

**UWAGA!!! W ramach ćwiczenia są wymagane loginy-hasła dostępu do Kali Linux OS, SSH, OpenVas, IP-adresy skanowanych narzędzi. Ta informacja będzie uzyskana od prowadzącego podczas zajęć.**

Skaner podatności OpenVas pozwala na automatyzowaną ocenę podatności (vulnerability assessment) i zarządzanie podatnościami (vulnerability management). OpenVas działa w sposób podobny do działania cyberprzestępcy, co pozwala wykrywać luki w systemach bezpieczeństwa przed momentem ich wykorzystania przez hackiera.

System pozwala na wykrycie podatności w dwóch generalnych trybach:

- Skanowanie z uwierzytelnianiem
- Skanowanie bez uwierzytelniania

**Skanowanie bez uwierzytelniania** pozwala na wykrycie hostów w sieci i podatności uruchomionych usług sieciowych.

**Skanowanie z uwierzytelnianiem** z kolei pozwala sprawdzić wewnętrzną konfigurację hostów i wykrywać podatności w aplikacjach i oprogramowaniu, które nie zostały uruchomione przez administratora hosta.

Generalnie, System OpenVas zawiera:

- Bazy danych
- Klientci
  - OpenVas CLI
  - Greenbone Security Assistant
- Serwisy:
  - OpenVas Scanner
  - OpenVas Manager

W **Bazach danych** są umieszczone testy podatności oraz dane użytkowników i służbowa informacja (wyniki testów, zaplanowane testy, parametry hostów (celi) do skanowania, loginy i t.d.)

**OpenVas CLI** pozwala zarządzać systemem poprzez złożenie komand w wierszu polecenia (terminału)

**Greenbone Security Assistant** pozwala zarządzać systemem za pomocą interfejsu webowego

**OpenVas Scanner** skanuje celi OpenVas Manager na podstawie poleceń przekazanych administratorem poprzez (OpenVas CLI lub Greenbone Security Assistant) zarządza pozostałymi elementami systemu. Organizuje współpracę pomiędzy elementami systemu.

## Celi ćwiczenia:

1. Zapoznać się z interfejsem OpenVas;
2. Nauczyć się konfigurować listy portów dla skanowania;
3. Nauczyć się konfigurować parametry celi i skanowania;
4. Nauczyć się planować zadania dla OpenVas;
5. Zobaczyć różnicę pomiędzy skanowaniem z uwierzytelnianiem i bez uwierzytelnianiem;
6. Sprawdzić podatność rzeczywistych systemów (dostępnych w laboratorium 204) za pomocą OpenVas.

Laboratorium odbędzie się w grupach dwuosobowych. Stanowisko laboratoryjne zawiera 2 komputery i 1 przełącznik Cisco.

Jeden komputer i Cisco są wykorzystane dla testów. Drugi komputer będzie spełniał funkcję skanera podatności.

Uruchom OpenVas

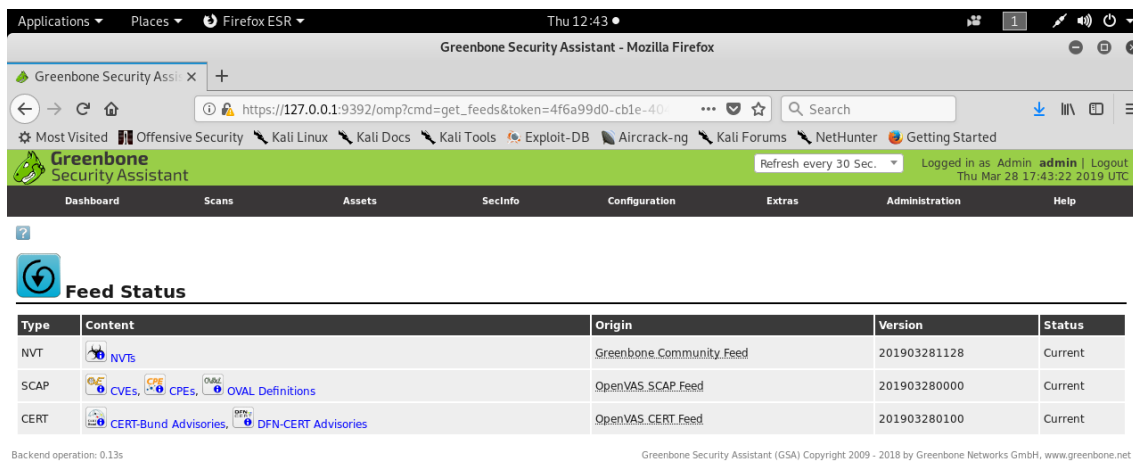
`# openvas-start`

Uruchom przeglądarkę internetową i połącz się z portem 9392 na 127.0.0.1  
Wpisz nazwę użytkownika i hasło, następnie zaloguj się.

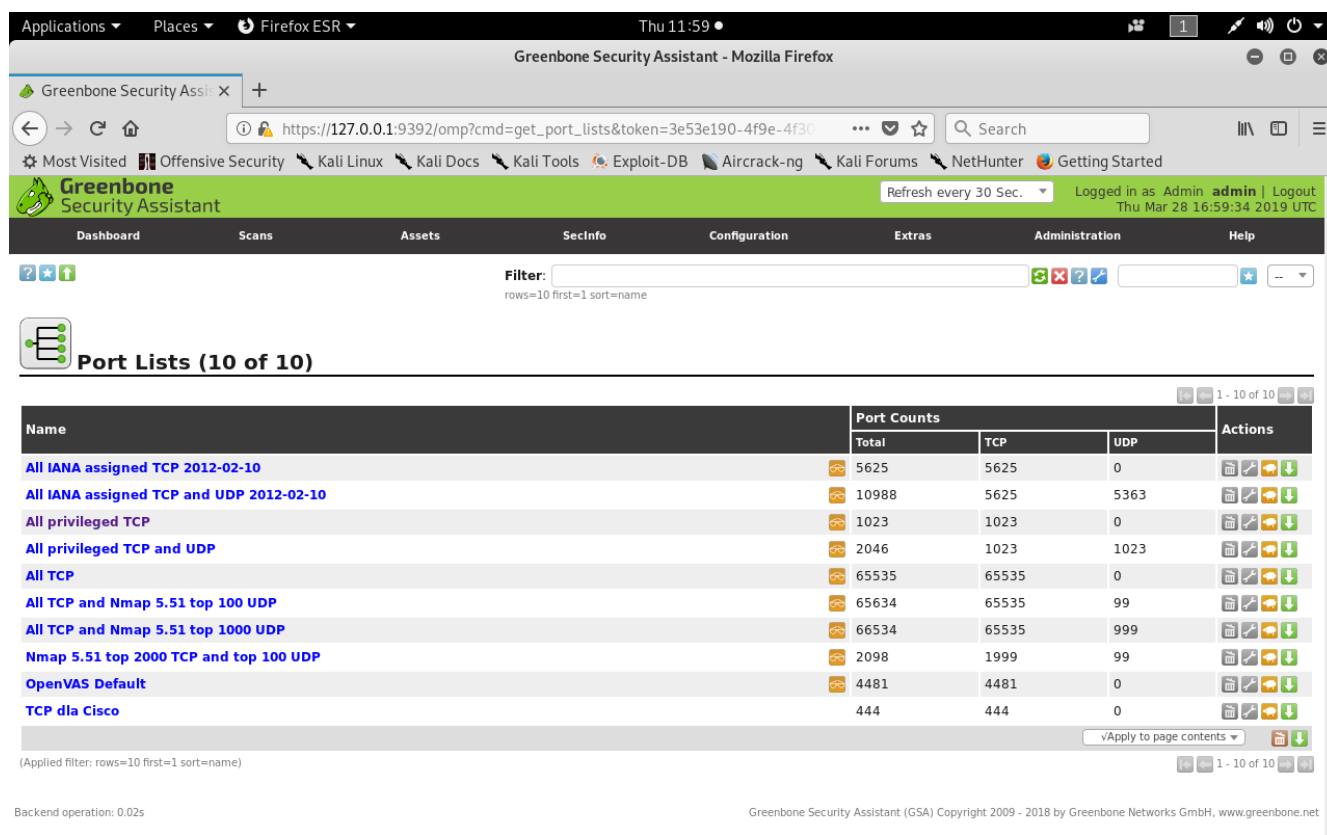
Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net



Sprawdź aktualność baz danych. “Extras” -> “Feed Status”



OpenVas skanuje celi na podstawie znanych list portów sieciowych. Zobacz które listy są dostępne:  
 “Configurations” -> “Port Lists”



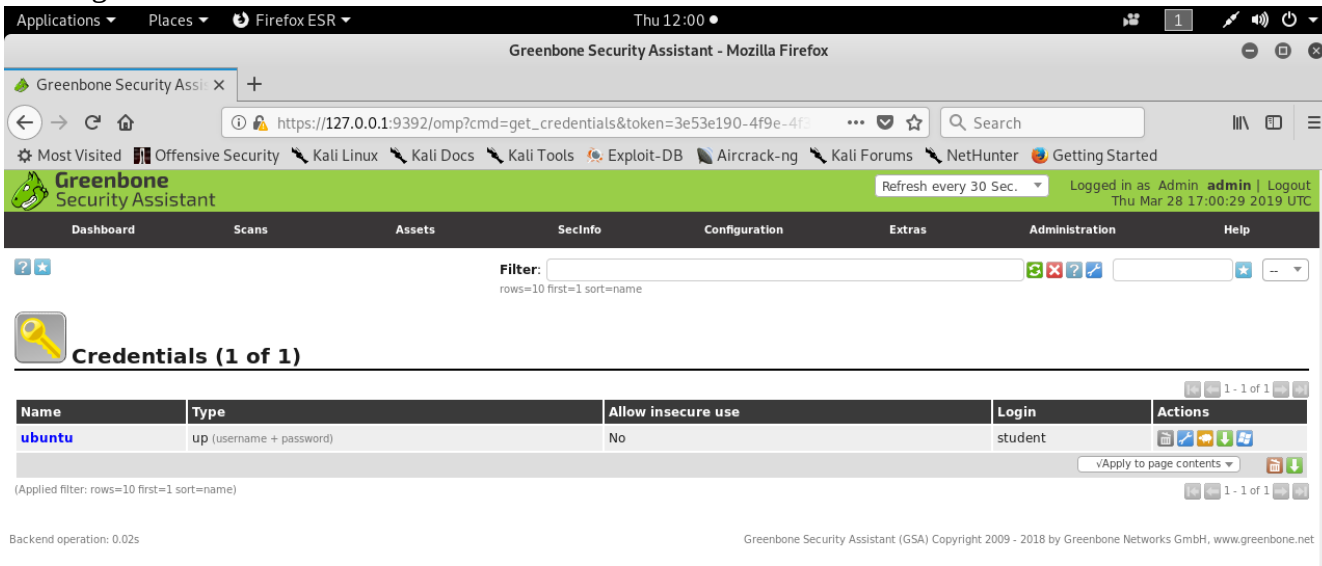
W ramach ćwiczenia będziemy skanowali przełącznik Cisco, komputery pod zarządzaniem OS Windows oraz Ubuntu Linux. Dla tych celów będziemy korzystać z listy “All privileged TCP” oraz właśnie założonej listy.





Sklonuj dowolną listą protów sieciowych (przycisk ) i skonfiguruj ją (przycisk ) w następujący sposób:

*nazwa: “TCP dla Cisco”.*

*Porty: TCP od 1 do 444.*

Dla skanowania z uwierzytelnianiem OpenVas korzysta z dostępnych profili logowania. Sprawdź dostępne profile logowania: “Configurations” -> “Credentials”

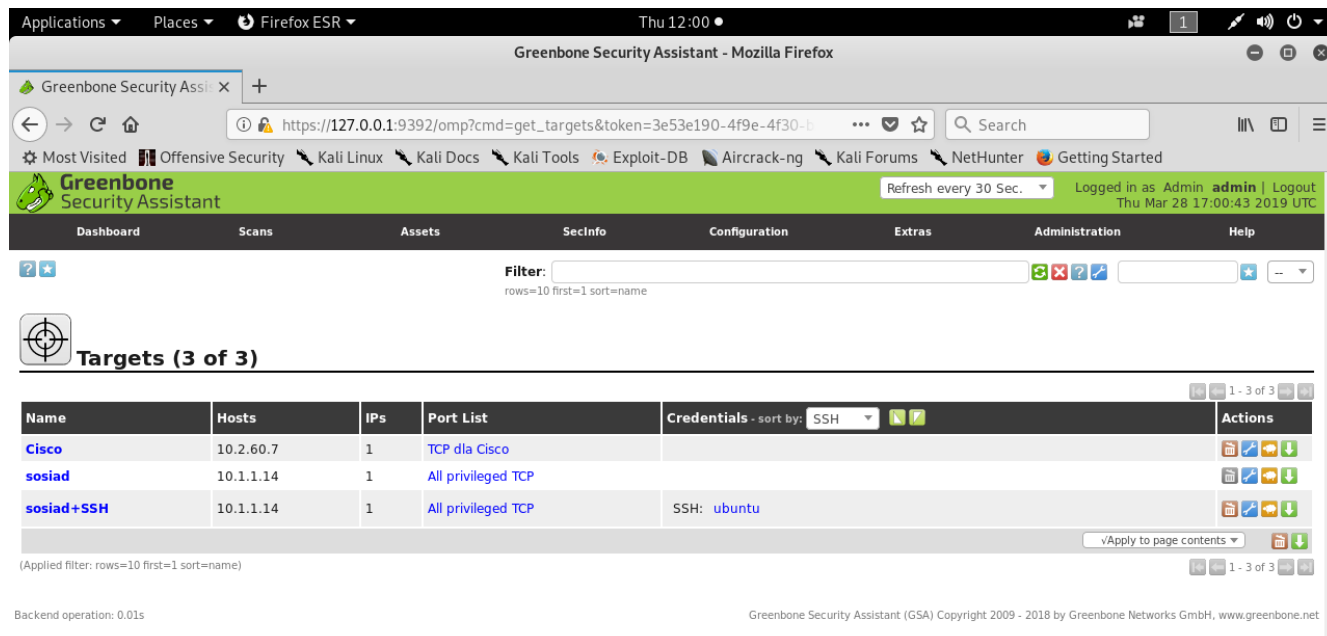


Name	Type	Allow insecure use	Login	Actions
ubuntu	up (username + password)	No	student	   

Załącz nowy profil:

*Nazwa: Ubuntu.*

Obejrzyj Celi do skanowania OpenVas:  
"Configurations" ->"Targets"



Greenbone Security Assistant - Mozilla Firefox

https://127.0.0.1:9392/omp?cmd=get\_targets&token=3e53e190-4f9e-4f30-b...

Greenbone Security Assistant

Refresh every 30 Sec. | Logged in as Admin admin | Logout Thu Mar 28 17:00:43 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: rows=10 first=1 sort=name

### Targets (3 of 3)

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Cisco	10.2.60.7	1	TCP dla Cisco		
sositad	10.1.1.14	1	All privileged TCP		
sositad+SSH	10.1.1.14	1	All privileged TCP	SSH: ubuntu	

(Applied filter: rows=10 first=1 sort=name)

Backend operation: 0.01s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Załóż nowe celi:

- + Nazwa "sositad"  
Port List: "All privileged TCP"
- + Nazwa "sositad+SSH"  
Port List: "All privileged TCP"  
Credentials for authenticated checks: SSH: ubuntu
- + Nazwa "Cisco"  
Port List: "TCP dla Cisco"

Obejrzyj dostępne konfiguracje testów:  
 “Configurations” → “Scan Configs”

The screenshot shows the Greenbone Security Assistant web interface. The browser address bar shows the URL: `https://127.0.0.1:9392/omp?cmd=get_configs&token=3e53e190-4f9e-4f30-b...`. The page title is "Scan Configs (8 of 8)". The table below lists the scan configurations:

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
<b>Discovery</b> (Network Discovery scan configuration.)	20	→	2721	→	[Icons]
<b>empty</b> (Empty and static configuration template.)	0	→	0	→	[Icons]
<b>Full and fast</b> (Most NVT's; optimized by using previously collected information.)	62	→	49689	→	[Icons]
<b>Full and fast ultimate</b> (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	62	→	49689	→	[Icons]
<b>Full and very deep</b> (Most NVT's; don't trust previously collected information; slow.)	62	→	49689	→	[Icons]
<b>Full and very deep ultimate</b> (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	62	→	49689	→	[Icons]
<b>Host Discovery</b> (Network Host Discovery scan configuration.)	2	→	2	→	[Icons]
<b>System Discovery</b> (Network System Discovery scan configuration.)	6	→	29	→	[Icons]

Backend operation: 0.01s  
 Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

W ramach ćwiczenia będziemy korzystać ze zmienionej listy “Full and fast ultimate”.

Sklonuj listę “Full and fast ultimate” i skonfiguruj ją w następujący sposób:

*nazwa: “lab204”.*  
*safe\_checks = yes*

Opcja “safe\_checks = yes” blokuje możliwość wykorzystanie niebezpiecznych testów (testów które mogą doprowadzić do awarii na skanowanym przez OpenVas systemu).

Obejrzyj dostępny zadania OpenVas:  
 “Configurations” → “Tasks”

The screenshot shows the Greenbone Security Assistant interface. At the top, there's a navigation bar with tabs for Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. Below this is a filter bar with a search input and a filter dropdown. The main content area is titled 'Tasks (1 of 1)'. It features three donut charts: 'Tasks by Severity Class (Total: 1)' with a yellow chart showing 1 Medium task; 'Tasks with most High results per host' with a message 'No Tasks with High severity found'; and 'Tasks by status (Total: 1)' with a blue chart showing 1 Done task. Below the charts is a table with the following data:

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
windows10	Done	1 (1)	Mar 28 2019	5.0 (Medium)		

At the bottom of the screenshot, there is a footer with the text: 'Backend operation: 0.01s' and 'Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net'.

Załóż nowe zadania:

- + Nazwa: "Windows10"  
 Scan Targets: "sosiad"  
 Scan Config: "lab204"
- + Nazwa: "Ubuntu"  
 Scan Targets: "sosiad"  
 Scan Config: "lab204"
- + Nazwa: "Ubuntu+SSH"  
 Scan Targets: "sosiad+SSH"  
 Scan Config: "lab204"
- + Nazwa: "Cisco"  
 Scan Targets: "Cisco"  
 Scan Config: "lab204"



**Zademonstruj konfigurację prowadzącemu.**

Uruchom Windows10 OS na komputerze sąsiada.  
Uruchom zadanie "Windows10".

- 1) Ile podatności zostało wykryte?**
- 2) ile czasu zajął test?**

Uruchom Ubuntu OS na komputerze sąsiada.  
Uruchom zadanie "Ubuntu".

- 1) Ile podatności zostało wykryte?**
- 2) ile czasu zajął test?**

Uruchom zadanie "Ubuntu+SSH".

- 1) Ile podatności zostało wykryte?**
- 2) ile czasu zajął test?**
- 3) jaka jest różnica w porównaniu do testu "Ubuntu"**

Uruchom zadanie "Cisco".

- 1) Ile podatności zostało wykryte?**
- 2) ile czasu zajął test?**

OpenVas analizuje poziom zagrożenia każdej podatności oraz prawdopodobieństwo poprawnego wykrycia (jakość wykrycia) - parametr QoD.

The screenshot shows the Greenbone Security Assistant (GSA) interface in Mozilla Firefox. The browser address bar shows the URL: `https://127.0.0.1:9392/omp?cmd=get_report&report_id=be788a5c-fa26-4d9...`. The interface is logged in as Admin admin. The main content area displays a report titled "Report: Results (1 of 12)". Below the title is a table with the following data:

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.1.1.14 (komp14.lab204.local)	135/tcp	[Icons]

Additional details for the report include: ID: be788a5c-fa26-4d99-8f03-2204e9ed377d, Modified: Thu Mar 28 17:00:51 2019, Created: Thu Mar 28 16:58:48 2019, Owner: admin. The backend operation time is 0.14s. Copyright information for Greenbone Security Assistant (GSA) is also visible at the bottom.

The screenshot shows the detailed results of the "DCE/RPC and MSRPC Services Enumeration Reporting" scan. The browser address bar shows the URL: `https://127.0.0.1:9392/omp?cmd=get_result&result_id=3021d11f-9f01...`. The interface is logged in as Admin admin. The main content area displays the report title "Result: DCE/RPC and MSRPC Services Enumeration Reporting". Below the title is a table with the following data:

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.1.1.14	135/tcp	[Icons]

The report includes a summary: "Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries." It also contains a "Vulnerability Detection Result" section with the following text: "Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:"

- Port: 49664/tcp
  - UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
  - Endpoint: ncacn\_ip\_tcp:10.1.1.14[49664]
- Port: 49665/tcp
  - UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
  - Endpoint: ncacn\_ip\_tcp:10.1.1.14[49665]
  - UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
  - Endpoint: ncacn\_ip\_tcp:10.1.1.14[49665]
- Port: 49666/tcp
  - UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
  - Endpoint: ncacn\_ip\_tcp:10.1.1.14[49666]
  - Annotation: Event log TCPIP

wartość QoD — zależy od sposobu wykrycia:

teoretycznie, jest możliwość podatności - (1%)

•

•

•

została wykryta podatna wersja oprogramowania — średni QoD - (80%)

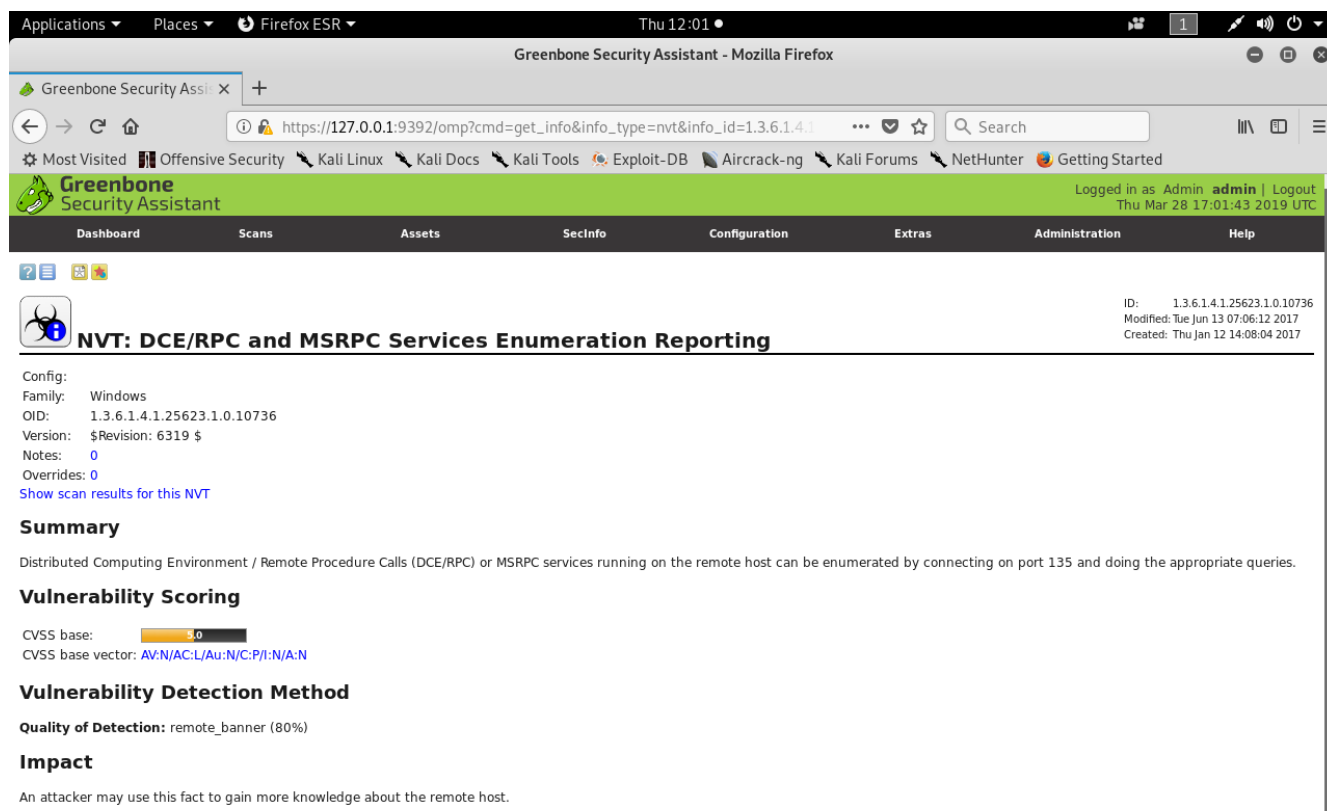
•

•

•

sukcesem zostało skończone wykorzystanie gotowego exploitu dla wykrytej podatności — wysoki QoD (100%)

Szczegóły sposobu wykrycia podatności są dostępne w "Vulnerability Detection Method" w opisie podatności.



The screenshot shows the Greenbone Security Assistant web interface in a Mozilla Firefox browser. The page displays details for a specific NVT (Network Vulnerability Test) titled "NVT: DCE/RPC and MSRPC Services Enumeration Reporting".

**Configuration:**

- Family: Windows
- OID: 1.3.6.1.4.1.25623.1.0.10736
- Version: \$Revision: 6319 \$
- Notes: 0
- Overrides: 0

[Show scan results for this NVT](#)

**Summary**

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Vulnerability Scoring**

CVSS base:  3.0  
CVSS base vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

**Vulnerability Detection Method**

**Quality of Detection:** remote\_banner (80%)

**Impact**

An attacker may use this fact to gain more knowledge about the remote host.

OpenVas jest zdolny dla automatycznego uruchomieniu zaplanowanych testów. Obejrzyj zaplanowane testy:

“Configurations” -> “Schedules”

Załącz nowy dowolny zaplanowany test.

Załącz nowe dowolne zaplanowane zadanie.

### **Zademonstruj konfigurację prowadzącemu.**

OpenVas pozwala ocenić tendencję zmiany poziomu bezpieczeństwa. Kolumna "Trend" w: “Configurations” → “Tasks”.

Uruchom znowu test Windows10.

**1) jak się zmienił Trend?**

**2) dlaczego?**

Zahamuj OpenVas:

**# *openvas-stop***