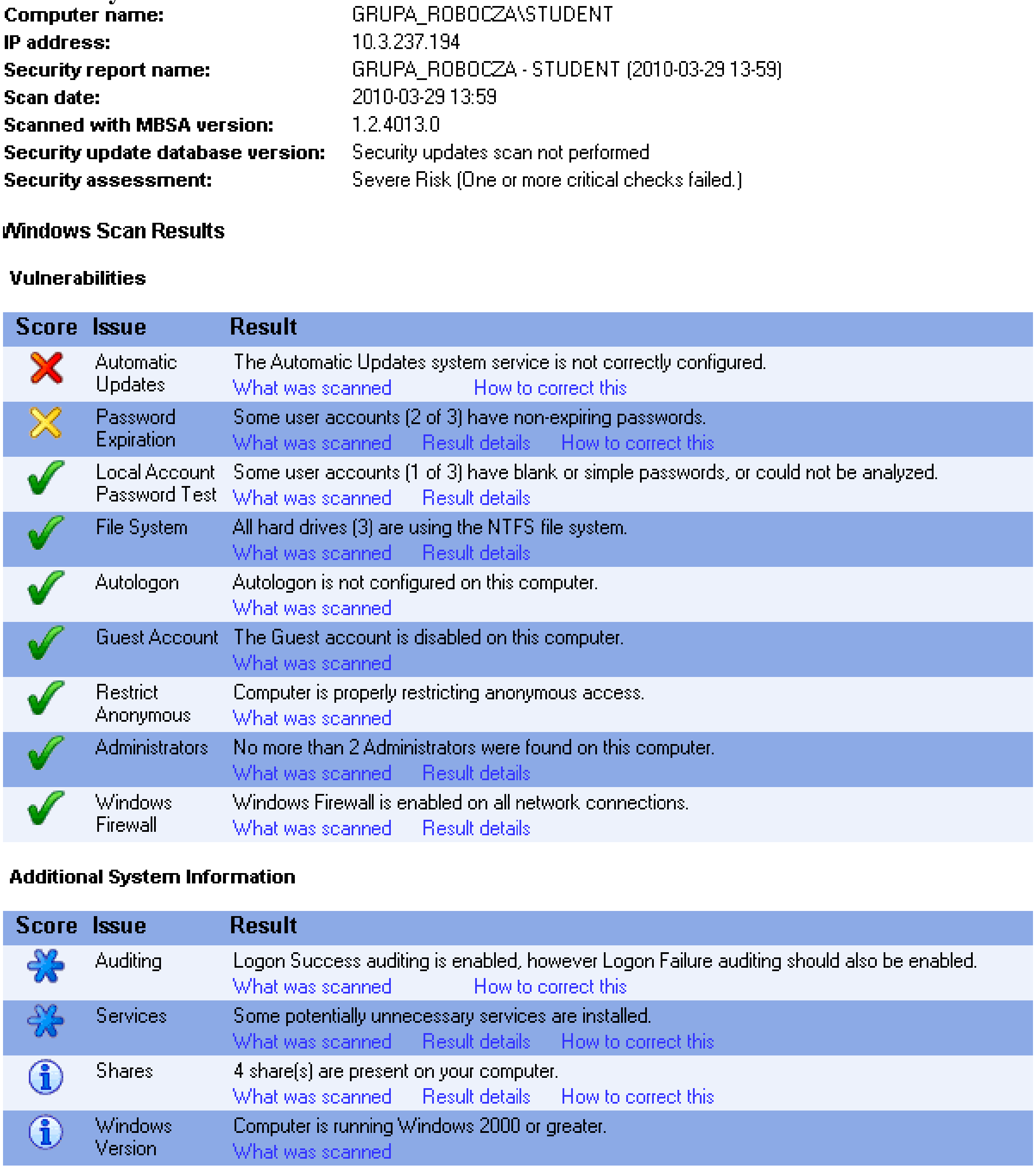
Ćwiczenie 3. Skanery stanu zabezpieczeń

Wykonał: Grzegorz Pol
Komputer: 237-16

Zadanie 1

Rys. 1.1 (poniżej) Obraz okna programu *Microsoft Baseline Security Analyzer* zawierającego nagłówek (strona *View security report*) oraz wykaz najpoważniejszych stwierdzonych usterek.



Computer name:	GRUPA_ROBOCZA\STUDENT
IP address:	10.3.237.194
Security report name:	GRUPA_ROBOCZA - STUDENT (2010-03-29 13-59)
Scan date:	2010-03-29 13:59
Scanned with MBSA version:	1.2.4013.0
Security update database version:	Security updates scan not performed
Security assessment:	Severe Risk (One or more critical checks failed.)

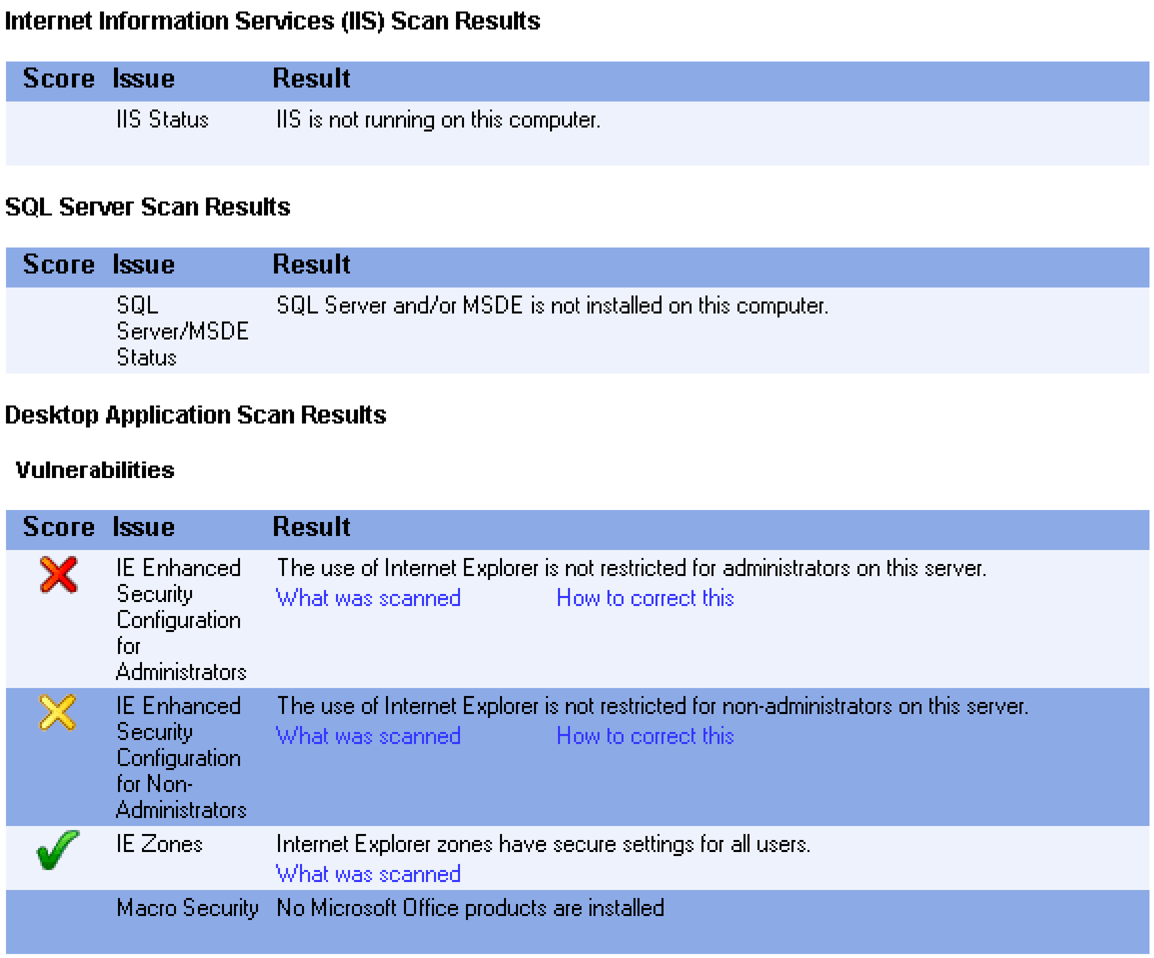
Windows Scan Results

Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates system service is not correctly configured. What was scanned How to correct this
✗	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (1 of 3) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	File System	All hard drives (3) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
✓	Windows Firewall	Windows Firewall is enabled on all network connections. What was scanned Result details

Additional System Information

Score	Issue	Result
✱	Auditing	Logon Success auditing is enabled, however Logon Failure auditing should also be enabled. What was scanned How to correct this
✱	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
ℹ	Shares	4 share(s) are present on your computer. What was scanned Result details How to correct this
ℹ	Windows Version	Computer is running Windows 2000 or greater. What was scanned



Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

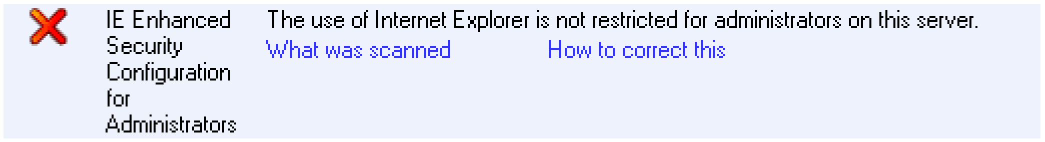
Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

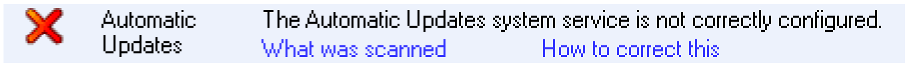
Vulnerabilities

Score	Issue	Result
✗	IE Enhanced Security Configuration for Administrators	The use of Internet Explorer is not restricted for administrators on this server. What was scanned How to correct this
✗	IE Enhanced Security Configuration for Non-Administrators	The use of Internet Explorer is not restricted for non-administrators on this server. What was scanned How to correct this
✓	IE Zones	Internet Explorer zones have secure settings for all users. What was scanned
	Macro Security	No Microsoft Office products are installed

Najpoważniejsze wykryte usterki:



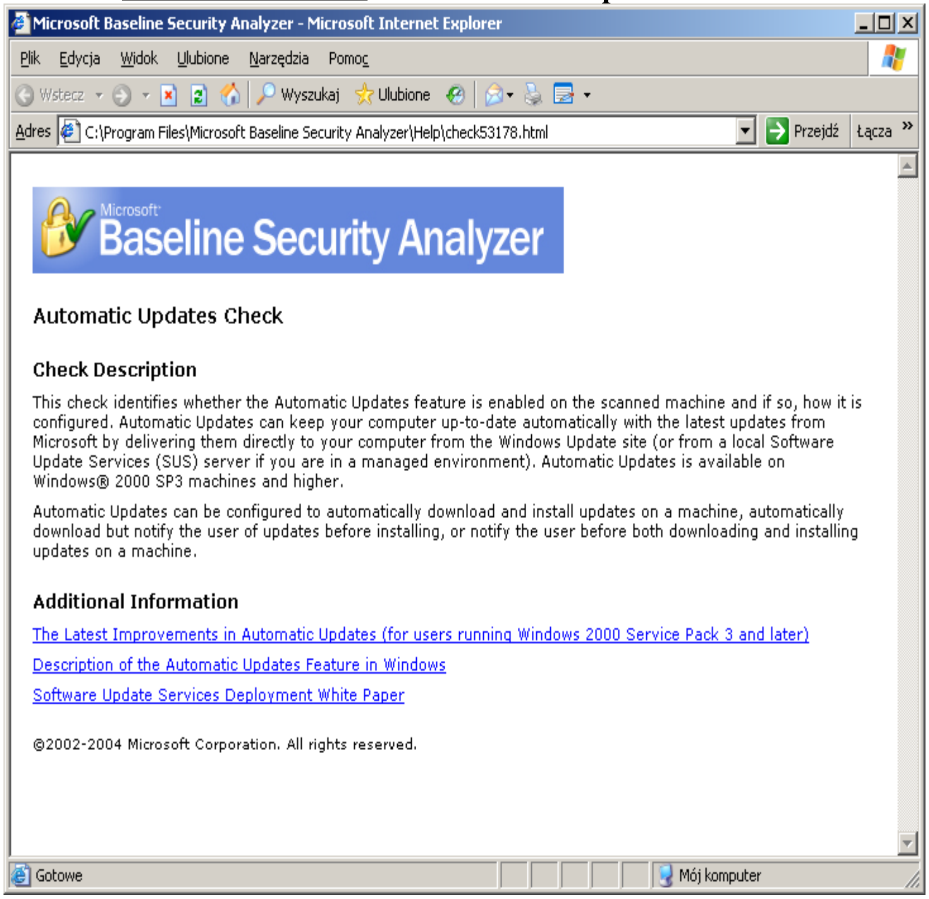
✗	IE Enhanced Security Configuration for Administrators	The use of Internet Explorer is not restricted for administrators on this server. What was scanned How to correct this



✗	Automatic Updates	The Automatic Updates system service is not correctly configured. What was scanned How to correct this

Rys. 1.2 (poniżej) Obraz najważniejszych elementów okna programu *Microsoft Baseline Security Analyzer* osiągalnego po wybraniu jednego z łączników *What was scanned*.

Łacznik *What was scanned* dla Automatic Updates Check


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz
Wyszukaj
Ulubione
Adres C:\Program Files\Microsoft Baseline Security Analyzer\Help\check53178.html
Przejdź
Łącza
Microsoft Baseline Security Analyzer
Gotowe
Mój komputer

Automatic Updates Check

Check Description

This check identifies whether the Automatic Updates feature is enabled on the scanned machine and if so, how it is configured. Automatic Updates can keep your computer up-to-date automatically with the latest updates from Microsoft by delivering them directly to your computer from the Windows Update site (or from a local Software Update Services (SUS) server if you are in a managed environment). Automatic Updates is available on Windows® 2000 SP3 machines and higher.

Automatic Updates can be configured to automatically download and install updates on a machine, automatically download but notify the user of updates before installing, or notify the user before both downloading and installing updates on a machine.

Additional Information

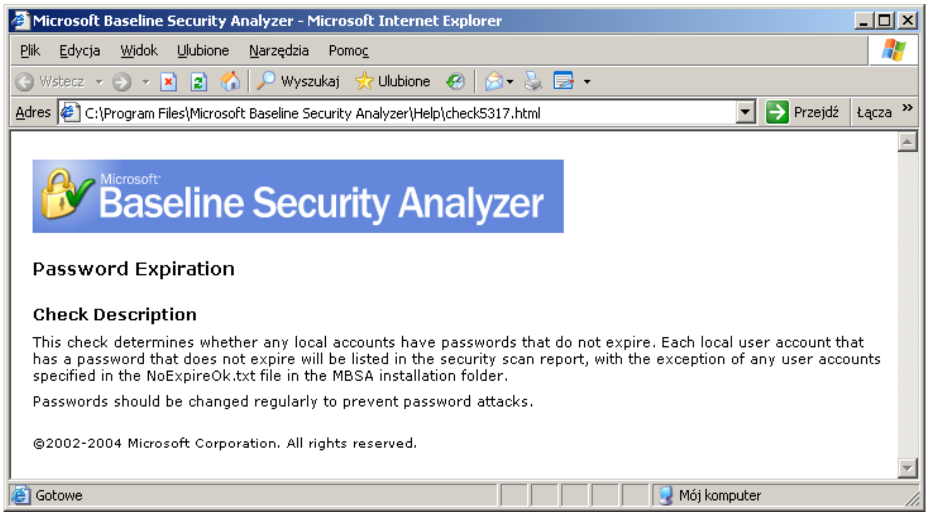
The Latest Improvements in Automatic Updates (for users running Windows 2000 Service Pack 3 and later)

Description of the Automatic Updates Feature in Windows

Software Update Services Deployment White Paper

©2002-2004 Microsoft Corporation. All rights reserved.

Łącznik *What was scanned* dla Password Expiration


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz
Wyszukaj
Ulubione
Adres C:\Program Files\Microsoft Baseline Security Analyzer\Help\check5317.html
Przejdź
Łącza
Microsoft Baseline Security Analyzer
Gotowe
Mój komputer

Password Expiration

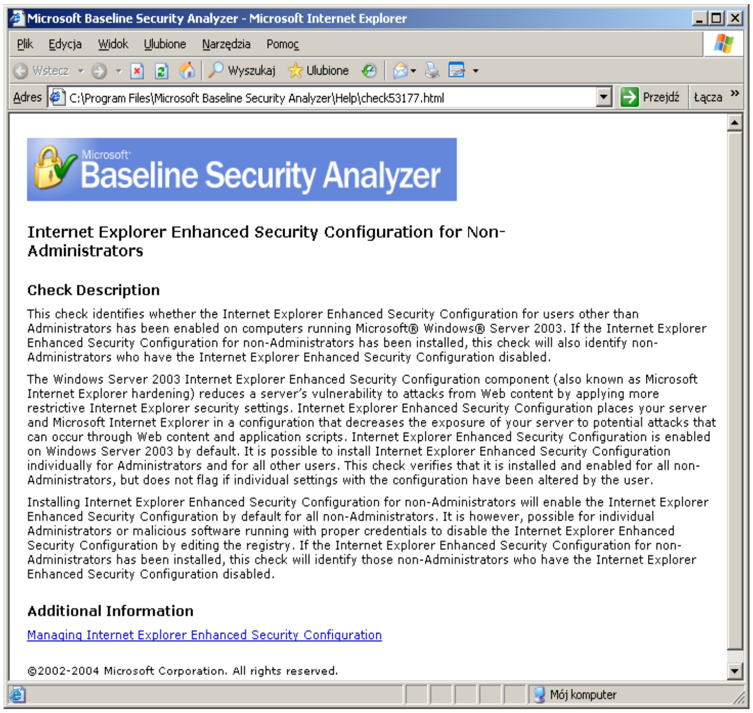
Check Description

This check determines whether any local accounts have passwords that do not expire. Each local user account that has a password that does not expire will be listed in the security scan report, with the exception of any user accounts specified in the NoExpireOk.txt file in the MBSA installation folder.

Passwords should be changed regularly to prevent password attacks.

©2002-2004 Microsoft Corporation. All rights reserved.

Łącznik *What was scanned* dla Internet Explorer Enhanced Security Configuration for Non Administrators


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz Wyszukaj Ulubione
Adres C:\Program Files\Microsoft Baseline Security Analyzer\Help\check53177.html
Przejdź Łącza
Microsoft Baseline Security Analyzer
Mój komputer

Internet Explorer Enhanced Security Configuration for Non-Administrators

Check Description

This check identifies whether the Internet Explorer Enhanced Security Configuration for users other than Administrators has been enabled on computers running Microsoft® Windows® Server 2003. If the Internet Explorer Enhanced Security Configuration for non-Administrators has been installed, this check will also identify non-Administrators who have the Internet Explorer Enhanced Security Configuration disabled.

The Windows Server 2003 Internet Explorer Enhanced Security Configuration component (also known as Microsoft Internet Explorer hardening) reduces a server's vulnerability to attacks from Web content by applying more restrictive Internet Explorer security settings. Internet Explorer Enhanced Security Configuration places your server and Microsoft Internet Explorer in a configuration that decreases the exposure of your server to potential attacks that can occur through Web content and application scripts. Internet Explorer Enhanced Security Configuration is enabled on Windows Server 2003 by default. It is possible to install Internet Explorer Enhanced Security Configuration individually for Administrators and for all other users. This check verifies that it is installed and enabled for all non-Administrators, but does not flag if individual settings with the configuration have been altered by the user.

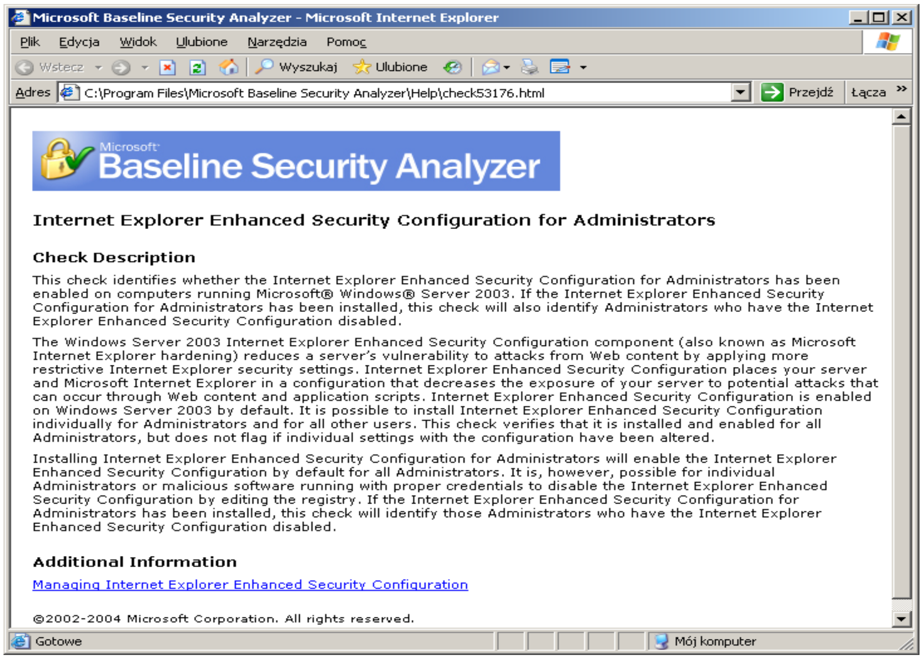
Installing Internet Explorer Enhanced Security Configuration for non-Administrators will enable the Internet Explorer Enhanced Security Configuration by default for all non-Administrators. It is however, possible for individual Administrators or malicious software running with proper credentials to disable the Internet Explorer Enhanced Security Configuration by editing the registry. If the Internet Explorer Enhanced Security Configuration for non-Administrators has been installed, this check will identify those non-Administrators who have the Internet Explorer Enhanced Security Configuration disabled.

Additional Information

Managing Internet Explorer Enhanced Security Configuration

©2002-2004 Microsoft Corporation. All rights reserved.

Łącznik *What was scanned* dla Internet Explorer Enchanced Security Configuration for Administrators


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Wstecz Wyszukaj Ulubione
Adres C:\Program Files\Microsoft Baseline Security Analyzer\Help\check53176.html
Przejdź Łącza
Microsoft Baseline Security Analyzer
Gotowe
Mój komputer

Internet Explorer Enhanced Security Configuration for Administrators

Check Description

This check identifies whether the Internet Explorer Enhanced Security Configuration for Administrators has been enabled on computers running Microsoft® Windows® Server 2003. If the Internet Explorer Enhanced Security Configuration for Administrators has been installed, this check will also identify Administrators who have the Internet Explorer Enhanced Security Configuration disabled.

The Windows Server 2003 Internet Explorer Enhanced Security Configuration component (also known as Microsoft Internet Explorer hardening) reduces a server's vulnerability to attacks from Web content by applying more restrictive Internet Explorer security settings. Internet Explorer Enhanced Security Configuration places your server and Microsoft Internet Explorer in a configuration that decreases the exposure of your server to potential attacks that can occur through Web content and application scripts. Internet Explorer Enhanced Security Configuration is enabled on Windows Server 2003 by default. It is possible to install Internet Explorer Enhanced Security Configuration individually for Administrators and for all other users. This check verifies that it is installed and enabled for all Administrators, but does not flag if individual settings with the configuration have been altered.

Installing Internet Explorer Enhanced Security Configuration for Administrators will enable the Internet Explorer Enhanced Security Configuration by default for all Administrators. It is, however, possible for individual Administrators or malicious software running with proper credentials to disable the Internet Explorer Enhanced Security Configuration by editing the registry. If the Internet Explorer Enhanced Security Configuration for Administrators has been installed, this check will identify those Administrators who have the Internet Explorer Enhanced Security Configuration disabled.

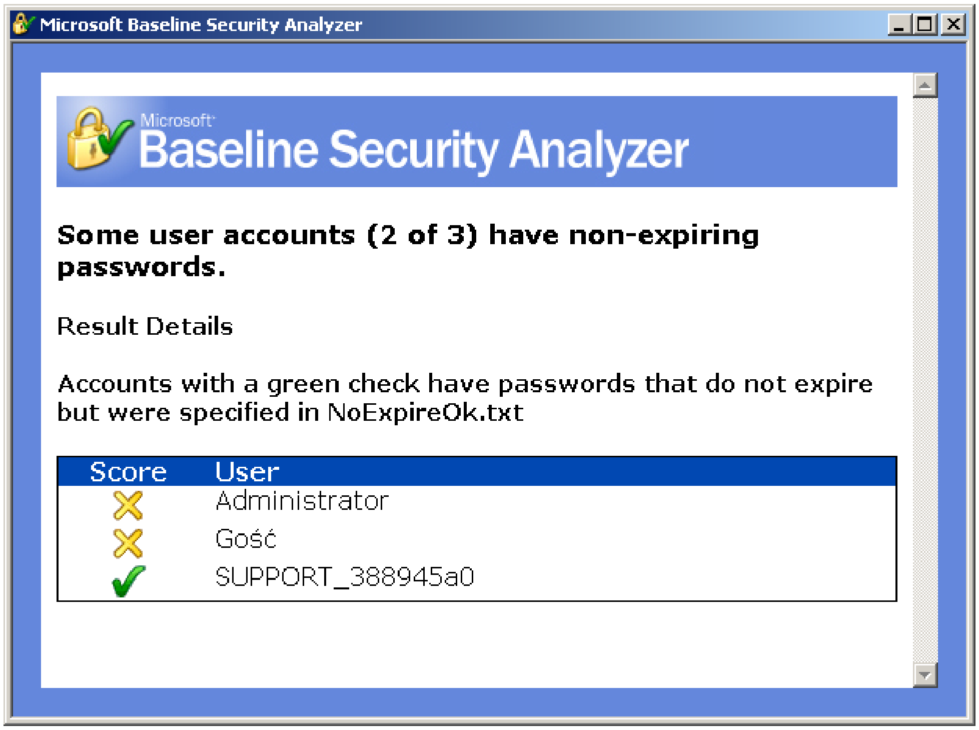
Additional Information

Managing Internet Explorer Enhanced Security Configuration

©2002-2004 Microsoft Corporation. All rights reserved.

Rys. 1.3 (poniżej) Obraz najważniejszych elementów okna programu *Microsoft Baseline Security Analyzer* osiągalnego po wybraniu jednego z łączników *<u>Result details</u>*.

Łącznik *<u>Result details</u>* dla Password Expiration


Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer

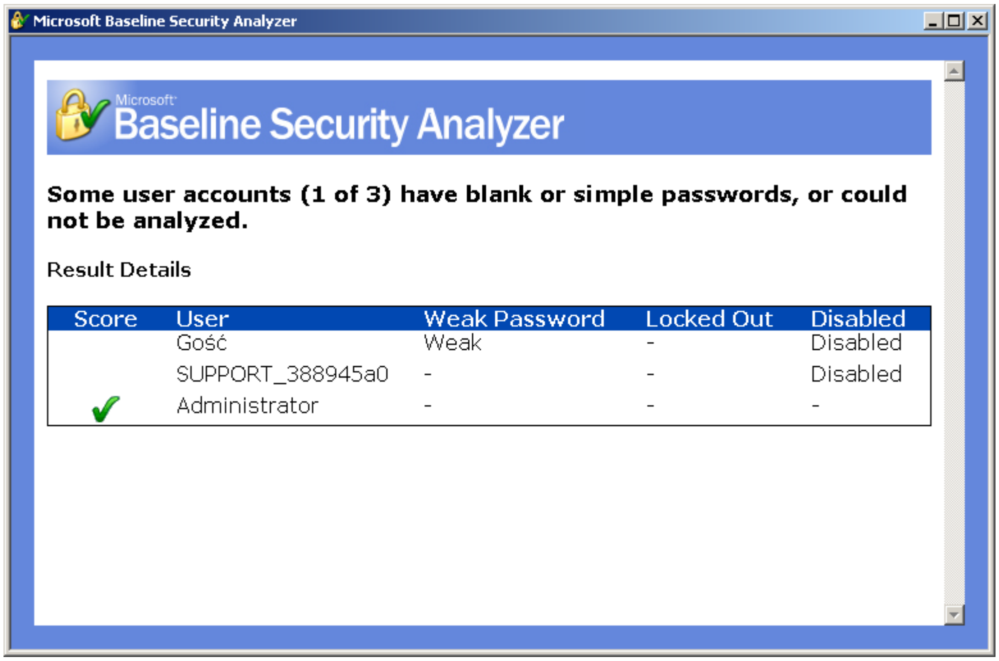
Some user accounts (2 of 3) have non-expiring passwords.

Result Details

Accounts with a green check have passwords that do not expire but were specified in NoExpireOk.txt

Score	User
✗	Administrator
✗	Gość
✓	SUPPORT_388945a0

Łącznik *<u>Result details</u>* dla Local acoount Password Test

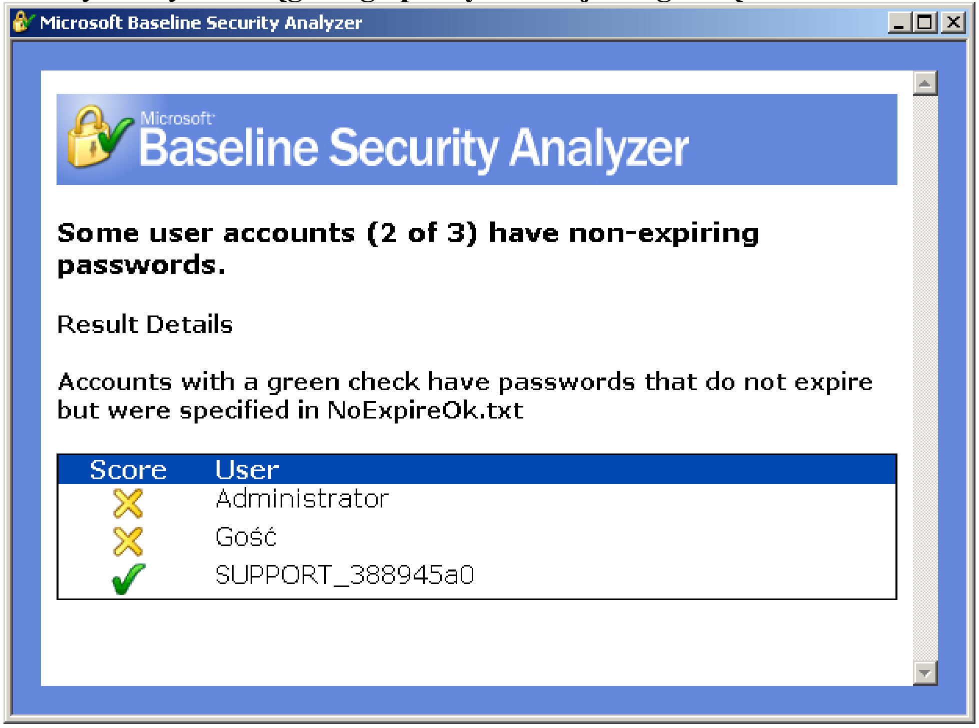

Microsoft Baseline Security Analyzer
Microsoft
Baseline Security Analyzer

Some user accounts (1 of 3) have blank or simple passwords, or could not be analyzed.

Result Details

Score	User	Weak Password	Locked Out	Disabled
	Gość	Weak	-	Disabled
	SUPPORT_388945a0	-	-	Disabled
✓	Administrator	-	-	-

Rys. 1.4 (poniżej) Obraz najważniejszych elementów okna programu *Microsoft Baseline Security Analyzer* osiągalnego po wybraniu jednego z łączników *How to correct this*.



Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer

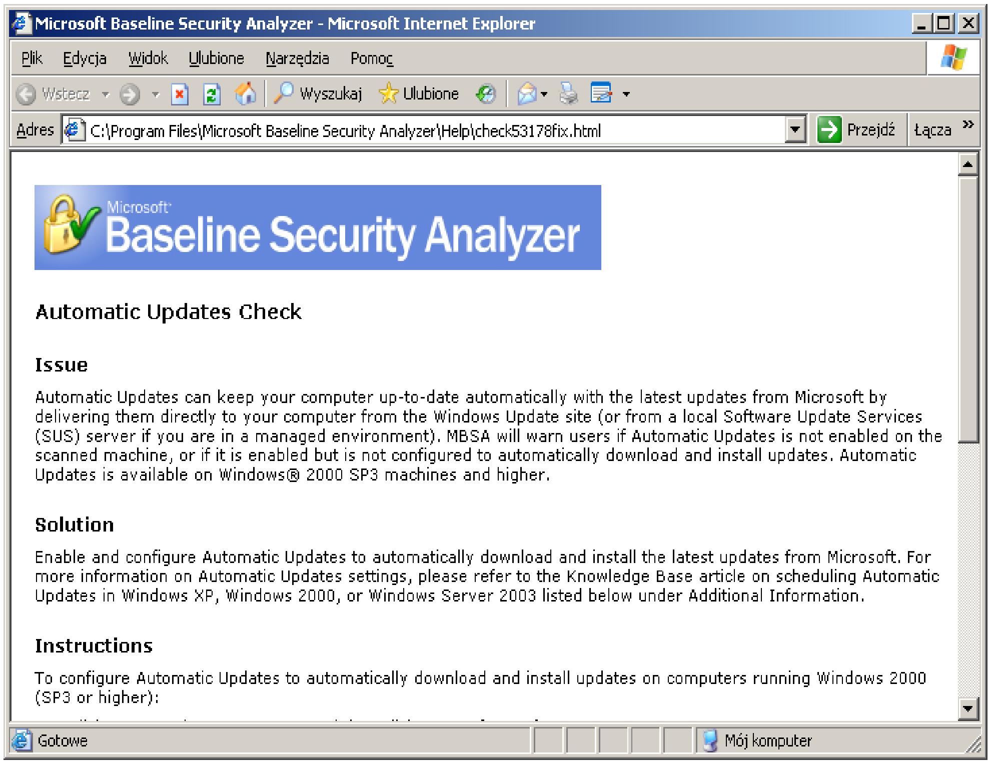
Some user accounts (2 of 3) have non-expiring passwords.

Result Details

Accounts with a green check have passwords that do not expire but were specified in NoExpireOk.txt

Score	User
✗	Administrator
✗	Gość
✓	SUPPORT_388945a0

Łącznik *How to correct* dla Automatic Updates



Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Plik
Edycja
Widok
Ulubione
Narzędzia
Pomoc
Wstecz
Wyszukaj
Ulubione
Adres
C:\Program Files\Microsoft Baseline Security Analyzer\Help\check53178fix.html
Przejdź
Łącza
Microsoft Baseline Security Analyzer
Gotowe
Mój komputer

Automatic Updates Check

Issue

Automatic Updates can keep your computer up-to-date automatically with the latest updates from Microsoft by delivering them directly to your computer from the Windows Update site (or from a local Software Update Services (SUS) server if you are in a managed environment). MBSA will warn users if Automatic Updates is not enabled on the scanned machine, or if it is enabled but is not configured to automatically download and install updates. Automatic Updates is available on Windows® 2000 SP3 machines and higher.

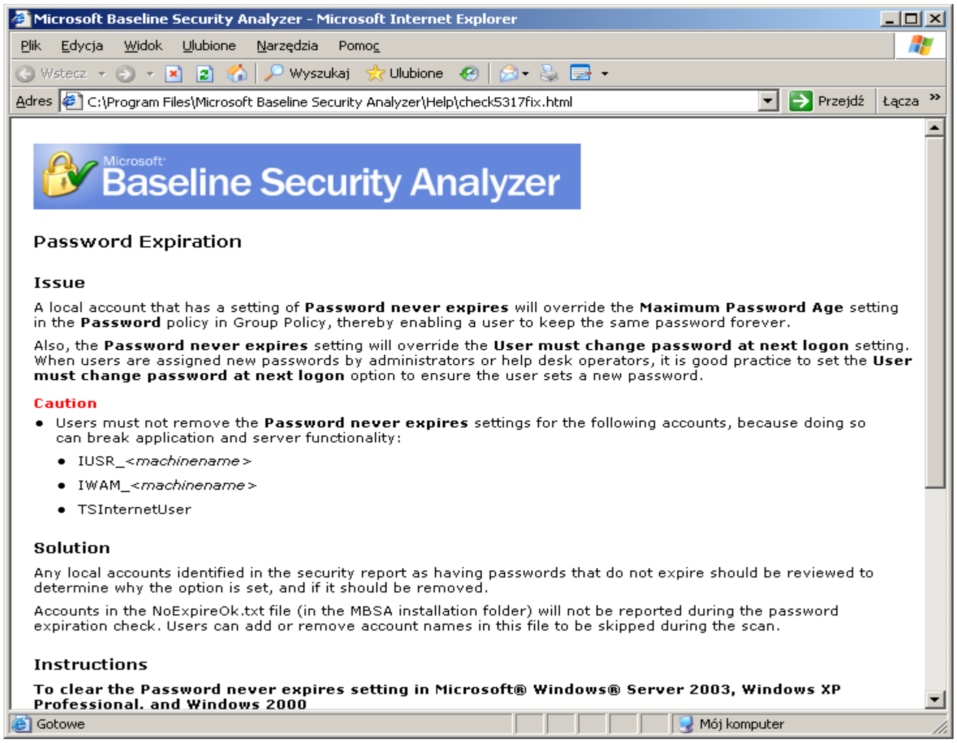
Solution

Enable and configure Automatic Updates to automatically download and install the latest updates from Microsoft. For more information on Automatic Updates settings, please refer to the Knowledge Base article on scheduling Automatic Updates in Windows XP, Windows 2000, or Windows Server 2003 listed below under Additional Information.

Instructions

To configure Automatic Updates to automatically download and install updates on computers running Windows 2000 (SP3 or higher):

Łącznik *How to correct* dla Password Expiration


Microsoft Baseline Security Analyzer - Microsoft Internet Explorer
Plik
Edycja
Widok
Ulubione
Narzędzia
Pomoc
Wstecz
Wyszukaj
Ulubione
Adres
C:\Program Files\Microsoft Baseline Security Analyzer\Help\check5317fix.html
Przejdź
Łącza
Microsoft
Baseline Security Analyzer
Gotowe
Mój komputer

Password Expiration

Issue

A local account that has a setting of **Password never expires** will override the **Maximum Password Age** setting in the **Password** policy in Group Policy, thereby enabling a user to keep the same password forever.

Also, the **Password never expires** setting will override the **User must change password at next logon** setting. When users are assigned new passwords by administrators or help desk operators, it is good practice to set the **User must change password at next logon** option to ensure the user sets a new password.

Caution

- Users must not remove the **Password never expires** settings for the following accounts, because doing so can break application and server functionality:
  - IUSR_<*machinename*>
  - IWAM_<*machinename*>
  - TSInternetUser

Solution

Any local accounts identified in the security report as having passwords that do not expire should be reviewed to determine why the option is set, and if it should be removed.

Accounts in the NoExpireOk.txt file (in the MBSA installation folder) will not be reported during the password expiration check. Users can add or remove account names in this file to be skipped during the scan.

Instructions

To clear the Password never expires setting in Microsoft® Windows® Server 2003, Windows XP Professional, and Windows 2000

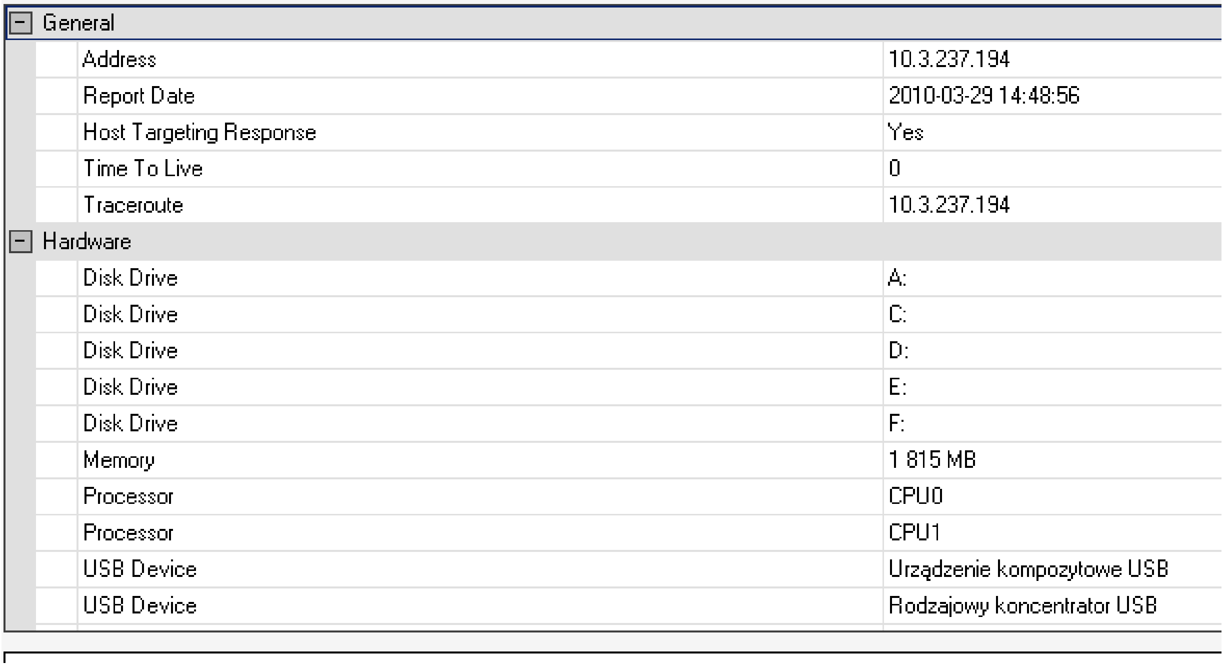
WŁASNE SPOSTRZEŻENIA I WNIOSKI do zadania 1:

Narzędzie te służy do sprawdzania stanu zabezpieczeń systemu w sieci (w naszym przypadku jest to Windows 2003 Server z dodatkiem SP1) oraz przeglądarki Internet Explorer (w naszym przypadku 6.0). Ponadto jesteśmy informowani o dostępnych udostępnionych poprawkach na serwerze firmy Microsoft, o jakości haseł, ważnych ustawień konfiguracyjnych. Po każdym skanowaniu program wyświetla nam raport: z informacjami co zostało zeskanowane, wynikiem szczegółowym oraz informacją pomocną do zabezpieczenia systemu/przeglądarki.

W naszym przypadku program zgłasza problemy dotyczące: automatycznych aktualizacji (zostały one przez nas wyłączone), długości wygasania hasła (nie wygasa), "dziurawą" przeglądarką. Wszystkie problemy w zakładkach są rozwiązywane sposobem: zainstaluj / odznacz / zaznacz. Zostały one tak skonstruowane aby początkujący użytkownik komputera mógł z nich skorzystać.

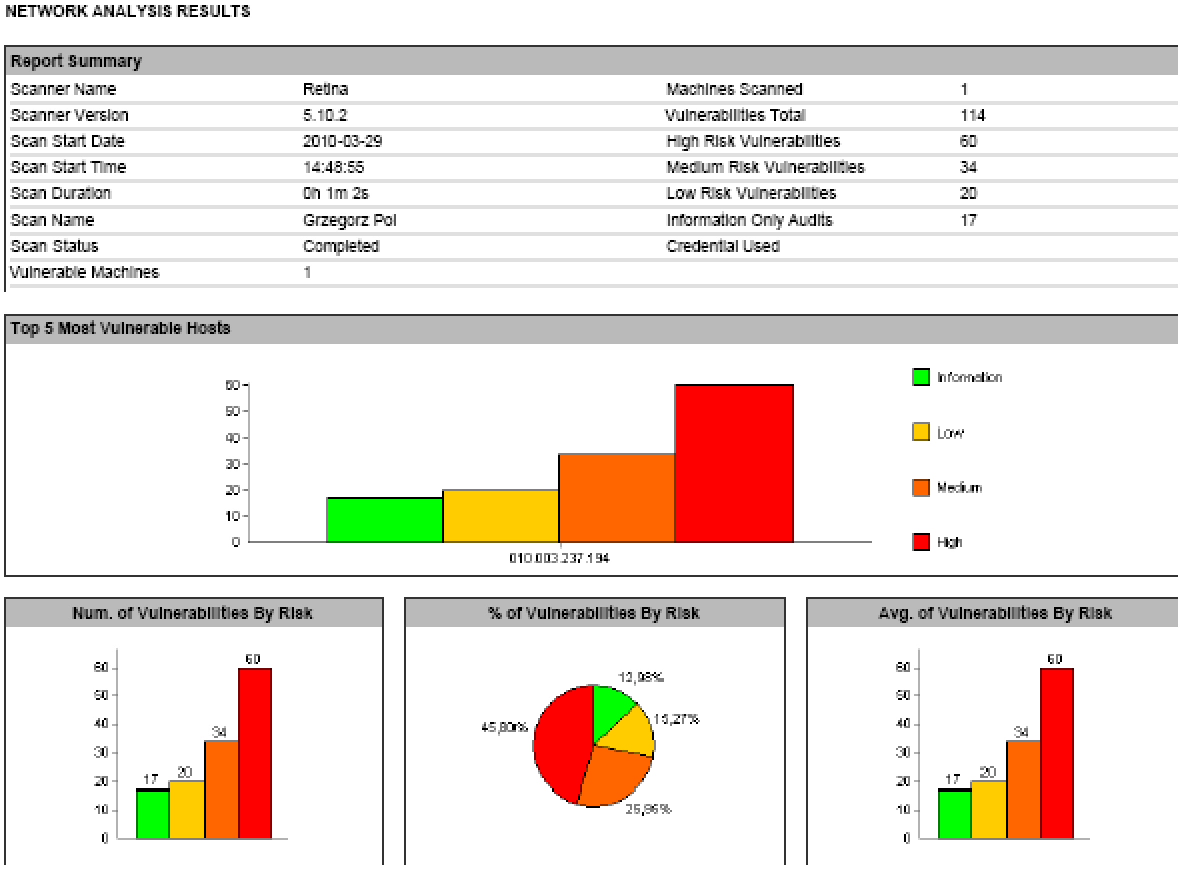
Zadanie 2

Rys. 2.1 (poniżej) Obraz głównego okna programu *Retina* po zakończeniu skanowania (pod zakładką *Audit*) z widocznymi informacjami identyfikującymi skanowany komputer.



⊟ General	
Address	10.3.237.194
Report Date	2010-03-29 14:48:56
Host Targeting Response	Yes
Time To Live	0
Traceroute	10.3.237.194
⊟ Hardware	
Disk Drive	A:
Disk Drive	C:
Disk Drive	D:
Disk Drive	E:
Disk Drive	F:
Memory	1 815 MB
Processor	CPU0
Processor	CPU1
USB Device	Urządzenie kompozytowe USB
USB Device	Rodzajowy koncentrator USB

Rys. 2.2 (poniżej) Obraz okna zawierającego całą sekcję *Network Analysis Results* raportu głównego (podsumowanie informacji w sekcji i wszystkie wykresy).



NETWORK ANALYSIS RESULTS

Report Summary			
Scanner Name	Retina	Machines Scanned	1
Scanner Version	5.10.2	Vulnerabilities Total	114
Scan Start Date	2010-03-29	High Risk Vulnerabilities	60
Scan Start Time	14:48:55	Medium Risk Vulnerabilities	34
Scan Duration	0h 1m 2s	Low Risk Vulnerabilities	20
Scan Name	Grzegorz Pol	Information Only Audits	17
Scan Status	Completed	Credential Used	
Vulnerable Machines	1		

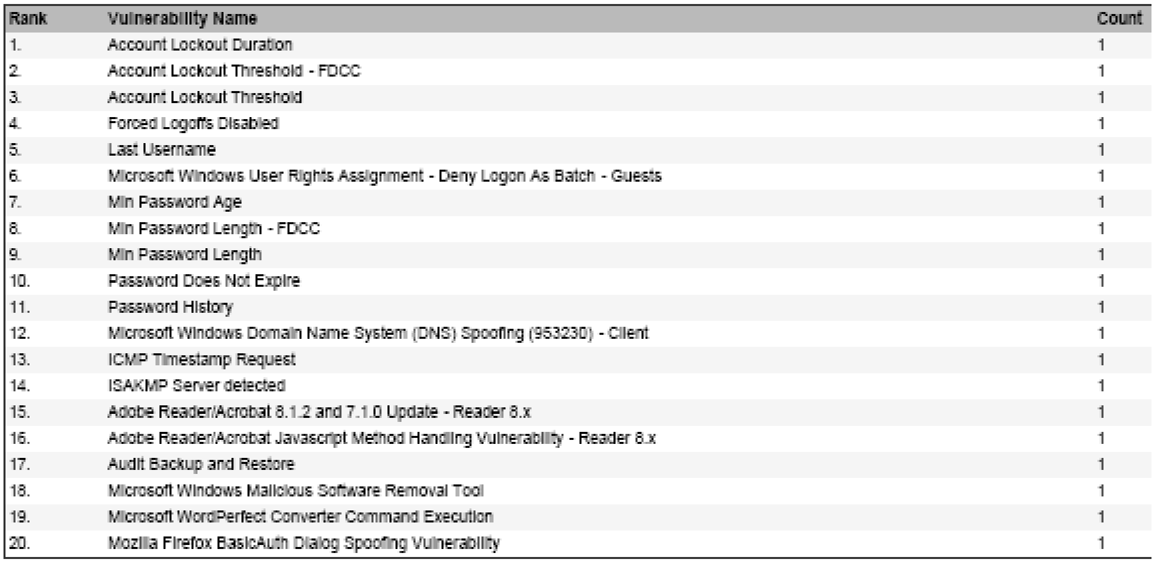
Top 5 Most Vulnerable Hosts

Num. of Vulnerabilities By Risk

% of Vulnerabilities By Risk

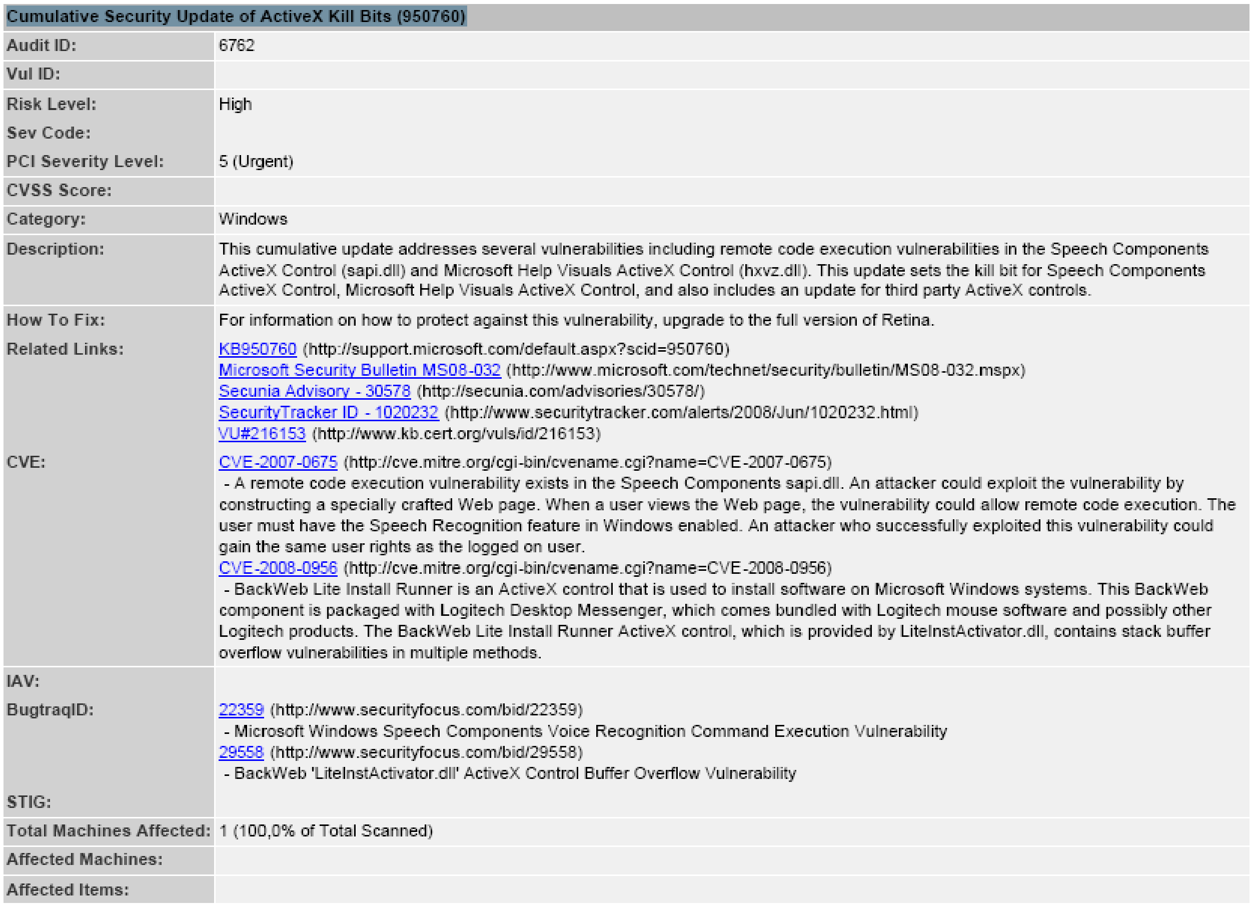
Avg. of Vulnerabilities By Risk

Rys. 2.3 (poniżej) Obraz okna zawierającego tabelę w sekcji *Top 20 Vulnerabilities* raportu głównego.



Rank	Vulnerability Name	Count
1.	Account Lockout Duration	1
2.	Account Lockout Threshold - FDCC	1
3.	Account Lockout Threshold	1
4.	Forced Logoffs Disabled	1
5.	Last Username	1
6.	Microsoft Windows User Rights Assignment - Deny Logon As Batch - Guests	1
7.	Min Password Age	1
8.	Min Password Length - FDCC	1
9.	Min Password Length	1
10.	Password Does Not Expire	1
11.	Password History	1
12.	Microsoft Windows Domain Name System (DNS) Spoofing (953230) - Client	1
13.	ICMP Timestamp Request	1
14.	ISAKMP Server detected	1
15.	Adobe Reader/Acrobat 8.1.2 and 7.1.0 Update - Reader 8.x	1
16.	Adobe Reader/Acrobat Javascript Method Handling Vulnerability - Reader 8.x	1
17.	Audit Backup and Restore	1
18.	Microsoft Windows Malicious Software Removal Tool	1
19.	Microsoft WordPerfect Converter Command Execution	1
20.	Mozilla Firefox BasicAuth Dialog Spoofing Vulnerability	1

Rys. 2.4 (poniżej) Obraz okna zawierającego cały opis i procedurę usunięcia usterki Cumulative Security Update of ActiveX Kill Bits (950760) z raportu *Procedury*



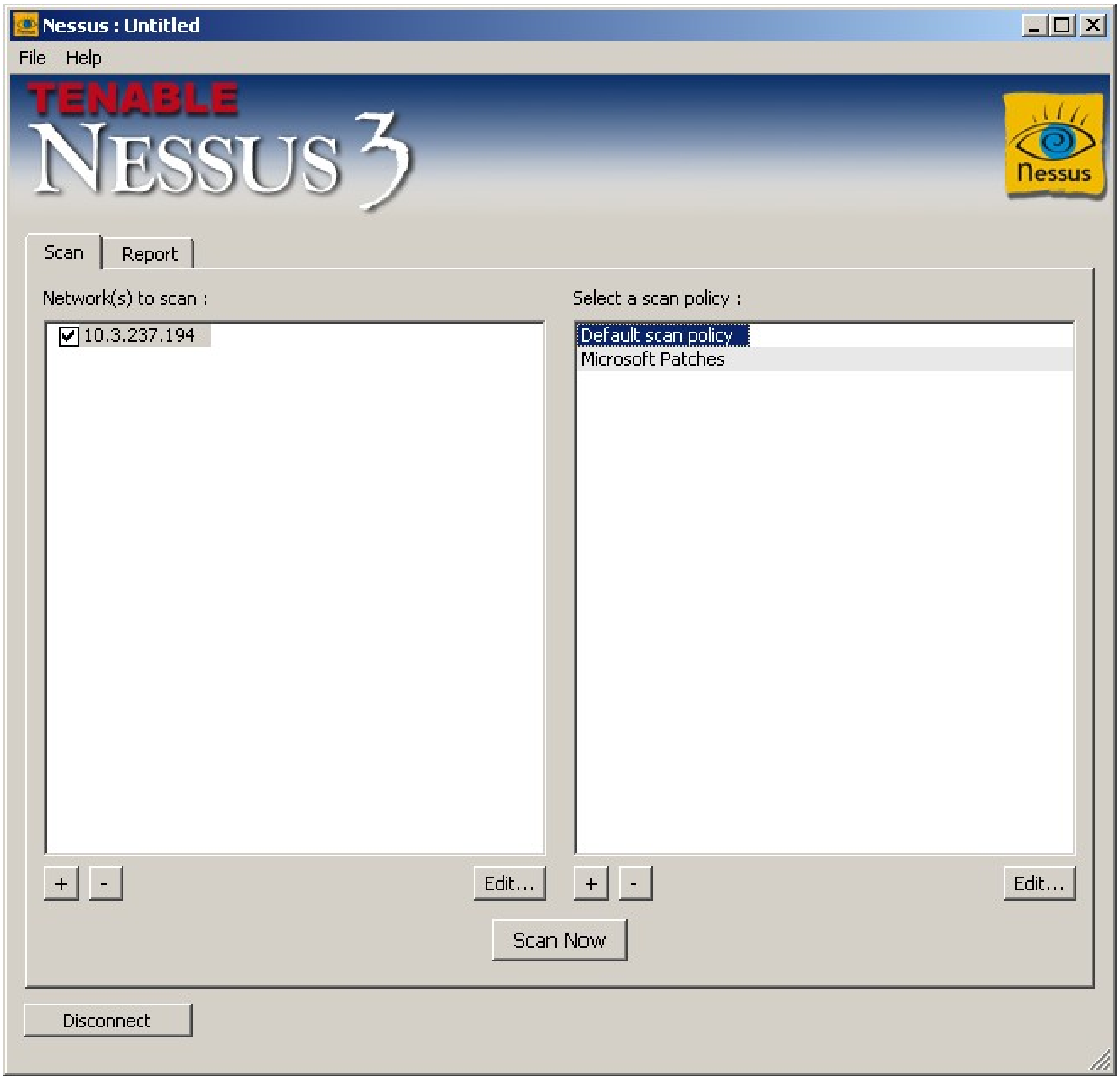
Cumulative Security Update of ActiveX Kill Bits (950760)	
Audit ID:	6762
Vul ID:	
Risk Level:	High
Sev Code:	
PCI Severity Level:	5 (Urgent)
CVSS Score:	
Category:	Windows
Description:	This cumulative update addresses several vulnerabilities including remote code execution vulnerabilities in the Speech Components ActiveX Control (sapi.dll) and Microsoft Help Visuals ActiveX Control (hxvz.dll). This update sets the kill bit for Speech Components ActiveX Control, Microsoft Help Visuals ActiveX Control, and also includes an update for third party ActiveX controls.
How To Fix:	For information on how to protect against this vulnerability, upgrade to the full version of Retina.
Related Links:	KB950760 (http://support.microsoft.com/default.aspx?scid=950760) Microsoft Security Bulletin MS08-032 (http://www.microsoft.com/technet/security/bulletin/MS08-032.mspx) Secunia Advisory - 30578 (http://secunia.com/advisories/30578/) SecurityTracker ID - 1020232 (http://www.securitytracker.com/alerts/2008/Jun/1020232.html) VU#216153 (http://www.kb.cert.org/vuls/id/216153)
CVE:	CVE-2007-0675 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0675) - A remote code execution vulnerability exists in the Speech Components sapi.dll. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. The user must have the Speech Recognition feature in Windows enabled. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user. CVE-2008-0956 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0956) - BackWeb Lite Install Runner is an ActiveX control that is used to install software on Microsoft Windows systems. This BackWeb component is packaged with Logitech Desktop Messenger, which comes bundled with Logitech mouse software and possibly other Logitech products. The BackWeb Lite Install Runner ActiveX control, which is provided by LiteInstActivator.dll, contains stack buffer overflow vulnerabilities in multiple methods.
IAV:	
BugtraqID:	22359 (http://www.securityfocus.com/bid/22359) - Microsoft Windows Speech Components Voice Recognition Command Execution Vulnerability 29558 (http://www.securityfocus.com/bid/29558) - BackWeb 'LiteInstActivator.dll' ActiveX Control Buffer Overflow Vulnerability
STIG:	
Total Machines Affected:	1 (100,0% of Total Scanned)
Affected Machines:	
Affected Items:	

WŁASNE SPOSTRZEŻENIA I WNIOSKI do zadania 2:

Retina Network Security Scanner to narzędzie służące do skanowania sieci w poszukiwaniu luk, które mogą okazać się niebezpieczne. Następnie program ocenia stopień zagrożenia każdej z nich i podaje najlepsze rozwiazania. Skanowanie sieci trwa dość krótko. Program dodatkowo generuje raporty zawierające sporą ilość wykresów co ułatwia przyswajanie informacji.

Zadanie 3

Rys. 3.1 (poniżej) Obraz okna klienta pakietu *Nessus* zawierającego informacje o wybranym obiekcie skanowania i wybranej zasadzie.



Network(s) to scan :

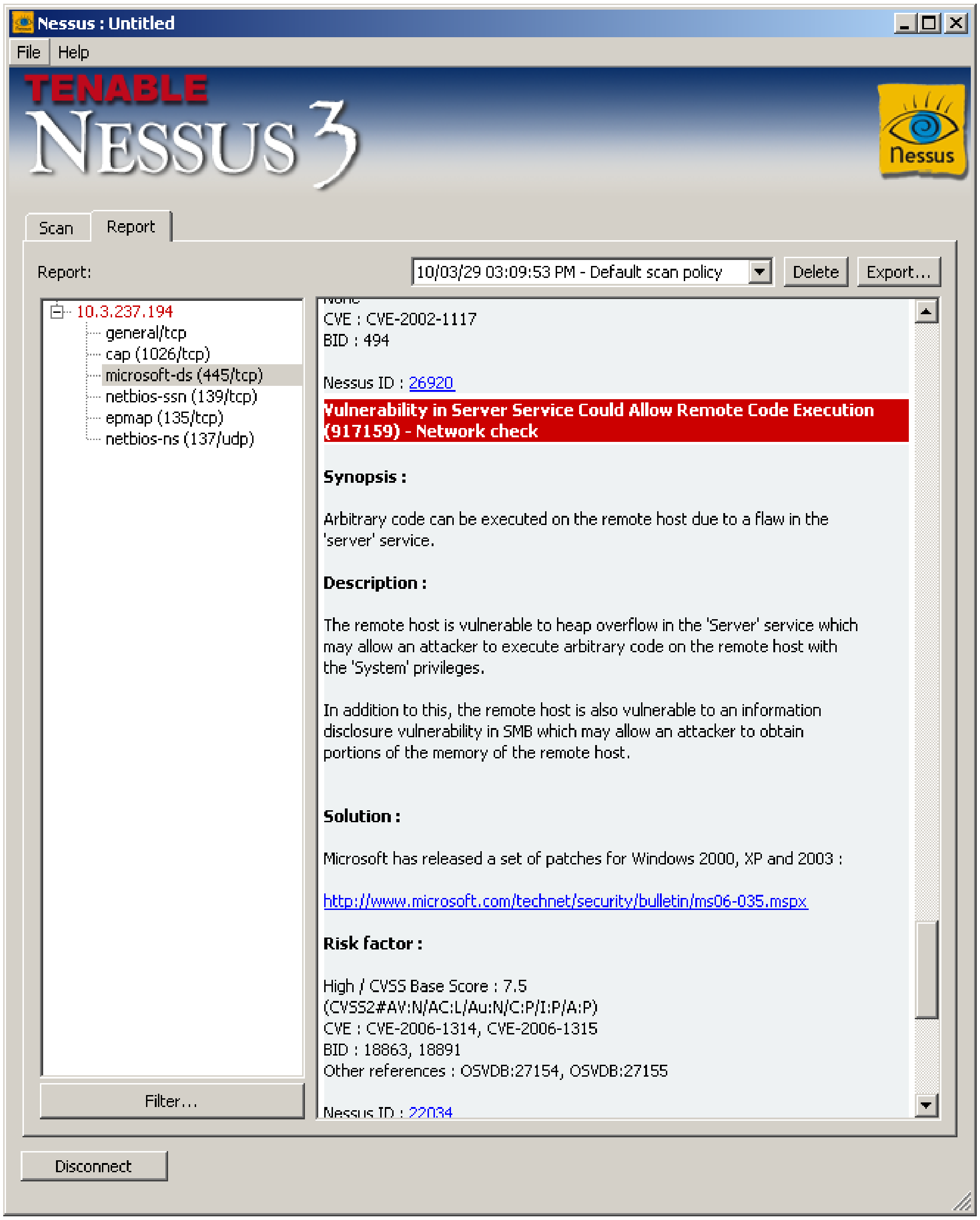
☑ 10.3.237.194

Select a scan policy :

Default scan policy

Microsoft Patches

Rys. 3.2 (poniżej) Obraz okna klienta pakietu *Nessus* zawierającego najważniejsze elementy opisu dowolnie wybranej usterki.



CVE : CVE-2002-1117
BID : 494

Nessus ID : 26920

Vulnerability in Server Service Could Allow Remote Code Execution (917159) - Network check

Synopsis :

Arbitrary code can be executed on the remote host due to a flaw in the 'server' service.

Description :

The remote host is vulnerable to heap overflow in the 'Server' service which may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

In addition to this, the remote host is also vulnerable to an information disclosure vulnerability in SMB which may allow an attacker to obtain portions of the memory of the remote host.

Solution :

Microsoft has released a set of patches for Windows 2000, XP and 2003 :

http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE : CVE-2006-1314, CVE-2006-1315
BID : 18863, 18891
Other references : OSVDB:27154, OSVDB:27155

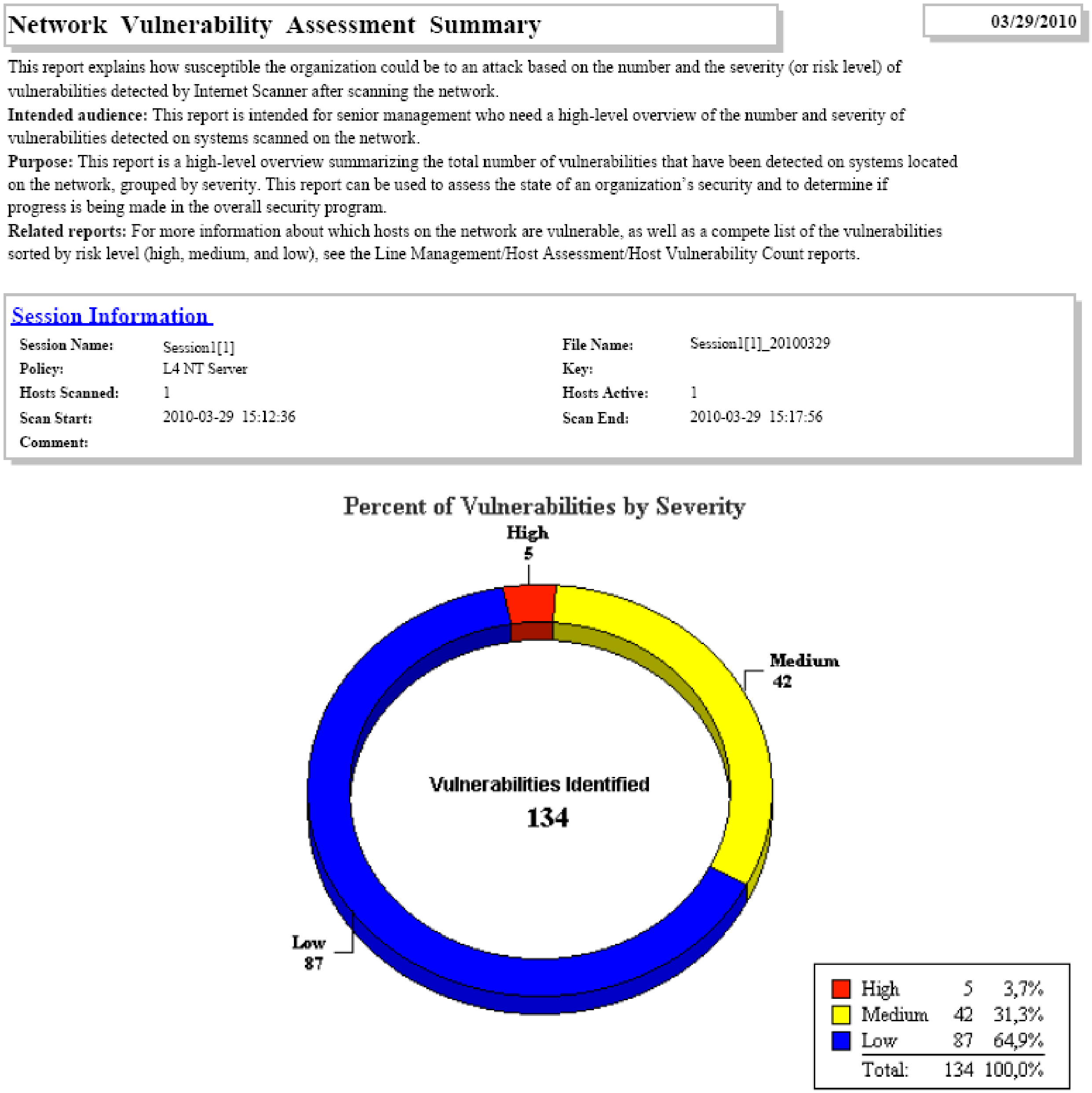
Nessus ID : 22034

WŁASNE SPOSTRZEŻENIA I WNIOSKI do zadania 3:

Nessus jest skanerem badającym ponad 20 tysięcy punktów w systemie zagrażających naszemu bezpieczeństwu. W ciągu kilku minut skaner dostarcza nam czytelny i przejrzysty raport w postaci drzewka, niestety pozbawiony wykresów. Raporta możemy zapisać w formacie *.as by móc odczytać później.

Zadanie 4

Rys. 4.1 (poniżej) Obraz okna zawierającego raport *NetworkVulnerability Assessment Summary.*



Network Vulnerability Assessment Summary

03/29/2010

This report explains how susceptible the organization could be to an attack based on the number and the severity (or risk level) of vulnerabilities detected by Internet Scanner after scanning the network.

Intended audience: This report is intended for senior management who need a high-level overview of the number and severity of vulnerabilities detected on systems scanned on the network.

Purpose: This report is a high-level overview summarizing the total number of vulnerabilities that have been detected on systems located on the network, grouped by severity. This report can be used to assess the state of an organization's security and to determine if progress is being made in the overall security program.

Related reports: For more information about which hosts on the network are vulnerable, as well as a compete list of the vulnerabilities sorted by risk level (high, medium, and low), see the Line Management/Host Assessment/Host Vulnerability Count reports.

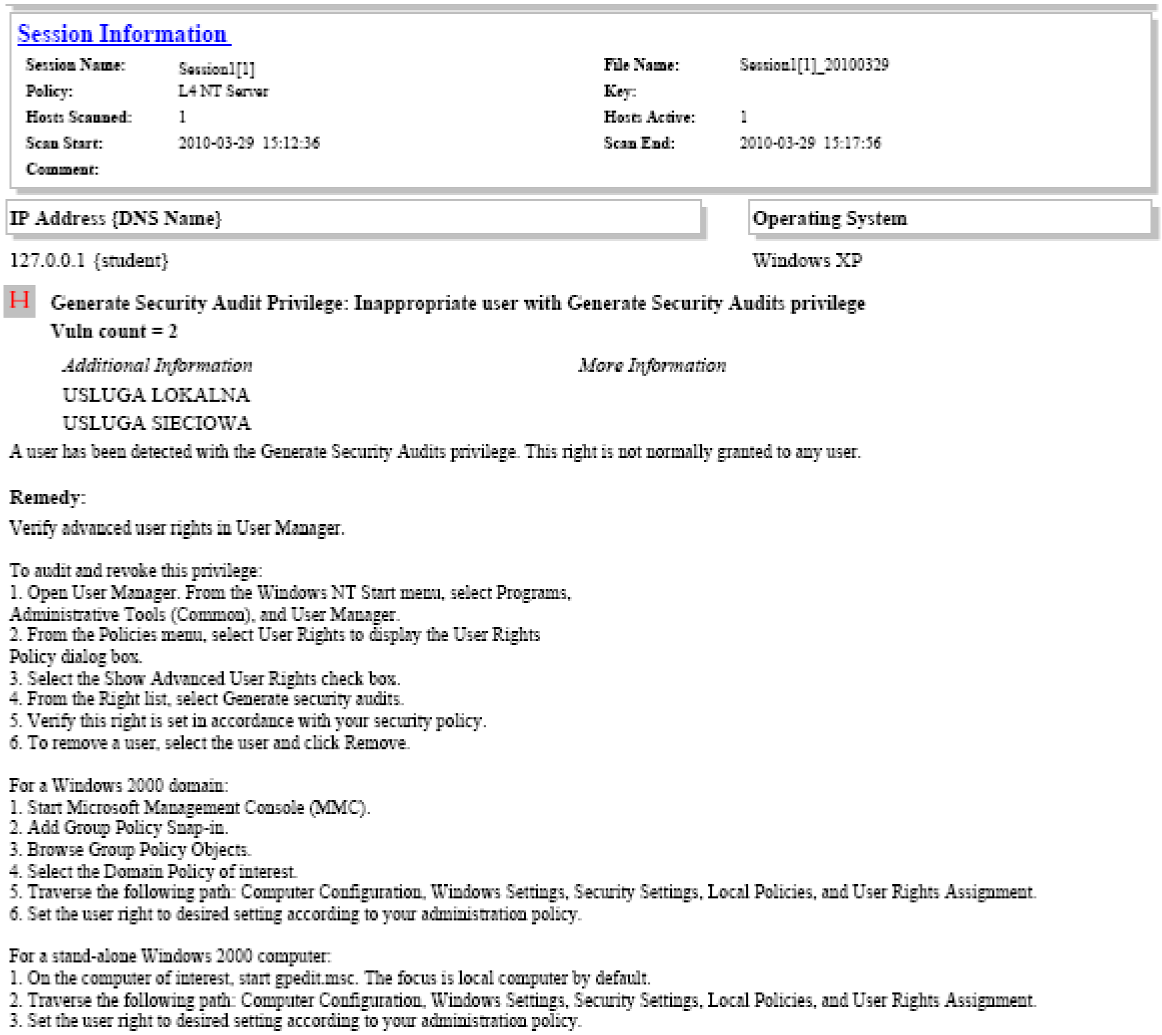
Session Information

Session Name:	Session1[1]	**File Name:**	Session1[1]_20100329
Policy:	L4 NT Server	**Key:**	
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	2010-03-29 15:12:36	**Scan End:**	2010-03-29 15:17:56
Comment:			

Percent of Vulnerabilities by Severity

🟥	High	5	3,7%
🟨	Medium	42	31,3%
🟦	Low	87	64,9%
	Total:	134	100,0%

Rys. 4.2 (poniżej) Obraz okna zawierającego fragment raportu *Technician - Vulnerability Assessment,* z opisem i procedurą usunięcia usterki Generate Security Audit Privilege: Inappropriate user with Generate Security Audits privilege Vuln count = 2



Session Information

Session Name:	Session1[1]	**File Name:**	Session1[1]_20100329
Policy:	L4 NT Server	**Key:**	
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	2010-03-29 15:12:36	**Scan End:**	2010-03-29 15:17:56
Comment:			

IP Address {DNS Name}	Operating System
127.0.0.1 {student}	Windows XP

H **Generate Security Audit Privilege: Inappropriate user with Generate Security Audits privilege**
Vuln count = 2

Additional Information	*More Information*
USLUGA LOKALNA	
USLUGA SIECIOWA	

A user has been detected with the Generate Security Audits privilege. This right is not normally granted to any user.

Remedy:

Verify advanced user rights in User Manager.

To audit and revoke this privilege:
1. Open User Manager. From the Windows NT Start menu, select Programs, Administrative Tools (Common), and User Manager.
2. From the Policies menu, select User Rights to display the User Rights Policy dialog box.
3. Select the Show Advanced User Rights check box.
4. From the Right list, select Generate security audits.
5. Verify this right is set in accordance with your security policy.
6. To remove a user, select the user and click Remove.

For a Windows 2000 domain:
1. Start Microsoft Management Console (MMC).
2. Add Group Policy Snap-in.
3. Browse Group Policy Objects.
4. Select the Domain Policy of interest.
5. Traverse the following path: Computer Configuration, Windows Settings, Security Settings, Local Policies, and User Rights Assignment.
6. Set the user right to desired setting according to your administration policy.

For a stand-alone Windows 2000 computer:
1. On the computer of interest, start gpedit.msc. The focus is local computer by default.
2. Traverse the following path: Computer Configuration, Windows Settings, Security Settings, Local Policies, and User Rights Assignment.
3. Set the user right to desired setting according to your administration policy.

WŁASNE SPOSTRZEŻENIA I WNIOSKI do zadania 4:

IIS Internet Security tak jak poprzednie programy służy do wykrywania luk w sieci. Program po dość długim skanowaniu (porównując z innymi badanymi dziś programami) umożliwia wygenerowanie bardzo szczegółowych raportów o błędach. Zostały one podzialone w zależności od zagrożenia na High, Medium, Low po to by użytkownik skupił się na poważniejszych z nich.