

Szykanie podatności na ataki na własną sieć lokalną.

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**.

The screenshot displays the GFI LANguard 2012 application window. The top menu bar includes Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, and Utilities. The 'Scan' tab is active.

Launch a New Scan

Scan Target: localhost | Profile: Full Scan

Credentials: Currently logged on user | Username: | Password: | Scan

[Scan Options...](#)

Scan Results Overview

Scan target: localhost

- 10.6.125.36 [W2K16-WOJCIECH] (Windows NT 10.0 Gold)
 - Vulnerability Assessment
 - High Security Vulnerabilities (49)
 - Medium Security Vulnerabilities (7)
 - Low Security Vulnerabilities (4)
 - Potential Vulnerabilities (1)
 - Network & Software Audit

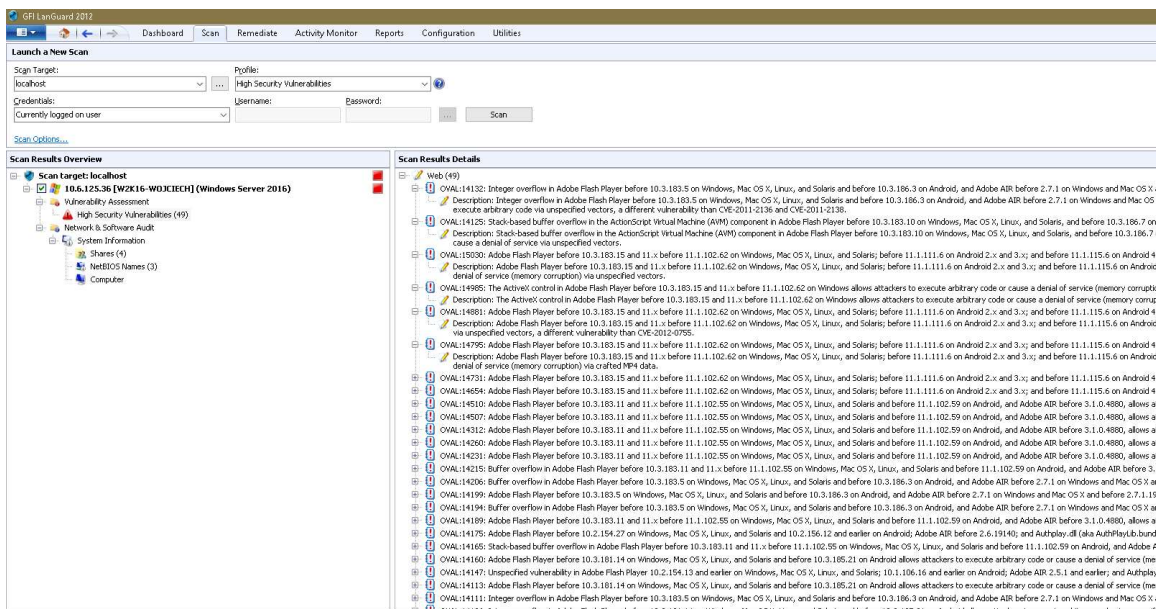
Scanner Activity Window

Time	Computer	Operation	Error Message
27-paź-23 08:25:28	W2K16-WOJCIECH	Enumerating installed applications.	Full security applications audit failed.
27-paź-23 08:25:55	W2K16-WOJCIECH	Missing patches scan	The patch management database is unavailable

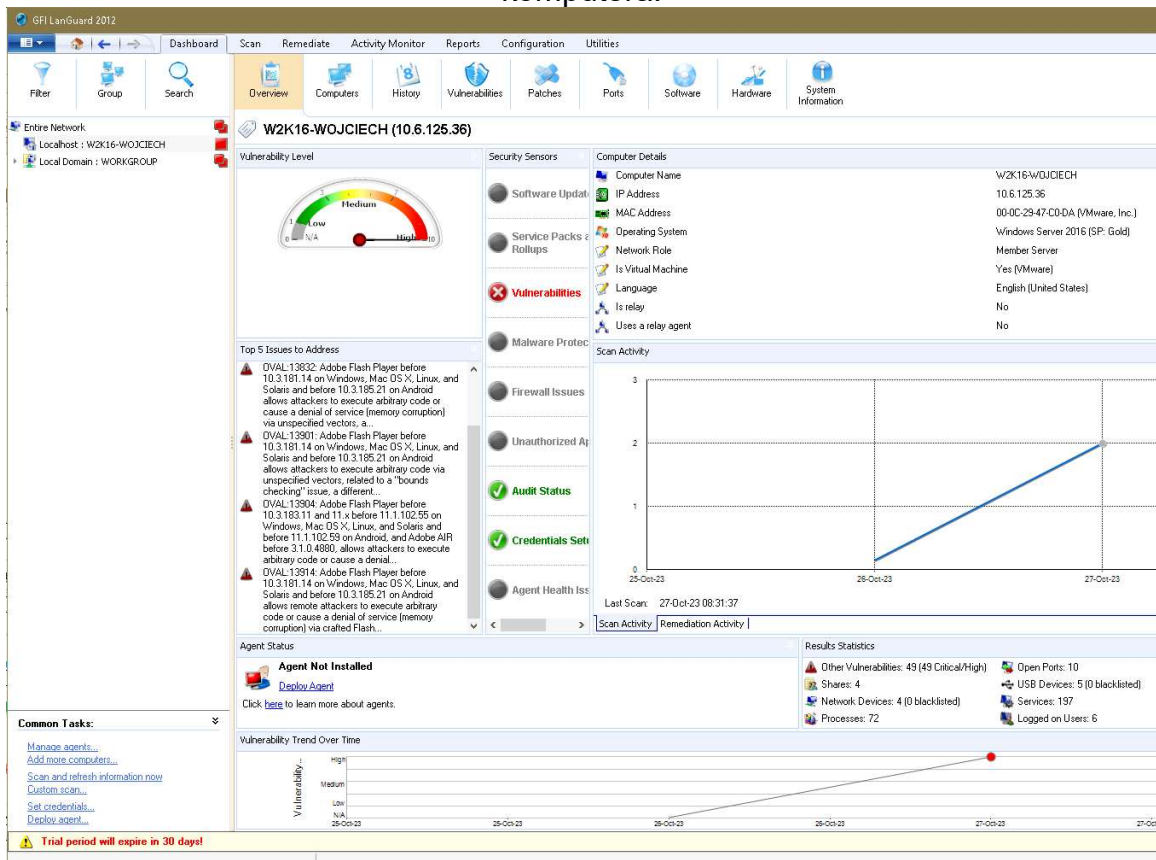
Network discovery | Scan thread 1 (idle) | Scan thread 2 (idle) | Scan thread 3 (idle) | **Errors**

⚠ Trial period will expire in 30 days!

Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki **Scan** i pozycji **High Security Vulnerabilities**



Obraz okna programu **GFI LANguard** uzyskanego po wybraniu zakładki **Dashboard**, przycisku **Overview** oraz łącza zawierającego nazwę skanowanego komputera.



Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki **Dashboard**, przycisku **Ports** oraz łącza zawierającego nazwę skanowanego komputera.

GFI LANguard 2012

Dashboard Scan Remediate Activity Monitor Reports Configuration Utilities

Filter Group Search Overview Computers History Vulnerabilities Patches Ports Software Hardware System Information

Entire Network
 Localhost : W2K16-WOJCIECH
 Local Domain : WORKGROUP

W2K16-WOJCIECH (10.6.125.36)

Port Types
 Open TCP Ports [3]
 Open UDP Ports [7]

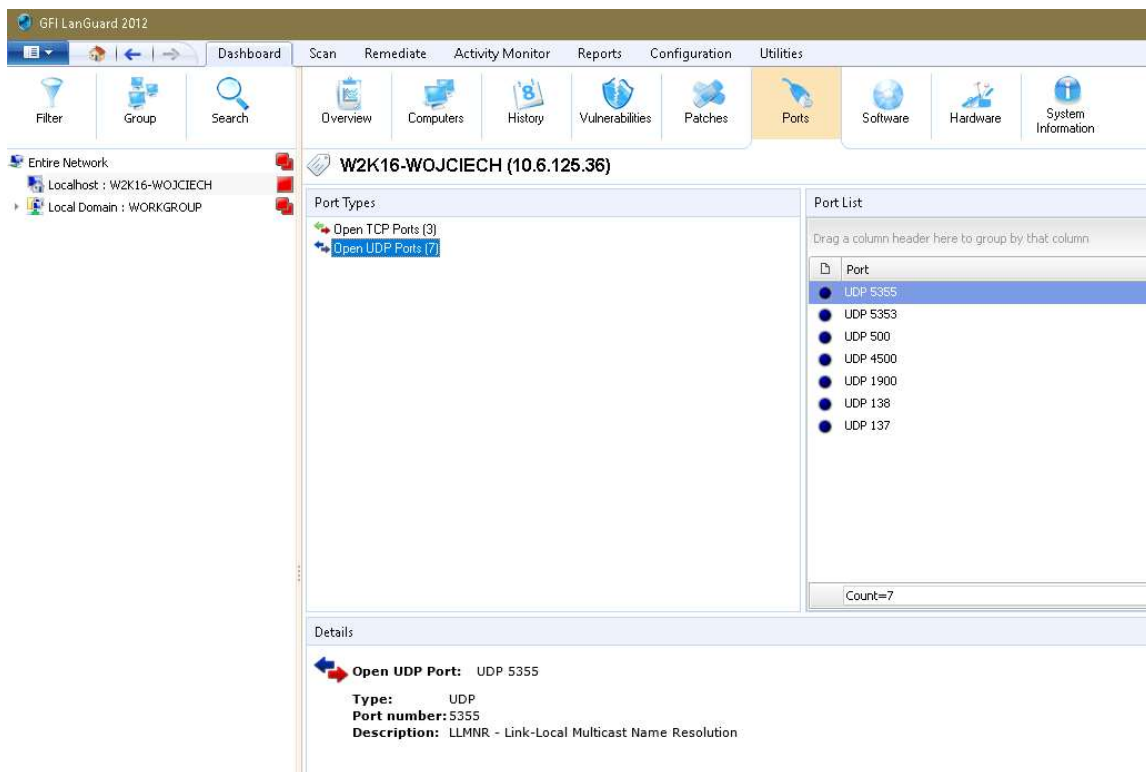
Port List
 Drag a column header here to group by that column

Port
TCP 445
TCP 139
TCP 135

Count=3

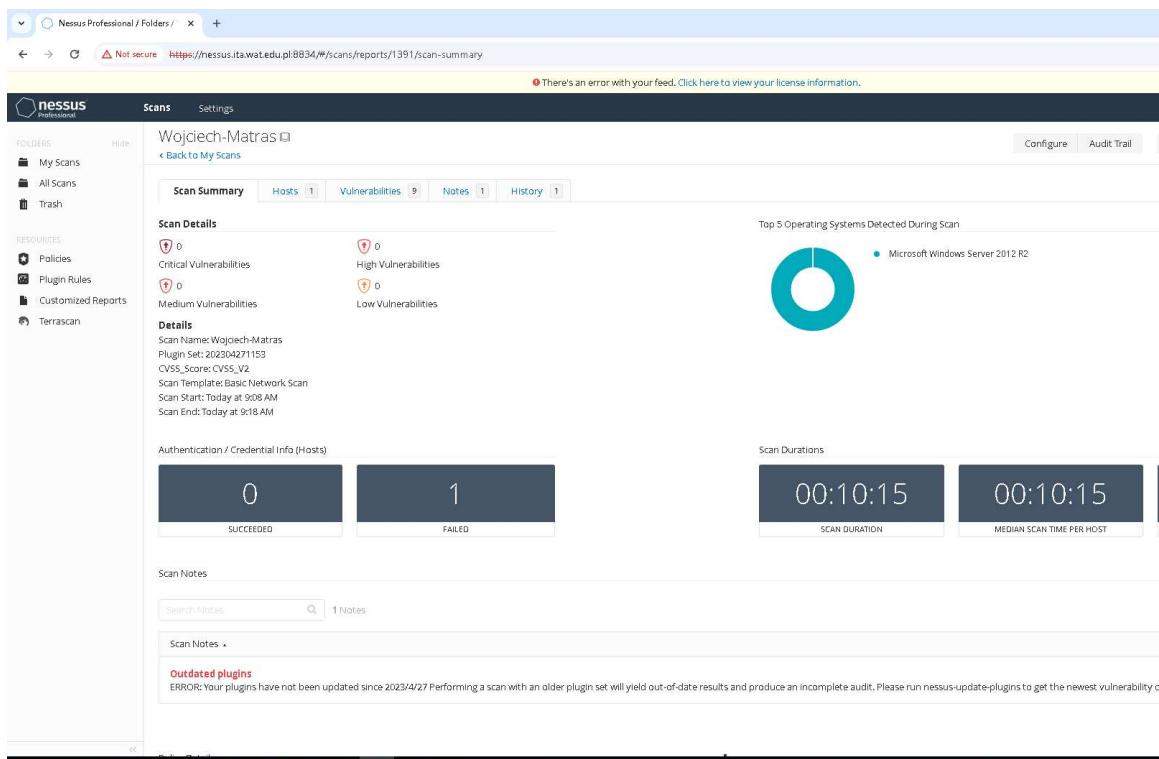
Details

Open TCP Port: TCP 445
 Type: TCP
 Port number: 445
 Process name: System
 Description: Microsoft-DS Active Directory, Windows shares



Skaner programu GFI LanGuard wykrył 49 dużych luk w zabezpieczeniach systemu. Oceniał w sposób przejrzysty wysokie, średnie oraz niskie zagrożenia w zabezpieczeniach systemu. Do prawie każdej luki podaje Score CVSS oraz opis problemu.

Widok okna aplikacji Nessus pokazujący wyniki skanowania hosta, z uwzględnieniem szczegółów wykonanego skanowania oraz liczby wykrytych podatności



Wojciech-Matras

Scan Summary | Hosts: 1 | **Vulnerabilities: 9** | Notes: 1 | History: 1

Filter: Search Vulnerabilities 9 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
INFO			Nessus SYN scanner	Port scanners	4	
INFO			Common Platform Enumeration (CPE)	General	1	
INFO			Device Type	General	1	
INFO			ICMP Timestamp Request Remote Date Disclosure	General	1	
INFO			Nessus Scan Information	Settings	1	
INFO			Open Port Re-check	General	1	
INFO			OS Identification	General	1	
INFO			TCP/IP Timestamps Supported	General	1	
INFO			Traceroute Information	General	1	

Scan Di

Policy: Status: Severity Scanner Start: End: Elapsed

Vulner

Fragment raportu **HTML** (Complete List of Vulnerabilities by Host) począwszy od słów „TABLE OF CONTENTS”, uwzględniający kilka pozycji zidentyfikowanych podatności w postaci listy rozwiniętej.

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.6.125.36

Vulnerabilities by Host

10.6.125.36



Severity	CVSS v2.0	VPR Score	Plugin	Name
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information

Hide

Fragment raportu **HTML** (Exploitable Vulnerabilities Report) prezentujący kilka pozycji zidentyfikowanych podatności, posortowanych ze względu na użytą wtyczkę (Hosts by Plugin).

TABLE OF CONTENTS

Exploitable Vulnerabilities Report

- No Results:

Exploitable Vulnerabilities Report

Exploitable vulnerabilities create gaps in the network's integrity, which attackers can take advantage of to gain access. Once inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant damage to systems. This report provides a summary of the most prevalent exploitable vulnerabilities.

No Results:

No Exploitable Vulnerabilities Found

No Exploitable Vulnerabilities found in these scan results

Widok wykrytej podatności protokołu **SMB**, pochodzący z dowolnego raportu, który uwzględnia opis wykonanego skanowania, zalecenia eliminacji podatności oraz przypisane wybrane miary liczbowe CVSS.

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, **SMB**, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2012 R2 Standard
Confidence level : 56
Method : MLSinFP
```

Not all fingerprints could give a match. If you think some or all of the following could be used to identify the host's operating system, please email them to os-signatures@nessus.org. Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

```
SinFP::
P1: 811113: P0x12: M8192: 08204ffff: M0460:
P2: 811113: P0x12: M8192: 08204ffff8103030804020800affffffff44454144: M0460:
P3: 000000: P0x00: M0: 00: M0
P4: 190501_7_p=139R
```

The remote host is running Microsoft Windows Server 2012 R2 Standard