# Global Information Assurance Certification Paper

**Internet Information Server Security Assessment: An Essential Audit**

Patricia Martinez

GSEC Version 1.2b

April 4, 2001

Information is the most valuable asset and resource to an organization. Securing your organization's system is an essential responsibility of a security professional. One must implement confidentiality, integrity and availability at all times. Confidentiality is making sure that only the authorized person or group can access particular information. Integrity is ensuring that sensitive information has not been changed or modified. Availability is having information accessible to authorized parties at reasonable times. The three principles are fundamental when offering services over the Internet. Failure to implement all three would result in loss of resources, a loss in revenue and a tainted reputation for an organization.

A security assessment aids in checking for confidentiality, integrity and availability. It is a set of procedures performed on a server that detects whether or not any possible vulnerabilities exist. This document will describe methods used when assessing an Internet Information Server. Internet Information Server (IIS) is web server that runs internet services on Microsoft's Windows NT and Windows 2000 server operating systems.

This paper will explain basic procedures that should be applied when auditing an organization's IIS web server. It is divided into four sections for easier comprehension and perusing. The first is Defining The Process, which will explain the reconnaissance methods that should be used. The second section, Performing The Assessment, will mention a few readily available tools. Reporting The Results, the third section, will include a sample report that should be complied for documentation purposes. The last section, Obtaining Permission, will explain how to obtain authorization in order to perform a security assessment on a web server.

One should perform a security assessment on an IIS server after the initial configuration and the appropriate patches and hot fixes have been applied to the server. At that point, the assessment will verify whether or not the server is properly secure. OK, so lets get started.

## DEFINING THE PROCESS

The following are basic reconnaissance procedures that should be performed:

- ICMP Test
- CGI Scan
- Port Scan

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol is a set of applications most commonly used for troubleshooting. Ping and Traceroute are the two applications associated with ICMP. Ping is a handy tool that will uncover a particular domain name's IP address and inform the user whether or not a server can accept request. It does this by sending a packet to a designated address and waiting for a response. The host will respond with an ICMP echo reply indicating that the server is alive. If there is no reply it is possible that the host does not exist or is down.

Traceroute records the path through the Internet between the requesting computer and the designated computer. It sends a packet to the first router and reports back. It continues to send packets to the remaining routers and reports each "stop". Each stop that is reported back is referred to as hop. Traceroute is a handy tool to use when trying to determine a network's infrastructure. The hops will list everything in front of the server such as the internet service provider, the router or the firewall associated with that particular server.

Common Gateway Interface (CGI)

Common Gateway Interface is the method of passing data back and forth between a web server and an application. It is part of the Hypertext Transfer Protocol (HTTP). It simply takes the information that is to be passed from the web server and sends it to the application program. The data is then processed and a confirmation is sent back to the web server.

CGI Scan

Microsoft Internet Information Server (IIS) contains several exploitable CGI scripts. By performing a CGI scan on a web server one will be able to see the exploitable scripts that are running. It is dangerous to have particular scripts running on the web server. If such script code was revealed a user could analyze the script for security holes, uncover the names and/or IP addresses of other servers that are hidden from the public or find out usernames and passwords required for script execution. IIS sample files contain many dangerous scripts. Below is a list of commonly exploited scripts:

- msadcs.dll
- showcode.asp
- viewcode.asp
- codebrws.asp
- winmsdp.exe

IIS also contains extensions such as .htr, .ida, .idc and idq. By appending these extensions to the end of a URL address sensitive information will be returned to the browser. It is always a good idea to remove the CGI scripts and file extensions that are not being used by the web server during the set up phase. The threat of attack will be greatly reduced.

Port Scan

A port is a connection place that uses TCP/IP to connect to a particular program on a server. There can be as many as 65,536 different ports or services. Ports are numbered from 0 to 65,535 and are normally divided into two categories. Ports ranging from 0 to 1023 are known as trusted or reserved ports. Ports 1024 and above are called ephemeral ports. Trusted ports normally have an assigned service running on it whereas ephemeral ports will usually have any service running on it.

A port scan is a process in which a message is sent to each port one at a time. The type of response received will indicate whether or not a particular port is being used. A port can be in an open, closed or filtered state. Below is a list of common ports.

| Port | Service |
|---|---|
| 7 | ECHO |
| 19 | CHARGEN |
| 21 | FTP |
| 23 | TELNET |
| 25 | STMP |
| 53 | DNS |
| 79 | FINGER |
| 80 | HTTP |
| 110 | POP |
| 137 | NETBIOS |
| 139 | NETBIOS |
| 443 | HTTPS |

PERFORMING THE ASSESSMENT

There are many available tools that can be use to perform a security assessment on an IIS web server. This section will mention the ones that are easily attainable, most accurate and provide clear results. It is important to familiarize oneself with these tools and functions on a test server before running them on a production IIS web server.

Whisker

Whisker is a web scanner that searches for commonly known CGI vulnerabilities. It is completely free and available at http://packetstorm.securify.com. Whisker uses anti-intrusion detection system tactics. It sends packet requests that confuse the IDS but allows the web server to understand it. It will report back what version of IIS is running and the vulnerable scripts that are detected.

Whisker is easy to use and extremely reliable. The results are also reported in a clear format. If exploitable CGI scripts are detected while running a Whisker scan, it is recommended one immediately removes those files from the web server.

Nmap

Nmap is a utility used for security auditing. It is cost free and open source, which means one is able to review the code and customize it. Nmap originated as a port scanner but now gathers more information as well. It will determine which hosts are up, what services are running on the host and identify the operating system the host is using. Nmap scanning techniques are adjustable. One can perform a TCP connect port scan, TCP SYN port scan, UDP port scan and ping scan. As well as timing one's scan as Paranoid, Sneaky, Polite, Normal, Aggressive or Insane. Nmap has many options and it is fun to use.

It clearly reports the scanning results as well. According to Brent Deterding, "It is an extremely versatile and useful information gathering tool that yields much of the necessary information about a machine and it's possible weaknesses." For specific information regarding Nmap, please refer to his practical Nmap - The Tool, It's Author and It's Implications.

NESSUS

Another auditing utility available is Nessus. Nessus is a free, open source and up-to-date tool. This tool will remotely audit a network by searching for security holes. Nessus allows one to specify an IP range and to search for particular vulnerabilities. If it detects a vulnerability, it will not only report the findings but also go a step further and try to exploit the security hole as well.

Nessus reports are complete and accurate. The report will list the security holes found and include recommendations on how to fix them. Greg Brooks states, "The issues that are found are reported as either informational, security warning or security holes and the risk factor of the problem is also identified by words such as 'Low' or 'Serious'." For a deeper look into Nessus, please refer to his practical Nessus-Get on Board or Nessus-A Very Capable Security Tool by Vernon Stark. Both practicals are wonderful resources if one is interested in finding out more information about Nessus.

REPORTING THE RESULTS

After the security assessment has been performed, the results should be documented and archived. Below is a sample executive summary of a security assessment.

# Security Assessment

A security audit was performed on the external IP X.X.X.X. This document will summarize the status of the server tested. If any vulnerabilities were detected a recommendation on how to fix the vulnerability would also be included. The network vulnerability scan was performed using a default security policy.

## Firewall Status

| Port | State | Service |
|---|---|---|
| 21/tcp | open | ftp |
| 25/tcp | open | stmp |
| 80/tcp | open | http |
| 139/tcp | open | netbios |
| 443/tcp | open | https |
| 6667/tcp | open | irc |

Recommendation:

*It is recommended that only the necessary ports such as 80 (http) and 443 (https) are left open to the public. This will reduce the risk of someone gaining unauthorized access to the web server.*

## CGI/Dangerous Script Status

The server was currently scanned for over 200 known possible vulnerabilities. At this time the following vulnerable CGI scripts and extension were detected:

-msadcs.dll
-showcode.asp
-.idq
-.htr

Recommendation:

*It is highly recommended that CGI scripts and extensions found be deleted from the web server. This will reduce the risk of someone obtaining sensitive information from the web server.*

**Confidential Information:**
This report contains confidential information intended for MyCompany.com. Do not release these results to any unauthorized parties.

## OBTAINING PERMISSION

A policy that states who has authority to run an assessment on the Internet Information Server and when the sever will be assessed should be implemented. The policy should also be signed by management to verify that permission has been granted to run the utilities in a production environment.

It is essential to run a security assessment after the initial configuration. It is just as vital to run the utilities routinely and after any modifications have been made to the server. A security assessment is a necessary checkpoint when running service over the Internet. Making an Internet Information Server less vulnerable reduces unwanted exposure and lessens the threat of an attack.

Enjoy the exploration of new security assessment tools and remember to keep abreast of current security announcements and new developments. Security holes are constantly discovered and exploited. An informative security professional is a tremendous asset to an organization.

## REFERENCES


Brooks, Greg. "Nessus-Get On Board." 15 February 2001.
URL: http://www.sans.org/infosecFAQ/audit/nessus2.htm (March 15, 2001)

Deterding, Brent. "Nmap-The Tool, It's Author and It's Implications." 13 July 2000.
URL: http://www.sans.org/infosecFAQ/audit/nmap.htm (March 15, 2001)

Ekotech. "TCP/UDP Port Numbers."
URL: http://www.ekotech.com/TCPUDP.htm (March 12, 2001)

Insecure. "NMAP -The Network Mapper."
URL: http://www.insecure.org/nmap/ (March 14, 2001)

Nessus. "Introduction."
URL: http://www.nessus.org/ (March 14, 2001)

NetworkICE. "Port Knowledgebase."
URL: http://networkice.com/advice/exploits/ports/default.htm (March 12, 2001)

Rain Forest Puppy. "A Look at Whisker's Anti-IDS tactics"
URL: http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html (March 13, 2001)

Stark, Vernon. "Nessus-A Very Capable Auditing Tool." 6 August 2000.
URL: http://www.sans.org/infosecFAQ/audit/nessus.htm

Techtarget. "The IT-Specific Encyclopedia"
URL: http://whatis.techtarget.com (March 11, 2001)