# Global Information Assurance Certification Paper

**GIAC/GSNA**

# Auditing Internet Explorer Browser Security



Kathleen Lim

GSNA Practical Assignment

Version 3.1, Option 1

*27 July 2004*

## *Abstract*

This paper has been prepared for the practical requirements of the GIAC Systems and Network Auditor (GSNA) certification. In this assignment, an audit of the organization's Internet browsing security controls for internal users will be performed. The objective of this the audit will be to evaluate Internet Explorer browser security configurations for PC Workstations and Servers in the organization and to examine the use of content filtering to provide additional protection against security threats to IE.

The most recent "hacks" highlighted by the media describe an exploit targeted at Microsoft's Internet Explorer browser. A CERT alert released on June 11, 2004 that describes a cross-domain vulnerability that takes advantage of IE's handling of security zones [7]. The vulnerability allows an attacker to execute ActiveX scripts in a security zone outside of the active web pages' current security zone (typically an Internet Zone set with more security restrictions). The web page containing malicious code may be able to wreak such havoc as changing registry keys. Microsoft released a patch for this vulnerability on July 2, 2004. This type of attack could also be prevented by disabling active scripting and ActiveX controls and increasing the security level on your Local Machine Zone. Thus, it is important not only to keep your Windows security patches and fixes up-to-date, but also to configure the Internet Explorer browser with strong security controls.

# Table of Contents

# **PART 1:** Research in Audit, Measurement Practice, and Control

## *Section A: Identify the system to be audited*

**Organization:**
Widgets 'N More, a mid-size Engineering Firm

**Audit Subject:**
The device that will be audited in this review will be a Microsoft Internet Explorer browser, version 6 with service pack 1 installed on a user's desktop PC. The specific details regarding the system configuration of the audit subject are as follows:

- Internet Explorer Browser 6, SP1
- Installed on PC Workstations
- Windows XP Professional, SP1
- Physically located in the corporate home office building
- Logically located on the company's LAN

**Scope of the Audit:**
For this paper, an audit of the organization's Internet browsing security controls for internal users will be performed. The objective of this the audit will be to evaluate Internet Explorer ("IE") browser security configurations for PC Workstations and Servers in the organization and to examine the use of content filtering to provide additional protection against security threats to IE.

*This audit will address:*

- security policy and procedures *specific* to only browser security configuration and Internet usage requirements
- written policies and procedures for internet use
- IE security configuration settings
- IE patches and fixes
- IE security protection at the firm's network border (content filtering)

*This audit will NOT address:*

- privacy (i.e. cookie handling)
- SSL and certificates
- IE browser security on systems connecting remotely to the company's network
- operating system configuration of the audited system
- physical security of the audited system
- content filtering device configuration

**Current Environment:**
The browser acts a vehicle through which the organization's users access the Internet for information gathering and for access to vendor's websites. Internet access is treated primarily as a privilege to most organizational users, as their day-to-day business activity does not rely on the Internet. Current Internet Usage Policy restricts Internet

browsing activities for legitimate business use. The firm does allow limited browsing for personal use. Illegal or inappropriate Internet use based on website content or interference with job responsibilities is prohibited.

**Role of the Browser:**
The role of the IE browser is primarily to provide a mechanism for accessing:

- Public websites for research purposes
- Firm's Intranet site for employment and firm information
- Public websites for limited personal use
- Service provider or business partner websites for business activity (example: accessing payroll check processing vendor's website for secure FTP upload of paycheck data)

The role of IE in the organization is that it serves as a necessary business enabler, which inherently carries residual risk. Contrary to a media or marketing company, the firm's core business practices do not involve frequent access to interactive websites requiring full browser viewing functionality (resulting in keeping an insecure browser configuration a "necessary evil"). Therefore, this audit program will be based on the assumption that effective IE security controls can be implemented in the organization.

Secure methods for accessing the Internet can help to:

- Prevent unauthorized access to the PC or server with Internet Explorer installed.
- Prevent unauthorized access to company data through PC or server with Internet Explorer installed.
- Prevent malicious code from being downloaded and spread through the company's network.
- Prevent unauthorized changes to Internet Explorer configuration due to intentional or unintentional changes by users or Administrators.

**Background information:**
The Widgets 'N More engineering firm's company standards on Internet Explorer browser configuration for all systems are as follows:

*For all public Internet Sites:*

- Scripting controls must be disabled in the Internet Zone.
- Trusted Sites and Intranet zones may run trusted, or signed, scripting functionality.
- Files may not be downloaded onto any company system without consent from the IT Security Administrator.

*For all Trusted and Local Intranet Sites:*

- The Security Administrator must approve all domains that are added to Trusted Sites Zone.
- The Security Administrator must approve all Intranet web sites prior to publishing the site to all Widgets 'N More system users.

### *Section B: Most Significant Risks to the System*

**Major Threats to the Browser:**

| NO. | Threat Description | Source of Threat | Threat Category |
|---|---|---|---|
| **1** | Attacks resulting from insecure browser configuration | Hacker, Disgruntled employee | Internal or External; Human or Non-human; Intentional |
| **2** | Attacks resulting from missing patches or fixes | Hacker, Disgruntled employee | Internal or External; Human or Non-human; Intentional |
| **3** | Untrained Personnel (IT and End Users) | Hacker, Disgruntled employee; Untrained employee; Application or Malicious Code | Intentional or Unintentional; Human or Non-Human; Internal |
| **4** | Download of malicious code from an Internet or Intranet site | Untrained Employee; Application or Malicious Code | Intentional or Unintentional; Human and Non-Human; Internal or External |

**Major Assets Directly Affected by the Role of the Browser to the Firm:**

| NO. | Major Assets |
|---|---|
| **1** | Firm's confidential or proprietary information or data |
| **2** | User's data |
| **3** | PC Workstations |
| **4** | Critical Servers |
| **5** | Firm's business productivity |

**Major Vulnerabilities of the Browser:**

| NO. | Vulnerability | Degree of Exposure | Potential Impact |
|---|---|---|---|
| **1** | Missing Patches or Updates | High | Can result in a system compromise, access to data and confidential information, |

| | | | |
|---|---|---|---|
| | | | or denial of service. |
| **2** | Unrestricted ability to execute scripts, download files, or accept cookies or certificates | High | Can result in IE misconfiguration or unsafe browsing practices leading to system compromise, unauthorized data access, DOS, etc. |
| **3** | Unfiltered access to unauthorized or insecure URLs | High | Can result in download of malicious code or viruses resulting in system compromise, unauthorized data access, DOS, etc. |

**Risk Table**

The following risks are a result of the threats and vulnerabilities listed on the previous tables.

| NO. | Risk | Threat | Vulnerability |
|---|---|---|---|
| **1** | Unauthorized Access to Confidential or Critical Data | Attacks resulting from insecure browser configuration<br><br>Attacks resulting from missing patches or fixes<br><br>Untrained Personnel (IT and End Users)<br><br>Download of malicious code from an Internet or Intranet site | Missing Patches or Updates<br><br>Unrestricted ability to execute scripts, download files, or accept cookies or certificates<br><br>Unfiltered access to unauthorized or insecure URLs |
| **2** | Denial-of-Service or Loss of Productivity | | |

### *Section C: Current State of Practice*

| NO. | Reference | Type | Benefit of Reference |
|---|---|---|---|
| **1** | *Internet Explorer Security – George Guninski Security Research.* George Guninski. (http://www.guninski.com/browsers.html) | Article | Describes most recent IE vulnerabilities and demonstrates exploits. Solutions for preventing |

| | | | |
|---|---|---|---|
| | | | vulnerabilities were incorporated into the Audit Checklist. |
| **2** | *Hacking Exposed, 4th Edition.* | Book | Describes common IE "hacks". Solutions for preventing vulnerabilities were incorporated into the Audit Checklist. |
| **3** | About URL Security Zones Templates. Microsoft Article. (http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/templates.asp) | Security Guide | Describes the configuration of URL Security Zones in Internet Explorer. |
| **4** | *Internet Explorer Security Options (Parts 1 through 6)*. Windows Network Magazine website. Randy Franklin Smith. (http://www.winnetmag.com/Article/ArticleID/21282/21282.html) | Article/ Security Guide | Magazine article that explains leading practices for configuring Internet Explorer security. |
| **5** | *Microsoft Internet Explorer 6.0 Security: Step-by-Step.* Chris Christianson. SANS GIAC Paper. | SANS Paper/ Security Guide | Configuration guide that provides a description of IE configuration settings. |
| **6** | *Configuring Internet Explorer Security Zones: A New Tool for the Security Community.* Ken Barber. SANS GIAC Paper. | SANS Paper/ Security Guide | Configuration guide that provides a description of IE security zone configuration and functionality. |
| **7** | Microsoft Knowledge Base Article 833633: *How to strengthen the security settings for the Local Machine zone in Internet Explorer.* Microsoft Article. (http://support.microsoft.com/default.aspx?scid=kb;en-us;833633) | Article/ Security Guide | Step-by-step guidance on increasing the security controls on the Local Machine zone. |
| **8** | JavaTester.org. (*http://www.javatester.org/enabled.html*) | Article | Site's scripts used to understand and test Java capabilities in the browser. |
| **9** | "Internet Explorer Security Zones" by Scott Schnoll. (http://www.nwnetworks.com/iezones.htm) | Paper/ Security Guide | Discussion paper on IE security zone configurations. |
| **10** | *ActiveX Controls and Office Security.* Microsoft Article. (http://www.microsoft.com/office/ork/2003/seven/ch23/SecA05.htm) | Security Guide | Article explaining ActiveX control capabilities. |

## PART 2: Create an Audit Checklist

### *Audit Checklist*

System: Internet Explorer 6.0, SP1 Audit Date: _____
Auditor: _____ Checklist Version: SANS 3.1

| No. | Description | Pass/Fail |
|---|---|---|
| | ***I. Security Policy*** | |
| **1** | Internet Use and Browser Security Policy exists | |
| | | |
| | ***II. Patch Management*** | |
| **2** | IE browser updates and patches are up-to-date | |
| | | |
| | ***III. Browser Configuration*** | |
| **3** | Unprivileged users are prevented from changing IE security policies | |
| **4** | User Authentication is Disabled or Allows Prompt for Logon Credentials | |
| | *Secure Internet Zone Configuration:* | |
| **5** | Disable All ActiveX Controls | |
| **6** | Disable the Ability to Download Files | |
| **7** | Disable or Restrict Java Permissions | |
| **8** | Active Scripting is disabled or restricted | |
| **9** | Standards Exist for Configuring Local Intranet, Trusted and Restricted Sites Security Zones | |
| **10** | Trusted Sites are appropriately defined | |
| **11** | Insecure Sites are Restricted | |
| **12** | Increase Security on Local Machine Zone | |
| | | |
| | ***IV. Protecting IE at the Enterprise level*** | |
| | *Content Filtering:* | |
| **13** | Compliance with IE Policy | |
| **14** | Log Retention | |

# I. Security Policy

## Internet Use and Browser Security Policy

| | |
|---|---|
| **Item #:** | 1 |
| **Title:** | Internet Use and Browser Security Policy Exists |
| **Reference:** | ➢ "Configuring Watchguard Proxies: A Guide to Supplementing Virus Protection and Policy Enforcement." [25]<br>➢ Personal Experience<br>➢ "Internet Explorer Enhanced Security Configuration: Browser Security – Best Practices" [3] |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | 1. Obtain the most current copy of the Internet Explorer security configuration policy or standards.<br>2. Review the company policy, and verify that the policy [25]:<br>a. Is published and communicated to all users.<br>b. Defines restrictions on types of Internet use.<br>c. Clearly identifies permissible downloads.<br>d. Restricts downloading of files from the Internet.<br>e. Clearly identifies configuration standards and restricts the nature or content of Internet sites visited or files transferred.*<br>f. Provides for monitoring of use and enforcement of restrictions.<br>g. Provides for exceptions to accommodate business justifications.<br>h. Internet browsing and downloading is not permitted on a server, unless there is a necessary justification for doing so (i.e. testing for network connectivity, accessing Microsoft Windows updates, etc.).<br>i. The policy gives guidance to users for "acceptable use." *Suggested policies for Internet users might include:*<br>i. Do not follow unsolicited links<br>ii. Do not ever "always trust" a certificate or signature<br>iii. Set Privacy settings (cookies) appropriately<br><br>Recommended Leading Practices:<br>➢ All domains or sites added to the Trusted Sites zone must have approval from the Information Security Department/Officer/Manager.<br>➢ All Intranet sites must undergo a secure code walk-through. All sites must have approval by the Information Security Department/Officer/Manager prior to being published on the company intranet. |

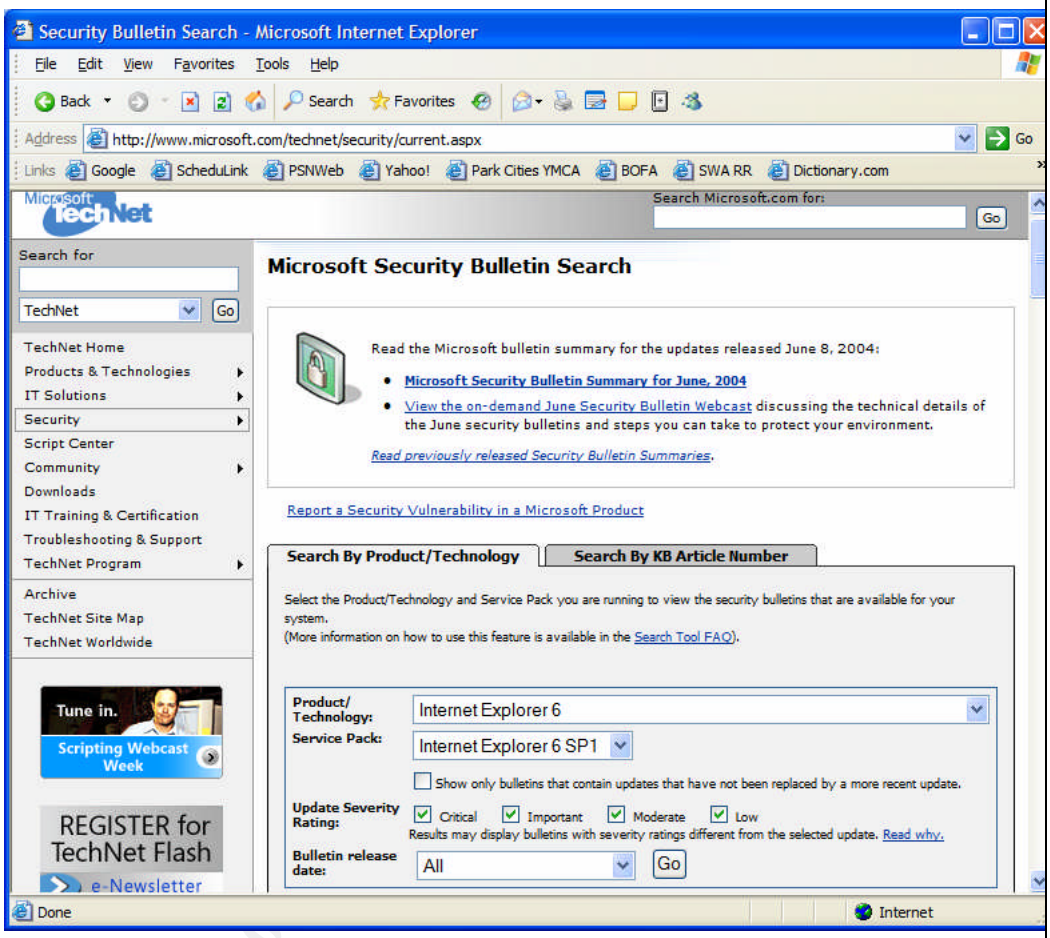
| | |
|---|---|
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## *II. Patch Management*

### Patches are Up-To-Date

Keeping patches up-to-date is a "must have" on almost any device security audit checklist. Keeping your system up-to-date with the latest service packs and critical patches helps to prevent or mitigate security vulnerabilities inherent in your software. Internet Explorer software is no different. Microsoft frequently releases IE updates and critical security fixes. Patch management is like a race to the finish: when a vulnerability becomes known to the free world (i.e. hackers), a patch will usually follow that address the vulnerability. A vigilant security administrator should install the patch as soon as possible, before a hacker discovers the vulnerability in your environment and attempts to run the exploit.

| | |
|---|---|
| **Item #:** | 2 |
| **Title:** | IE browser updates and patches are up-to-date |
| **Reference:** | ➢ "Critical Updates" from the Microsoft Internet Explorer web site [30]<br>➢ SANS GSNA Course Material [31]<br>➢ Personal Experience |
| **Risk:** | Vulnerability No. 1 |
| **Testing Procedure:** | Review the Policy:<br>1. Obtain the organization's most recent security policy and verify that the policy requires that critical security patches and fixes are kept up-to-date on all systems.<br><br>TEST PROCEDURE PREPARTION:<br>Go to Microsoft's website to verify the most current IE critical update available: http://www.microsoft.com/technet/security/current.aspx.<br>At the TechNet page, select the IE version 6, and choose SP1. |




Click on the latest critical updates that have been applied within the last 30 days. For each critical update, click on the "Technical Details" link of the most recent IE update to view the patch details. Under the "Security Update Information," the article should describe the steps needed to verify a particular patch was installed.

2. Verify IE Cumulative Security Updates are installed: There are typically several ways you can validate a system patch was installed. It is strongly advised that you should perform at least two of the options below to ensure that you have performed an accurate validation of installed system patches.

TEST OPTION A: Check the Microsoft registry for the associated entry by either navigating or using the "Find…" function. [To quickly get to the Registry Editor, go to START > RUN… > Type "`regedit`".] Here's an example of a full registry path to locate a the February 2004 IE Critical Update's registry entry:

| | |
|---|---|
| | `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Hotfix\KB832894`<br><br>Right-click on the registry folder “tree” on the left window pane, and choose “Export”. Save the output as a text file, and save the data as your audit evidence.<br><br>TEST OPTION B: At the IE browser to “About Internet Explorer” dialog box on the “Help” menu.<br>  <br><br><br>TEST OPTION C: Use Microsoft Security Baseline Analyzer to obtain a System Report including installed patch details. You can download MSBA at http://www.microsoft.com/technet/security/tools/mbsahome.mspx .<br><br>TEST OPTION D: Go to the system Control Panel and to “Add or Remove Programs.” Each installed hotfix should be listed after the installed applications.<br><br>2. Take a screenshot of the current hotfix or cumulative patch version. Add this documentation to your working papers. |
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |

| | |
|---|---|
| **Findings:** | |

## *III. Browser Configuration*

AUTHOR'S NOTE:
The following control objectives (audit checklist items) and testing procedures are directed at assessing the audited system's Internet Explorer configuration by evaluating the browser's reaction to different events (i.e. Java, ActiveX, JavaScript, user authentication challenges, URLs in different security zones, etc.). The security parameters set may also be identified by reviewing the options selected in the "Security tab" in the "Internet Options" window. You can also find numerous browser configuration detection scripts on the Internet, such as Cyscape's BrowserHawk [12] and BrowserSpy [13]. You may also want to manually review each IE setting that you will be testing in this audit checklist to validate your findings.

### Unprivileged users are prevented from changing IE security policies

Imagine that you are the system administrator, and after weeks of preparation and hard work, you finally have fully deployed a securely configured Internet Explorer browser to all of your organization's users. Then, one by one, your users discover that you have taken away their ability to watch the latest movie trailer on the Internet. As a result, the smart intern has figured out a way to reconfigure IE's Internet Zone with the permissions necessary to surf interactive web sites and download files as desired.

To avoid this scenario, organizations may choose to use Group Policy update IE to take away the ability to modify the "Security" tab of Internet Options from standard users. To modify this control, an administrator must modify the Group Policy settings to apply policies based on the user's location in the domain. Randy Franklin Smith describes how to roll IE policies out to your organization in a Windows Network Magazine article [9, Part 6]:

1. Launch the Group Policy Editor.
2. In the policy template you would like to modify, go to User Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel.
3. Click on "Disable the Security page," and set the policy to "Enabled" in the pop-up window.
4. Click "OK" to apply the change.

| | |
|---|---|
| **Item #:** | 3 |
| **Title:** | Users are prevented from changing IE policies |
| **Reference:** | ➢ *Internet Explorer Security Options, Part 6* on Windows Network Magazine website [9] |
| **Risk:** | Vulnerability 2 & 3 |

| | |
|---|---|
| **Testing Procedure:** | 1. Obtain the organization's most recent configuration procedures or standards (that are specific to IE or in general to system management). Review the documentation to verify the standards include preventing unprivileged users the ability to modify security settings or configurations.<br>***2. To validate that users do not have access to change IE's security configuration:***<br>a. On an end user's workstation, log on as an unprivileged user.<br>b. Launch IE, and go to Security > Internet Options.<br>c. Verify that the Security tab is not available or that the Security options cannot be changed by the user. |
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## User Authentication

User authentication can be configured in Internet Explorer in four ways:

| | |
|---|---|
| Anonymous logon | Disables HTTP authentication and uses guest access for CIFS (Common Internet File System). |
| Automatic logon only in Intranet zone | Logs on automatically on all intranet sites and prompts for username and password for sites in all other zones. |
| Automatic logon with username and password | Configures Internet Explorer to attempt to logon using Windows NT Challenge Response (also known as NTLM authentication). If NTLM is supported by the server, the logon uses the user's network user name and password for logon. If NTLM is not supported, the user is prompted for a username and password. |
| Prompt for username and | Prompts once per session for username and |

| | |
|---|---|
| password | password. Once successfully logged on, the credentials are silently used for the remainder of the session. |

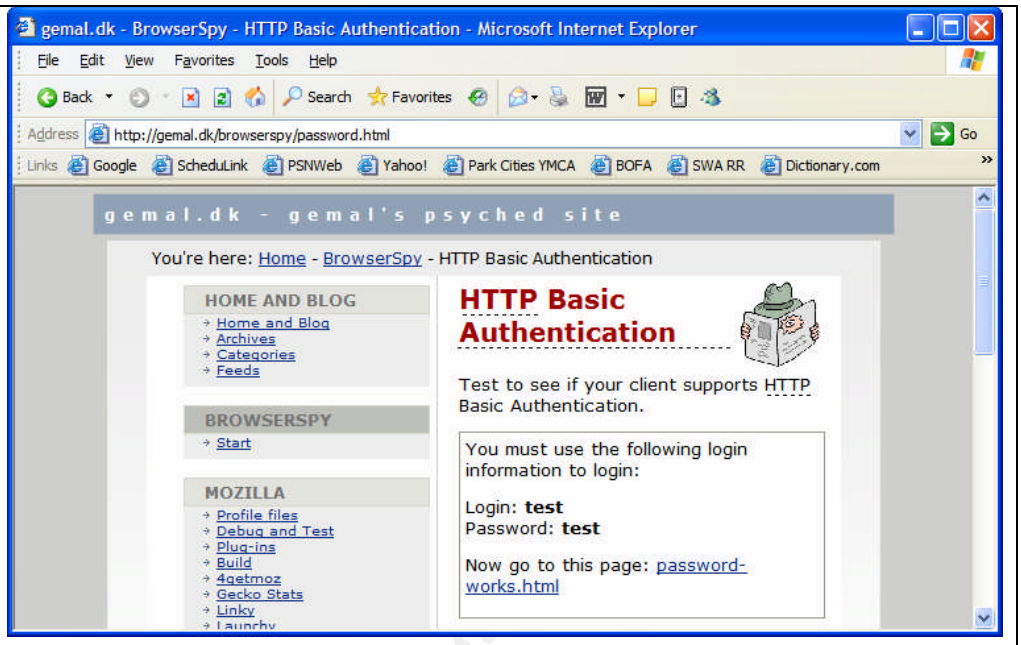
*Internet Explorer Security Zones* article by Scott Schnoll [15].

A Windows Network Magazine article, written by Randy Franklin Smith, recommends the following settings for each IE security zone [9, Part 6]:

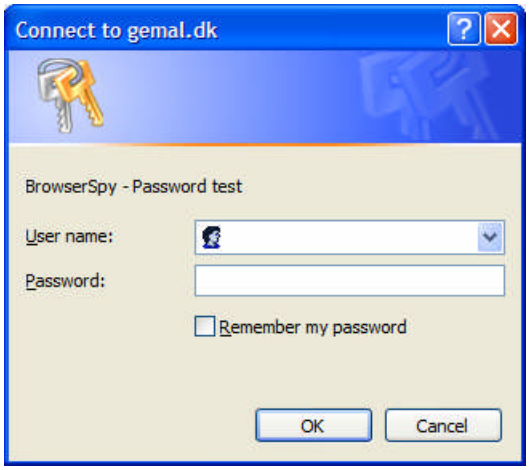
| ZONE | SETTING |
|---|---|
| Trusted Sites Zone | Automatic logon only in Intranet zone |
| Local Intranet zone | Automatic logon only in Intranet zone |
| Internet Zone | Prompt for username and password or Anonymous logon |
| Restricted Sites Zone | Prompt for username and password or Anonymous logon |

*From "Internet Explorer Options, Part 5" article written by Randy Franklin Smith (http://www.winnetmag.com/Article/ArticleID/21199/21199.html) [9, Part 6].*

| | |
|---|---|
| **Item #:** | 4 |
| **Title:** | User Authentication is Disabled or Allows Prompt for Logon Credentials |
| **Reference:** | ➢ *Internet Explorer Security Options, Part* 5 on Windows Network Magazine website [9] |
| **Risk:** | Vulnerability 3 |
| **Testing Procedure:** | The following is a general test to verify HTTP Basic Authentication is enabled in your IE browser (If "Anonymous Logon" is checked) in the INTERNET ZONE:<br><br>1. Go to the Gemal DK web site to utilize their HTTP browser authentication page: http://gemal.dk/browserspy/password.html, then click on the "password-works.html" link. This website provides different URLs that assess the configuration of your browser. |




2. When you try to access the password-works.html page:
   a. if a user ID and password prompt does not appear, you should get the following message: "**It didn't work!** Your client doesn't support HTTP Basic Authentication!"
   b. if a user ID and password prompt appears (see figure below), then your browser is not using the "Anonymous Logon" setting in your browser. If you do receive a prompt, enter "test" as the user name, and "test" as the password. The web site should return a message that says, "**It worked!** Your client supports HTTP Basic Authentication!"




*BrowserSpy's HTTP authentication test prompt*

The following is a general test to verify if HTTP Basic Authentication is enabled in your IE browser (If "Anonymous Logon" is checked) in the TRUSTED SITE or INTRANET SITE:

1. In IE, go to Tools > Internet Options > Security tab.
2. Click on the Trusted Sites icon to configure this zone.
3. Click on the "Sites…" button to add an URL to the Trusted Sites or Intranet Sites list.
4. Now, repeat steps 1-3 above to validate if "Antonymous Logon" is enabled in the Trusted Sites zone.

To verify the "Automatic logon only in Intranet zone" or "Automatic logon with username and password" settings, you will need to create a unique scenario in which your current logon and password also are the same credentials needed to authenticate via your browser to a target URL. For example:

- You are logged on to your PC with your network user name and password, and you access your email via OWA (Outlook Web Access).
- You are logged on to your PC with the "Guest" account (although, if you are following security best practices you would have disabled this vendor default account upon installation), and you are accessing a web site with the same Guest authentication credentials.

If you can create Scenario A above, you should be able to easily test both User Authentication settings by access OWA via your company's Intranet URL (i.e. http://widgetsnmore/owa), then using the Internet URL counterpart (i.e. https://www.widgetsnmore.com/owa). The following is a test case for these scenarios:

| Current Zone of Target URL | Authentication Credentials | Reaction of IE Browser | Probable IE Setting |
|---|---|---|---|
| *Intranet Zone<br><br>Trusted Sites Zone | Network User ID and password logon on your PC<br><br>Browser credentials are also the network User ID credentials | No user ID and password prompt but successful authentication to target URL | *Automatic logon only in Intranet zone<br><br>Automatic logon with username and password |
| | | User ID and Password Prompt | Prompt for username and password |
| | | No user ID and password prompt, but NO successful authentication to | Anonymous logon |

| | | | | |
|---|---|---|---|---|
| | | | target URL | |
| | Internet Zone | Browser credentials NOT the same as your current PC logon User ID credentials | User ID and Password Prompt | Prompt for username and password<br><br>Automatic logon only in Intranet zone<br><br>Automatic logon with username and password |
| | | | No user ID and password prompt, but NO successful authentication to target URL | Anonymous logon |

| | | |
|---|---|---|
| **Test Nature:** | OBJECTIVE: YES | SUBJECTIVE: |
| **Evidence:** | | |
| **Findings:** | | |

## *Secure Internet Zone Configuration*

### Internet Explorer Security Zones

Configuring strong browser security definitely has its trade-offs. Disabling the ability to use ActiveX, Java, or scripting technology often results in reduced functionality when browsing web sites. To address this, Internet Explorer is configured with different security zones allowing you to establish varying levels of functionality for Internet, Intranet, and defined Trusted and Restricted sites. The focus of this paper is to specifically address the configuration settings for only the Internet Zone. Although the audited organization's line of business may require users to enjoy unrestricted Internet browsing and downloaded, the security implications still remain. The objective of the following checklist items is geared to mitigate the risks of vulnerabilities, including: download and execution of malicious code, modifying your local PC's file system and registry possibly resulting in a denial-of-service or access to your PC.

The default browser security level for the Internet zone is set to Medium, which allows for "safe Internet browsing," while allowing signed ActiveX controls and scripting to enable website functionality.

## ActiveX

ActiveX, defined simply, is a Component Object Model (COM) or an OLE object. ActiveX controls are like mini-programs that can perform many different actions on your computer from providing a drop-down box on a web page form, downloading and reading a text file on your desktop, to changing registry key values. They are self-registering programs that update your Windows registry upon initial "run-time" on your computer. ActiveX functionality adds "bells and whistles" to websites and the user's Internet experience; however, ActiveX controls present a security risk in that this code, by design, does not operate within a safe region, or sandbox, within your Internet Explorer browser. Malicious code could easily masquerade as a legitimate ActiveX control and install a backdoor on your computer or cause a denial-of-service. [25]

To help address the inherent security risks of ActiveX controls, Microsoft has added the capability for developers to "sign" their code to prove authenticity. Authenticode, or signed ActiveX code, should give both the browser (and the IE user) the assurance that:

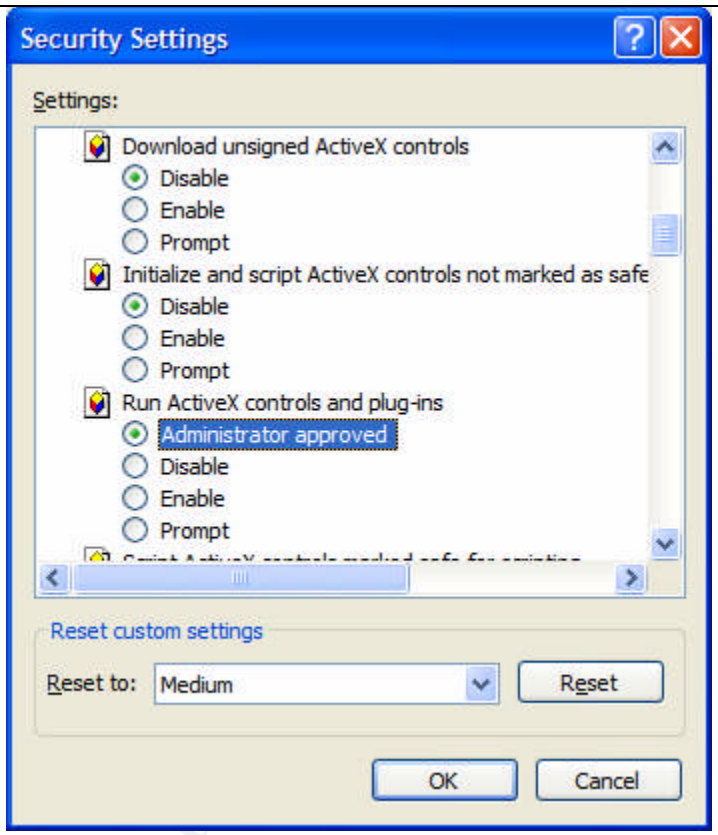
- The developer's identity is known, and legitimate
- The code was designed to have no unsafe or insecure functions or capabilities [27]

However, although signed ActiveX controls from well-known, trusted sources, such as Microsoft or Symantec, should reasonably be trusted, there is no assurance that the code is not illegitimate or harmful. By accepting digitally signed code via your IE browser, you are essentially assuming that the developer dutifully prepared and performed a comprehensive examination of his/her code for potential security flaws.

To identify if a website is using ActiveX controls, do a "View Source" and look for any <OBJECT> tags.

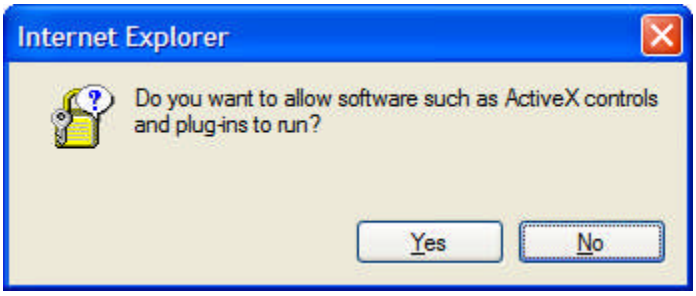
| | |
|---|---|
| **Item #:** | 5 |
| **Title:** | Internet Zone: Disable All ActiveX Controls |
| **Reference:** | ➢ Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition [1]<br>➢ *Internet Explorer Security Options, Part* 2 on Windows Network Magazine website [9] |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | Review the Policy:<br>1. From review of the current security policy or configuration standards documentation, verify that the organization requires |

| | |
|---|---|
| | for ActiveX functionality to be disabled, at a minimum, in the IE Internet Zone.<br><br>**To verify that all ActiveX functionality is disabled in the Internet Zone:**<br><br>2. In IE, go to Tools > Internet Options… > Security tab. Click on the "Custom Level…" button. In the "ActiveX controls and plug-ins" section, verify that all options listed are set to "Disable." The following settings should be reviewed:<br>➢ Download signed ActiveX controls<br>➢ Download unsigned ActiveX controls<br>➢ Initialize and script ActiveX controls not marked as safe for scripting<br>➢ Run ActiveX controls and plug-ins<br>➢ Script ActiveX controls marked safe for scripting<br><br>If the browser you are auditing does have Authenticode settings available, review the settings for these parameters under the ".NET Framework-reliant components":<br>➢ Run components not signed with Authenticode<br>➢ Run components signed with Authenticode<br><br>Again, these settings should be set to "Disable." |

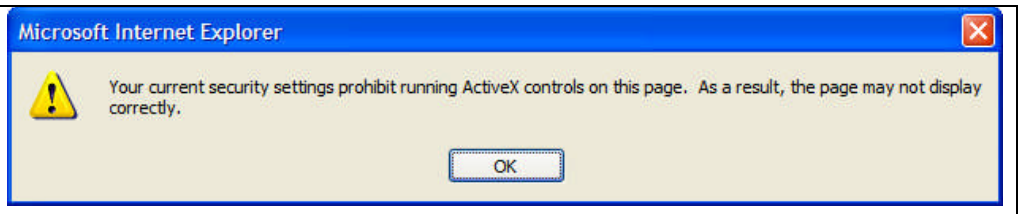



**Perform substantive testing to verify that "Run ActiveX controls and plug-ins" is set to "Prompt" or "Disabled":**

3. Go to this web page: http://www.guninski.com/mscheckf.html, http://www.cnn.com, or http://www.espn.com . Your browser should immediately give you this pop-up message:

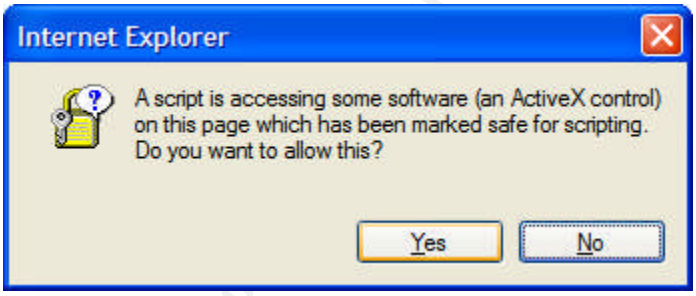



If your browser has disabled ActiveX controls, the page will return with this error message:




**Perform substantive testing to verify that "Script ActiveX controls marked safe for scripting" is set to "Prompt":**

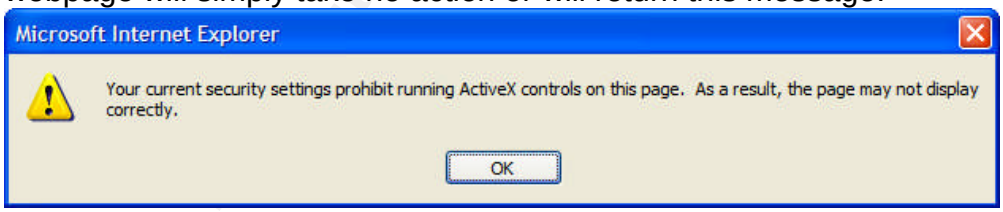
4. Go the AOL web site at http://www.aol.com . If you see this pop-up message, then this parameter is set to "prompt":



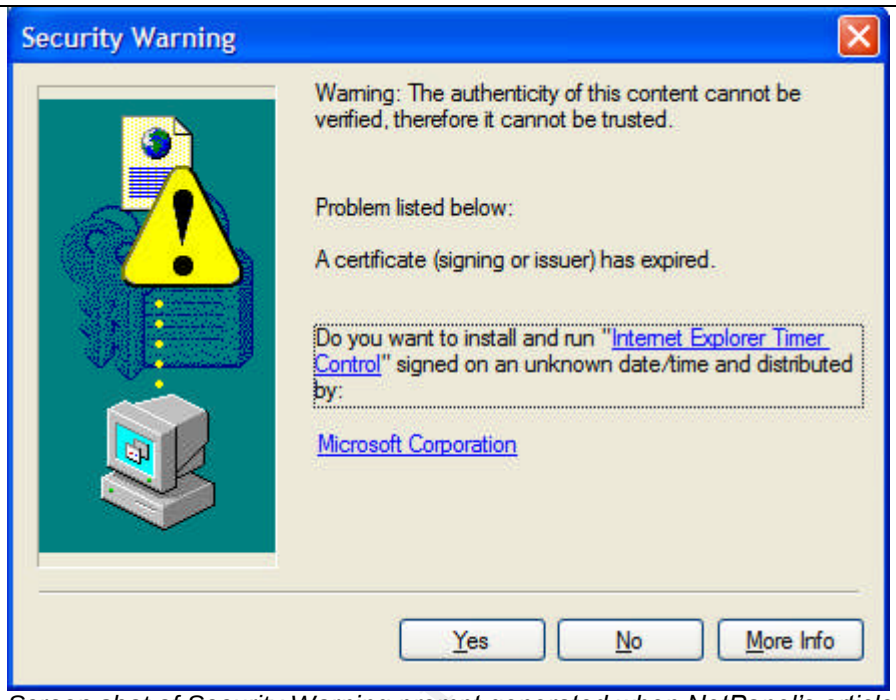

**Perform substantive testing to evaluate IE's handling of ActiveX unsigned controls (including controls with Authenticode):**

5. Click on the link to verify how your browser reacts to an ActiveX control that is not signed with an Authenticode signature: http://www.newkirk.com/iraroth2.HTM . If your browser is set to "prompt", you should see the following Security Warning message box:


At the prompt, simple hit NO, and close the IE browser window. If you browser is set to “Disable” for all unsigned ActiveX code, this webpage will simply take no action or will return this message:




Your browser should also give you messages such as these if the signature is expired or appears to be not valid:

| | |
|---|---|
| |  <br>*Screen shot of Security Warning prompt generated when NetPanel's article on ActiveX was accessed (http://www.netpanel.com/articles/internet/actx-use.htm).* |
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## Disable the Ability to Download Files

In any instance that a file is created on a computer, you run the risk that a virus may infect your computer or that malicious code may be installed and executed. The Internet is a fairly common vehicle used to locate applications or tools needed for home or business reasons. Depending on your company's stance on unauthorized or unlicensed software, the ability to download executable files may also reduce compliance with the organization's policies.

| | |
|---|---|
| **Item #:** | 6 |
| **Title:** | Internet Zone: Disable the Ability to Download Files |
| **Reference:** | ➢ Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition [1]<br>➢ *Internet Explorer Security Options, Part* 2 on Windows Network Magazine website [9] |

| | |
|---|---|
| **Risk:** | Vulnerability 2 |
| **Testing Procedure:** | **Review the Policy:**<br>1. Review the company's acceptable Internet use policy and/or system configuration procedures or standards documentation. Verify that the company prohibits or restricts users from the ability to download files from the Internet, unless an appropriate business justification is approved by management.<br><br>**<u>To verify that the "File Download" and "Font Download" options are disabled:</u>**<br><br>5. Access a site that is the Internet Security Zone. This should be a URL that is not on the local Intranet, Trusted or Restricted Sites Zones. To verify that the website is in the Internet Zone, make sure the "Internet" icon is present in the IE status bar on the bottom right of the browser window. [HINT: If you can't see the Status Bar, go to View > Status Bar to enable this feature.]<br>6. Go to any web site that gives you the option to download files. You can go to http://www.download.com and click on any of the "Download Now" buttons. [NOTE: If the downloads.com URL is listed on your Trusted, Intranet or Restricted Sites security zones, this test procedure will not accurately assess the security settings of the Internet Zone. If this is the case, please access another web site that would be included in the Internet Zone, and attempt to download any file.]<br>7. When you try to download a file, you should either receive a Security Alert pop-up warning, or simply no action will occur. |
| **Test Nature:** | OBJECTIVE: \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## Java

HTML-based programs built with Java are commonly integrated into web pages. The Java applets typically are executed whenever a browser is opened or the user triggers an action on the web page (i.e. clicking on a button or link). Applets are Java programs that run on the client-side. Unlike ActiveX, Java was designed to run in a sandbox

environment to eliminate potential security risk caused by code execution on the Local Machine. Although Java was designed to build inherently secure code, Hacking Exposed authors state: "Java security has been broken numerous times because of the age-old problem of implementation not supporting the design principles."

How can you tell if a web page is using a Java applet? While viewing the URL, go to "View Source" and search for the <applet> tag.

If you wish to enable Java to maintain browser functionality (and not bring your web browsing experience to a screeching halt), Internet Explorer allows you to set different "safety" permissions on the type of Java applets that will be allowed to run on your PC. Randy Franklin Smith's article on WinNetMag.com explains that setting High safety on your Microsoft VM settings restricts Java programs from accessing your local PC's files and settings outside of Internet Explorer. In essence, you are restricting the Java sandbox to your browser, not your entire PC. See http://www.winnetmag.com/Article/ArticleID/21026/21026.html for more details.

Internet Explorer handles Java security by setting different safety levels for the browser. The browser may be configured with three default safety levels: High, Medium, or Low. If Java Applets must be permitted for browsing functionality, the "High Safety" setting is preferred. If you don't need to access sites that run Java Applets, "Disable" Java Applets completely.

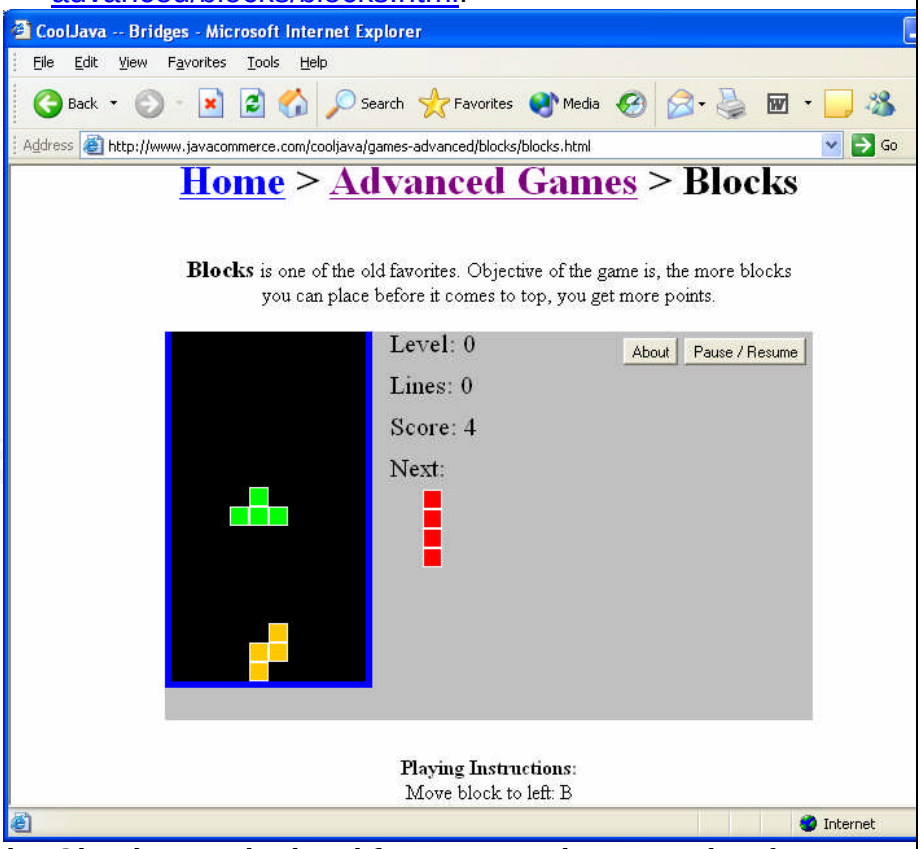
| | |
|---|---|
| **Item #:** | 7 |
| **Title:** | Internet Zone: Disable or Restrict Java Permissions |
| **Reference:** | ➢ Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition [1]<br>➢ *Internet Explorer Security Options, Part* 4 on Windows Network Magazine website [9]<br>➢ JavaTester.org [22]<br>➢ Sun Microsystems' "Test your Java™ Virtual Machine" website [21] |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | Review the Policy:<br>1. From review of the current security policy or configuration standards documentation, verify that the organization requires for Java functionality be disabled, at a minimum, in the IE Internet Zone.<br><br>**Verify that Java is set to "High Safety" or "Disabled":**<br><br>2. Go to Internet Options, and verify that "High Safety" or "Disable" is selected under the Microsoft VM section. |

In the following steps, you will verify how your browser reacts to untrusted and trusted code. The "high safety" setting should be configured to accept trusted Java code, and prompt or not accept untrusted Java code.

3. ***Check if Java is Enabled.*** To see if Java is enabled on your browser, you can use Sun's "Test Java Virtual Machine" web page: http://java.com/en/download/help/testvm.jsp. You can also use Michael Horowitz's JavaTester.org web site: http://www.javatester.org/enabled.html.

If Java is Enabled:

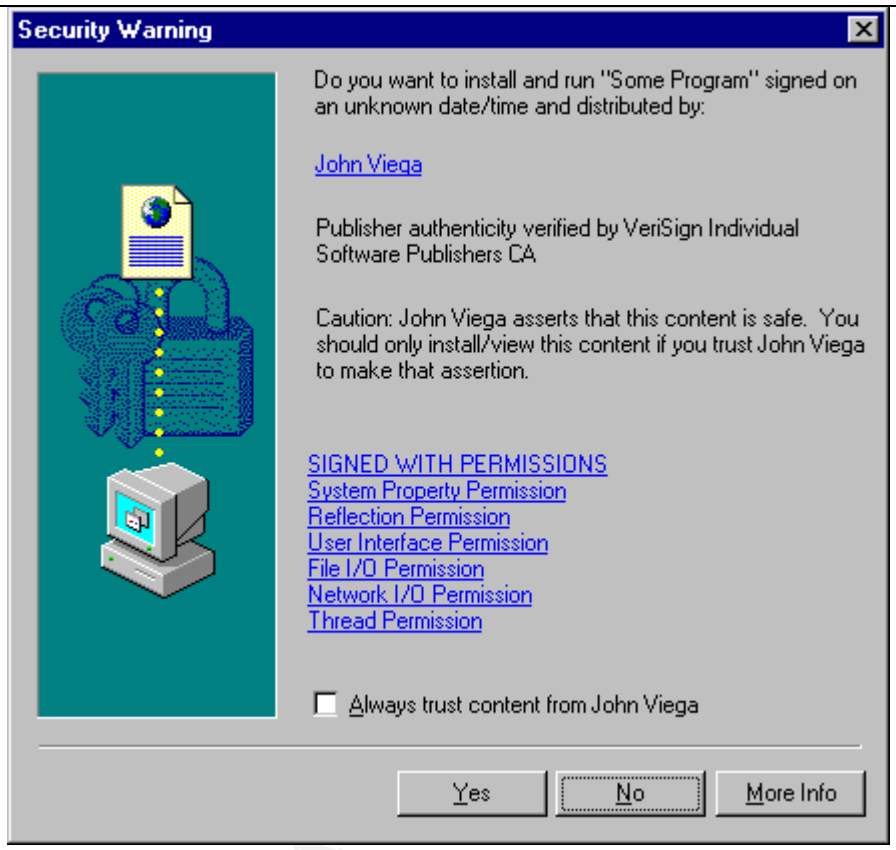
***a. Check security level for trusted Java code.*** The Java applet game at the following link runs trusted Java applets: If you browser allows the block game to run, your browser automatically accepts trusted Java code. http://www.javacommerce.com/cooljava/games-advanced/blocks/blocks.html.




***b. Check security level for untrusted Java code.*** If you have your security set to prevent automatic downloaded of untrusted code, IE should prompt you if any signed applets could not be verified based on the publisher authenticity, and if the certificate is valid or not expired. ***Try this web***

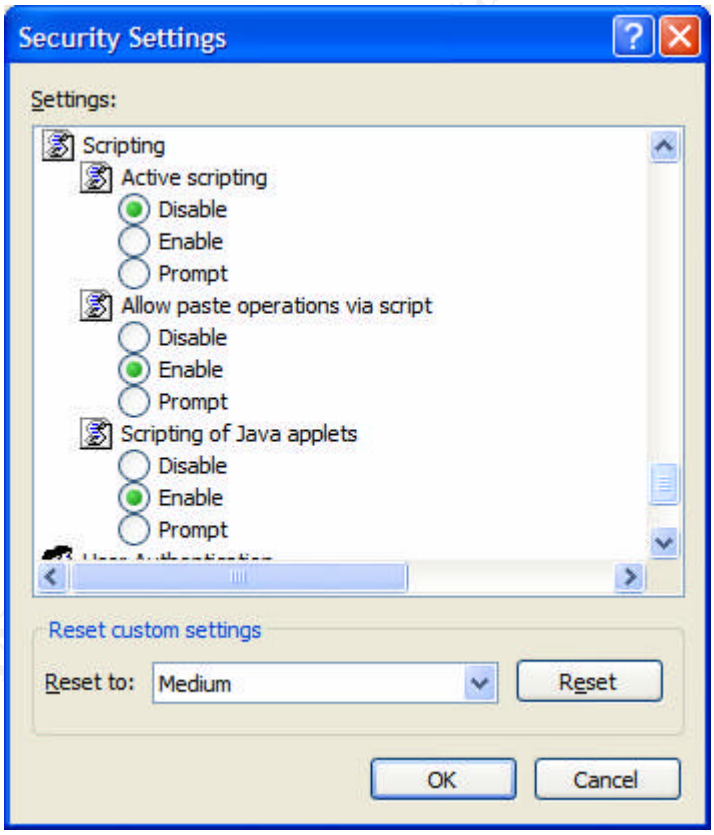
***site to test how your browser responds to trusted code:*** http://www.brookscole.com/compsci_d/templates/student_resources/0534953654_deckerhirchfield/aeonline/course/6/2/index.html.


*This is a warning message that will be produced if you have Sun's Java plug-in installed.*

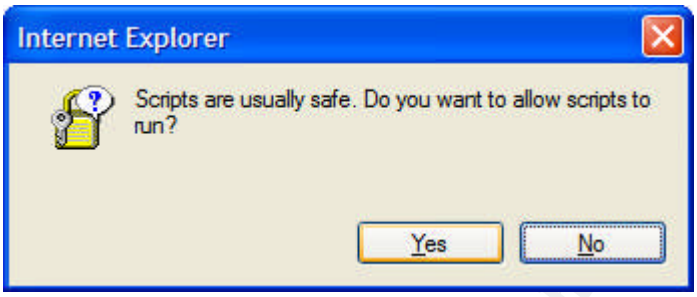
| | |
|---|---|
| |  |
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## Active Scripting is Disabled

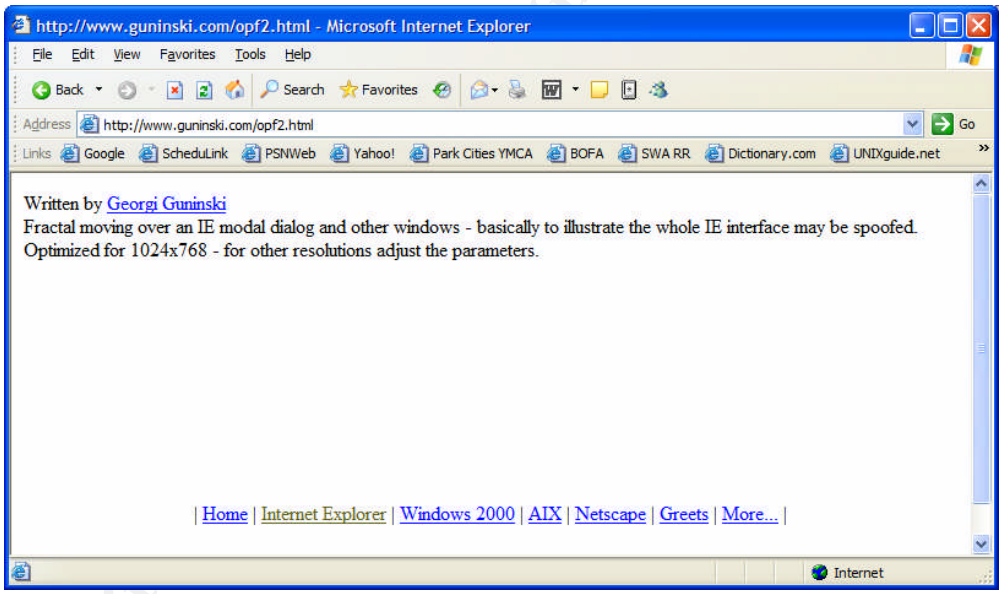
The term “Active Scripting” used by Internet Explorer simply refers to active scripts that are “programs written in JavaScript, or sometimes Microsoft's VBScript and ActiveX.” If you ever go to a URL that has an ".asp" extension, you are most likely running a script, or program off of that server” [28]. The configuration setting “Scripting” in the IE Security tab generally refers to client-side scripts. Although these scripts generally are more restricted in their capabilities, Randy Franklin Smith notes: “Although a client-side script's functionality is much more limited and safer than ActiveX, attackers can use active scripting to write viruses and other malicious code” [9, Part 5].

| | |
|---|---|
| **Item #:** | 8 |
| **Title:** | Internet Zone: Active Scripting is disabled or restricted |
| **Reference:** | ➢ Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition [1]<br>➢ *Internet Explorer Security Options, Part* 5 on Windows Network Magazine website [9]<br>➢ George Guninski's web site [16] |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | Review the Policy:<br>1. From review of the current security policy or configuration standards documentation, verify that the organization requires active scripting functionality to be disabled, at a minimum, in the IE Internet Zone.<br>  <br><br>*Screen shot of the "Scripting" configuration options in IE.*<br>2. In your browser, go to the following URL: http://www.guninski.com/opf2.html. This is a JavaScript demonstration presented by George Guninski.<br>a. If "Active Scripting" is set to "Prompt," you will subsequently |

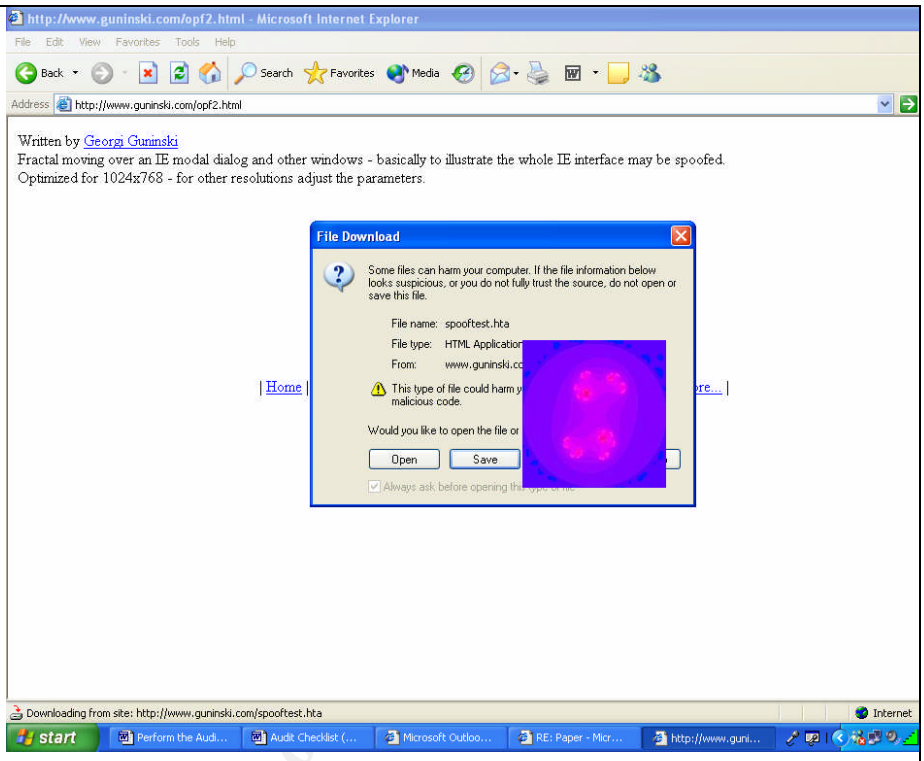
see this message box:




b. If this Active Scripting is disabled, your IE window will simply only display text:




c. If Active Scripting is enabled, you should see this IE interface "spoofing" trick:

| | | |
|---|---|---|
| | |  |
| **Test Nature:** | | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | | |
| **Findings:** | | |

## Secure Local Intranet, Trusted Sites, and Restricted Sites Zone Configuration

AUTHOR'S NOTE:
The audit checklist items described above are focused on a review of the Internet Zone. The control objectives are focused on auditing IE to assess the security of the browser when accessing public URLs. However, using these checklist items as a guide for configuring a secure browser may also result in limited viewing functionality as you surf the Internet. To address this limitation, an organization may decide to accept less stringent browser controls for accessing URLs that have been determined to be reasonable secure, such as internally-developed Intranet websites and well-known and trusted URLs. Internet Explorer's URL security zones make these varying levels of browser security controls possible.

By design, URLs listed on these zones must be explicitly defined in Internet Explorer. This audit checklist does not explicitly address each security setting for these zones, but rather the policies, procedures and process for adding domains (and sub-domains) to these IE security zones. The approach used in this audit program is to address the URL definitions within the Local Intranet and Trusted Sites zone configurations, as typically these are the web sites that are trusted to be secure by the organization. This audit plan has determined the following security zone tests as critical control objectives. However, you may use the Secure Internet Zone checklist items to evaluate security for the other IE zones as well.

| | |
|---|---|
| **Item #:** | 9 |
| **Title:** | Standards Exist for Configuring Local Intranet, Trusted and Restricted Sites Security Zones |
| **Reference:** | ➢ Personal Experience |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | 1. Verify existence of organizational policies, procedures and/ or standards for identifying and approving URLs defined in the Local Intranet, Trusted Sites, and Restricted Sites IE security zones.<br>2. Interview the appropriate personnel and obtain documented evidence that the organization's standards are being followed.<br>3. For each URL added to the Trusted Sites, Local Intranet or Restricted Sites listing, obtain documented evidence that the domain was approved in accordance with the organization's policies. |
| **Test Nature:** | OBJECTIVE: \| SUBJECTIVE: YES |
| **Evidence:** | |
| **Findings:** | |

## Trusted Sites Configuration

The Internet Explorer default for this zone is Low Security.

| | |
|---|---|
| **Item #:** | 10 |
| **Title:** | Trusted Sites are Defined Appropriately |
| **Reference:** | ➢ Microsoft's "Internet Explorer Enhanced Security Configuration" [3] |
| **Risk:** | Vulnerability 2 & 3 |

| | |
|---|---|
| **Testing Procedure:** | Review the Policy:<br>1. From review of the current organization's policies and standards, verify the standard indicates all domains or sites added to the Trusted Sites zones must have approval from Information Security management.<br><br>Assess the appropriateness of Trusted Sites:<br><br>2. Go to the Trusted Sites Zone and review all sites listed. In IE, go to: Tools > Internet Options…. > Security tab. Verify that:<br>a. Are the sites appropriate with respect to the organization? An engineering firm should have no reason to set http://www.celebritygossip.com as a Trusted Site. Obtain evidence of the business justification for each trusted domain (or sub-domain) listed.<br>b. Have the listed web sites been reviewed by the Security Administrator and approved by management?<br><br>Perform Substantive Testing to Validate Trusted Domains:<br>3. For each URL listed, perform the following audit steps:<br>a. Enter the respective URL in the IE browser. Check the Status Bar to confirm that the site is in the Trusted Sites Zone.<br>b. Randomly select at least three other URLs that are NOT listed in the Trusted Sites zone. Check the Status Bar to confirm that the site does NOT display in the Trusted Sites Zone.<br><br>NOTE the following when reviewing the sites listed in the Trusted Sites Zone:<br>➢ When you add a Web page to the zone, you are including all pages in that DOMAIN. For example, if you add http://www.utexas.edu/alumni/events, you are adding http://www.utexas.edu. If you want to add http://www.bus.utexas.edu, you will have to add this separately because it is a separate domain.<br>➢ A web page can only be part of one zone at a time; you can't add the page to both the Trusted Sites zone and the Restricted Sites zone. (IE will not let you do this!)<br>➢ Entries listed with wildcards, like *.utexas.edu will explicitly add all subdomains for the given domain. For example, if the entry *.utexas.edu is listed as a Trusted Site, both http://www.bus.utexas.edu and http://www.engr.utexas.edu subdomains will be "trusted". |

| | | |
|---|---|---|
| **Test Nature:** | OBJECTIVE: | SUBJECTIVE: YES |
| **Evidence:** | | |
| **Findings:** | | |

## Restricted Sites Configuration

The browser default setting for the Restricted Sites zone is High security.

| | |
|---|---|
| **Item #:** | 11 |
| **Title:** | Insecure Sites are Restricted |
| **Reference:** | ➢ Microsoft's "Internet Explorer Enhanced Security Configuration" [3] |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | Review the Policy:<br>1. From review of the current organization's policies and standards, verify the standard indicates all domains or sites added to the Trusted Sites zone must have approval from Information Security management.<br><br>Assess that all ActiveX, Java, and File Download Capabilities are Disabled:<br>2. In IE, go to: Tools > Internet Options…. > Security tab. In the Restricted Sites Zone, review all domains listed.<br>a) For each URL that is listed, visit each web site. Check the Status Bar to confirm the site has been successfully added to the "Restricted sites" list.<br>b) In IE, go to: Tools > Internet Options…. > Security tab. Go to the Restricted Sites Zone, and click on the "Custom Settings" button to view the security for this zone. Verify the zone is set to the default "High" security level by validating that all options are set to "disable" or "prompt."<br><br>Perform Substantive Testing to Validate Restricted Domains:<br>1. For each URL listed, perform the following audit steps:<br>c. Enter the respective URL in the IE browser. Check the Status Bar to confirm that the site is in the Restricted Sites Zone.<br>d. Randomly select at least three other URLs NOT listed in |

| | |
|---|---|
| | the Restricted Sites zone. Check the Status Bar to confirm that the site does NOT display in the Restricted Sites Zone. |
| **Test Nature:** | OBJECTIVE: / SUBJECTIVE: YES |
| **Evidence:** | |
| **Findings:** | |

## Local Machine Zone Settings

Several known exploits, such as Blaster, HTAExploit or MiMail, have taken advantage of the "My Computer" security zone settings or the "Local Computer" zone settings. In the Windows operating system environment, the security configuration for your machine can also be configured to prevent ActiveX and Java controls from being executed outside your browser's "sandbox." However, configuring this fifth IE Security Zone does require changes to the Windows registry. [Author's Note: Be wary of changing registry keys. If these modifications are not performed correctly, you can cause your system to seriously malfunction (i.e. you may not be able to boot into Windows properly, open Explorer folders, etc.). Tools do exist to help to automate these registry entries, such as PivX's Quik-Fix (http://www.pivx.com/qwikfix/).]

| | |
|---|---|
| **Item #:** | 12 |
| **Title:** | Increase Security on Local Machine Zone |
| **Reference:** | ➢ How to strengthen the security settings for the Local Machine zone in Internet Explorer (Microsoft Knowledgebase Article 833633) [14]<br>➢ Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition [1] |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | Verify the default security settings on the Local Machine Zone are strengthened.<br><br>1. Go the system registry by START > RUN… > type regedit.<br>2. Follow the current path in the registry tree to view the settings for the Local Machine Zone: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone\0` |

NOTE: If you use the Security Zones:
Use only machine settings option to apply Group Policy to all users, the Local Machine Zone settings should be configured in HKEY_LOCAL_MACHINE. However, if you permit users to set their own Internet Explorer security settings, configure the registry values at HKEY_CURRENT_USER.

3. Verify the following recommended registry values are configured:

The following table lists the appropriate registry value names and the default and recommended (strengthened) registry values for certain types of potentially damaging operations.

| Registry Value Name (Type) | Default Registry Value Data | Recom-mended Registry Value Data | URL action | Zone Setting |
|---|---|---|---|---|
| 1200 (DWORD) | 0 (enabled) | 3 (disabled) | URLACTION_ACTIVEX_RUN | Run ActiveX Controls and plug-ins |
| 1201 (DWORD) | 1 (prompt) | 3 (disabled) | URLACTION_ACTIVEX_OVERRIDE_OBJECT_SAFETY | Initialize and script ActiveX controls not marked as safe |
| 1400 (DWORD) | 0 (enabled) | 1 (prompt) | URLACTION_SCRIPT_RUN | Active scripting |
| 1406 (DWORD) | 0 (enabled) | 1 (prompt) | URLACTION_CROSS_DOMAIN_DATA | Access data sources across domains |
| 1C00 (Binary) | 00 00 02 00 | 00 00 00 00 | URLACTION_JAVA_PERMISSIONS | Java permissions |

*This slightly modified table is from the Knowledgebase Article 833633. The table lists the recommended Microsoft values, as described in the article*.

| | | |
|---|---|---|
| **Test Nature:** | OBJECTIVE: YES | SUBJECTIVE: |
| **Evidence:** | | |
| **Findings:** | | |

## *IV. At the Perimeter: Content Filtering*

SANS defines active content filtering and monitoring as:

> Tools that perform active content monitoring examine material entering a computer/network for potentially damaging content, cross-referencing what they scan with continuously updated definitions libraries. [29]

An organization can utilize content filtering technologies to create a "defense in depth" strategy that protects against intrusion via Internet sites. An active content filtering positioned at the network's perimeter can help to:

- Reduce malicious content from entering the network
- Protect users who unintentionally visit inappropriate or insecure web sites
- Prevent users from intentionally accessing web sites that do not adhere to the company's acceptable use policy [25].

### Content Filtering: Compliance with IE Policies

| | |
|---|---|
| **Item #:** | 13 |
| **Title:** | Content Filtering: Compliance with IE Policies |
| **Reference:** | ➢ "Configuring Watchguard Proxies: A Guide to Supplementing Virus Protection and Policy Enforcement." [25]<br>➢ Personal experience |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | 1. Obtain a copy of the browser configuration standards for the organization.<br>2. Obtain a system-generated report of the current content filtering device's configuration, and identify, at a minimum, how ActiveX and Java code is filtered at the network perimeter.<br>3. Compare both configuration standards to assess if the content filtering device conflicts with the company's browser configuration standards. |
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## Content Filtering: Log Retention

In the event of a compromise, malicious code or virus outbreak, system administrators may commonly review device logs in an attempt to identify the cause of the problem. Similar to retaining an IDS or firewall logs to provide a history of network traffic, content filtering device logs may be retained to provide an audit trail of events.

| | |
|---|---|
| **Item #:** | 14 |
| **Title:** | Content Filtering: Log Retention |
| **Reference:** | ➢ "Configuring Watchguard Proxies: A Guide to Supplementing Virus Protection and Policy Enforcement." [25]<br>➢ Personal experience |
| **Risk:** | Vulnerability 2 & 3 |
| **Testing Procedure:** | 1. View online or obtain a system-generated report detailing the content filtering device's auditing parameters are enabled.<br>2. Verify that the archived log files are logically restricted from modification from any unauthorized individuals, including those with privileged rights to modify the device's configuration.<br>3. Verify that the log data is archived in such a way that it cannot be modified, such as copying the files to write-once media.<br>4. Randomly sample a minimum of 15 calendar dates spanning the company's required retention period, dating back from the performance of this audit. Correlate the time stamps on the content filtering device's activity log to validate that logging was occurring throughout the period of reliance. |
| **Test Nature:** | OBJECTIVE: YES \| SUBJECTIVE: |
| **Evidence:** | |
| **Findings:** | |

## **PART 3:** Conduct the Audit Testing, Evidence & Findings

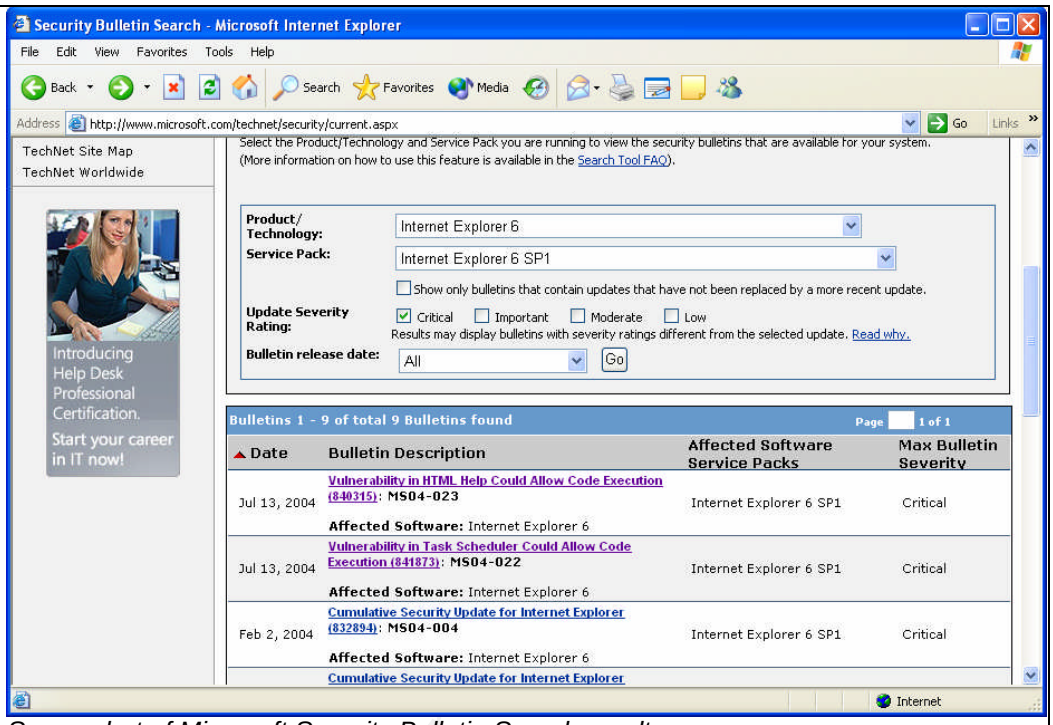
| | |
|---|---|
| **Item #:** | 1 |
| **Title:** | Security Policy |
| **Evidence:** | 1. PASS: The Widgets 'N More "Acceptable Internet use" policy, last revised in June 2003 was obtained.<br>a. PASS: Per discussion with the Information Systems Manager and the Human Resources Manager, all permanent and temporary employees or contractors must sign a hard copy of the "Acceptable Use Policy" prior to obtaining a network User ID.<br>NOTE: An assessment of the effectiveness of the processes of policy communication throughout the organization is not in scope for this audit program.<br>b. PASS: The policy defines that Internet Use must be used only for approved business purposes. The policy clearly states that the Internet must not be used for personal use.<br>c. PASS: The policy prohibits the ability to any files from public URLs.<br>d. FAIL: The policy does not explicitly define permissible downloads. However, per interviews with the Information Systems Manager, the company's de facto standard is to allow file downloads from Intranet and Trusted Sites, which encompass engineering research and business partner web sites.<br>e. FAIL: The company does not have documented browser or content filtering configuration standards.<br>f. PASS: The policy does indicate that all Internet use is subject to audit, and all Internet usage may be monitored.<br>g. FAIL: A required business justification must be documented on a "Request for Internet Access" form and approved by the user's supervisor. However, there is not a process in place to document exceptions. For example, an accountant may request the ability to download statement files from the company's bank's web site. This request and approval process is not a formally documented procedure.<br>h. PASS: Documented server administration policies, distributed to the Windows system administrators, state that Internet browsing and downloaded is not permitted on the server unless it is reasonably required for system maintenance purposes.<br>i. FAIL: Company guidelines for acceptable use do not encourage users to not "click on" suspicious or unknown links given in email or on web page to eliminate security |

| | |
|---|---|
| | risks, such as installing unknown viruses. However, the policy does not give detailed guidance on how users should handle digital signatures, certificates and cookies. (NOTE: This audit will NOT address an audit of security and IE configuration for privacy settings.) |
| **Findings:** | Exceptions noted:<br><br>1. Widgets 'N More does not maintain a comprehensive "acceptable use policy" that addresses user behavior when surfing the Internet.<br>2. The company has not documented minimum browser configuration standards.<br>3. A procedure has not been created that addresses the appropriate protocol for handling exceptions to the acceptable Internet use policy. |

| | |
|---|---|
| **Item #:** | 2 |
| **Title:** | IE browser updates and patches are up-to-date |
| **Evidence:** | 1. PASS: A general statement in the company's IT security policy does state that all critical security patches must be applied, at a maximum, within 3 business days. All applicable cumulative security updates or system upgrades (i.e. service packs) must also be applied timely.<br><br>I reviewed Microsoft's web site and identified the following critical patches that were released in the last 30 days include: |

| | | | |
|---|---|---|---|
| Jul 13, 2004 | Vulnerability in HTML Help Could Allow Code Execution (840315): **MS04-023**<br><br>**Affected Software:** Internet Explorer 6 | Internet Explorer 6 SP1 | Critical |
| Jul 13, 2004 | Vulnerability in Task Scheduler Could Allow Code Execution (841873): **MS04-022**<br><br>**Affected Software:** Internet Explorer 6 | Internet Explorer 6 SP1 | Critical |
| Feb 2, 2004 | Cumulative Security Update for Internet Explorer (832894): **MS04-004**<br><br>**Affected Software:** Internet Explorer 6 | Internet Explorer 6 SP1 | Critical |

*Excerpt from Microsoft's Security Bulletin search results.*




*Screenshot of Microsoft Security Bulletin Search results page.*

TEST OPTION A: FAIL
The following registry settings were verified to prove that these two updates were applied on the system:

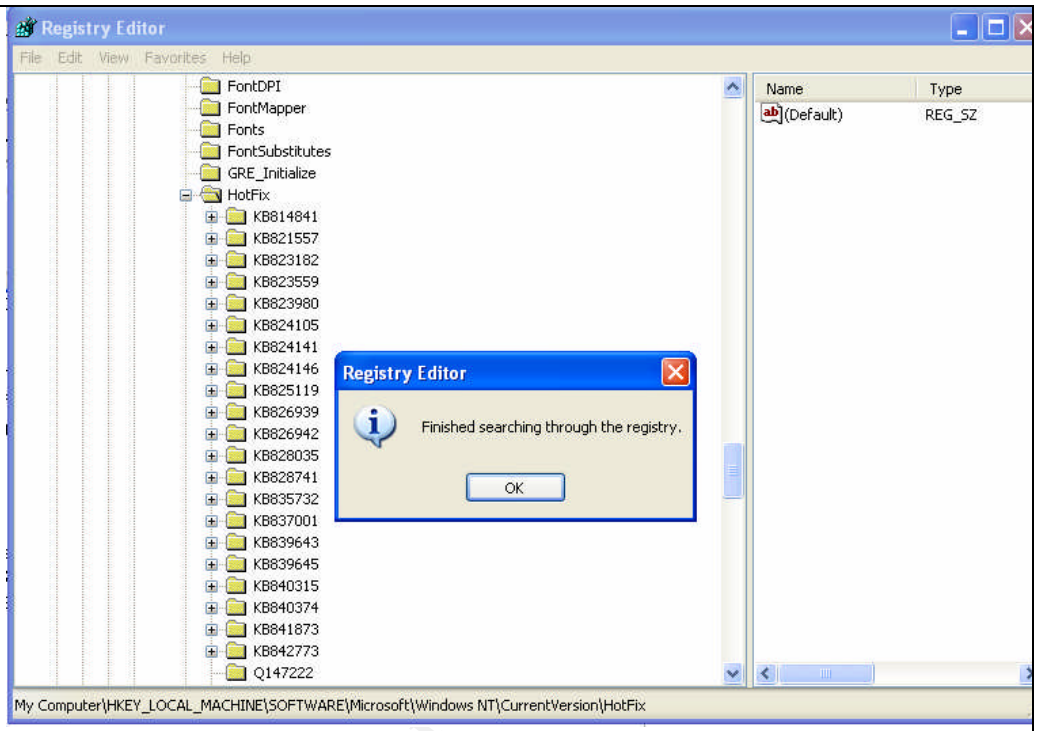
- 840315
- 841873

The following excerpts were taken from a registry key values exported in a text format:

```
Key Name:          HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\HotFix\KB840315
Class Name:        <NO CLASS>
Last Write Time:   7/19/2004 - 6:17 PM
```

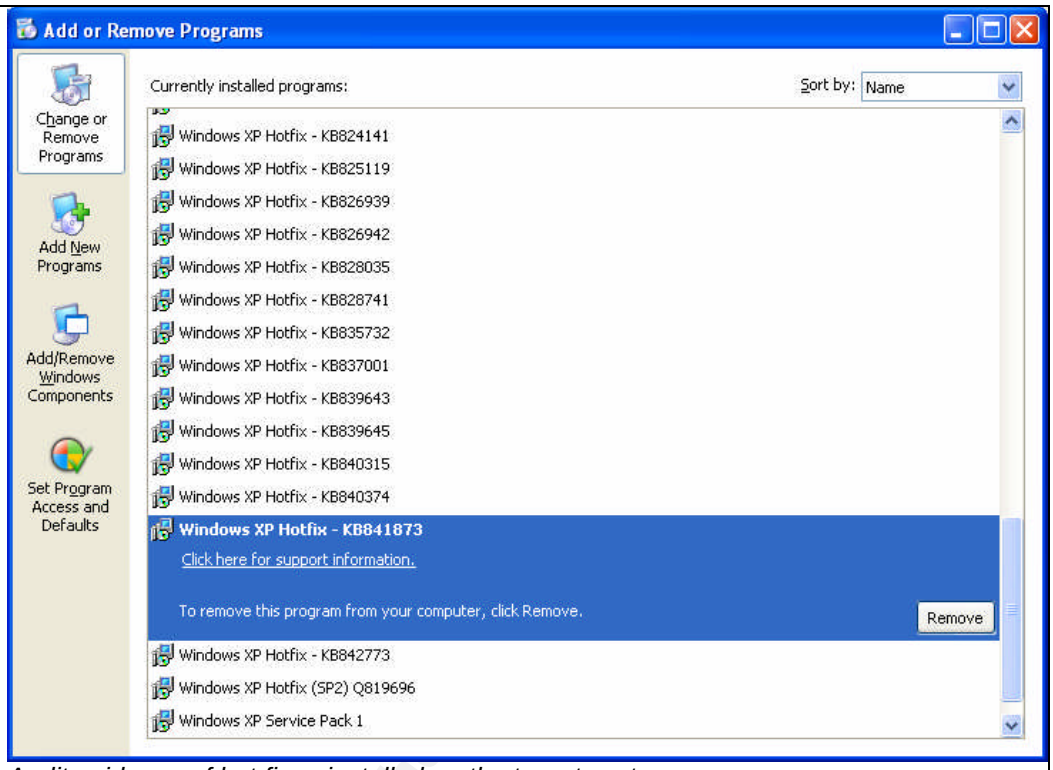
```
Key Name:          HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\HotFix\KB841873
Class Name:        <NO CLASS>
Last Write Time:   7/19/2004 - 6:18 PM
```

However, I could not validate that the Cumulative Security Update (832894) released in February 2004 was not installed through review of the registry (see figure below)



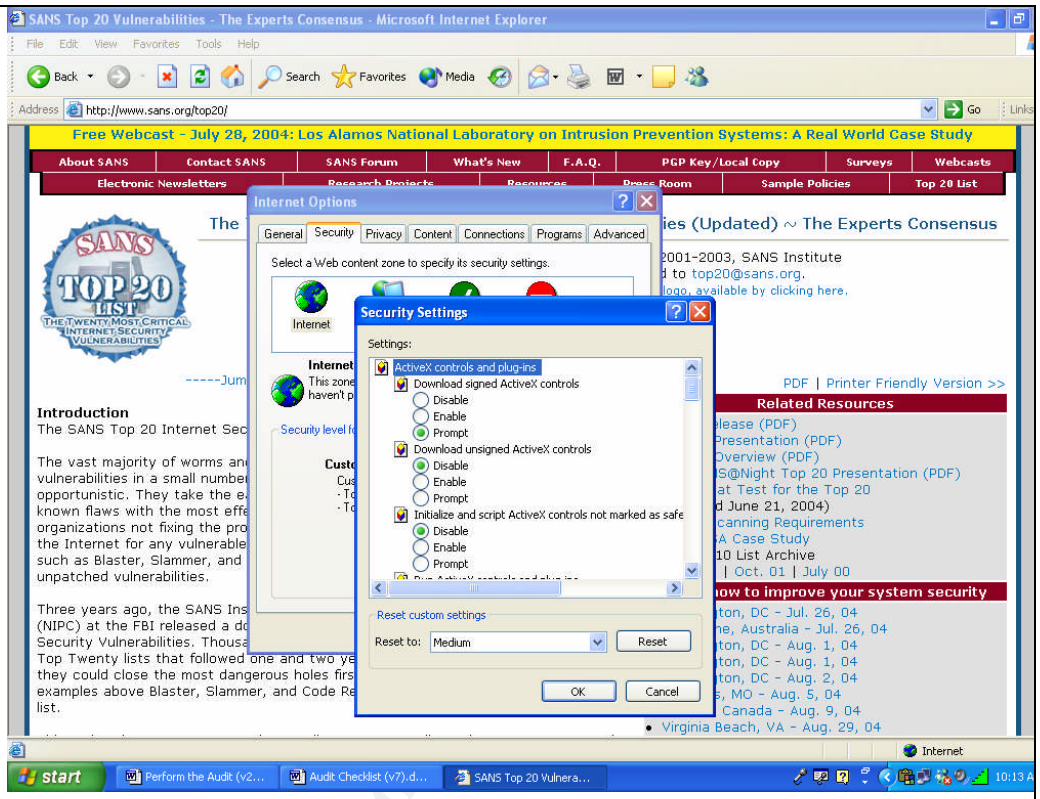

*This screen shot displays the "Find" results when the registry key "832894" was searched.*

TEST OPTION D: FAIL:
To confirm my findings noted in the previous audit step, I also reviewed the "Add or Remove Programs" menu in the "Start Menu" to identify all Windows XP Hotfixes that had been applied (see screenshot below). I could not validate that the cumulative security update was applied.

| | |
|---|---|
| |  <br>*Audit evidence of hot fixes installed on the target system.* |
| **Findings:** | Exceptions noted:<br>The most recent IE security update was not applied. |

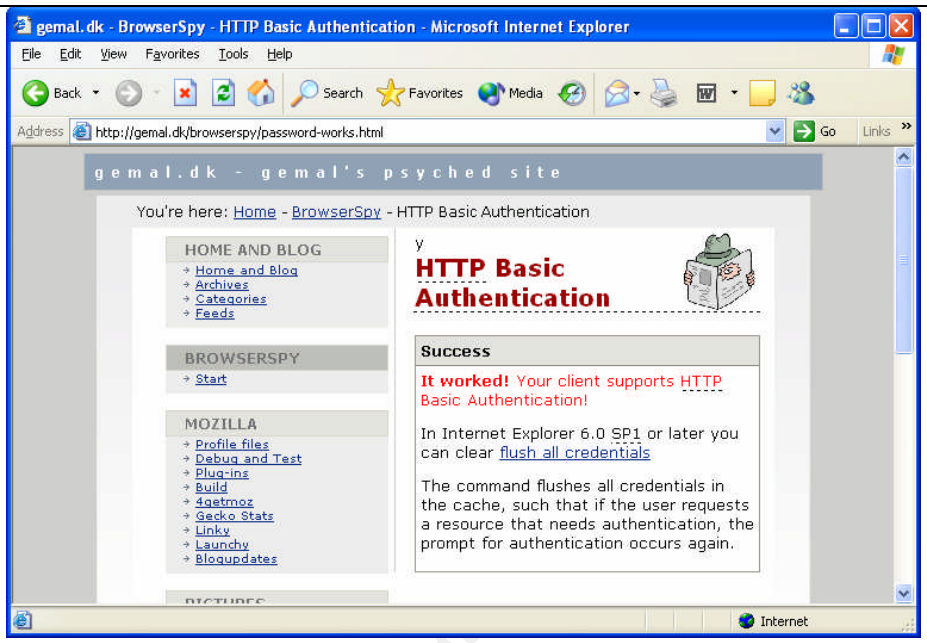
## Unprivileged users are prevented from changing IE security policies

| | |
|---|---|
| **Item #:** | 3 |
| **Title:** | Unprivileged users are prevented from changing IE security policies |
| **Evidence:** | 1. PASS: Widgets 'N More's IT Security Policy does note that "the ability to perform administrative or 'super user' functions on all systems must be limited to only management-approved personnel. All privileged users must have an appropriate business justification that does not present a segregation of duties issue, and access must be provisioned with the principle of least privilege." It was determined that these policy statements were reasonable based on guidance generally accepted by the information security community, from such sources as NIST, SANS, and CobiT.<br>2. FAIL: The Security tab is visible to the unprivileged user, and browser did accept a change made to the Security configuration. |

| | |
|---|---|
| |  |
| **Findings:** | Exceptions noted:<br>Users are not restricted from modifying security configuration of the Internet Explorer. |

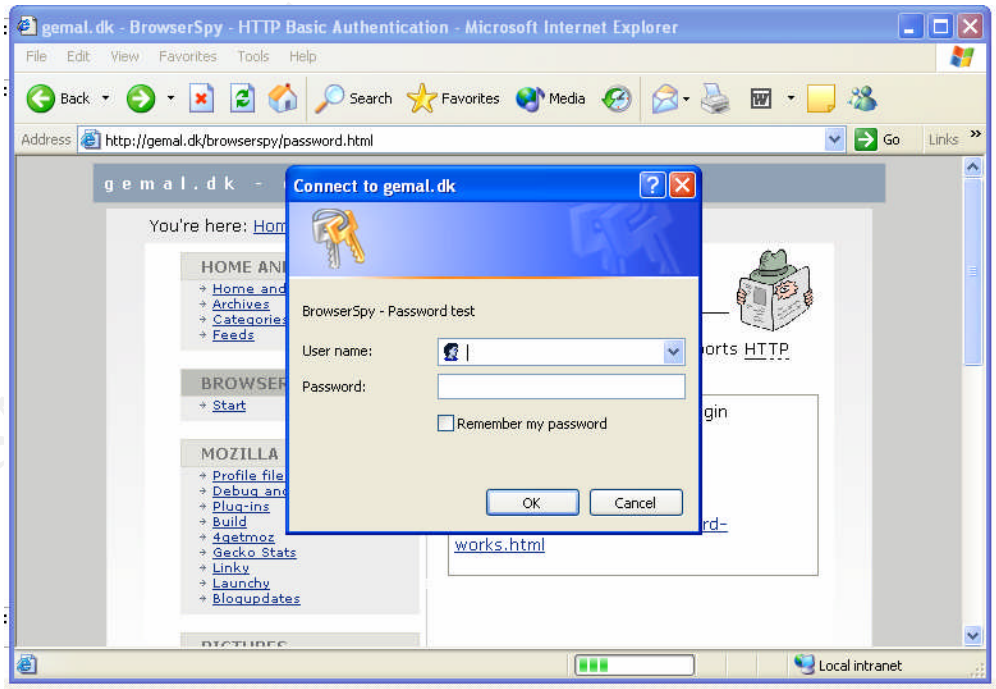
## User Authentication

| | |
|---|---|
| **Item #:** | 4 |
| **Title:** | User Authentication is Disabled or Allows Prompt for Logon Credentials |
| **Evidence:** | TEST for ANONYMOUS LOGON SETTING: PASS<br>1. When accessing the test web site, was prompted with a user ID and password window. After successfully authenticating, received this message from the browser: |




Judging from the browser's reaction, I was able to verify that "Anonymous Logon" was not enabled.

2. Added the http://gemal.dk domain to the "Intranet Sites" listing. Again, attempted to access the password prompt page:




"Anonymous Logon" is not enabled in the Intranet Zone. From that browser reaction, I could deduce that "Anonymous Logon in Intranet Zone" or "Anonymous Logon with user name and password" is enabled.

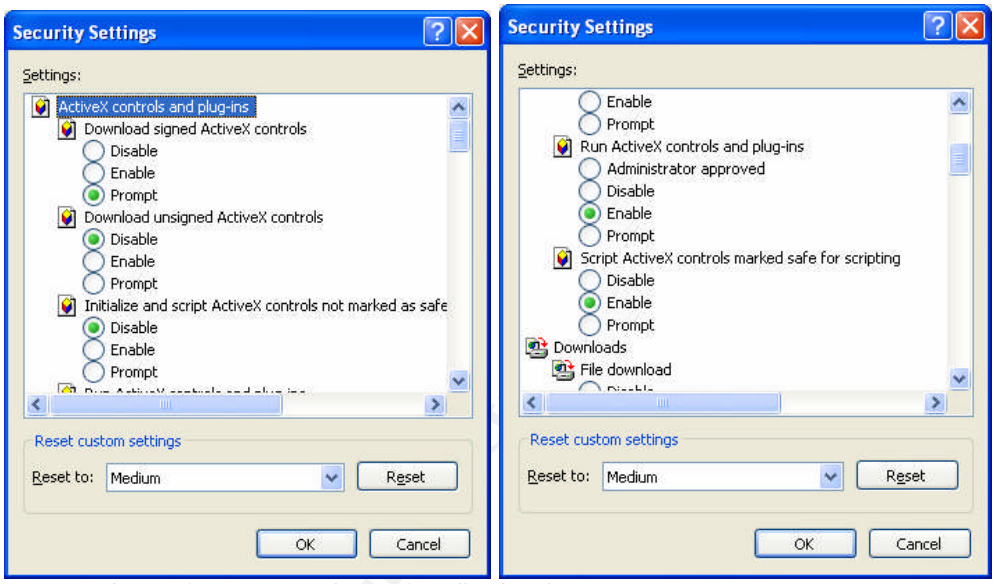
| | |
|---|---|
| | 3. While logged on to the audited PC as a Local Administrator, created a user account with the following credentials:<br>User ID: test<br>Password: test<br>4. Logged out of the local computer, and logged back in as the "test" user ID. Once again, accessed gemal.dk's web site. When clicking on the password-works.html link, I was not prompted with a web prompt. From that browser reaction, I could deduce that "Anonymous Logon in Intranet Zone" or "Anonymous Logon with user name and password" is enabled.<br>5. Removed the gemal.dk web site from the Trusted Sites list, which causes the browser to treat the domain as an Internet site. Again, I visited the test password-works.html page. I was prompted for a user ID, as a result. From this reaction, I was able to determine that the "Anonymous Logon in Intranet Zone" setting was probably enabled for the Internet Zone. |
| **Findings:** | No exceptions noted. |

### Secure Internet Zone Configuration: ActiveX

| | |
|---|---|
| **Item #:** | 5 |
| **Title:** | Disable All ActiveX Controls |
| **Evidence:** | 1. FAIL: Widgets 'N More does not have a documented browser configuration standard that prohibits or restricts ActiveX functionality.<br>2. FAIL: The following is a summary table of the audit test findings: |

| Pass/Fail | Parameter | Expected Setting | Current Setting |
|---|---|---|---|
| FAIL | Download signed ActiveX controls | Disable | Prompt |
| PASS | Download unsigned ActiveX controls | Disable | Disable |
| FAIL | Initialize and script ActiveX controls not marked as safe for scripting | Disable | Disable |
| FAIL | Run ActiveX controls and plug-ins | Disable | Enable |
| FAIL | Script ActiveX controls marked safe for scripting | Disable | Enable |
| Unable to | Run components not signed | Disable | Setting |

| | | | |
|---|---|---|---|
| Determine | with Authenticode | | not available |
| Unable to Determine | Run components signed with Authenticode | Disable | Setting not available |



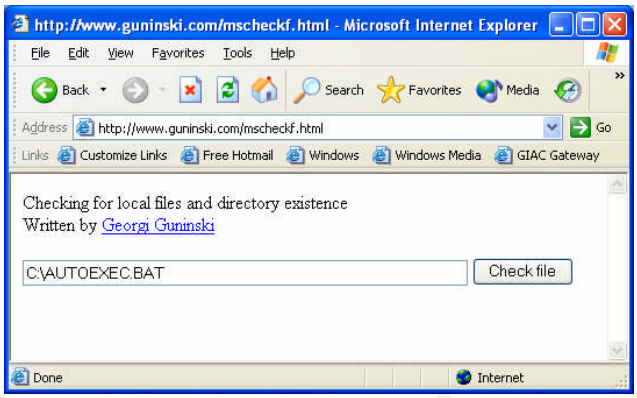

*Screen shots of current settings of audited IE browser.*

3. FAIL: I accessed the following web sites and was not presented with any Security Warning message boxes (see figures below):
   - http://www.cnn.com
   - http://www.aol.com
   - http://www.guninski.com/mscheckf.html

   The web sites loaded in IE with no sign of error. Per these testing results, the "enabled" setting for "Run ActiveX controls and plug-ins" was verified.


*Screen shot of IE's immediate result when the CNN web site was accessed.*


*Screen shot of IE's immediate result when the ESPN web site was accessed.*

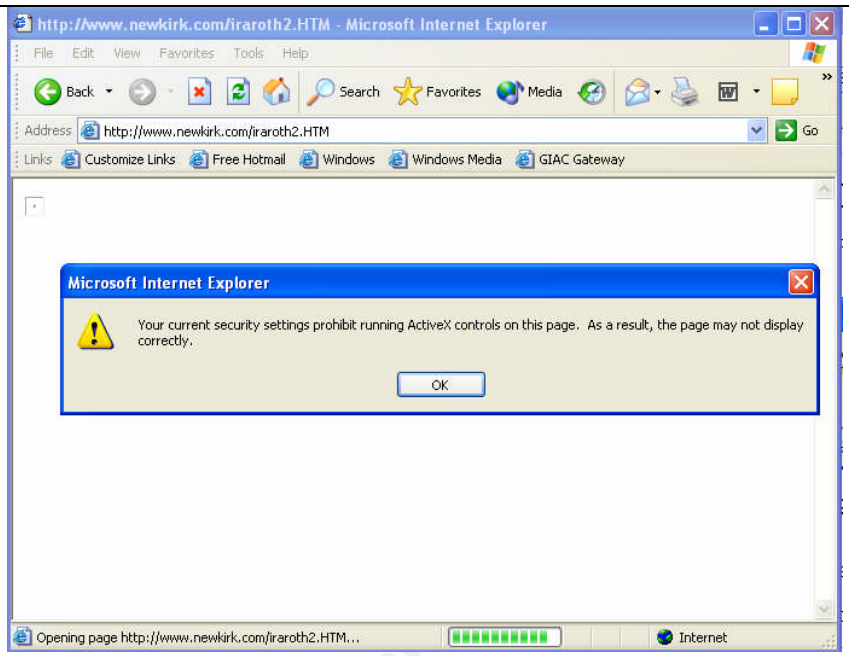



*Screen shot of IE's immediate result when George Guninski's ActiveX test page was accessed.*

4. FAIL: After entering the AOL web site in IE, I was not presented with any Security Warning message boxes (see figures below). Per these testing results, the "enabled" setting for "Script ActiveX controls marked safe for scripting" was verified.


*Screen shot of IE's immediate result when the ESPN web site was accessed.*

5. PASS: Although the audited browser does not have Authenticode functionality, IE still prohibited the unsigned ActiveX control embedded at the http://www.newkirk.com/iraroth2.HTM web page.

| | |
|---|---|
| |  |
| **Findings:** | Exceptions noted:<br>Although the Internet Zone is configured to prevent unsigned ActiveX controls from executing, all ActiveX code that is signed or "marked safe" is allowed. This continues to be a risk because malicious code may have been embedded, or the authenticated code signer may not have performed any secure code reviews. |

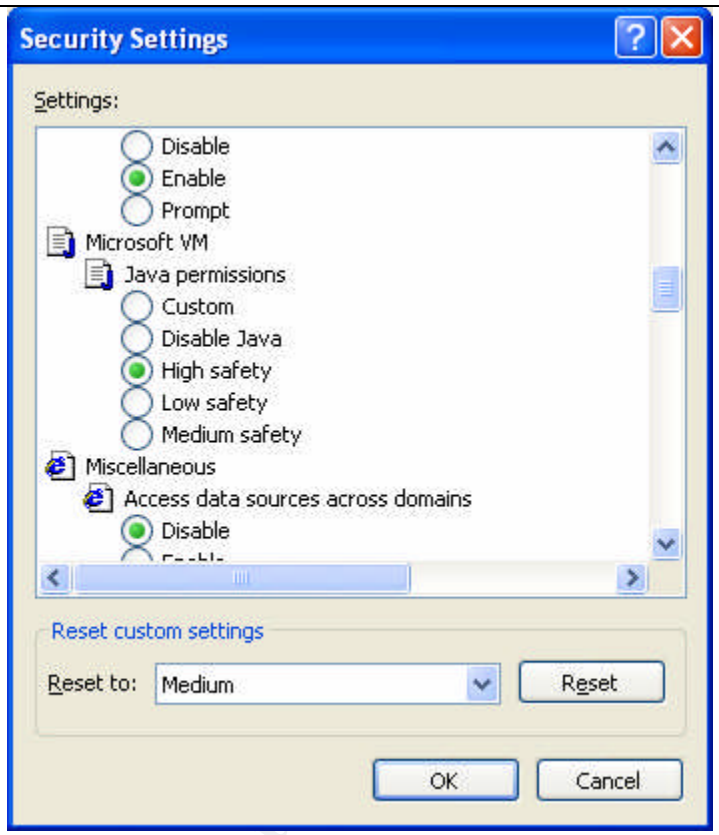
### Secure Internet Zone Configuration: File Downloads

| | |
|---|---|
| **Item #:** | 6 |
| **Title:** | Disable the Ability to Download Files |
| **Evidence:** | 1. PASS: Documented policies do state that the company prohibits or restricts users from the ability to download files from the Internet, unless an appropriate business justification is approved by management.<br>2. FAIL: When I attempted to download an executable file, the browser did prompt for permission to download a file and allowed me to save the file to my desktop. |

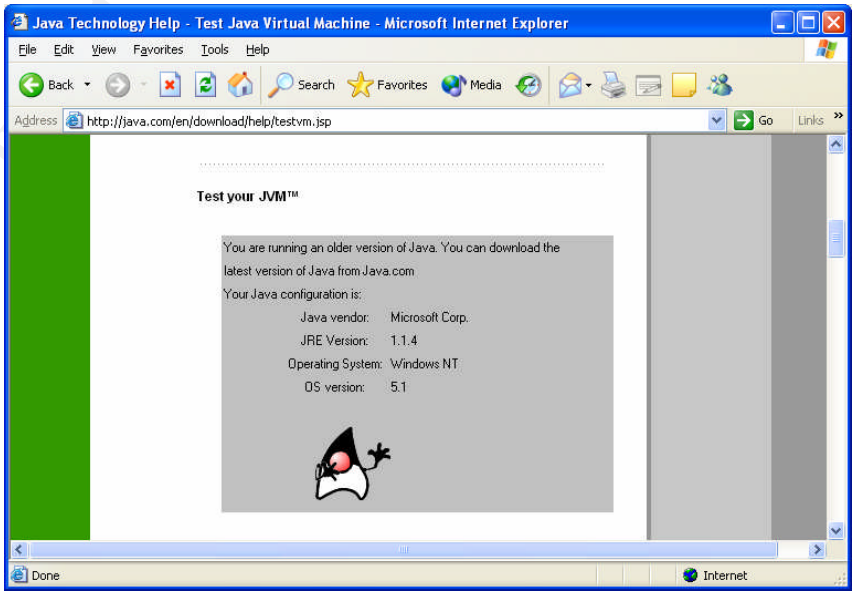
| | |
|---|---|
| |  |
| **Findings:** | Exceptions noted:<br>The ability to download files from the Internet is not disabled. |

### Secure Internet Zone Configuration: Java

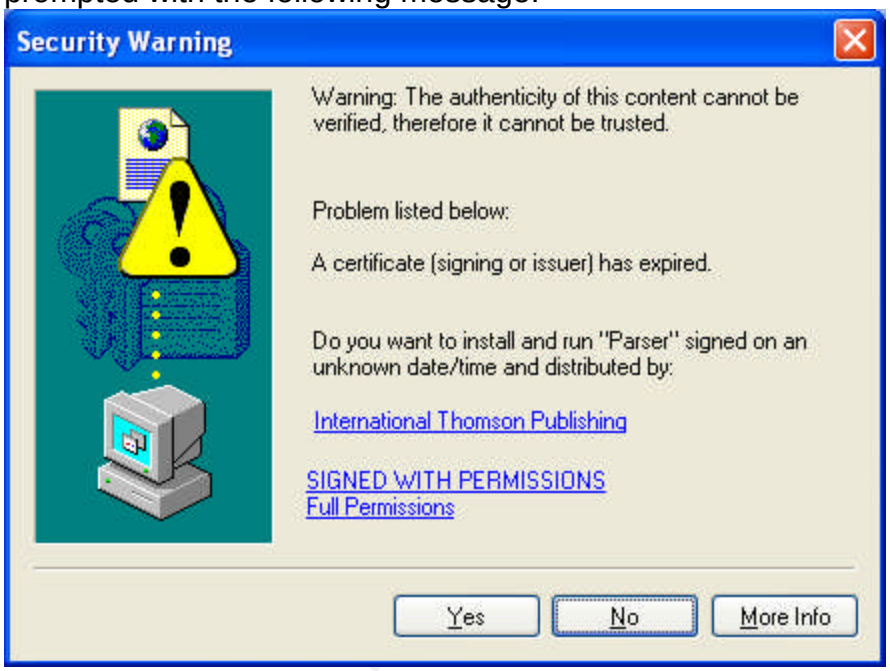
| | |
|---|---|
| **Item #:** | 7 |
| **Title:** | Disable or Restrict Java Permissions (Microsoft VM) |
| **Evidence:** | 1. FAIL: Widgets 'N More does not have a documented browser configuration standard that prohibits or restricts Java functionality.<br>2. Through review of the Security tab of "Internet Options," validated that "High Safety" was set for Java security on the browser. |




3. a. PASS: The Java browser did accept trusted Java code.
   b. FAIL: Using Internet Explorer, I visited the Sun's Java Tester and JavaTester.org web sites and verified from the web page's results that a Java Virtual Machine was installed, and Java is enabled on the Internet Zone of the browser.

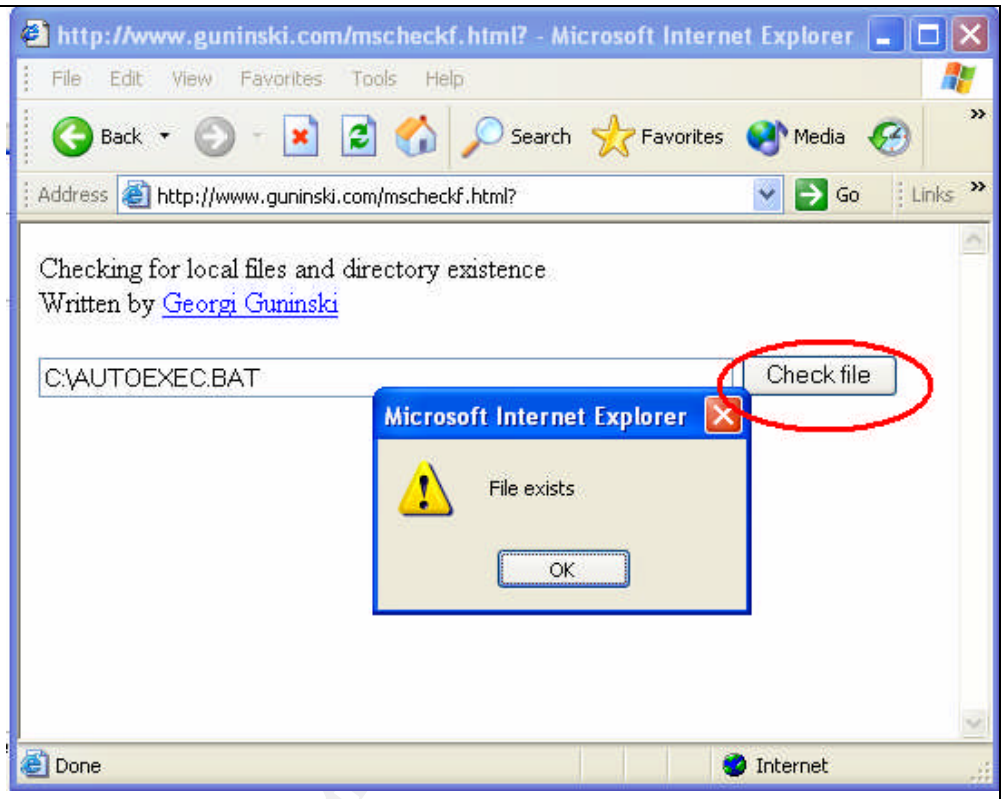



When I attempted to access the brookscole.com web site, I was

| | |
|---|---|
| | prompted with the following message:<br>  <br> |
| **Findings:** | Exceptions noted:<br>Although Java security is restricted, documented policies or standards for browser configuration do not exist. |

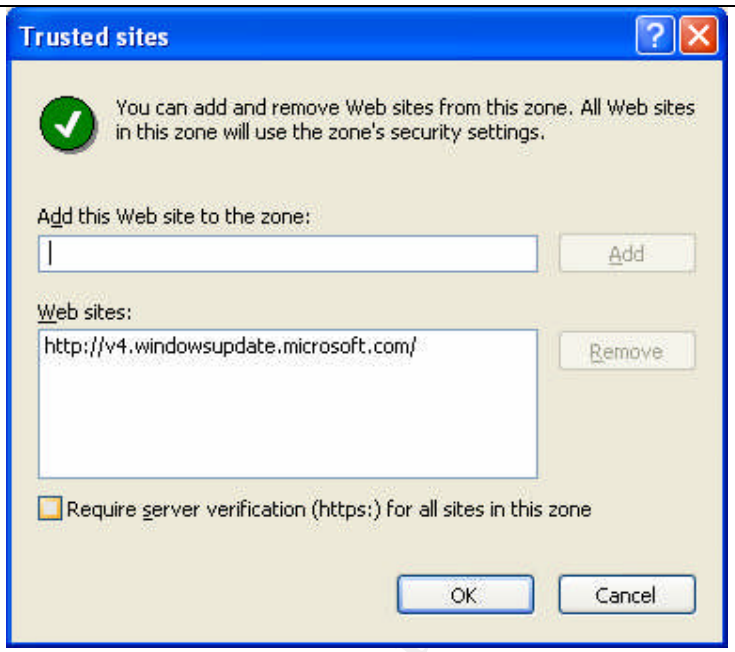
### Secure Internet Zone Configuration: Active Scripting

| | |
|---|---|
| **Item #:** | 8 |
| **Title:** | Scripting is disabled or restricted |
| **Evidence:** | 1. FAIL: Widgets 'N More does not have documented browser security configuration standards that address active scripting settings.<br>2. FAIL: When the Guninski test URL was accessed via the browser, there was no security prompt message returned. The "Check File" function of the web page, which checks if a file exists on your local computer, did run without error. |

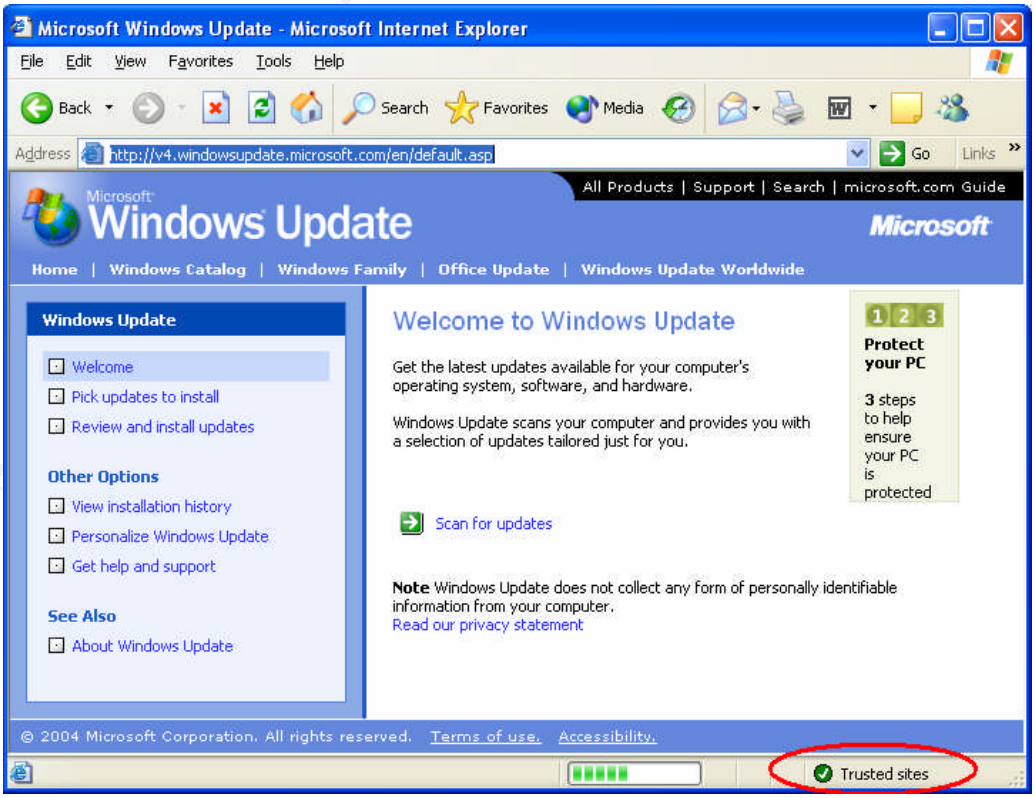
| | |
|---|---|
| |  |
| **Findings:** | Exceptions noted:<br>Active Scripting options should be disabled in the Internet Zone. |

## Trusted Sites Configuration

| | |
|---|---|
| **Item #:** | 10 |
| **Title:** | Trusted Sites are Appropriate |
| **Evidence:** | 1. FAIL: The organization does not have formal policies and procedures, or configuration standards that outline the evaluation and approval process for adding Trusted Sites to the IE security zone.<br>2. PASS: From review of the URLs listed in the Trusted Sites Zone, it is reasonable to assume that the "Windows Update" web site is an appropriate trusted site (depending on what your opinion is about Microsoft). |




3. a) PASS: The Microsoft Windows Update URL was entered in the browser to verify that the browser recognizes it as a "Trusted Site."



| | |
|---|---|
| | b) PASS: In order to assess if other web sites were NOT included in the Trusted Sites list, I randomly chose three web sites:<br>➢ http://www.cnn.com<br>➢ http://www.espn.com<br>➢ http://www.whitehouse.gov<br>  <br> |
| **Findings:** | Exceptions noted:<br>Trusted sites appear to be reasonable. However, the organization lacks documented policies and procedures for evaluating, approving and configuring Trusted Sites in IE. |

## Restricted Sites Configuration

| | |
|---|---|
| **Item #:** | 11 |
| **Title:** | Insecure Sites are Restricted |
| **Evidence:** | 1. FAIL: The organization does not have formal policies and procedures, or configuration standards, which outline the process for identifying sites that should be restricted and for subsequently reviewing and implementing restricted IE zone security accordingly.<br>2. N/A: No Restricted Sites are defined.<br>3. PASS: Although no restricted domains are explicitly defined, |

| | |
|---|---|
| | the Restricted security zone does indicate a high level of security, with notably all code and file download functionality disabled. |
| **Findings:** | Exceptions noted:<br>The organization does not have formal policies and procedures for identifying restricted sites and, subsequently, configuring the browser accordingly. |

# PART 4: Audit Report or Risk Assessment

## I. Executive Summary

The scope of this audit was to assess the security posture of an Internet Explorer browser installed on a PC workstation at Widgets 'N More. Prior to the audit, the test workstation's hard drive was completed erased, and the company's standard Windows XP and Internet Explorer installation was applied. The scope of this review includes only

- The security policies and procedures specific to Internet usage and IE browser configuration
- Security settings of Internet Explorer (in the "Security" tab of IE's Internet Options menu)
- Content filtering device configuration and logging practices

This audit's findings revealed that the Internet Explorer browser configuration maintains a poor security posture. Although Widgets 'N More has a documented Acceptable Internet Use policy, there are opportunities to improve IE configuration standards to mitigate the risk of browser-based attacks. The following is a summary of the gaps noted, in order of highest to lowest risk:

| GAP | Risk Rating |
|---|---|
| Lack of policy and browser configuration standards | **High** |
| Poor security restrictions for "Active Content" (i.e. ActiveX controls, JavaScript and VBScript) | **High** |
| IE Security Updates (patches) are not consistently applied | **High** |
| No process is in place for maintaining configuration for appropriate Local Intranet, Trusted, and Restricted web sites | **High** |
| Users are not restricted from the ability to reconfigure IE security | **Medium** |
| Lack of policy and browser configuration standards | **Medium** |

## II. Audit Findings

Below is a chart capturing the summary findings from this audit of an Internet Explorer 6 SP1 browser, installed on a PC workstation located at Widgets 'N More's corporate headquarters. Note that the audit checklist items below denoted with an asterisk (*) indicate that the browser security settings were acceptable, but the requirement for documented policy and standards was not met.

| No. | Checklist Item Description | Pass/Fail |
|---|---|---|
| 1 | Internet Use and Browser Security Policy exists | **Fail** |
| 2 | IE browser updates and patches are up-to-date | **Fail** |
| 3 | Unprivileged users are prevented from changing IE security policies | **Fail** |
| 4 | User Authentication is Disabled or Allows Prompt for Logon Credentials | **Pass** |
| | *Secure Internet Zone Configuration:* | |
| 5 | Disable All ActiveX Controls | **Fail** |
| 6 | Disable the Ability to Download Files | **Fail** |
| 7 | Disable or Restrict Java Permissions | **Fail*** |
| 8 | Active Scripting is disabled or restricted | **Fail** |
| 10 | Trusted Sites are appropriately defined | **Fail*** |
| 11 | Insecure Sites are Restricted | **Fail*** |

*NOTE: The asterisk (*) indicates that the item failed only due to the lack of documented policy and standards.*

### Audit Finding #1 – *Lack of policy and browser configuration standards*

Although Widgets 'N More does have a documented Internet Acceptable Use policy, the organization lacks standards for users' Internet "surfing behavior" and browser configuration.

**Risk - *High***

Without clear policies and procedures developed to support the organization's objectives to prevent or mitigate the risks of browser-based attacks, both system administrators and users cannot implement consistent security browser security controls.

### Audit Finding #2 – *Poor security restrictions for "Active Content"*

Audit test results revealed that the security level for public Internet sites enforces minimal security restrictions for "active content," such as ActiveX and JavaScript. Generally, code from a recognized source (trusted or signed code) may be executed, although only minimum restrictions are enforced to prevent malicious code from being downloaded and run on user's local PCs.

**Risk - *High***
Browser-based attacks and the introduction of malicious code and viruses to an organization are largely a result of code execution and file downloads by accessing a web site with Internet Explorer. Although mitigating controls such as content filtering at the network border, disabling IE's active content capabilities for public Internet web sites is strongly recommended.

### Audit Finding #3 – *IE Security updates are not consistently implemented*

Current security patches were applied to the audited IE browser; however, the most recent "cumulative security update" (released February 2004) was not applied. This exception indicates a lack of compliance with the organization's IT security policies.

**Risk - *High***
Attacks against IE browsers may also be a result of known vulnerabilities that exist on a system where current patches have not been applied. These vulnerabilities are generally related to flaws in the IE browser design. If the system is comprised due to browser vulnerabilities, unauthorized access to systems and data may result.

### Audit Finding #4 – *No process is in place for maintaining security controls for appropriate Local Intranet, Trusted, and Restricted web sites*

There is currently no process in place for identifying URLs to be added to the IE security zone configuration.

**Risk - *Medium***
In order to ensure that the organization's business needs are met, required web sites needed for business purposes may be explicitly configured to allow full browser viewing functionality.

### Audit Finding #5 – *Users are not restricted from the ability to reconfigure IE security*

The IE browser configuration settings allow unprivileged (non-administrative) users the ability to modify IE's security configuration.

**Risk - *Medium***

The lack of controls implemented to limit a user from undoing a secure browser configuration deployment increases the organization's risk of attack. IE may be deployed to disable all ActiveX, Java, and file download capability to maintain a high level of security when browsing the Internet, which generally results in limiting functionality accessing Internet websites. As a result, users may circumvent security controls and reconfigure IE to allow for more browsing functionality.

## *II. Audit Recommendations*

### Audit Recommendation #1 – *Develop, Communicate, and Implement Browser Security Policies*

Widgets 'N More should consider establishing and communicating the following policy, procedures and standards:

- Standard browser configuration deployment
- Communication of safe "Internet browsing" practices to users
- Restrictions on "active content" (at the browser and the network border) and file downloads
- Establish a process for identifying, evaluating and approving trusted websites

A project plan for effective policy development should be limited to the publication of an official company policy. A standard must be applied in practice throughout the organization, and compliance with the policy must be enforced. The company should consider the following action items to include with policy development:

- *Develop a plan to communicate the policies to all Internet users* (including IT, business users, payroll and non-payroll employees)
- *Obtain evidence that the users have acknowledged the policy.* [NOTE: Obtaining a documented audit trail is critical for such regulatory requirements as Sarbanes-Oxley, and various US and international privacy acts. Even if Widgets 'N More's current legal and regulatory requirements do not require this level of documentation, it would be mindful to adhere to these documentation requirements.]
- *Ensure that the standards can be realistically enforced.* A post-review process might be in order if both the system administrators and users cannot adhere to the recommended browser security configuration standards.
- *Establish procedures to monitor on-going compliance with the policy.* Controls should be put in place to prevent or detect policy violations. Periodic audits may also be considered.

The cost associated with internal policy development is determined by the amount of man hours allocated to the project. The initial creation of policies generally is the most significant and time-consuming phase of policy development; however, annual policy reviews during a period with little shift in the technology or business environment may even be completed in the matter of one meeting. Generally, the level of staff involvement, organizational "politics", and conflicts with other projects or peak business periods are critical factors in estimating the level of effort and time associated with policy development.

Although having security-minded IT and business users help to mitigate the risks from Internet-based attacks, there is no compensating control for a comprehensive, effective, and enforced policy.

### Audit Recommendation #2 – *Establish a Process for Configuring and Deploying Strong IE Security Controls*

To implement and maintain strong security controls when accessing Internet websites, the organization should consider establishing standard procedures for assessing IE security settings. Widgets 'N More should not only address the poor security settings discovered in this audit, but consider developing a sustainable program for maintaining a strong defense against browser-based attacks.

System administrators should subscribe to CERT, Microsoft email distribution lists, or other security advisory services to receive timely updates of new browser patches and newly discovered IE vulnerabilities. As each alert is received, IT staff should evaluate alerts the implication on the organization's environment, in order to take the necessary action steps (i.e. install a patch, update the browser or content filtering device configuration, etc.). IT staff should keep current on new viruses and IE vulnerabilities by researching recent news postings, and by obtaining the appropriate training. Organizational employees using the Internet should also be trained on safe Internet-browsing practices.

The organization should perform periodic reviews to evaluate the standard Internet Explorer configuration that is installed on all company PC workstations and servers. To configure IE securely, it is recommended that, at a minimum, the following controls be implemented:

- Keep browser security critical patches up-to-date
- Disable ActiveX, Java, and Scripting functionality
- Always prompt users to authenticate
- Disable file downloads
- If the Local Intranet and Trusted Sites security zones are used:

- If active content is required, allow only allow signed or “safe” code to run
- Only add required, secure URLs with an approved business justification to the Local Intranet and Trusted Sites zones

IE browser configuration should be evaluated for compliance with the company’s policies, procedures and standards. Also, this audit checklist presented in this paper may also be used as a guideline for applying strong IE security controls. If the IT department maintains computer installation and configuration “minimum baseline standard” checklists, IE configuration reviews could also be incorporated into this server or workstation build process.

Just as Windows system administrators must maintain operating system patches and configuration settings, the same protocol must be followed with Internet Explorer. Staff time invested in identifying new IE vulnerabilities, and maintaining a high level of security for browsers installed on the company’s computers, should be a minimal cost if IE maintenance tasks are integrated with existing system administration processes.

The risks associated with poor security configuration of IE may be mitigated by an effective content filtering device that examines incoming Internet traffic at the company’s network border. However, due to network performance trade-offs that result from strict content filtering rules, a more effective and realistic solution in addressing IE security risks is to implement strong security policies at the user’s desktop *and* the network perimeter.

---

# References


[1] McClure, Stuart, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition. Berkeley, California: McGraw-Hill/Osborne, 2003.

[2] "Internet Explorer 6 Administration Kit Service Pack 1: Deployment Guide." Microsoft web site. © 2004. URL: http://www.microsoft.com/windows/ieak/techinfo/deploy/60/en/default.mspx.

[3] "Internet Explorer Enhanced Security Configuration." Microsoft web site. © 2004. URL: http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/iesechelp.asp.

[4] "Description of Internet Explorer security zones registry entries." Microsoft web site. © 2004. 26 May 2004. http://support.microsoft.com/default.aspx?scid=kb;en-us;182569.

[5] "ActiveX Controls." Microsoft MSDN site. © 2004. URL: http://msdn.microsoft.com/library/default.asp?url=/workshop/components/activex/activex_node_entry.asp.

[6] "About URL Security Zones Templates." Microsoft MSDN web site. © 2004. URL: http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/templates.asp.

[7] "US-CERT Technical Cyber Security Alert TA04-163A: Cross Domain Redirect Vulnerability in Internet Explorer." US-CERT. 11 June 2004. URL: http://www.us-cert.gov/cas/techalerts/TA04-163A.html.

[8] "US-CERT Technical Security Alert TA04-184A. Internet Explorer Update to Disable ADODB.Stream ActiveX Control." US-CERT. 2 July 2004. URL: http://www.us-cert.gov/cas/techalerts/TA04-184A.html.

[9] Smith, Randy Franklin. "Internet Explorer Security Options (Parts 1 through 6)." Windows Network Magazine. Randy Franklin Smith. 7 June 2001. URL: http://www.winnetmag.com/Article/ArticleID/21282/21282.html.

[10] "Microsoft Security Bulletin Search." Microsoft. © 2004. URL: http://www.microsoft.com/technet/security/current.aspx.

[11] "Microsoft Baseline Security Analyzer V1.2." Microsoft. 6 July 2004. URL: http://www.microsoft.com/technet/security/tools/mbsahome.mspx.

[12] "Cyscape BrowserHawk Features and Benefits." Cyscape. July 2004. URL: http://www.cyscape.com/products/bhawk/features.asp.

[13] Gemal, Henrik. "BrowserSpy." Gemal.dk. © 1995-2004. URL: http://gemal.dk/browserspy/.

[14] "How to strengthen the security settings for the Local Machine zone in Internet Explorer (Microsoft Knowledgebase Article 833633)." Microsoft. 21 Jan 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;833633.

[15] Schnoll, Scott. "Internet Explorer Security Zones." SANS web site. © 2002. URL: http://www.sans.org/rr/papers/67/287.pdf.

[16] Guninski, George. "Internet Explorer Security – George Guninski Security Research." George Guninski web site. URL: http://www.guninski.com/browsers.html.

[17] Guninski, George. "Checking for Files and Directory Existence." George Guninski web site ("Internet Explorer" section). URL: http://www.guninski.com/mscheckf.html.

[18] Guninski, George. Fractal moving over an IE modal dialog and other windows." George Guninski web site ("Internet Explorer" section). URL: http://www.guninski.com/opf2.html.

[19] "IRA Select Internet Release Notes." Newkirk. URL: http://www.newkirk.com/iraroth.HTM.

[20] "Using ActiveX on the Web." NetPanel. 30 Sept 1997. URL: http://www.netpanel.com/articles/internet/actx-use.htm.

[21] "Test your Java™ Virtual Machine." Sun Microsystems. URL: http://java.com/en/download/help/testvm.jsp.

[22] Horowitz, Michael. "Is Your Web Browser Java Enabled?" JavaTester.org. 17 June 2004. URL: http://www.javatester.org/enabled.html.

[23] "Blocks." JavaCommerce.com. URL: http://www.javacommerce.com/cooljava/games-advanced/blocks/blocks.html .

[24] "Lab 6.2: Parsing Out." Brooks/Cole. © 1998. URL: http://www.brookscole.com/compsci_d/templates/student_resources/0534953654_deckerhirchfield/aeonline/course/6/2/index.html.

[25] Mercer, Allan. "Configuring Watchguard Proxies: A Guide to Supplementing Virus Protection and Policy Enforcement." SANS Paper. 5 Sept 2003. URL: http://www.sans.org/rr/papers/21/1255.pdf.

[26] "Designing Secure ActiveX Controls." Microsoft MSDN web site. © 2004. URL: http://msdn.microsoft.com/ workshop/components/activex/security.asp.

[27] "Introduction to Code Signing." Microsoft MSDN web site. © 2004. URL: http://msdn.microsoft.com/workshop/components/activex/security.asp.

[28] Unknown Author. "Disabling Active Scripting in Internet Explorer". URL: http://acd.ucar.edu/~fredrick/win2k/active_scripting/.

[29] Definition of Active Content Filtering/ Monitoring from the "Roadmap to Security Tools and Services Online" web page, Version 10.0. SANS web site. Winter 2004. URL: http://www.sans.org/tools/roadmap.php#ActiveContentMonitoring.

[30] "Internet Explorer: Critical Updates." Microsoft Internet Explorer web site. © 2004. URL: http://www.microsoft.com/windows/ie/downloads/critical/default.mspx.

[31] SANS Track 7 – Auditing Networks, Perimeters and Systems (Course Material 2004). The SANS Institute. © 2003.

***The following web sites were not researched for information on this paper's subject matter but are referenced in the testing procedures as URLs to access for browser functionality tests:***

Download.com web site. URL: http://www.download.com/.

CNN web site. URL: http://www.cnn.com.

ESPN web site. URL: http://espn.go.com/.

AOL.com web site. URL: http://www.aol.com.

University of Texas web site. URL: http://www.utexas.edu.

PivX's Quik-Fix. URL: http://www.pivx.com/qwikfix/.