintaining the web server at a current version makes the efforts of a malicious user to exploit the web service more difficult.

Documentable: No**Documentable
Explanation:****Potential
Impacts:****Responsibility:** System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG190 - Netscape Windows (Manual)

Server by default is installed in a directory named server4. The file to be examined is ns-httpd.exe.

Right click on this file and select the version tab. Results should be 6.x.

Also, from the Administrative Server screen the version number is apparent. Verified versions of NES/iPlanet or SUN web server 6.x , as seen by right clicking on the ns-httpd.exe file and examining the Properties, Version tab.

NES versions can also be found and verified in the web errors logs entries.

*Note – Netscape Enterprise Server 3.x and 4.x are no longer vendor supported.

If the web server is not using a vendor-supported version of the web server software, this is a finding.

WG190 - Netscape Unix (Manual)

Current versions of web servers are: Netscape Enterprise Server 6.x: iPlanet 6.x , SUN ONE Web Server 6.0, SUN JAVA System Web Server 6.1

You can do the following to determine the version of the web server software:

Netscape: find / -name ns-httpd –print

Move to the directory containing ns-httpd

Run ./ns-httpd –v

If the web server is not using a vendor-supported version of the web server software, this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Many vulnerabilities are associated with old versions of web server software. As hot fixes and patches are issued, these solutions are included in the next version of the server software. Maintaining the web server at a current version makes the efforts of a malicious user to exploit the web service more difficult. Current versions of web servers are: IIS 4.0 for NT, IIS 5.0 and 5.1 for Windows 2000, Netscape 4.x or 6.x for UNIX or NT, and Apache 1.3.26 or later for UNIX. (Apache 2.0.39 for Windows is the only enterprise caliber version available for Windows.)

Documentable: No

Documentable

Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: Web Software NES/iPlanet - Uni (Manual)

Netscape: find / -name ns-httpd –print

Move to the directory containing ns-httpd
Run ./ns-httpd -v

The DoD source for NES (iPlanet) software is: http://netscape.intelligent.net/disa_new/ *Note – Netscape Enterprise Server 3.x and 4.x are no longer vendor supported.

Vulnerability Key: V0002247

STIG ID: WG200

Release Number: 6

Status: Active

Short Name: WG200

Long Name: Non-administrators are allowed access to the directory tree, the shell, or other operating system functions and utilities.

IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data

Categories: 2.2 Least Privilege

Effective Date: 10 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category I

Vulnerability Discussion: As a rule, accounts on a web server are to be kept to minimum. Only administrators, web managers, developers, auditors, and web authors require accounts on the machine hosting the web server. This is in addition to the anonymous web user account. The resources to which these accounts have access must also be closely monitored and controlled. Only the SA needs access to all the system's capabilities, while the Web Manager and associated staff require access and control of the web content and web server configuration files. The anonymous web user account must not have access to system resources as that account could then control the server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG200 - Windows (Manual)

Search all of the systems hard drives for the command.com and cmd.exe files. The allowed permissions on these files are:

System	Full Control
Administrators	Full Control

If any other accounts have any permissions to any command.com or cmd.exe file, this is a Finding.

NOTE: Examine the list of user accounts and determine the group affiliations for the user account in question. Verify with the SA, Web Manager or IAO that the non-administrator accounts are mission essential. If they are mission essential, and this is documented locally, this would not be a finding.

NOTE: CREATOR OWNER would not be a finding if the CREATOR OWNER is an administrative account. If it is not, this is a finding.

To determine account memberships, Right Click on My Computer and select Manage. The Select Local Users and Groups.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category I

Vulnerability Discussion: As a rule, accounts on a web server are to be kept to minimum. Only administrators, web managers, developers, auditors and web authors require accounts on the machine hosting the web server. This is in addition to the anonymous web user account. The resources to which these accounts have access must also be closely monitored and controlled. Only the SA needs access to all the system's capabilities, while the Web Manager and associated staff require access and control of the web content and web server configuration files. The anonymous web user account must not have access to system resources as that account could then control the server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.10
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG200 - Unix (Manual)

Use the command more /etc/passwd to get a list of accounts. Examine the list of user accounts, noting any privileged (ids 0 to 100) UIDs or GIDs (0 to 100). Also examine their shells to see if they are /etc/bin or /etc/sbin.

Verify with the system administrator or IAO that the non-privileged accounts are mission essential.

If there are non-privileged accounts, which are not essential, this is a finding.

Proposed Questions:

If operating system accounts are being used to limit access to a web application, do these accounts have access to other system resources?

Are such accounts in a Group? Does the Group have access to other system resources?

If the IAO has not ensured that web applications restricted by userid and password only permit web users access to the web application and not other operating resources.

If non-privileged accounts are allowed access to the directory tree, the shell, or other operating system functions and utilities, this is a finding.

Vulnerability Key: V0006577

STIG ID: WG204

Release Number: 3

Status: Active

Short Name: WG204

Long Name: Additional services are not installed on a separate partition.

IA Controls: DCPA-1 Partitioning the Application

Categories: 2.2 Least Privilege

Effective Date: 29 Jun 2005

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: To ensure a secure and functional web server, a detailed installation and configuration plan should be developed and followed. This will eliminate mistakes that arise as a result of ad hoc decisions made during the default installation of a server. Planners should not attempt to support multiple services such as Domain Name Service (DNS), e-mail, databases, search engines, and indexing or streaming media on the same server that is providing the web publishing service. In the case of File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transport Protocol (NNTP), a well-defined need for these services should be documented by the IAO prior to their installation on the same platform as a web server. Primary and secondary Domain Controllers, in the Windows environment, will not share a common platform with a web server World Wide Web (WWW) service.

Documentable: No

Documentable Explanation:
Potential

Impacts:**Responsibility:** System Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.3
Web Site Administration Policies & Procedures, With Amendments and Corrections
incorporated in red italics (latest corrections from 11 January, 2002)**Checks:** WG204 (Manual)

Query the SA to ascertain if and where the additional services are installed.

Confirm that the additional service or application is not installed on the same partition as the
operating systems root directory nor the web document root, if it is this is a finding.**Vulnerability Key:** V0002248**STIG ID:** WG220**Release Number:** 4**Status:** Active**Short Name:** WG220**Long Name:** Access to the web administration tool is not restricted to the Web Manager and the Web Manager's
designees.**IA Controls:** ECCD-1 Changes to Data
ECCD-2 Changes to Data**Categories:** 2.2 Least Privilege**Effective Date:** 10 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II**Vulnerability
Discussion:** The key web service administrative and configuration tools must only be accessible by the web
server staff. As these services control the functioning of the web server, access to these tools is
crucial. This would include access to the Web Admin Server in Netscape, the IIS Management
Console, the Apache httpd.conf file or in Oracle, sysadmin.cfg.**Documentable:** No**Documentable
Explanation:****Potential****Impacts:****Responsibility:** Web Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated
in red italics (latest corrections from 11 January, 2002)

Checks: Guide to the Secure Configuration and Administration of Microsoft Internet Information
WG220 - Netcape (Manual)
The Administrative server, requires its own userid and password. This server is to be accessed only by the, SA, Web Manager, Webmaster or their designees. Query site personnel on this point.

If accounts other than the SA and Web Manager or Web Manager designees have access to the web administration tool or equivalent, this is a finding.

Vulnerability Key: V0013687**STIG ID:** WG237**Release Number:** 4**Status:** Active**Short Name:** WG237**Long Name:** Remote authors or content providers are not able to upload files to the DocumentRoot directory without being scanned to ensure no viruses or malicious code exists.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 8.1 Encrypted Data in Transit**Effective Date:** 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Remote web authors should not be able to upload files to the DocumentRoot directory structure without virus checking and checking for malicious or mobile code. A remote web user whose agency has a Memorandum of Agreement (MOA) with the hosting agency and has submitted a DoD form 2875 (System Authorization Access Request (SAAR)) or an equivalent document will be allowed to post files to a temporary location on the server. All posted files to this temporary location will be scanned for viruses and content checked for malicious or mobile code. Only files free of viruses and malicious or mobile code will be posted to the appropriate DocumentRoot directory.

Documentable: No**Documentable Explanation:****Potential Impacts:****Responsibility:** System Administrator
Web Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.6**Checks:** WG237 - Generic (Manual)

Remote web authors should not be able to upload files to the DocumentRoot directory structure without virus checking and checking for malicious or mobile code.

Query the SA to determine if there is anti-virus software active on the server with auto-protect enabled or to determine if there is another process in place for the scanning of files / content being posted by remote authors.

If there is no virus software on the system with auto-protect enabled or if there is not a process in place to ensure all files being posted are being virus scanned before being saved to the document root, this is a finding.

Vulnerability Key: V0002255

STIG ID: WG270

Release Number: 4

Status: Active

Short Name: WG270

Long Name: The web server's htpasswd files (if present) do not reflect proper ownership and permissions.

IA Controls: ECAN-1 Access for Need-to-Know

Categories: 2.2 Least Privilege

Effective Date: 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: In addition to OS restrictions, access rights to files and directories can be set on a web site using the web server software. That is, in addition to allowing or denying all access rights, a rule can be specified that allows or denies partial access rights. For example, users can be given read-only access rights to files, to view the information but not change the files. This check verifies that the htpasswd file is only accessible by system administrators or web managers, with the account running the web service having group permissions of read and execute. htpasswd is a utility used by Netscape and Apache to provide for password access to designated web sites. I

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectin 3.10

Checks: WG270 - Windows (Manual)
Search for the httpasswd.exe file. Right click the httpasswd file, if present. Select the Properties window, select the Security tab.

Examine the access rights for the file. The SA or Web Manager account should have Full Control, the account running the web service should have read and execute permissions.

If entries other than Administrators, Web Manager account, or System are present, this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: In addition to OS restrictions, access rights to files and directories can be set on a web site using the web server software. That is, in addition to allowing or denying all access rights, a rule can be specified that allows or denies partial access rights. For example, users can be given read-only access rights to files, to view the information but not change the files. This check verifies that the httpasswd file is only accessible by system administrators or web managers, with the account running the web service having group permissions of read and execute. httpasswd is a utility used by Netscape and Apache to provide for password access to designated web sites. I

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 3.10

Checks: WG270 - Unix (Manual)

Locate the httpasswd file. Find / -name httpasswd.
Permissions should be r-x r - x - - - (550)

If permissions on httpasswd are greater than 550, this is a finding.

Owner should be the SA or Web Manager account, if another account has access to this file, this is a finding.

Vulnerability Key: V0013619

STIG ID: WG275

Release Number: 2

Status: Active

Short Name: WG275

Long Name: The web server, although started by superuser or privileged account, is not run using a non-privileged account.

IA Controls: ECLP-1 Least Privilege

Categories: 2.2 Least Privilege

Effective Date: 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Running the web server with excessive privileges presents an increased risk to the web server. In the even the web server service is compromised, the context by which the web server is running will determine the amount of damage that may be caused by the attacker. If the web server is run as an administrator or equivalent account, the attacker will gain administrative access through the web server. If on the other hand the web serve is run with least privilege required to function, the capabilities of the attacker will be greatly decreased.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10

Checks: WG275 - Unix Generic (Manual)

The reviewer will need to determine which account the web server is using to run and then determine the privileges that account has. If the account has administrative or super user privilege, then the SA will need to provide justification showing that this type of account is necessary for the function and operation of the web server.

Use the command `ps -ef` to get a list of processes and to determine the account that is being used to run the web server.

Use the command `more /etc/passwd` to examine the account and determine if it is running as a privileged account. If the account has a ID of 100 or greater, the account is not privileged.

If the web server is being run with excessive privileges, this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	Comments:
--	-----------

☐ Not Reviewed**Condition:** Web Server AND Windows (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Running the web server with excessive privileges presents an increased risk to the web server. In the even the web server service is compromised, the context by which the web server is running will determine the amount of damage that may be caused by the attacker. If the web server is run as an administrator or equivalent account, the attacker will gain administrative access through the web server. If on the other hand the web serve is run with least privilege required to function, the capabilities of the attacker will be greatly decreased.

Documentable: No**Documentable
Explanation:****Potential
Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.10**Checks:** WG275 - Windows Generic (Manual)

The reviewer will need to determine which account the web server is using to run and then determine the privileges that account has. If the account has administrative or super user privilege, then the SA will need to provide justification showing that this type of account is necessary for the function and operation of the web server.

Right Click on My Computer and select Manage.

Then Select Local Users and Groups.

Examine the account that is used to run the web server and determine the group affiliations.

If the account has is a member of a privileged group, Administrators, and the web server is running with this account, this is a finding.

Vulnerability Key: V0002256**STIG ID:** WG280**Release Number:** 3**Status:** Active**Short Name:** WG280**Long Name:** The access control files are owned by a privileged web server account.

IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data

Categories: 2.2 Least Privilege**Effective Date:** 11 May 2001☐ Open

Comments:

- ☐ Not a Finding
- ☐ Not Applicable
- ☐ Not Reviewed

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: This check verifies that the key web server system configuration files are owned by the SA or Web Manager controlled account. These same files which control the configuration of the web server, and thus its behavior, must also be accessible by the account which runs the web service. If these files are altered by a malicious user, the web server would no longer be under the control of its managers and owners; properties in the web server configuration could be altered to compromise the entire server platform.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator

Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Sectoin 3.10

Checks: Web Access Control Files NES-U (Manual)

Locate the .htaccess file. find / -name .htaccess and find / -name .nsconfig

Permissions should be rw- r w - - - - (660) or more restrictive

If permissions on .htaccess are greater than 660, this is a finding.

Owner should be the non-privileged web server account or equivalent which runs the web service; however, the group permissions represent those of the user accessing the web site that must execute the directives in .htaccess.

- ☐ Open
- ☐ Not a Finding
- ☐ Not Applicable
- ☐ Not Reviewed

Comments:

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: This check verifies that the key web server access control files, if present, have the proper permissions assigned to them. The files include .htaccess, .nsconfig, and the adminacl or httpacl directory. The presence and use of these files implies a limited or certificate-based web server. While Web Managers, SAs or Webmasters need access to these files and the web service process must be able to read them, there is no need for any other users to have access to these files. These files can be associated with web servers on UNIX and NT systems. A key file which may contain similar information for IIS is metabase.bin and for Oracle is syadmin.cfg.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9

Checks: Web Access Control Files NES-W (Manual)
If the .htaccess.html file is in use, the SA or Web Manager account may have Full Control, the non-privileged web server account running the web service should have read and execute permissions.

If entries other than Administrators, the Web Manager accounts, or System for any degree of access are present, this is a finding.

Vulnerability Key: V0002259

STIG ID: WG300

Release Number: 6

Status: Active

Short Name: WG300

Long Name: Web server system files do not conform to minimum file permission requirements.

IA Controls: ECCD-1 Changes to Data
ECCD-2 Changes to Data

Categories: 2.2 Least Privilege

Effective Date: 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: This check verifies that the key web server system configuration files are owned by the SA or Web Manager controlled account. These same files which control the configuration of the web

server, and thus its behavior, must also be accessible by the account which runs the web service. If these files are altered by a malicious user, the web server would no longer be under the control of its managers and owners; properties in the web server configuration could be altered to compromise the entire server platform.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.9
Web Site Administration Policies & Procedures, With Amendments and Corrections
incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG300 - Netscape Unix (Manual)
Ensure file permissions meet minimum standards

REPRESENTATIVE DIRECTORY NAME	OWNER	GROUP	PERMISSIONS
cgi-bin/all files	root	webadmin	775/775
config/all files	root	webadmin	770/660
htdocs/all files	root	webadmin	775/664
icons/all files	root	webadmin	770/660
logs /all files	root	webadmin	750/640
bin/all files	root	webadmin	750/750

If the file permissions are not at least as restrictive as above, this is a finding.

NOTE: There may be additional directories based the local implementation, and permissions should apply to directories of similar content. Ex. all web content directories should follow the permissions for htdocs.

Vulnerability Key: V0002261

STIG ID: WG330

Release Number: 3

Status: Active

Short Name: WG330

Long Name: A public web server does not limit email to outbound only.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 14.4 Unneeded Ports, Protocols, Hardware, and Services

Effective Date: 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC /

--	--	--	--

Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
Classified		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Incoming E-mail has been known to provide hackers with access to servers. Disabling the incoming mail service prevents this type of attacks. Additionally, Email represents the main use of the Internet. It is specialized application that requires the dedication of server resources. To combine this type of transaction processing function with the file serving role of the web server creates an inherent conflict. Supporting mail services on a web server opens the server to the risk of abuse as an email relay. This check verifies, by checking the OS, that incoming e-mail is not supported.

Documentable: No**Documentable Explanation:****Potential Impacts:****Responsibility:** System Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 5.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG330 - Windows (Manual)
This check verifies, by checking the OS, that incoming e-mail is not supported.

Windows:

Select START >> Programs >> Administrative Tools >> Services

Scroll down and review all the entries. If there is a mail program (SMTP service), then the reviewer must run that program to see if it will accept incoming e-mail. (There are too many different programs for detailed instructions.)

The reviewer should also check the Programs menu and sub-menus under start to see if there are any installed mail programs. The reviewer can also check the Add/Delete programs icon in the Control Panel to see if there are any e-mail programs installed.

If there is an e-mail program installed and that program has been configured to accept inbound e-mail, this is a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)**Policy:** All Policies

MAC / Confidentiality Grid:		I - Mission Critical	II - Mission Support	III - Administrative
Classified		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Incoming E-mail has been known to provide hackers with access to servers. Disabling the incoming

Discussion: mail service prevents this type of attacks. Additionally, Email represents the main use of the Internet. It is specialized application that requires the dedication of server resources. To combine this type of transaction processing function with the file serving role of the web server creates an inherent conflict. Supporting mail services on a web server opens the server to the risk of abuse as an email relay. This check verifies, by checking the OS, that incoming e-mail is not supported.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 5.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG330 - Unix (Manual)

This check verifies, by checking the OS, that incoming e-mail is not supported.

UNIX:

Use the command `ps -ef | grep sendmail` to see if the sendmail daemon has been started on the system.

If there is an e-mail program installed and that program has been configured to accept inbound e-mail, this is a finding.

Vulnerability Key: V0013620

STIG ID: WG355

Release Number: 2

Status: Active

Short Name: WG355

Long Name: A private web server's list of CAs considered trusted is not limited to those with a trust hierarchy that leads to the DoD PKI Root CA or to an approved External Certificate Authority (ECA) or are required for the server to function.

IA Controls: IATS-1 Token and Certificate Standards
IATS-2 Token and Certificate Standards

Categories: 1.2 PKI

Effective Date: 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Severity: Category II

Vulnerability Discussion: A PKI certificate is a digital identifier that establishes the identity of an individual or a platform. A server that has a certificate provides users with third-party confirmation of authenticity. Most web browsers perform server authentication automatically; the user is notified only if the authentication fails. The authentication process between the server and the client is performed using the SSL/TLS protocol. Digital certificates are authenticated, issued, and managed by a trusted Certification Authority (CA). The use of a trusted certificate validation hierarchy is crucial to the ability to control access to your server and prevent unauthorized access. This hierarchy needs to lead to the DoD PKI Root CA or to an approved External Certificate Authority (ECA) or are required for the server to function.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.12.1

Checks: WG355 - Generic (Manual)

The reviewer will need to have the SA or Web Manager show the list of CA's the server is trusting to authenticate users. The procedure to do this could vary by the web server product and Operating System that is being used.

The PKE InstallRoot 3.0 System Administrator Guide (SAG), dated 9 Nov 2006, contains a complete list of DoD, ECA, and IECA CAs.

NOTE: There are non DoD roots that must be on the server in order for it to function. Some applications, such as anti-virus programs, require root CAs to function.

If the trusted CAs that are used to authenticate users to the web site does not lead to an approved DoD CA, this is a finding.

Vulnerability Key: V0002225

STIG ID: WG370

Release Number: 5

Status: Active

Short Name: WG370

Long Name: /bin/csh or /bin/sh is configured as a viewer for documents of type application/x-csh, application/x-sh, on the UNIX server.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Effective Date: 12 Nov 1999

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Users should not be allowed to access the shell programs. Shell programs might execute shell escapes and could then perform unauthorized activities which could damage the security posture of the web server. A shell is a program that serves as the basic interface between the user and the operating system. In this regard, there are shells which are security risks in the context of a web server and which are unauthorized in the context the Secure Features Users Guide.

Documentable: No**Documentable
Explanation:****Potential
Impacts:****Responsibility:** System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.1
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG370 Unix (Manual)
For Unix Systems Only.

Locate the Apache httpd.conf directory under the server root directory. Search the httpd.conf file for the presence of the following directives:

Action
AddHandler

If either of these exist and they configure /bin/csh, or any other shell as a viewer for documents, this is a finding.

If either do not exist, or they are not defining shells as viewers, this is not a finding.

Vulnerability Key: V0002266**STIG ID:** WG380**Release Number:** 5**Status:** Active**Short Name:** WG380**Long Name:** Vulnerable programs have not been removed from the web server.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 11.4 Disposition**Effective Date:** 17 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	----------------------------------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Several filenames and programs designed to enhance web functionality have been identified in connection with the intrusions and vulnerabilities specific to web servers. The presence of any of these files on your system should be reviewed carefully because they indicate that the web server is vulnerable to well-known malicious exploits. In many cases these vulnerabilities are found in the example installed with systems. More recently, trojans have been copied to web servers via a corrupt web request which compromises the contents of main memory on the server. Microsoft Internet Information Server (IIS) web sites can be configured to allow password change requests from remote users. By sending a malformed request to "_AuthChangeUrl", a remote attacker can cause a denial of service attack against IIS. When this attack is performed against IIS 4.0, the program stops servicing requests completely, and CPU utilization increases to 100 percent. IIS 5.0 is not as severely affected, although it stops responding to password change requests.

Documentable: No**Documentable****Explanation:****Potential****Impacts:****Responsibility:** System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.1
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG380 - Windows (Manual)

Query the SA to determine if all directories that contain vulnerable programs have been removed from the server.

If any vulnerable programs are found on the web server, this is a finding.

NOTE: Examples of vulnerable scripts and programs include the following:

- TextCounter Versions 1.0 - 1.2 (PERL) and 1.0 - 1.3 (C++)
- guestbook.cgi
- bndform.cgi
- Cachmgr.cgi
- Classified.cgi
- Count.cgi
- dumpenv.pl
- Excite Web Search Engine
- mail-lib.pl
- Glimpse (PERL scripts) Web Search Engine
- info2www, Versions 1.0-1.1
- Webdist.cgi
- php.cgi
- files.pl
- nph-test.cgi
- nph-publish
- FormMail (PERL scripts)
- “phf” phone book script

Executables specific to Windows platform :

- ntalert.exe

-syslogged.exe
 -tapi.exe
 -20.exe
 -21.exe
 -25.exe
 -ecware.exe
 -nc.exe
 -80.exe
 -139.exe
 -1433.exe
 -1520.exe
 -26405.exe
 -i.exe
 -newdsn.exe
 -notworm
 -readme.exe
 -Wink<random characters>.exe

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Several filenames and programs designed to enhance web functionality have been identified in connection with the intrusions and vulnerabilities specific to web servers. The presence of any of these files on your system should be reviewed carefully because they indicate that the web server is vulnerable to well-known malicious exploits. In many cases these vulnerabilities are found in the example installed with systems. More recently, trojans have been copied to web servers via a corrupt web request which compromises the contents of main memory on the server.

Documentable: No

Documentable Explanation:

Potential Impacts:

Responsibility: System Administrator
Web Administrator

References: Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG380 - Unix (Manual)

Query the SA to determine if all directories that contain vulnerable programs have been removed from the server.

If any vulnerable programs are found on the web server, this is a finding.

NOTE: Examples of vulnerable scripts and programs include the following:

-TextCounter Versions 1.0 - 1.2 (PERL) and 1.0 - 1.3 (C++)
 -guestbook.cgi
 -bndform.cgi
 -Cachmgr.cgi
 -Classified.cgi
 -Count.cgi
 -dumpenv.pl
 -Excite Web Search Engine
 -mail-lib.pl
 -Glimpse (PERL scripts) Web Search Engine
 -info2www, Versions 1.0-1.1
 -Webdist.cgi
 -php.cgi
 -files.pl
 -nph-test.cgi
 -nph-publishphp.cgi
 -FormMail (PERL scripts)
 -"phf" phone book script

Execute a find command for the above files and if any are found, this is a finding.

Vulnerability Key: V0013621

STIG ID: WG385

Release Number: 1

Status: Active

Short Name: WG385

Long Name: All web server documentation, sample code, example applications, and tutorials have not been removed from a production web server.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 12.4 CM Process

Effective Date: 27 Apr 2007

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category I

Vulnerability Discussion: Delete all directories that contain samples and any scripts used to execute the samples. If there is a requirement to maintain these directories at the site on non-production servers for training purposes, etc., have NTFS permissions set to only allow access to authorized users, i.e., Web Admins and Administrators. Sample applications or scripts have not been evaluated and approved for use and may introduce vulnerabilities to the system.

Documentable: No

Documentable**Explanation:****Potential****Impacts:**

Responsibility: System Administrator
Information Assurance Officer
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.3

Checks: WG385 (Manual)
Query the SA to determine if all directories that contain samples and any scripts used to execute the samples have been removed from the server.

Each web server has its own list of sample files and this may change as with the software versions, but following are some examples of what to look for. (This should not be the definitive list of sample files, this is just an example of the common samples that are provided with the associated web server. This list will be updated as additional information is discovered):

IIS: \inetpub\iissamples*. *
Apache: \apache\manual*. *

If there is a requirement to maintain these directories at the site for training purposes, etc., have permissions set to only allow access to authorized users, i.e., WebAdmins and administrators

If any sample files are found on the web server, this is a finding.

NOTE: For IIS installations, the presence of the Adminscripts directory would not be a finding if the permissions were restricted to Administrators and WebAdmins.

Vulnerability Key: V0002230

STIG ID: WG420

Release Number: 7

Status: Active

Short Name: WG420

Long Name: Backup interactive scripts are present on the system.

IA Controls: ECSC-1 Security Configuration Compliance

Categories: 2.2 Least Privilege

Effective Date: 01 Dec 1999

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Copies of backup files will not execute on the server, but can be read by the anonymous user if special precautions are not taken. Such backup copies contain the same sensitive information as the actual script being executed and as such are useful to malicious users. Techniques and systems exist today which search web servers for such files and are able to exploit the information contained in them. Backup copies of files are automatically created by some text editors such as emacs and edit plus. The emacs editor will write a backup file with an extension ~ added to the name of the original file; edit plus will create a .bak file. Of course, this would imply the presence and use of development tools on the web server, a finding under WG130. Having backup scripts on the web server provides one more opportunity for malicious persons to view these scripts and use information found in them.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator

Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG420 - Windows (Manual)

Find on all hard drives *.bak, *.old, *.temp, *.tmp, *.backup, or 'copy of..'

Once the files are found, the reviewer must determine if the files are in the document or home directory of the web sever.

If files with these extensions are in this directory this is a finding. If not the reviewer must make a determination as to the relationship said file or files has with the web server.

If the files are stored in a repository (not in the document root) as backups for the web server this is also a finding.

If the files have no relationship with web activity, such as a backup batch file for operating system utility, this is not a finding.

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND UNIX (Target: Netscape Instance 6.1)

Policy: All Policies

MAC / Confidentiality Grid:

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Copies of backup files will not execute on the server, but can be read by the anonymous user if special precautions are not taken. Such backup copies contain the same sensitive information as the actual script being executed and as such are useful to malicious users. Techniques and systems exist today which search web servers for such files and are able to exploit the information contained in them. Backup copies of files are automatically created by some text editors such as emacs and edit plus. The emacs editor will write a backup file with an extension ~ added to the

name of the original file; edit plus will create a .bak file. Of course, this would imply the presence and use of development tools on the web server, a finding under WG130. Having backup scripts on the web server provides one more opportunity for malicious persons to view these scripts and use information found in them.

Documentable: No

Documentable

Explanation:

Potential

Impacts:

Responsibility: System Administrator
Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2
Web Site Administration Policies & Procedures, With Amendments and Corrections incorporated in red italics (latest corrections from 11 January, 2002)

Checks: WG420 - Unix (Manual)

Search for backup copies of CGI scripts on the web server or ask the SA or Web Admin if they keep backup copies of CGI scripts on the web server.

Common backup extensions are: *.bak, *.old, *.temp, *.tmp, *.backup, *.???. This would also apply to .jsp files.

```
UNIX: find /      name "*.bak" -print
      find /      name "*.*" -print
      find /      name "*.old" -print
```

Once the files are found, the reviewer must determine if the files are in the document or home directory of the web sever.

If files with these extensions are in this directory this is a finding. If not the reviewer must make a determination as to the relationship said file or files has with the web server.

If the files are stored in a repository (not in the document root) as backups for the web server this is also a finding.

If the files have no relationship with web activity, such as a backup batch file for operating system utility, this is not a finding.

Vulnerability Key: V0002271

STIG ID: WG440

Release Number: 4

Status: Active

Short Name: WG440

Long Name: Monitoring software does not include CGI or equivalent programs in the set of files which it checks.

IA Controls: ECAT-1 Audit Trail, Monitoring, Analysis and Reporting
ECAT-2 Audit Trail, Monitoring, Analysis and Reporting

Categories: 12.4 CM Process

Effective Date: 25 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: By their very nature, CGI type files permit the anonymous web user to interact with data and perhaps store data on the web server. In many cases CGI scripts exercise system level control over the servers resources. Thus these files make appealing targets for the malicious user. If these files can be modified or exploited, the web server can be compromised. These files must be monitored by a security tool that reports unauthorized changes to these files.

Documentable: No**Documentable
Explanation:****Potential
Impacts:****Responsibility:** System Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.2**Checks:** WG440 (Manual)

CGI or equivalent files must be monitored by a security tool that reports unauthorized changes. It is the purpose of such software as to monitor key files for unauthorized changes.

The reviewer should query the IAO, SA and Web Manager or Webmaster on this point and verify the information provided by asking to see the template file or configuration file of the software being used to accomplish this security task.

Example file extensions for files considered to provide active content are, but not limited to: .cgi, .asp, .aspx, .class, .vb, .php, .pl, .c.

If the site does not have a process in place to monitor changes to CGI program files, this is a finding.

Vulnerability Key: V0002264**STIG ID:** WG470**Release Number:** 3**Status:** Active**Short Name:** WG470**Long Name:** Wscript.exe and Cscript.exe are accessible by users other than the SA and Web Manager.**IA Controls:** ECCD-1 Changes to Data
ECCD-2 Changes to Data**Categories:** 2.2 Least Privilege**Effective Date:** 11 May 2001

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Web Server AND Windows (Target: Netscape Instance 6.1)**Policy:** All Policies**MAC /
Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Severity: Category II

Vulnerability Discussion: Windows Scripting Host (WSH) is installed under either a Typical or Custom installation option of a Microsoft Network Server. This technology permits the execution of powerful script files from the Windows NT command line. This technology is also classified as a Category I Mobile Code. If the access to these files is not tightly controlled, a malicious user could readily compromise the server by using a form to send input to these scripting engines. This is a web related vulnerability which could exist on any NT / Win 2000 system regardless of the web server software being used on the platform.

Documentable: No**Documentable
Explanation:****Potential
Impacts:****Responsibility:** System Administrator**References:** WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 4.11
Guide to the Secure Configuration and Administration of Microsoft Internet Information**Checks:** WG470 (Manual)

Start >> Find >> Files and Folders >> Search for instances of Wscript.exe and Cscript.exe

Move to these files, if found, and right click on them to view their Properties.

Permissions should only exist for System, the SA and Web Manager, who may have Full Control. User accounts with access to these files that are unknown or unintended to the SA or Web Manager should be removed.

If these files have permission for others than SA, System, or Web Manager, this is a finding.

Vulnerability Key: V0006724**STIG ID:** WG520**Release Number:** 3**Status:** Active**Short Name:** WG520**Long Name:** Web server and/or operating system information is advertised.**IA Controls:** ECSC-1 Security Configuration Compliance**Categories:** 11.2 Dissemination**Effective Date:** 29 Jun 2005

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

Condition: Netscape Instance (Target: Netscape Instance 6.1)

Policy: All Policies

MAC /

**Confidentiality
Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sensitive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Severity: Category III

**Vulnerability
Discussion:** The web server response header of an http response can contain several fields of information including the requested html page. The information included in this response can be web server type and version, operating system and version, and ports associated with the web server. This provides the malicious user valuable information without the use of extensive tools.

Documentable: No

**Documentable
Explanation:**

**Potential
Impacts:**

Responsibility: Web Administrator

References: WEB SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE Section 3.2
Guide to the Secure Configuration and Administration of Microsoft Internet Information

Checks: WG520 - Netscape (Manual)

Use explorer, filemanager or command line utility to locate the magnus.conf file for the given web site. Default location should be:

Default Windows location: \netscape\servers\%server name%\config\
Default UNIX location: /user/netscape/servers/%server name%/config/

Look for the existence of the ServerString directive. The ServerString directive has been added to allow administrators to change the Server header in a response. The String none, will cause the header to not be sent at all or it can be modified to give erroneous information.

Example:

```
ServerString "My Server ver. 1.0"  
ServerString none
```

One of two conditions must be met:

1. The ServerString directive is set to none
2. The ServerString directive is set to provide invalid information

If the web server or operating system information are sent to the client via the server response header, this is a finding.

Vulnerability Count - 35