GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

© SANS Institute 2000 - 2005, Author retains full rights.

Information Assurance at the PC Level

by Carlton Bowen

GIAC Security Essentials Practical
Version 1.2f
December 10, 2001

© SANS Institute 2000 - 2005 Author retains full rights.

Information Assurance at the PC Level
Carlton Bowen
December 10, 2001

Introduction

Information security is often approached by an organization from the top down, with a solitary measure at each level. For example, a company may attempt to secure the network level with a firewall, the server level with password authentication, and the personal computer (PC) level with virus scan software. Due to the larger number of PC's (or workstations) in typical organizations, compared to servers for example, and the fact that workstations are often viewed as less critical or non critical resources, security at the PC level may be dearth or non-existent. On the other hand, each workstation presents a risk to the IT infrastructure in that it may be used to gain unauthorized access to organization resources, utilize those resources in an undesirable way (e.g. to launch Distributed Denial of Service attacks), and introduce unwanted (and possibly malicious) software.

This paper contemplates a bottom up approach to information security, where attention is given to information assurance at the PC level initially, rather than as an after thought. Information assurance for an individual PC is examined within the context of threat vectors, with an emphasis on risk mitigation and how to achieve it. Basic security measures are enumerated for each threat vector with a "how to" approach.

The information security field and information technology in general are always evolving, so the information presented herein is by no means all inclusive. Rather, security at the PC level is explored within a structured framework in an attempt to elucidate basic security concepts and to demonstrate some of the current applications of those concepts.

Basic Security Concepts

Information assurance is defined as: "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities".[1] Less formally and in the present context, providing information assurance means taking the actions necessary to protect a PC and the information on it from unauthorized access and use while maintaining its availability and integrity for authorized use.

One way to approach information assurance is with the **Protect, Detect, React model** (implied in the above definition of information assurance). The first step is "Protect", and involves hardening the PC, or implementing defensive measures on the PC or computer system to make it more resistant to attack. The second step is "Detect", and involves detecting when an

© SANS Institute 2000 - 2005, Author retains full rights.

attack has occurred or is occurring. The third step is "React"; it is the action taken to maintain information assurance on a PC or computer system when the system has been or is being attacked. Another step that might be considered part of the "React" step, is recovery. Recovery is carried out to restore information assurance to a PC or computer system that has been compromised.

Threat Vectors are different areas an attack may come from. The five basic threat vectors are: 1) Outsider Attack from Network, 2) Outsider Attack from Telephone, 3) Insider Attack from Local Network, 4) Insider Attack from Local System, and 5) Attack from Malicious Code.[2] Numerous known attacks exists for each threat vector. For example, consider the hundreds of viruses (one type of malicious code) listed as "in the wild" at http://www.virusbtn.com/WildLists/. When implementing information assurance at the PC level each threat vector should be considered.

Risk mitigation means reducing or eliminating risk. A basic concept that helps mitigate risk is "**defense in depth**". Defense in depth means having multiple layers of defense, so if one layer is penetrated another intact layer of protection is encountered. Defense in depth leads to more robust security.

Another basic security concept that helps to mitigate risk is the "**principle of least privilege**". The principle of least privilege means only having the rights granted and the services installed necessary to do the job. Traditionally the principle of least privilege dealt with user rights, for example whether a particular user ID was granted rights to read or write changes to a specific file or folder. The principle of least privilege can also be applied more broadly, to include, for example, installed services. An example is the Internet Information Server (IIS) service that comes with Windows 2000. If the Windows 2000 workstation is not being used as a web server, the principle of least privilege suggests the IIS service should not be started or enabled.

Scenario

One way to examine information assurance at the PC level is to consider a PC by itself. To do this a scenario will be used where an individual user of a PC has full administrative rights and responsibilities for that PC. This scenario is likely in many typical settings, for example in a law office, a software development company (or other IT based business where users have a lot of IT knowledge and leeway in administering their own desktop/laptop environments), or a small office/home office environment. In this scenario, the PC might be a laptop or desktop computer that is using the Microsoft Windows 2000 operating system. The user has dial up access to the internet and a network connection to a LAN with internet access. Security measures for the LAN, such as a network firewall, are not considered; only security measures for the individual PC are considered in this scenario.

Using this scenario the five primary threat vectors will be examined and basic security

© SANS Institute 2000 - 2005

Author retains full rights.

concepts will be applied. The hope is that by looking at some of the current basic security practices for this operating system and scenario, greater information assurance at the PC level can be achieved.

A Graphical View of the scenario

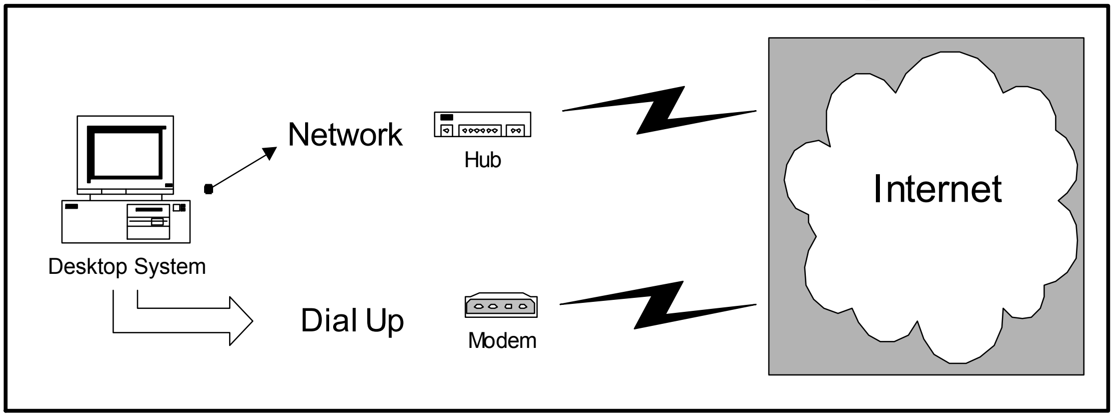

Figure 1

Threat Vector 1 - Outsider Attack from Network

Just about daily new vulnerabilities for an operating system are found and posted to the internet. Therefore one of most basic protections for a PC is to keep the OS up to date with patches and fixes for these known vulnerabilities. This is an ongoing task. Just because the OS starts out up-to-date by no means ensures it will be up-to-date the next day, the next week, the next month, or the next year.

How often to check for new updates is a matter of security policy. The user will want to have a security policy that addresses this issue in the given scenario because the user is responsible for administering his own PC. The entry in a security policy for this area could be as simple as "check Microsoft's web site at least monthly for critical updates and security fixes. Review and install them as appropriate."

How To:

1. Go Microsoft's web site at http://www.microsoft.com/windows2000/downloads/default.asp
2. Click on "Service Packs" and make sure you have the most recent one installed (SP2 as of Nov 2001)
3. Do the same for the "Critical Updates" and the "Advanced Security Updates" links.
   Note: You will have to install "Critical Updates" and "Advanced Security Updates" one by one.

© SANS Institute 2000 - 2005

Author retains full rights.

4. After selecting the update you want to install, in the upper right hand corner make sure the correct language is selected and click "GO".
5. In most cases you will download a file, then manually go to that file location and execute the file to install the update.
6. Service Pack level can be determined by right clicking on "My Computer", then selecting "Properties". The "General" tab displays the OS level, including Service Pack, under the "System" section.
7. Installed Critical Updates and Advanced Security Updates can be determined by clicking Start > Settings > Control Panel. Double click "Add/ Remove Programs". Installed updates are listed as "Windows 2000 Hotfixes".
Note: Internet Explorer and Microsoft Office products should also be kept up to date.[3]

Additional measures to both protect and detect should also be implemented to help establish defense in depth on the system. One valuable tool to do this is a host based Intrusion Detection System (IDS).

There are several host based IDS's and personal firewalls on the market today, such as "NetworkIce" from Internet Security Systems (http://www.networkice.com/products/soho_solutions.html) and "Zone Alarm" from Zone Labs (http://www.zonelabs.com). Well known product vendors such as Symantec (http://www.symantec.com/sabu/nis/npf) and McAfee (http://www.mcafee.com/myapps/firewall/ov_firewall.asp) also offer products in this category.

How To:

1. There is no substitute for doing the necessary homework. Available products should be researched and evaluated before making a final decision. Some examples of what to look for and consider can be found in Tina Zych's "Personal Firewalls: What are they, how do they work?"[4]
2. Most vendors offer a trial version of their IDS products. "Try before you buy" is a good idea.
3. Once an IDS has been selected and installed, become familiar with how to change the default configuration. The principle of least privilege should be applied when determining security settings -- only what is needed should be allowed. Adjustments to the settings can be made later as necessary.
4. Become familiar with the alert messages and what they mean.
5. The security policy should have in it what to do when an attack is underway. One possible approach is outlined by Chris Morris in "What Do You Do After You Deploy the IDS?".[5]

One of the most common access methods to an outside network is through a web browser. Communication is two way, so access is opened not only from the browser, but also to the browser, when surfing the web. Some basic security steps can be taken by configuring web browser security settings. Again the principle of least privilege should be applied, but be advised there is a tradeoff between security and convenience when it comes to web browser settings.

© SANS Institute 2000 - 2005, Author retains full rights.

Start off by configuring the browser to only allow what is needed, then adjust the settings as necessary. Depending on usage, some features can be disabled (e.g. file download) even though they are sometimes used. In these situations the feature can be enabled immediately before it is used, and then disabled when it is no longer immediately needed. What is enabled and disabled will depend on typical web usage.

How To: (Internet Explorer 5.5)

1. Click on Tools > Internet Options > Advanced Tab. Scroll down to the "Security" section (near the bottom).
2. Customize the settings. For example, you may want to deselect older encryption levels such as "SSL 2.0", and select newer encryption levels such as "SSL 3.0".
3. Click on the "Security Tab", then the "Custom Level" button. Here many features may be enabled or disabled. Go through the list and set the desired level for each feature. One approach may be to disable everything, then see what common web usage doesn't work acceptably. Adjust the settings appropriately at that time. The author's experience is that some sites require "Active Scripting" to work at all, many sites require some level of Active X controls enabled for the entire page to display correctly but are still useable with no Active X controls enabled, and a few sites require "Cookies" to be enabled to work at all. I will note that a lot of sites that would normally set cookies (if cookies were enabled) work just fine when cookies are disabled; the sites that don't work at all with cookies disabled are the exception not the rule.

Threat Vector 2 - Outsider Attack from Telephone

Many computers have a modem and are connected to a telephone line. Sometimes the computer's user or owner doesn't realize their PC has a modem and that it is being used. For example, in the home environment, a spouse may have originally set up and configured the family computer. The other spouse regularly uses the computer but is oblivious to the fact that the computer has a modem and that it is connected to a phone line. An example in the office environment is when a phone line is plugged into a PC modem's "Line In" slot, with a nearby telephone plugged into the same PC modem's "Phone" slot. In this example the modem is being used to jump dial tone to the telephone. The telephone will have dial tone even when the computer is turned off. In both examples, when the computer is turned on, an attacker could potentially gain access to the computer through the modem.

Use of a modem may bypass normal security measures. For Example, a law office's network goes down. As a backup, many of the attorneys in the firm dial up to their local ISP, bypassing the firm's network level firewall, the firm's router with egress and ingress filtering, and the firm's network intrusion detection system. All of these are security measures that exist on the firm's normal network connection, but are bypassed when the attorneys in this example dial up to their local ISPs.

© SANS Institute 2000 - 2005, Author retains full rights.

Some of the security measures mentioned previously, such as a host based IDS and an up to date OS, can help mitigate some of the risk introduced by dial up internet access in the example above. The reality though is, how many people in these non-corporate type environments are even aware of the risks and will have implemented appropriate security measures?

The law office example is a good one because ostensibly the data stored on the lawyer' s computers will often be confidential or proprietary. In this example, the need for backup dial up internet access may also be compelling. After considering the example, the conclusion may be reached that a couple of additional measures are needed. One measure is instruction to achieve at least a minimal level of ubiquitous security awareness. Another measure is having a security policy addressing, among other things, dial up internet access, even in one user/administrator one computer scenarios. The policy might specify any PC used for dial up access have a host based IDS installed and properly configured.

A well known modem vulnerability is the auto answer feature. If a modem is configured to "auto answer", an attacker might dial the number and gain PC access when the owner is not present or aware. All fax machines are auto answer, and since many of today's modems are "fax modems", they have the auto answer feature as well.[6]

Basic security measures for this vulnerability are "know your system" and disable auto answer on any installed modems. For an enterprise environment a war dialer could be used to detect workstations with auto answer turned on, but in the given scenario only a single PC is considered.

How To:

1. Know your system. Know if your system has a modem and if a phone line is connected to it.
2. Right click on "My Computer", select "Properties", click on the "Hardware" tab and then on the "Device Manager" button. Installed modems are indicated by the modem icon (expand to see how many modems are installed).
3. If a modem is installed, verify "auto answer" is turned off. See the documentation that came with the modem or the vendors web site as procedures for this vary by modem type.

Threat Vector 3 - Insider Attack from Local Network

The insider attack from the local network is an attack by someone with access to the same local network the PC is connected to. In the given scenario, the user might be an attorney who connects to the local area network while in the office. The insider in this case might be another attorney, a secretary, the office manager...anyone with access to the local network from "the inside" (they don't have to hack into the local network from the outside; they have inside access).

The host based intrusion detection recommended earlier will detect and block some attacks from this threat vector, but to achieve defense in depth, additional security measures

© SANS Institute 2000 - 2005, Author retains full rights.

should also be implemented. Two such basic measures are enabling logging and using strong passwords.

Windows 2000 does not enable logging or auditing by default. The administrator must enable and configure the logging and auditing features. Logging and auditing are important detection layers that helps determine if a system has been penetrated and to what extent. Logging and auditing should be enabled in Windows 2000. Of course, "Enabling audit policies doesn't do much good if they are never checked."[7] How often to check the logs should be specified in the security policy.

How To:

1. Login with an Administrator equivalent User ID
2. Click on "Start" > "Settings" > "Control Panel". Double click "Administrative Tools", then "Local Security Policy".
3. Select "Local Policies" then "Audit Policy". Make the desired settings for each item listed.
4. Click on "Start" > "Settings" > "Control Panel". Double click "Administrative Tools", then "Event Viewer".
5. Select "Security Log" to view the contents of the security log.

If an insider knows or can guess another local user's password, gaining access to that system becomes as simple as logging on. Of course obvious passwords, such as first initial last name, first name, last name, birthday, etc. should be avoided. Beyond that, attackers can use automated tools to guess passwords. Strong passwords should be used to help mitigate the threat of password cracking.

Strong passwords are long (eight characters or more), are not words, include symbols and or numbers, and are changed frequently.[8] The PC owner should establish a password policy as part of their broader security policy for their self-administered PC. This policy would address how often passwords are changed and would specify strong password requirements, such as those mentioned above.

How To:

1. Press "Ctrl-Alt-Del", and click the "Change Password" button.
2. Use a new password that is "strong" as defined above.

Threat Vector 4 - Insider Attack from Local System

The insider attack from the local system is carried out by someone with physical access to the computer. The attacker could be anyone with physical access (cleaning crew, co-worker, etc). To help mitigate threats from this vector, physical security and other security measures, such as a BIOS password, can be implemented. When a system is left unattended, it should be secured.

© SANS Institute 2000 - 2005, Author retains full rights.

How To: (Physical Security)

1. Have a security policy for the PC that addresses physical security. For example, our security policy might state "The PC will reside in a physical location that will be locked whenever a trusted party is not present". This could mean locking the car doors while going into the convenience store (in the case of a laptop being taken home, for example), locking the office when no one is there, locking the house when no one is home, etc.

How To: (BIOS password)

1. Shut down the computer if it is not already turned off.
2. Power on the system. On boot up the keystroke sequence for "Setup" should be displayed. For example, on some Dell computers, the message "Press F2 to enter Setup" appears in the upper right hand corner. Just the keystroke may appear (e.g. "F10" in the corner of the screen) without a message. Ctrl-alt-Insert and Esc are other common keystroke sequences used by various manufacturers to enter the BIOS.
3. The setup option for setting the password will vary depending on the BIOS vendor, but once in the BIOS the user should be able to find the option to set the BIOS password (often in the "Security" section), then "Save Changes and Exit".
4. After saving the changes and rebooting, the password will be prompted for each time the PC is started.

For an in-depth look at BIOS security, see Robert Allgeuer's "Why Bother About BIOS Security?".[9]

How To: (Unattended System)

1. Press Ctrl-Alt-Del simultaneously and click the "Lock Computer" button.
2. Alternatively, a screen saver password can also be set so that when the system is idle for a specified period of time, the screen is locked.
2.a. Right click on the desktop, select "Properties" then the "Screen Saver" tab.
2.b. Select a screen saver from the drop down list, click the "Password Protected" box, and specify the time in the "Wait" box.
3. Click "Apply", then "OK".
4. If using the screen saver method, make sure the screen saver comes on and is password protected before leaving the computer unattended.
5. Locking the computer as in step 1 is the preferred method.

Threat Vector 5 - Attack from Malicious Code

Malicious code tops the list of security breaches in a recent InfoWorld survey, with 44% of 500 respondents stating they had experienced a breach due to a virus in the past 12 months.[10]

© SANS Institute 2000 - 2005

Author retains full rights.

In many ways this threat vector is difficult to protect against, as the above statistic indicates. The mainstay measure is desktop virus scanning software but this software is limited to only detecting known viruses. Keeping signature files up to date and keeping up with the latest virus threats are important, but additional measures should also be considered.

One important tool in mitigating the risk of malicious code is having a good security policy. The security policy should specify how often to scan for viruses (daily or at startup), how often to check for new virus signature updates (perhaps weekly), and what to do when malicious code is found (perhaps isolate the system, remove the malicious code and it's entries, or possibly even rebuild the system). The policy might also require all e-mail attachments and diskettes to be scanned with anti-virus software before being used.

<u>How To:</u> (for McAfee Virus Scan)

1. Open the "Virus Scan Console" either from the System Tray or from "Start" > "Programs" > "Network Associates" > "Virus Scan Console".
2. Select an existing task, right click, select "Properties", then the "Schedule" tab.
3. Specify how often, at what time, etc. to run the selected task.
4. Or click "Add a New Task" and specify the desired information.
5. Automatic update of the virus signature file can be scheduled by selecting the "Auto Update" task, right clicking, selecting "Properties", then the "Schedule" tab and specifying how often, when, what time, etc.

E-mail has become the primary means of spreading malicious code, so the e-mail client being used and how it is configured should be considered. In the given scenario with Microsoft Windows 2000 as the OS, the likely e-mail client is Microsoft Outlook. As with browser security settings in Microsoft products, there are tradeoffs between convenience and security in e-mail client settings too. For example Outlook's "auto preview" feature saves a mouse click or two, but may also inadvertently execute malicious code. Outlook can be configured to prompt before executing attachments, giving the user the option of saying "No" if the attachment is thought to contain malicious code. but some may consider the pop up window an annoyance. Possible measures include disabling "Auto Preview" and the "Preview Pane" to prevent e-mails from being opened automatically and ensuring "attachment security" is set to "High". Both measures provide some additional security.

<u>How To:</u> (Outlook 2000)

1. From within Outlook 2000, select "View" from the menu, then disable the "Preview Pane" and/or "Auto Preview" if desired.
2. Select "Tools" then "Options" from the menu. Click on the "Security" tab, then the "Attachment Security" button. Ensure the "High" option is selected to warn about attachments before executing them.

© SANS Institute 2000 - 2005

Author retains full rights.

Other measures that may help protect against or minimize the consequences of malicious code include password protecting the e-mail client, flagging executable files and MS Word template files as read only, setting Microsoft Word 2000 Macro security to "High", and backing up critical files to read only media. Applying the principle of least privilege and other basic security concepts also helps provide additional protection against malicious code. For example, as mentioned before, IIS comes with Windows 2000, but it is not enabled by default. By not enabling IIS, the user gains some protection against the Code Red virus.[11]

How To: (Password protect Outlook 2000)

1. To password protect the Outlook 2000 e-mail client, from within Outlook select "Tools" then "Services" from the menu. Select "Personal Folders", then click the "Properties" button. Click "Change Password", then provide a password that is not blank.
2. You may be unable to assign a password if the "Corporate or Workgroup" installation option was not used.
3. To view or change the installation option used, from within Outlook 2000, select "Tools" then "Options" from the menu.
4. Click the "Mail Services" tab, then the "Reconfigure Mail Support" button.
5. Note that if the selected option is changed at this point, the original installation media (Outlook 2000 CD) may be required.

How To: (Flag executable and template files read only)

1. Search for executable files ("Start" > "Search", enter "*.exe" for example)
2. Select the desired file and right click, "Properties".
3. The "General" tab has an "Attributes" section with the "Read Only" check box. If not checked, click it to flag the file read only.
4. Select "Apply" and "OK" to save the changes.
5. Do the same for the Microsoft Word global template file, but use "normal.dot" for the search criteria.

How To: (Set Word 2000 Macro Security)

1. From within Microsoft Word 2000, Select "Tools" > "Macro" > "Security" from the menu.
2. Verify "High" is selected on the "Security Level" tab.

How To: (Backup to read only media)

1. Identify critical data, perhaps the "My Documents" folder if using default file save locations,

© SANS Institute 2000 - 2005, Author retains full rights.

all .pst files (contains e-mail), the personal address book if used (*.pab), etc.
2. Use a CD writer and the accompanying software to save the identified critical data periodically to a write once read many CD.

Conclusion

The security measures used to help mitigate risk for one threat vector are not confined to having efficacy for only that vector. Rather, the various current applications of security measures and concepts work together to help achieve more robust and comprehensive security than would otherwise exist.

In this paper information assurance has been approached from the bottom up, with the PC level considered first. To accomplish this, a single PC was considered in a given scenario. Basic security concepts were introduced and then applied. PC level security was examined for each of five threat vectors, with an emphasis on achieving risk mitigation. Implementation of possible measures and application of basic security concepts was demonstrated based on research of current practices. The perspective has been general enough to suggest a structured way of approaching PC security and the implementation of constantly evolving security best practices. By considering information assurance at the PC level, conclusions can be adapted and applied throughout an organization to achieve more robust security and greater information assurance at all levels.

© SANS Institute 2000 - 2005, Author retains full rights.

End Notes

[1] Stocksdale, Greg. "NSA Glossary of Terms Used in Security and Intrusion Detection." April, 1998, as updated and maintained by the SANS Institute.
URL: http://www.sans.org/newlook/resources/glossary.htm#I
See also http://www.dtic.mil/doctrine/jel/new_puibs/jp1_02.pdf (definition was also available at this URL but appears to have been removed now).

[2] NorthCutt, Stephen and Novak, Judy. Network Intrusion Detection, An Analyst's Handbook, Second Edition. Indianapolis: New Riders Publishing, September 2000. 391-392.

[3] The Center for Internet Security. Level One Benchmark Windows 2000 Operating System (V1.0 Benchmark). November 6, 2001: 9. Available for download from
URL: http://www.cisecurity.org/bench_win2000.html.

[4] Zych, Tina. Personal Firewalls: What Are They, How Do They Work?. August 22, 2000.
URL: http://www.sans.org/giactc/GSEC.htm, Grad # 0081.

[5] Morris, Chris. What Do You Do After You Deploy the IDS?. January 3, 2001.
URL: http://www.sans.org/giactc/GSEC.htm, Grad #0358.

[6] Modem Express Tech Library. "Auto answer" (definition).
URL: http://www.modemexpress.com/support/auto-answer.html

[7] The Center for Internet Security. Level One Benchmark Windows 2000 Operating System (V1.0 Benchmark). November 6, 2001: 14. Available for download from
URL: http://www.cisecurity.org/bench_win2000.html.

[8] Microsoft Corporation. Security Administration Operations Guide. April 2001. URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp

[9] Allgeuer, Robert. Why Bother About BIOS Security?. July 23, 2001.
URL: http://www.sans.org/giactc/GSEC.htm, Grad #1118

[10] Connolly, P.J. "IT Security Outlook Appears Gloomy." InfoWorld. November 19,

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2000 - 2005

Author retains full rights.

2001: page 48.

[11] CERT/CC. "CERT Advisory CA-2001-13 Buffer Overflow in IIS Indexing Service DLL". August 16, 2001. URL: http://www.cert.org/advisories/CA-2001-13.html.

© SANS Institute 2000 - 2005, Author retains full rights.