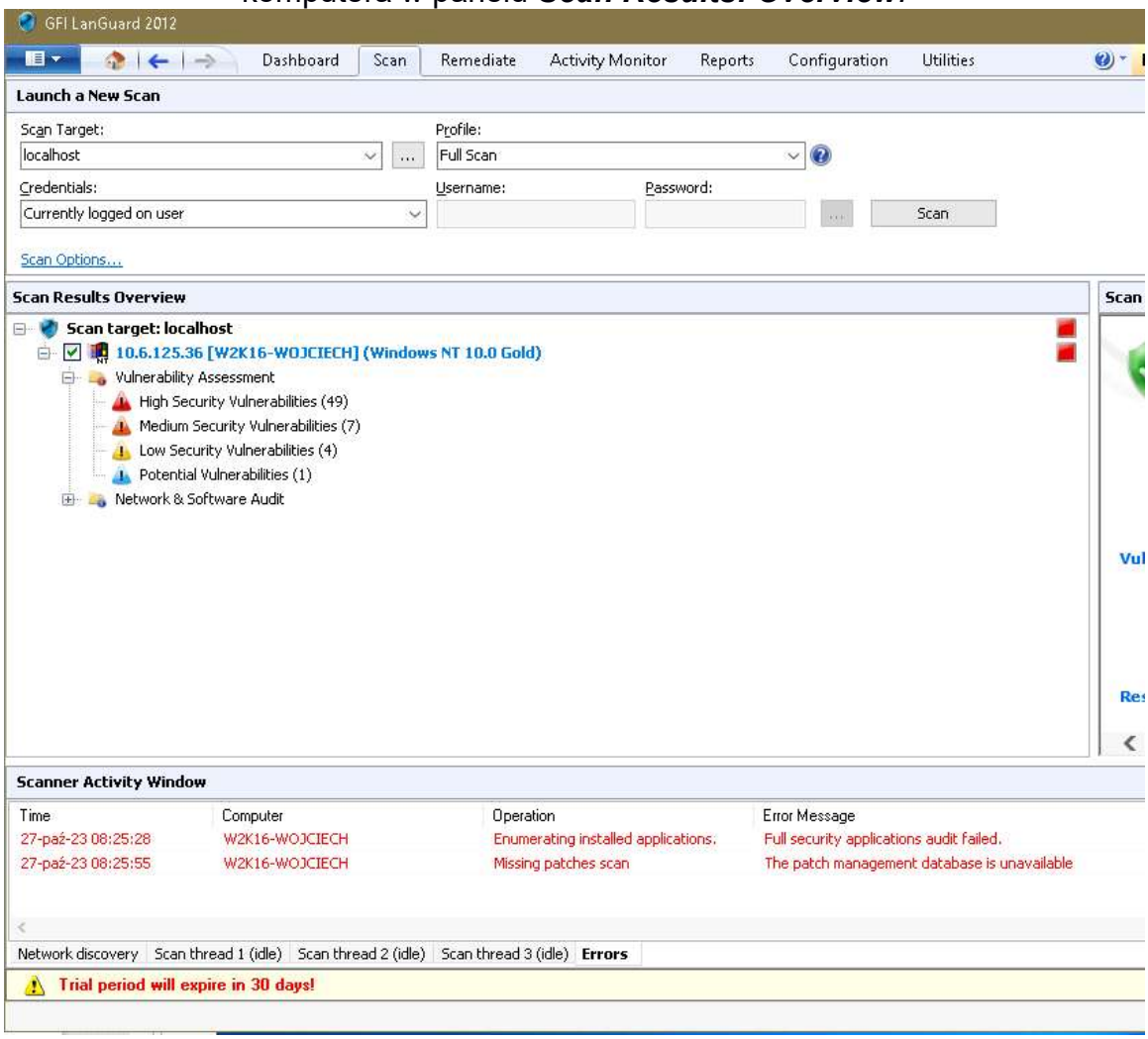
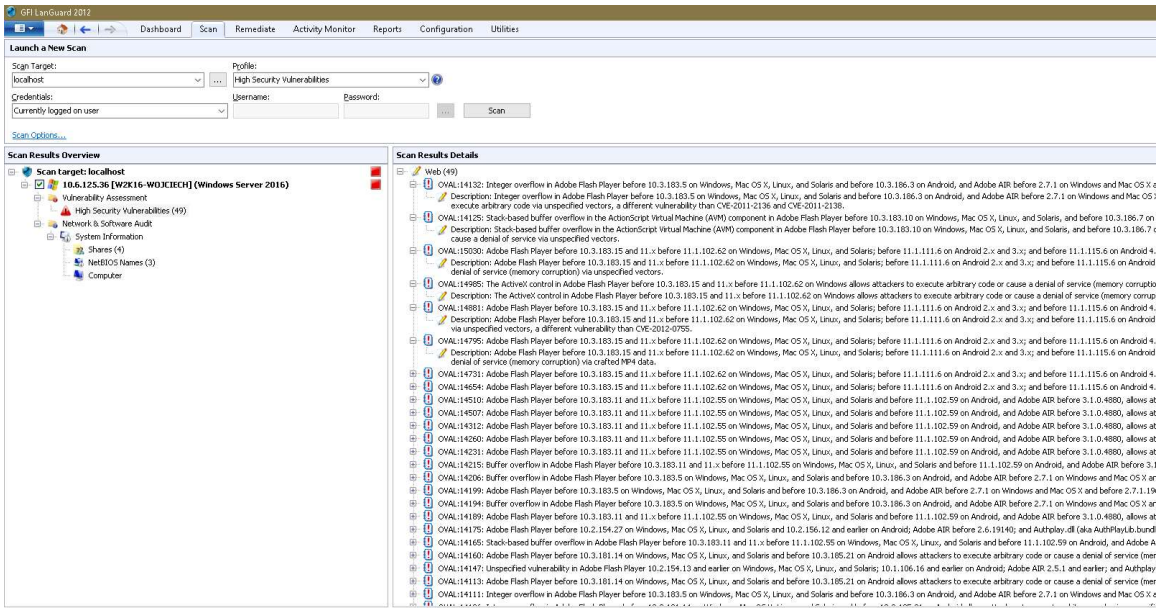
Szykanie podatności na ataki na własną sieć lokalną.

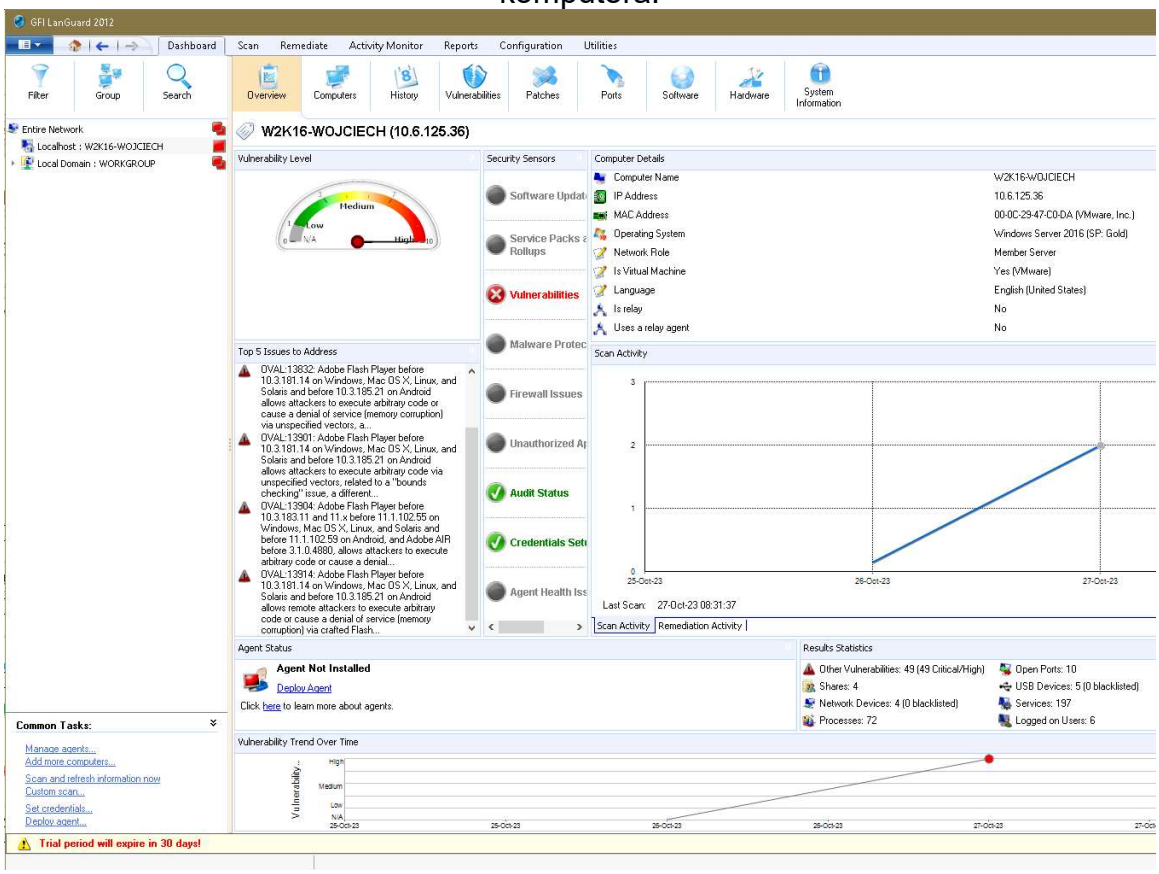
Obraz okna programu *GFI LANguard* prezentującego podsumowanie wyników skanowania, uzyskanego po wybraniu zakładki ***Scan*** i pozycji z nazwą i adresem komputera w panelu ***Scan Results: Overview***.



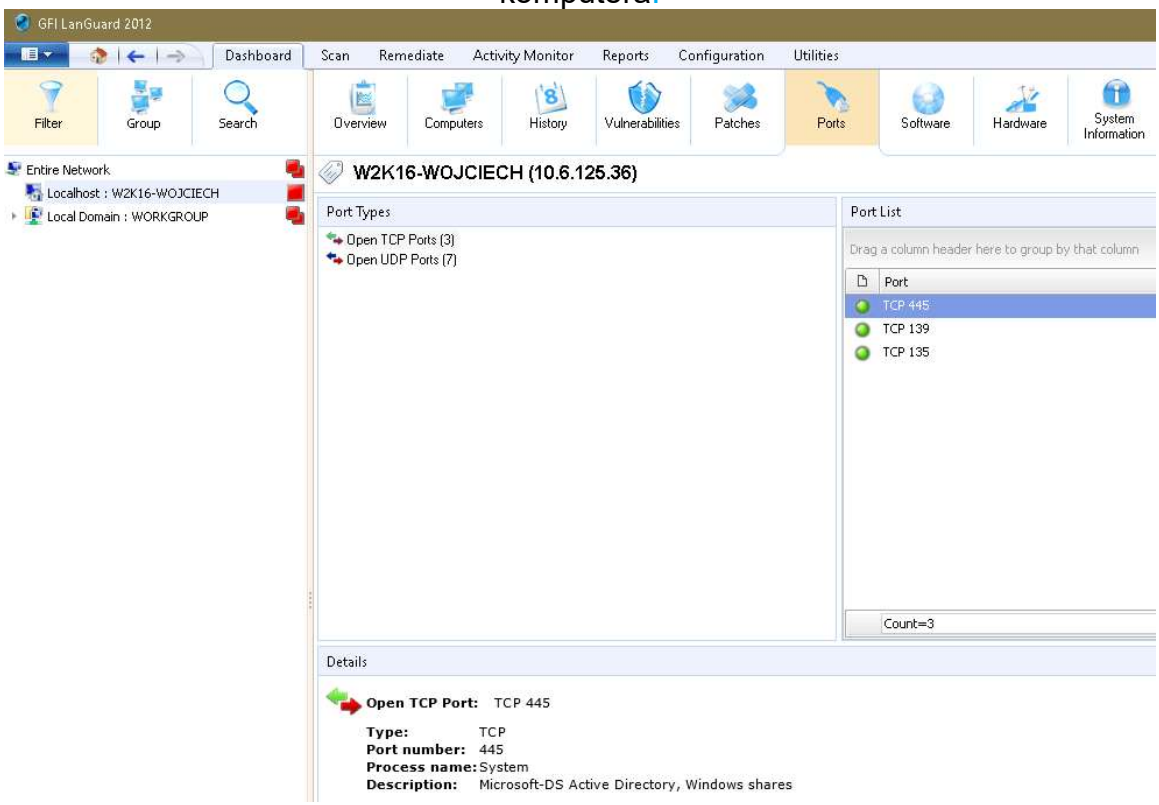
Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki ***Scan*** i pozycji ***High Security Vulnerabilities***

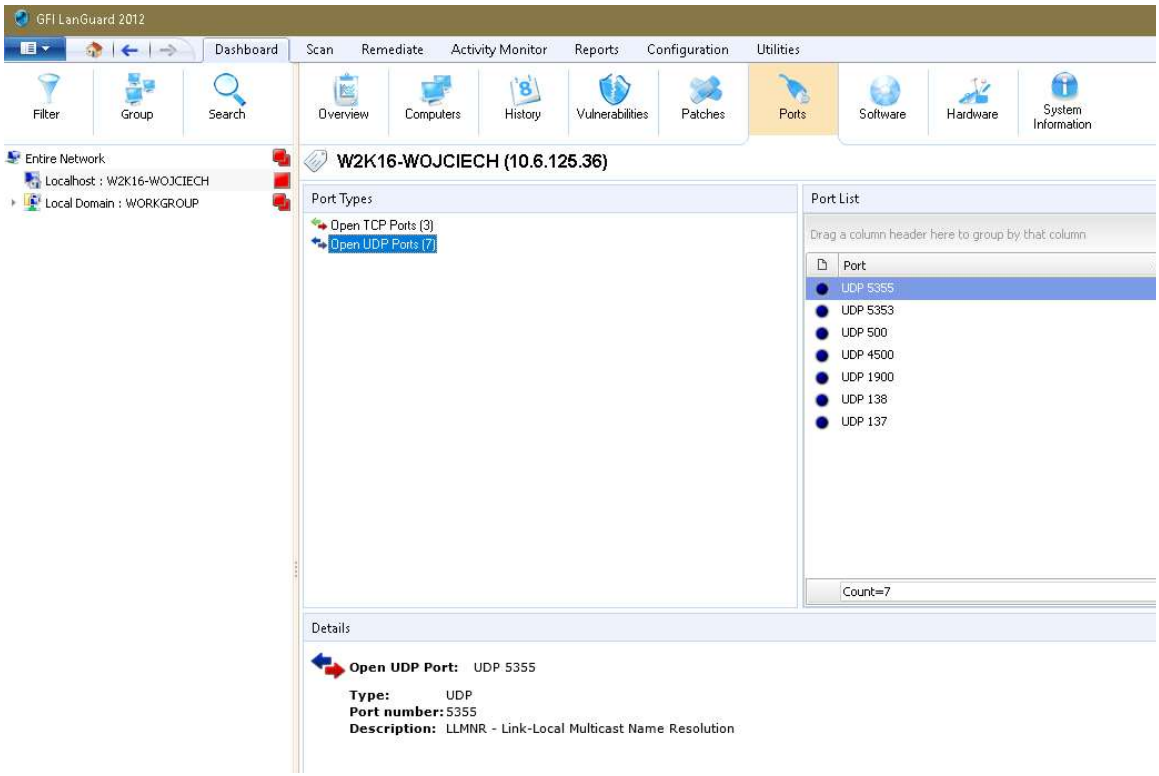


Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki ***Dashboard***, przycisku ***Overview*** oraz łącza zawierającego nazwę skanowanego komputera.



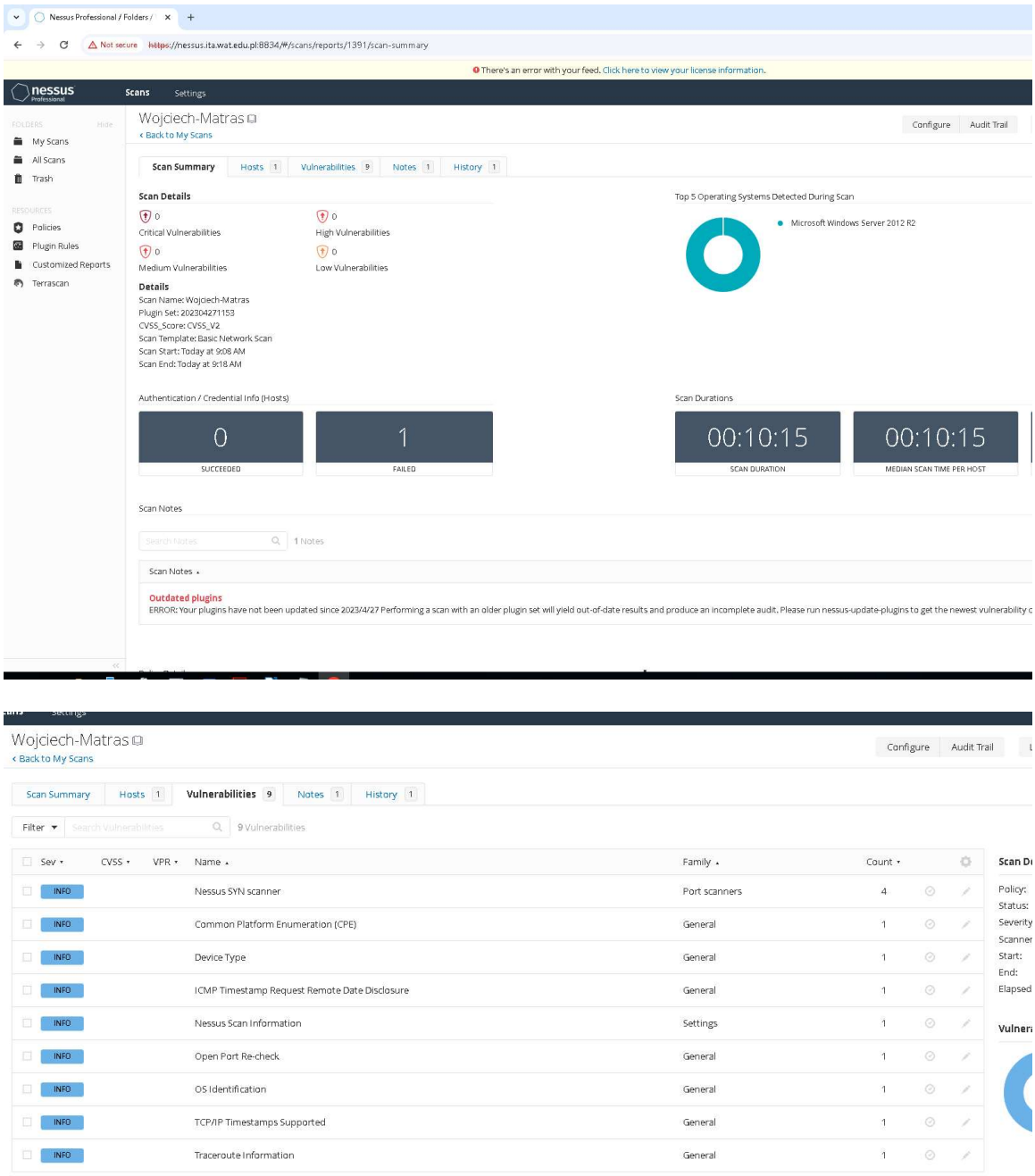
Obraz okna programu *GFI LANguard* uzyskanego po wybraniu zakładki ***Dashboard***, przycisku ***Ports*** oraz łącza zawierajcego nazwę skanowanego komputera.





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

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



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

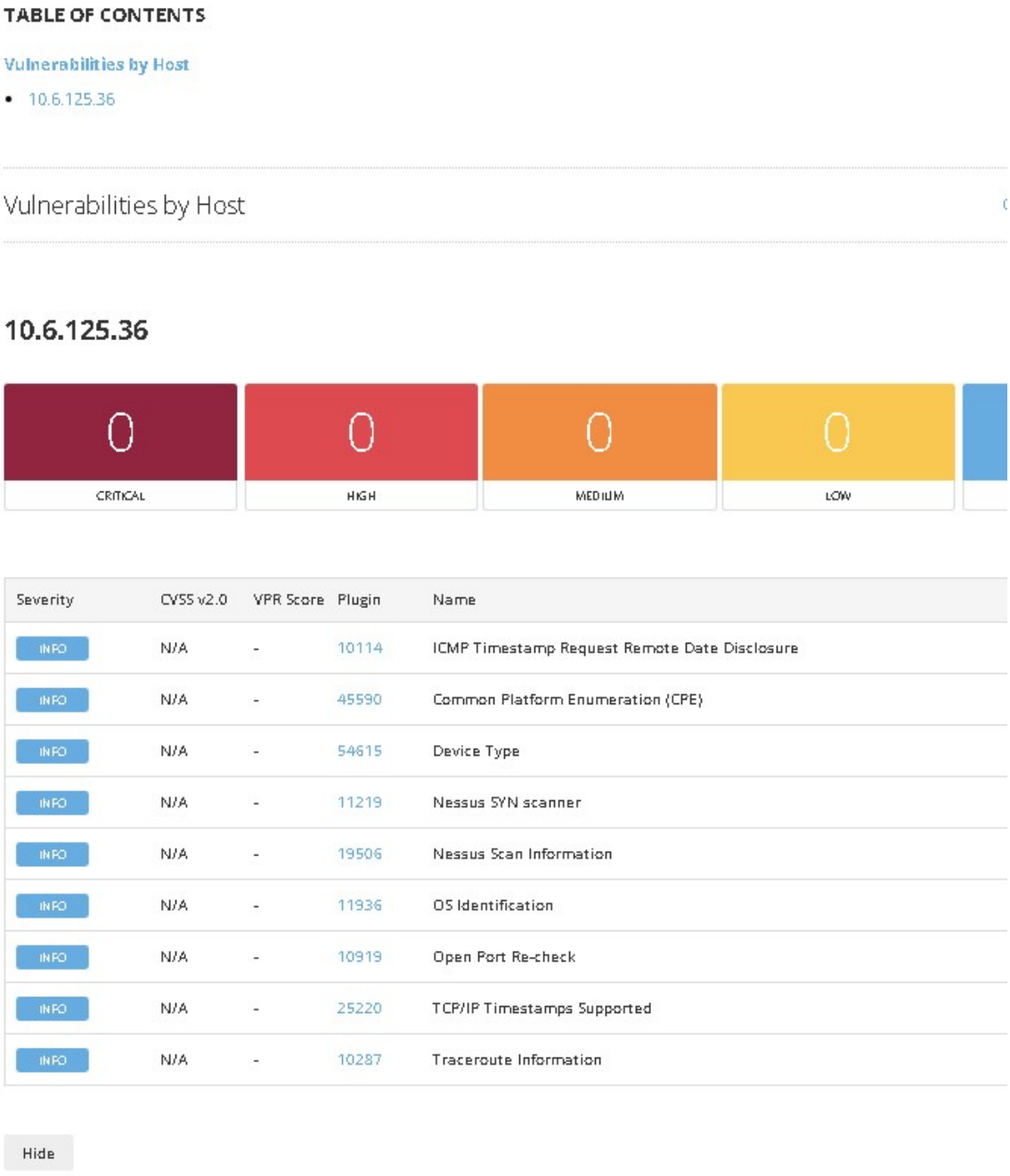


TABLE OF CONTENTS

Vulnerabilities by Host

- 10.6.125.36

Vulnerabilities by Host

10.6.125.36

0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW

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).

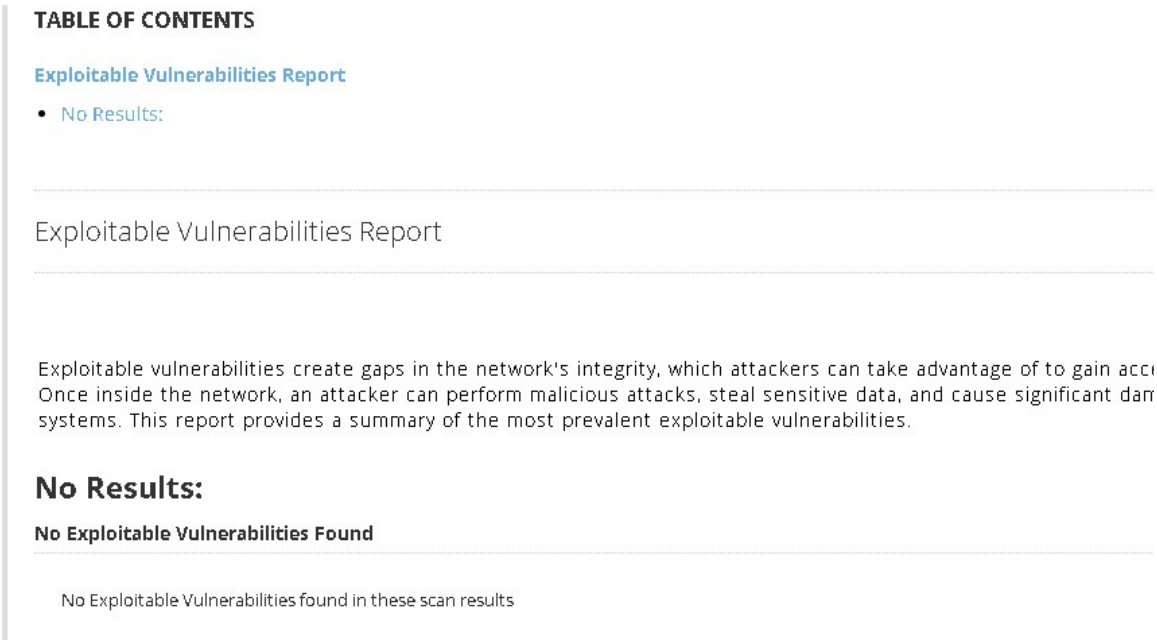


TABLE OF CONTENTS

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 acc
Once inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant dan
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 sy 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:B11113:F0x12:W8192:O0204ffff:M1460:
P2:B11113:F0x12:W8192:O0204ffff010303000402080affffffff44454144:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:190501_7_p=139R


The remote host is running Microsoft Windows Server 2012 R2 Standard
```