

Temat 01.2 Skanery stanu zabezpieczeń

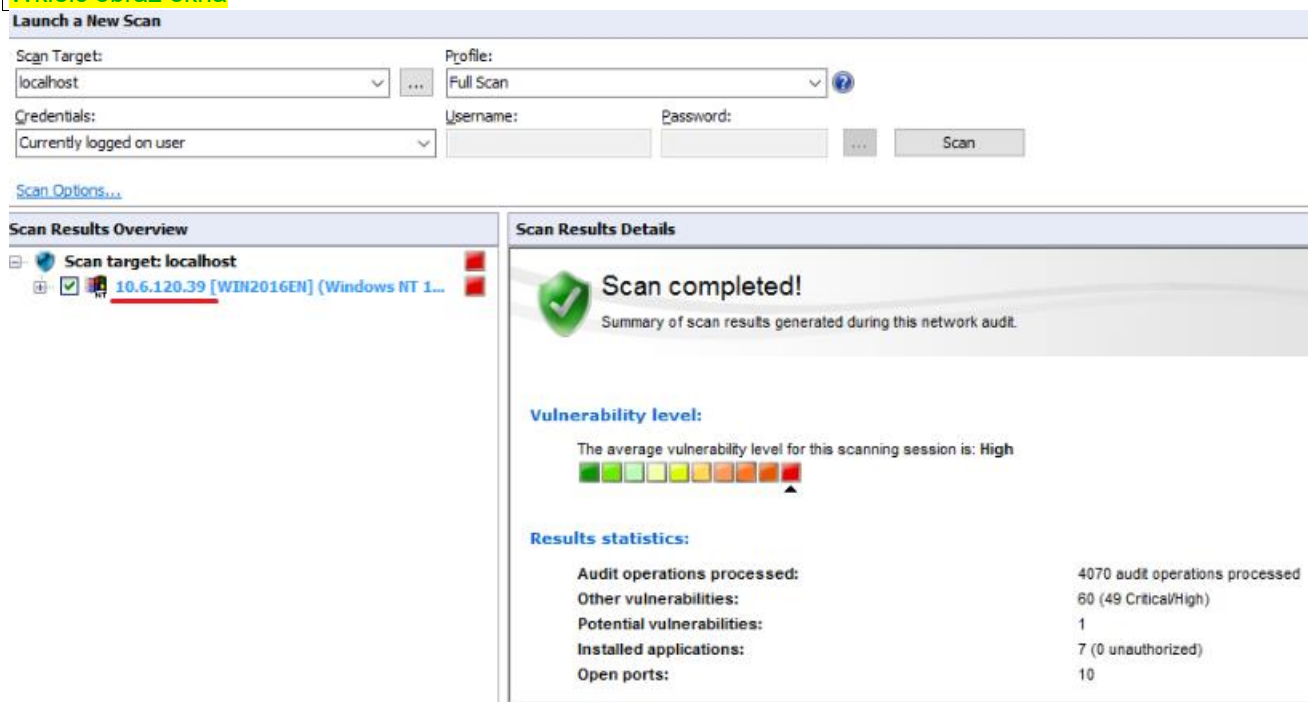
Wykonał(a): Bartosz Miazga

Stanowisko: 14

Zadanie 1 Testowanie skanera GFI LanGuard

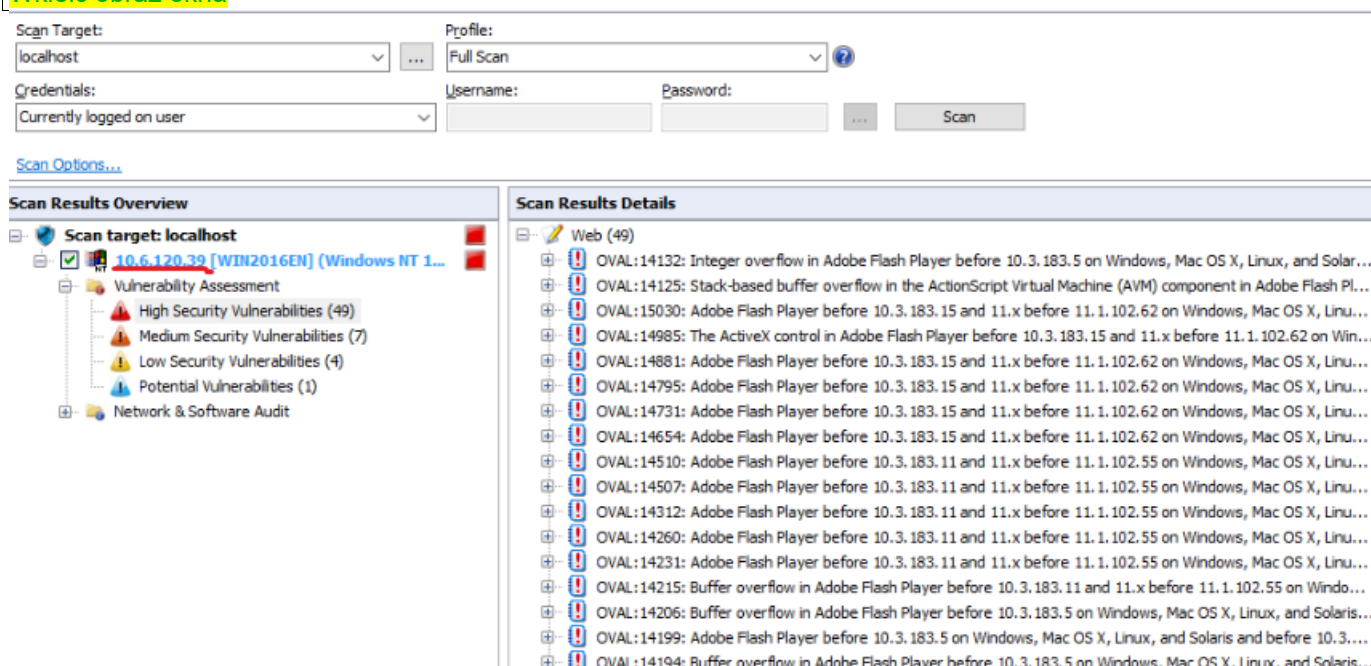
1.1 (poniżej) Obraz okna programu *GFI LANguard* prezentującego podsumowanie wyników skanowania, uzyskanego po wybraniu zakładki **Scan** i pozycji z nazwą i adresem komputera w panelu **Scan Results: Overview**. W obu panelach powinny być zaznaczone dane identyfikujące skanowany komputer. Kontener **Vulnerability Assessment** powinien być w pełni rozwinięty. Panel *Scanner Activity Windows* może być niewidoczny.

Wkleić obraz okna



1.2 (poniżej) Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki **Scan** i pozycji **High Security Vulnerabilities** (w panelu **Scan Results: Overview**). Powinny być zaznaczone dane identyfikujące skanowany komputer. Panel *Scanner Activity Windows* może być niewidoczny.

Wkleić obraz okna



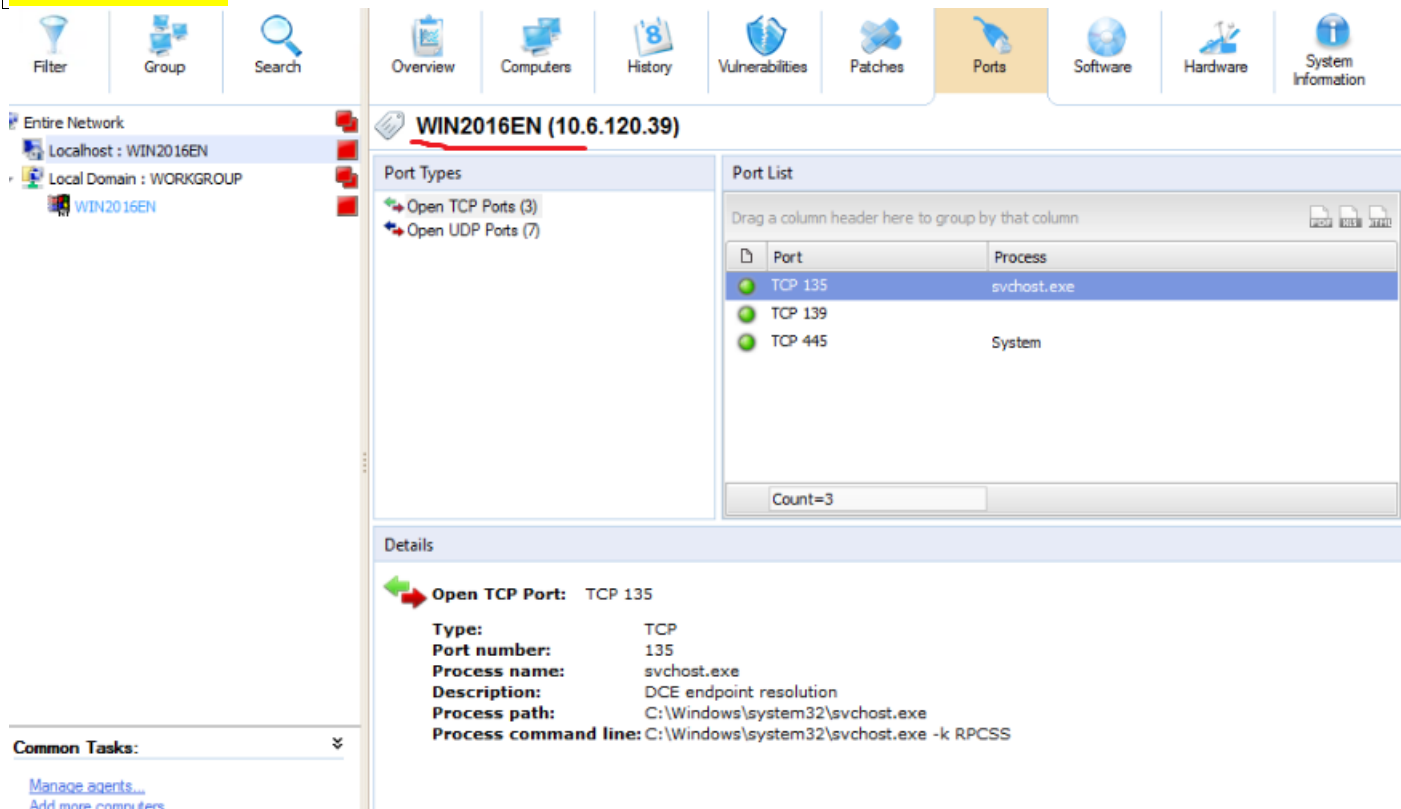
1.3 (poniżej) Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki **Dashboard**, przycisku **Overview** oraz łącza zawierającego nazwę skanowanego komputera. Powinny być zaznaczone dane identyfikujące skanowany komputer. Panel *Scanner Activity Windows* może być niewidoczny.

Wkleić obraz okna



1.4 (poniżej) Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki **Dashboard**, przycisku **Ports** oraz łącza zawierającego nazwę skanowanego komputera. Powinny być zaznaczone dane identyfikujące skanowany komputer. Panel *Scanner Activity Windows* może być niewidoczny.

Wkleić obraz okna



Ocena skanera wykorzystywanego podczas realizacji zadania 1:

Skaner GFI LANguard jest rozbudowany, prezentowane wyniki sortuje według stopnia zagrożeń. Skanuje podatności aplikacji zainstalowanych na komputerze, z ich dokładnym opisem.

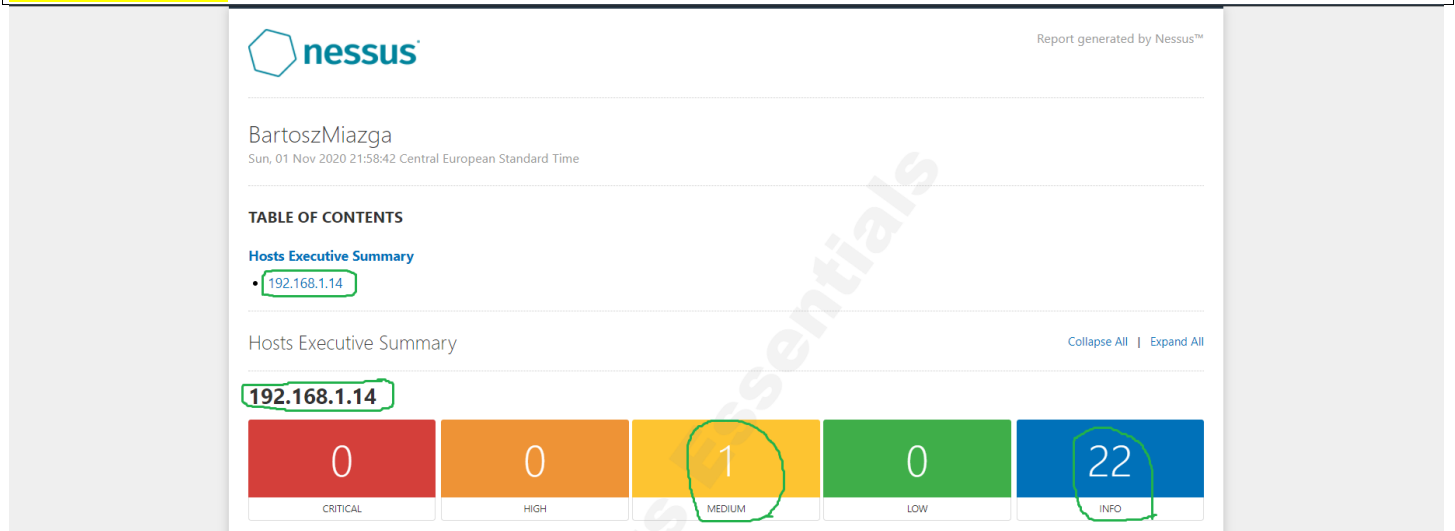
Zadanie 2 Testowanie skanera NESSUS

Programem Nessus skanowałem własny komputer jeszcze przed zajęciami.

2.1 (poniżej) Fragment raportu **Detailed RTF Report** lub **Detailed HTML Report** prezentujący całą

ostatnią sekcję raportu z zaznaczonymi danymi skanowanego komputera oraz informacją o ilości wykrytych podatności

Wkleić obraz okna



2.2 (poniżej) Fragment raportu **Detailed RTF Report** lub **Detailed HTML Report** prezentujący jedną z sekcji PORT CIFS (co najmniej akapity **Synopsis** i **Description**). Powinny być zaznaczone dane identyfikujące skanowany komputer.

Wkleić obraz okna



2.3 (poniżej) Fragment raportu **Detailed RTF Report** lub **Detailed HTML Report** prezentujący jedną z sekcji PORT DCE-RPC (co najmniej akapity **Synopsis** i **Description**). Powinny być zaznaczone dane identyfikujące skanowany komputer.

Wkleić obraz okna

DCE Services Enumeration

INFO

Nessus Plugin ID 10736

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Plugin Details

Severity: Info

ID: 10736

File Name: dctest.nasl

Version: 1.56

Type: combined

Agent: windows

Family: Windows

Published: 2001/08/26

Updated: 2020/08/20

Dependencies: 11011

Asset Inventory: True

OS Identification: True

Risk Information

Risk Factor: Info

2.4 (poniżej) Fragment raportu **Detailed RTF Report** lub **Detailed HTML Report** prezentujący jedną z sekcji PORT SMB. [Powinny być zaznaczone dane identyfikujące skanowany komputer.](#)

Wkleić obraz okna

Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

INFO

Nessus Plugin ID 106716

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Plugin Details

Severity: Info

ID: 106716

File Name: smb_dialects_enabled.nasl

Version: 1.6

Type: remote

Agent: windows

Family: Windows

Published: 2018/02/09

Updated: 2020/03/11

Asset Inventory: True

Risk Information

Risk Factor: Info

Ocena skanera wykorzystywanego podczas realizacji zadania 2:

Nessus to rozbudowany skaner, wskazuje on zagrożenia sieciowe komputera z dokładnym opisem wrażliwości. Daje możliwość przeskanowania całej sieci z jednego urządzenia. Skaner dokonuje podziału zagrożeń na następujące grupy : Critical, High, Medium , Low oraz Info. Ponadto można szeregować liste zagrożeń według różnych kryteriów: Name , Family, Count, Sev, można ustalić porządek rosnący lub malejący. Istnieje także możliwość generowania raportów ze skanowania na różne sposoby, np. jako plik html. Wszystko to sprawia, że jest to bardzo czytelne i intuicyjne narzędzie.


Warto też wspomnieć, że Nessus oferuje szeroką gamę możliwości skanowania. Poza Basic Network Scan ,możemy zlecić wykonanie Advanced Scan, Malware Scan, Web Application Tests i wielu innych.

Zadanie 3 Testowanie skanera MBSA

3.1 (poniżej) Obraz okna programu *Microsoft Baseline Security Analyzer* zawierającego nagłówek (strona **Report Details for ...**) z informacjami identyfikującymi skanowany komputer oraz wykaz najpoważniejszych stwierdzonych usterek.

Wkleić obraz okna

Report Details for WORKGROUP - WIN2016EN (2020-11-06 09:52:33)







 Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: WORKGROUP\WIN2016EN
IP address: 10.6.120.39
Security report name: WORKGROUP - WIN2016EN (06-Nov-20 09:52)
Scan date: 06-Nov-20 09:52
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: Security updates scan not performed

Sort Order: Score (worst first) ▼

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	The Automatic Updates system service is not running. What was scanned How to correct this
	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.
	Local Account Password Test	Some user accounts (2 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details
	File System	All hard drives (7) are using the NTFS file system.

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

Wkleić obraz okna



Automatic Updates Check

Check Description

This check identifies whether the Automatic Updates feature is enabled on the scanned computer 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 Microsoft Update site, Windows Update site, or from a local Windows Server Update Services (WSUS) server if you are in a managed environment. Automatic Updates is available on Windows® 2000 SP4 computers and higher.

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

Additional Information


[Description of the Automatic Updates Feature in Windows](#)

[Windows Server Update Services \(WSUS\) Server](#)

©2002-2007 Microsoft Corporation. All rights reserved.

3.3 (poniżej) Obraz najważniejszych elementów okna programu *Microsoft Baseline Security Analyzer* osiągalnego po wybraniu jednego z łączników **Result details**.


Wkleić obraz okna

 Microsoft
Baseline Security Analyzer

No more than 2 Administrators were found on this computer.

Result Details


Score	User
✓	Administrator
✓	LANGUARD_11_USER

 Microsoft
Baseline Security Analyzer

All hard drives (2) are using the NTFS file system.

Result Details

Score	Drive Letter	File System
✓	C:	NTFS
✓	Z:	NTFS

 Microsoft
Baseline Security Analyzer

Some user accounts (4 of 5) 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
⚠	DefaultAccount
⚠	Guest
⚠	LANGUARD_11_USER
⚠	POMOCNIK

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

Wkleić obraz okna



Microsoft

Baseline Security Analyzer

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 Microsoft Update site, Windows Update site, or from a local Windows Server Update Services (WSUS) server if you are in a managed environment). MBSA will warn users if Automatic Updates is not enabled on the scanned computer, or if it is enabled but is not configured to automatically download and install updates. Automatic Updates is available on Windows® 2000 SP3 computers and higher.

The Automatic Updates control panel settings have been enhanced in Windows XP Service Pack 2, and the steps used to configure the feature have changed from those steps documented in MBSA for prior Windows versions. These enhancements also appear in Windows 2000 Service Pack 3 and above for computers that have automatically updated from Windows Update to obtain the latest Automatic Updates client version.

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.

Instructions

You must be logged on as a computer administrator to complete this procedure.

To change Automatic Updates settings in Windows Server 2003, Windows XP Professional, or Windows 2000

1. Open **System**, and then click the **Automatic Updates** tab.

– or –

If you are running Windows 2000, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Automatic Updates**.

2. Click **Automatic** (recommended).

3. Under **Automatically download recommended updates for my computer and install them**, select the day and time

Ocena skanera wykorzystywanego podczas realizacji zadania 3:

Skaner znajduje podstawowe zagrożenia systemowe takie jak na przykład: wyłączona automatyczna aktualizacja, brak wszystkich aktualizacji, wygaśnięcie hasła. Skaner jest czytelny i prosty w użyciu.

Zadanie 4 Ocena porównawcza testowanych skanerów

Skaner Microsoft Baseline Security Analyzer jest skanerem najprostszym, dającym najmniej możliwości skanowania komputera. Otrzymane raporty nie dają zbyt wiele informacji. Pozostałe 2 skanery są rozbudowane, dają bardzo dużo różnych opcji skanowania komputera, skaner Nessus umożliwia przeskanowanie całej sieci. Skanery Nessus oraz GFI LANguard generują różne raporty, dlatego w celu zdobycia pełnego obrazu bezpieczeństwa należało by skorzystać z obydwu.

Własne uwagi, wnioski i propozycje dotyczące przebiegu ćwiczenia, mające na celu polepszenie procesu kształcenia:

Brak, wszystko dobrze wytłumaczone.