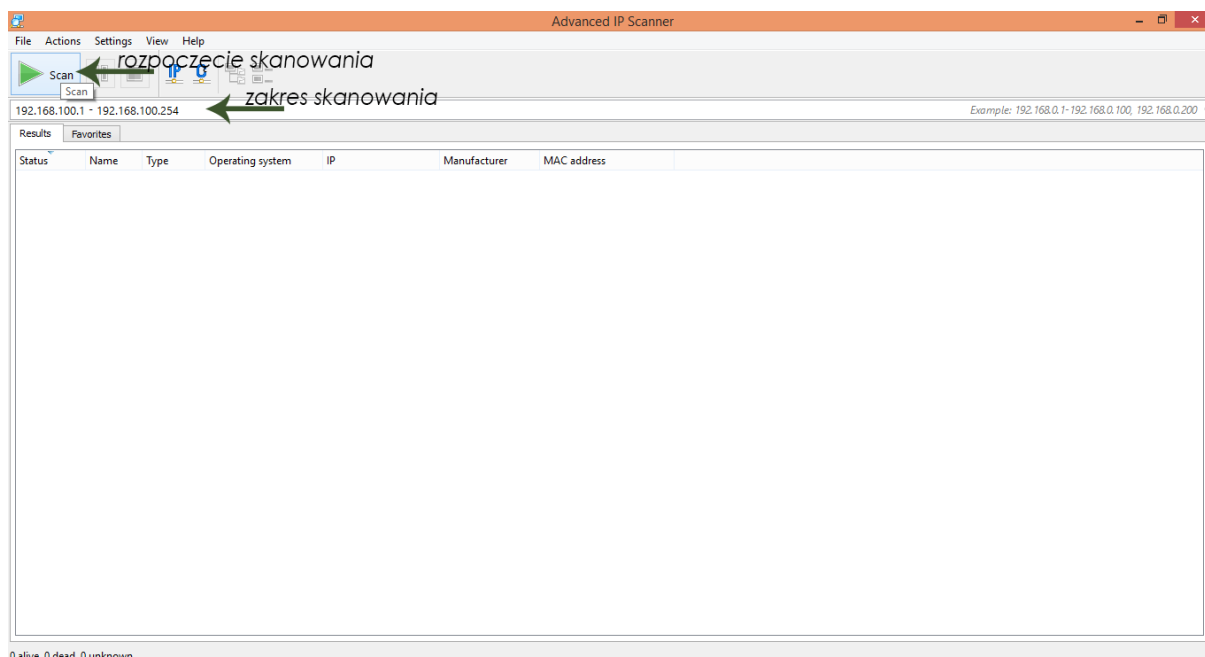


Przegląd darmowych programów wykorzystywanych w skanowaniu sieci:

- Advanced IP Scanner
- Nmap
- OpenVAS

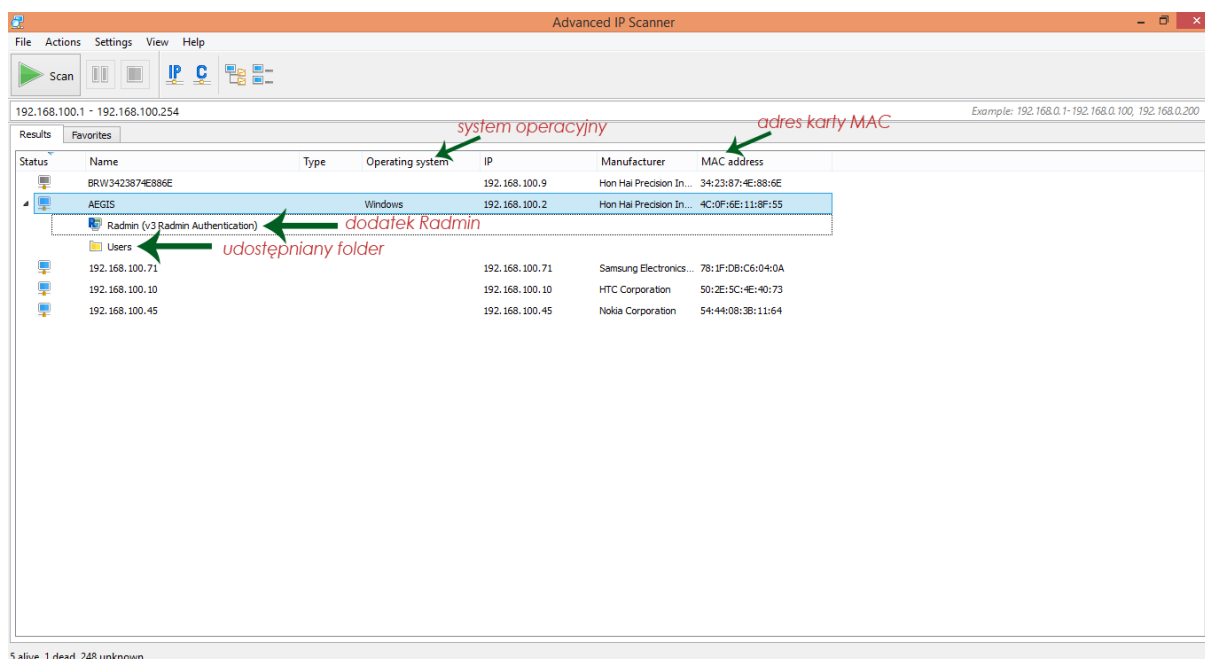
1. **Advanced IP Scanner** jest bardzo prosty w obsłudze. Zaraz po uruchomieniu pojawi nam się okno, w którym rzuca w oczy się duży przycisk **Scan** oraz zakres skanowania (rys. 1).



(rys. 1)

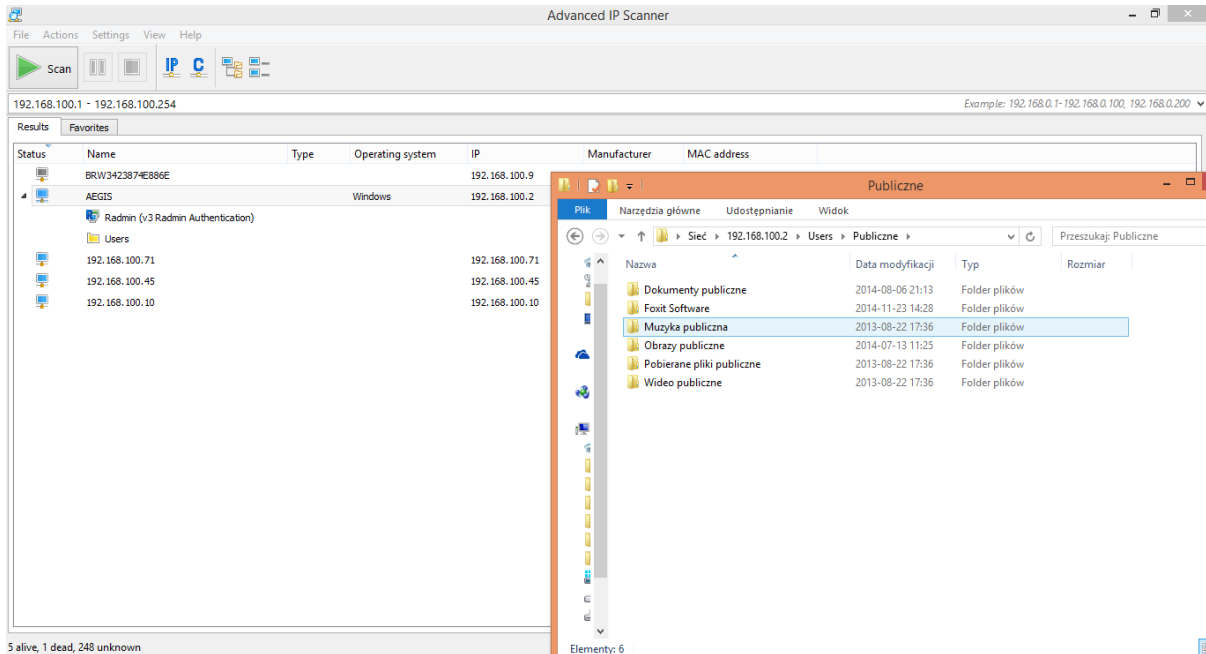
Zakres skanowania jest automatycznie wykrywany przez program, ale możemy go wpisać ręcznie.

Po wciśnięciu przycisku **Scan** i odczekaniu paru sekund ukaże się nam wynik naszego skanowania (rys. 2).

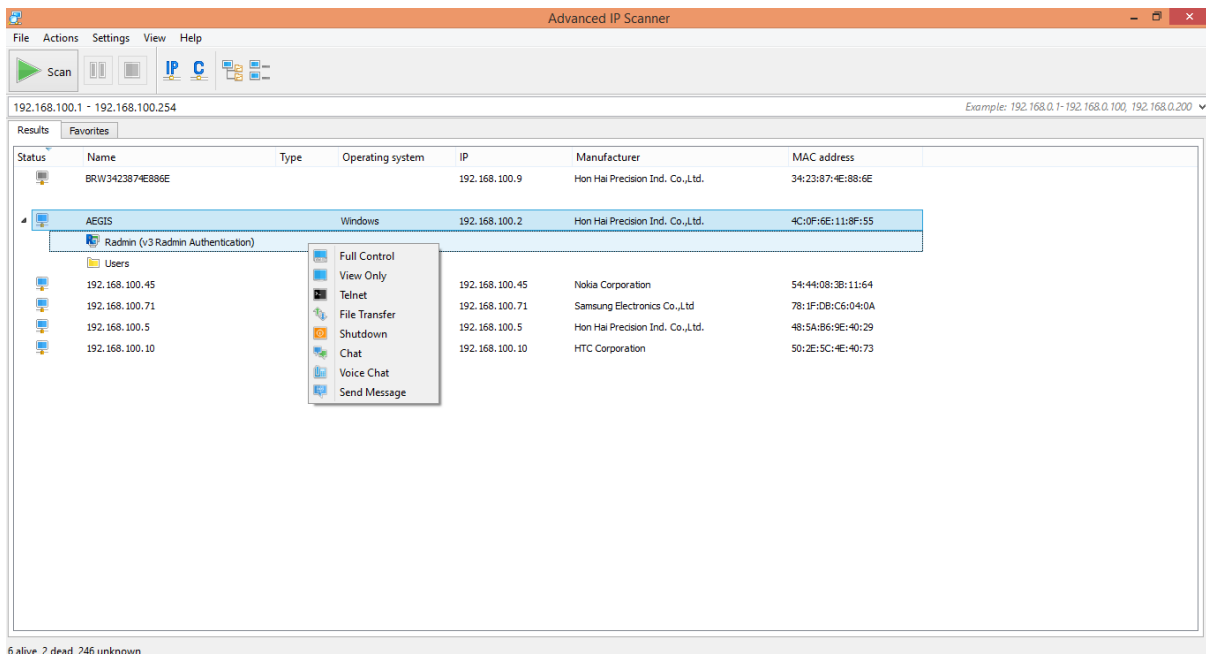


(rys. 2)

W oknie można zauważyć, że w obecnej sieci znajdują się 5 urządzeń. **Advanced IP Scanner** nie tylko pobrał adresy IP, ale także adresy MAC oraz na jakim systemie operacyjnym pracuje komputer. **Advanced IP Scanner** ma możliwość pokazania, jaki folder udostępnia dany komputer (rys. 3) oraz po zainstalowaniu dodatku Radmin kontroli nad nim (rys. 4).



(rys. 3)



(rys. 4)

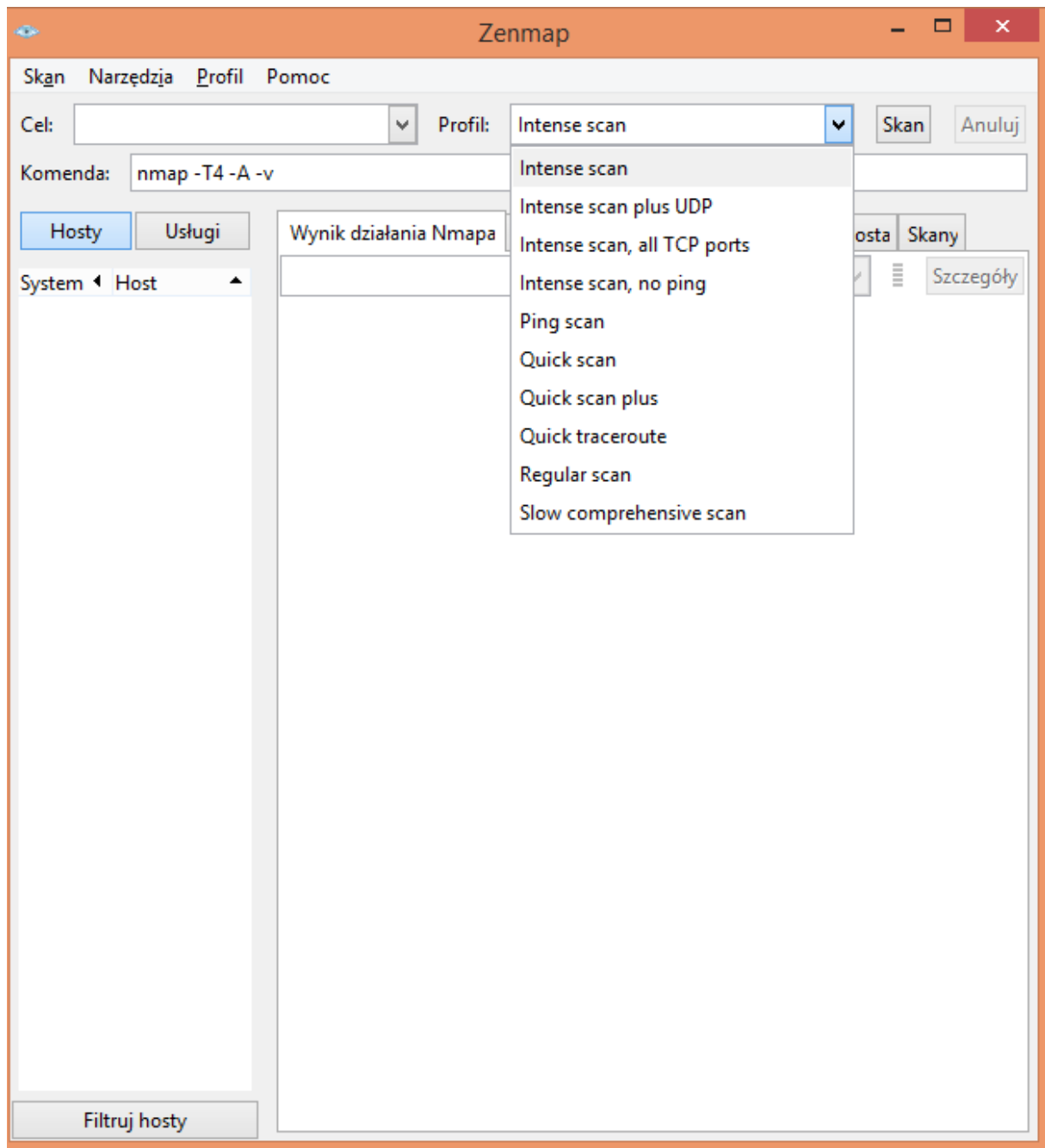
Aby cokolwiek zrobić na komputerze potrzebujemy loginu i hasła oraz zainstalowanego klienta programu Radmin na docelowym komputerze.

Advanced IP Scanner jest prostym, ale użytecznym narzędziem do kontroli nad siecią.

2. Kolejnym programem jest **Nmap** (Linux), **Nmap - Zenmap GUI** (Windows).

Główną zaletą Nmap jest możliwość skanowania całej sieci jak i też przeskanowanie konkretnego adresu IP.

Zenmap GUI jest łatwiejszy w obsłudze, ponieważ wystarczy wpisać adres IP celu, następnie wybrać profil i to wystarczy, aby zacząć skanowanie. Program daje możliwość wybrania profilu, ale także jego edycji jak i tworzenia własnych, dzięki temu nie ma potrzeby zapamiętywać długich komend.



Wybrane opcje programu <http://nmap.org/man/pl/>:

Użycie: nmap [Typ(y) skanowania] [Opcje] {specyfikacja celu}

SPECYFIKACJA CELU:

Można podać nazwy hostów, adresy IP, sieci, itp.

Przykłady: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <plik_wejściowy>: Odczytanie listy hostów/sieci z pliku

-iR <ilość hostów>: Wybranie losowych adresów

--exclude <host1[,host2][,host3],...>: Wyłączenie hostów/sieci

--excludefile <plik_wyłączeń>: Wyłączenie listy hostów/sieci z pliku

WYKRYWANIE HOSTÓW:

-sL: Lista skanowania - tylko wyświetla listę hostów do skanowania

-sP: Skanowanie Ping - tylko wykrywanie dostępności hostów

-PO: Traktuj wszystkie hosty jako dostępne - pomijanie wykrywania

-PS/PA/PU [lista_portów]: Wykrywanie TCP SYN/ACK lub UDP na wybranych portach

-PE/PP/PM: Zykrywanie za pomocą ICMP echo, timestamp, zapytania o maskę sieci

-n/-R: Nie używaj zapytań DNS/Zawsze odpytuj DNS [domyślnie: czasami]

--dns-servers <serv1[,serv2],...>: Używaj określonych serwerów DNS

--system-dns: Używaj systemowych ustawień DNS

TECHNIKI SKANOWANIA:

-sS/sT/sA/sW/sM: Skanowania TCP SYN/Connect()/ACK/Window/Maimon

-sN/sF/sX: Skanowania TCP Null, FIN i Xmas

--scanflags <flagi>: Ręczne narzucanie flag TCP

-sI <host zombie[:port]>: Idlescan

-sO: Skanowanie protokołów IP

-b <host pośredni ftp>: Skanowanie FTP bounce

SPECYFIKACJA PORTÓW I KOLEJNOŚCI SKANOWANIA:

-p <zakres portów>: Skanuj tylko podane porty

Przykład: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080

-F: Szybkie skanowanie - tylko porty zawarte w pliku nmap-services

-r: Skanuj porty kolejno - wyłączenie losowania kolejności

DETEKCJA USŁUG/WERSJI:

-sV: Wykrywaj wersję usługi na otwartych portach

--version-intensity <poziom>: Od 0 (tylko niektóre) do 9 (Używaj wszystkich testów)

--version-light: Limituj do najpopularniejszych testów (poziom 2)

--version-all: Używaj wszystkich testów (poziom 9)

--version-trace: Pokazuj dokładne informacje podczas skanowania (do usuwania błędów)

DETEKCJA OS:

-O: Włączenie wykrywania systemu operacyjnego

--osscan-limit: Limitowanie wykrywania OS do obiecujących hostów

--osscan-guess: Zgaduj wersję OS bardziej agresywnie

WYDAJNOŚĆ I ZALEŻNOŚCI CZASOWE:

- T[0-5]: Ustaw szablon (wyższy jest szybszy)
- min-hostgroup/max-hostgroup <rozmiar>: Rozmiary grup do równoległego skanowania
- min-parallelism/max-parallelism <msec>: Zrównoleglenie testów
- min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msec>: Specyfikuje czas testów
- max-retries <ilość>: Ustala ilość możliwych powtórzeń testu
- host-timeout <msec>: Pomijaj po zadanym czasie
- scan-delay/--max-scan-delay <msec>: Ustalenie opóźnienia pomiędzy testami

OPCJE FIREWALL/IDS:

- f; --mtu <wartość>: fragmentacja pakietów (opcjonalnie z podanym MTU)
- D <decoy1,decoy2[,ME],...>: Ukrywaj skanowanie za pomocą innych hostów
- S <Adres_IP>: Podmieniam adres nadawcy
- e <interfejs>: Używaj podanego interfejsu
- g/--source-port <portnum>: Używaj podanego portu źródłowego
- data-length <num>: Dodawaj losowe dane do wysyłanych pakietów
- ttl <wartość>: Ustaw czas życia pakietów
- spoof-mac <adres mac/prefix/producent>: Podmieniam adres MAC
- badsum: Wysyłaj pakiety z nieprawidłową sumą kontrolną TCP/UDP

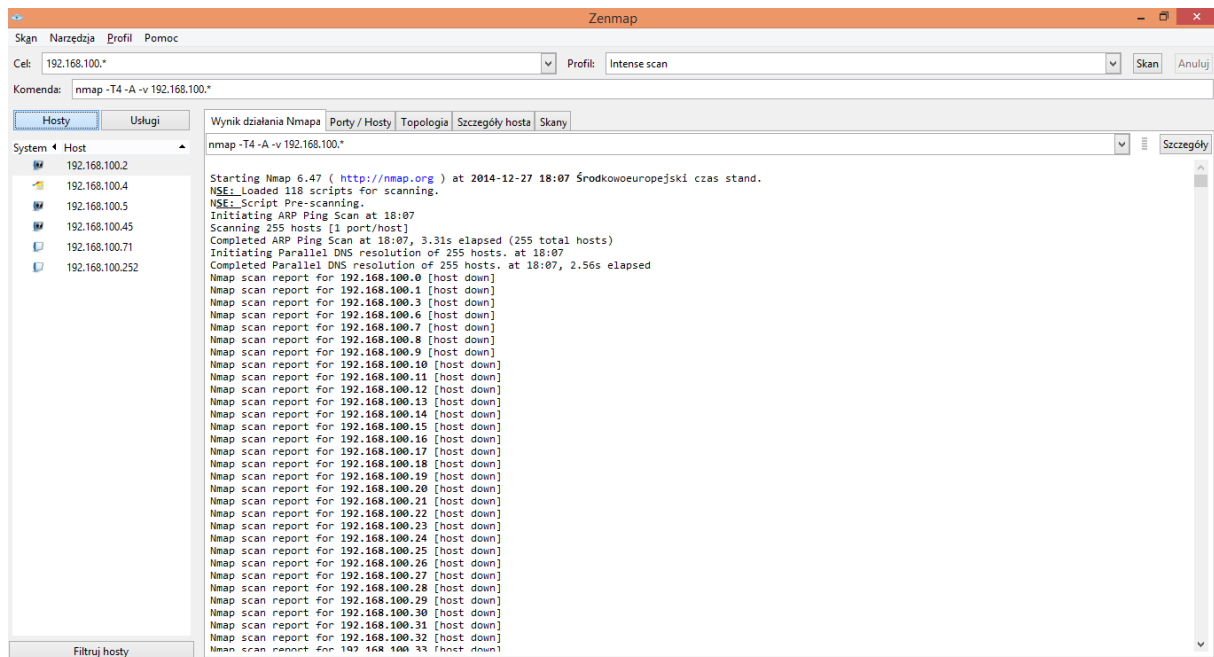
WYJŚCIE:

- oN/-oX/-oS/-oG <plik>: Zapisz wyniki w podanym pliku normalnie, w XML, s|<rlpt klddi3 i formacie grepwalnym
- oA <nazwabazowa>: Zapisz wyniki w trzech formatach jednocześnie
- v: Podwyższenie poziomu raportowania (podwójne użycie powiększa efekt)
- d[poziom]: Ustaw lub podwyższ poziom debugowania (do najwyższego 9)
- packet-trace: Pokazuj wszystkie wysyłane i odbierane pakiety
- iflist: Wyświetl listę interfejsów i routingu (do wykrywania błędów)
- append-output: Dołącz nowe wyniki do już istniejących w pliku
- resume <nazwapliku>: Wznów przerwane skanowanie
- stylesheet <ścieżka/URL>: plik styli XSL do konwersji wyników w XML do formatu HTML
- webxml: Domyślny styl z Insecure.Org
- no-stylesheet: Wyłączenie dodawania styli do plików z wynikami XML

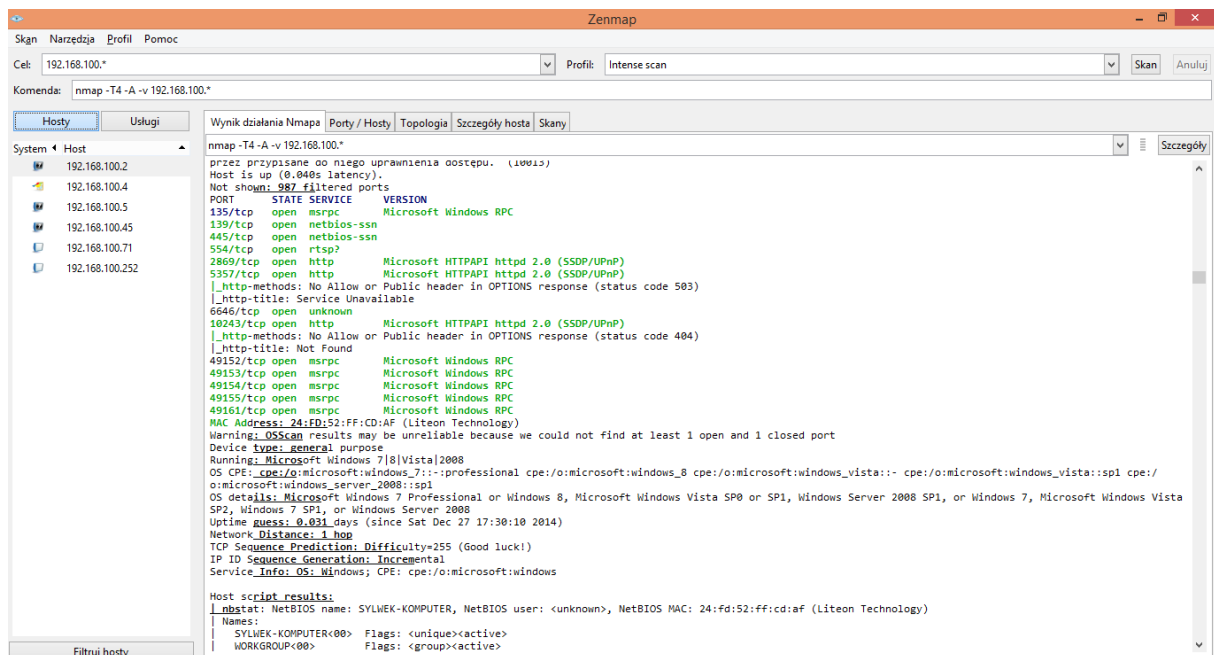
RÓŻNE:

- 6: Włączenie skanowania IPv6
- A: Włączenie detekcji OS i wersji usług
- datadir <katalog>: Podanie katalogu z plikami danych Nmapa
- send-eth/--send-ip: Wysyłaj za pomocą ramek ethernet lub pakietów IP
- privileged: Zakładaj że użytkownik ma odpowiednie uprawnienia
- V: Wyświetl numer wersji Nmapa
- h: Wyświetl stronę pomocy

Zenmap jest dobrym narzędziem do skanowania całej sieci (rys. 1).



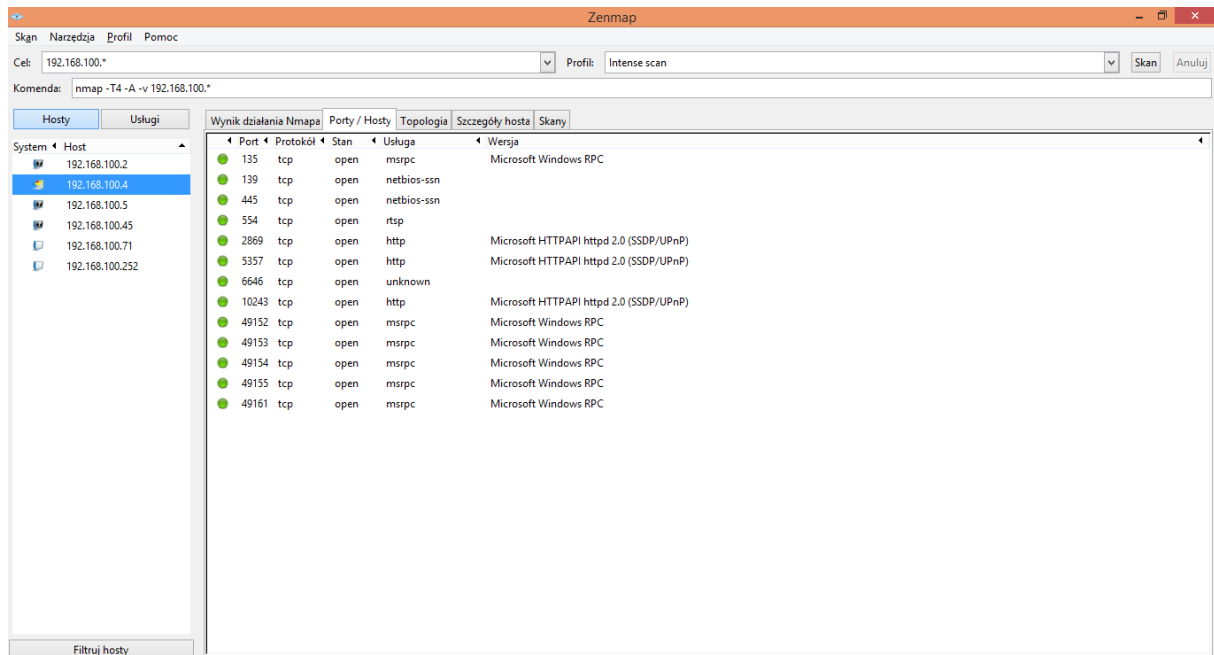
Dzięki takiemu zastosowaniu mamy podgląd całej naszej sieci wraz z portami na każdym adresie IP. Im większa sieć tym dłuższy czas skanowania, który możemy zmniejszyć poprzez wybranie interesującego nas profilu.



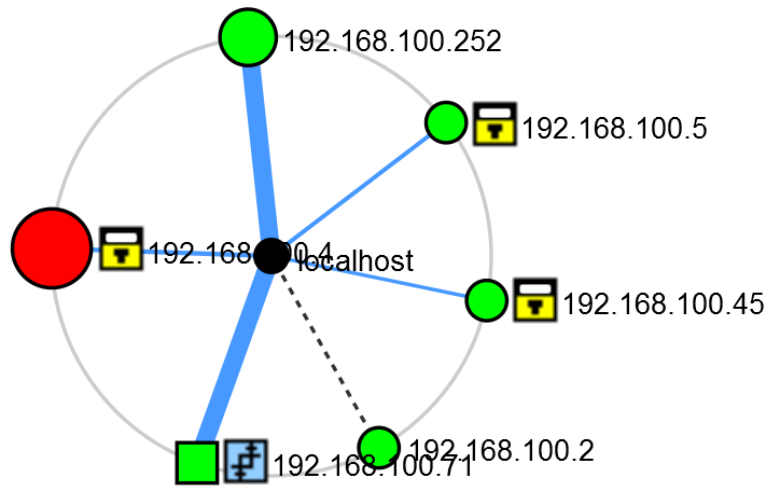
Wyniki skanowania można zapisać do katalogu, a następnie poddawać porównaniu albo przeszukiwaniu.

Zakładki:

- **porty/hosty** - wykaz otwartych portów, ich wersja oraz jaką usługę świadczą dla danego hosta



- **topologia** - graficzny podgląd sieci



- **szczegóły hosta** - informacje na temat hosta, ile ma portów otwartych, jaki posiada system, adres MAC oraz inne ciekawe informacje.

The screenshot shows the Zenmap application window. At the top, the title bar reads "Zenmap". Below it, the "Cel:" field contains "192.168.100.*" and the "Profil:" dropdown is set to "Intense scan". The "Komenda:" field shows "nmap -T4 -A -v 192.168.100.*".

The main interface has several tabs: "Hosty", "Usługi", "Wynik działania Nmapa", "Porty / Hosty", "Topologia", "Szczegóły hosta", and "Skany". The "Szczegóły hosta" tab is active, displaying details for host "192.168.100.4".

On the left, a "System" tree shows a list of hosts: 192.168.100.2, 192.168.100.4 (selected), 192.168.100.5, 192.168.100.45, 192.168.100.71, and 192.168.100.252.

The main content area for host 192.168.100.4 includes:

- Status hosta**: Stan: up, Otwarte porty: 13, Filtrowane porty: 987, Zamknięte porty: 0, Przeskanowane porty: 1000, Czas od włączenia: 2693, Ostatnie uruchomienie: Sat Dec 27 17:30:10 2014.
- Adresy**: IPv4: 192.168.100.4, IPv6: Niedostępne, MAC: 24:FD:52:FF:CD:AF.
- System operacyjny**: Nazwa: Microsoft Windows 7 Professional or Windows 8, Dokładność: 100% (indicated by a green progress bar).
- Użyte porty**: Port-Protokół-Stan: 135 - tcp - open.
- Klasy systemów operacyjnych**: Typ: general purpose, Producent: Microsoft, Rodzina systemów operacyjnych: Windows, Generacja systemu operacyjnego: 8, Dokładność: 100% (indicated by a green progress bar).
- Sekwencja TCP**, **Sekwencja IP ID**, and **Sekwencja TCP TS** are listed as empty.

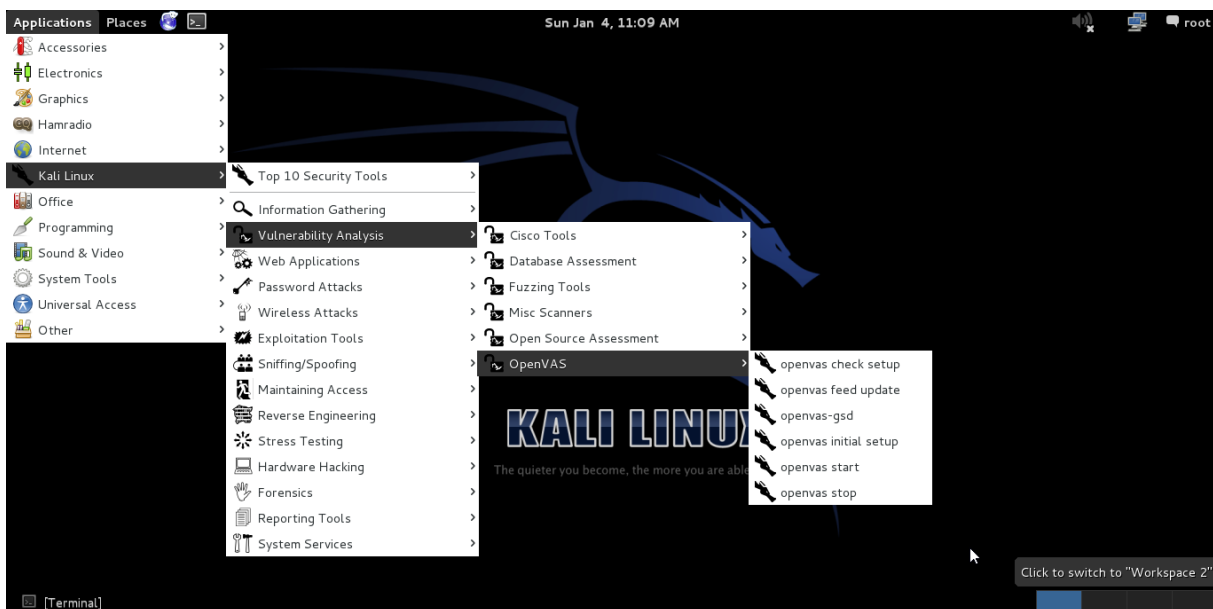
At the bottom left, there is a "Filtruj hosty" button.

3. **OpenVas** jest to darmowy skaner podatności, którego celem jest sprawdzanie poziomu zagrożenia i enumeracja podatności systemów komputerowych oraz sieci z wykorzystaniem bazy specjalnie przygotowanych testów. Jednym z etapów realizacji testów penetracyjnych jest wyszukiwanie oraz analizowanie podatności skanowanej maszyny.

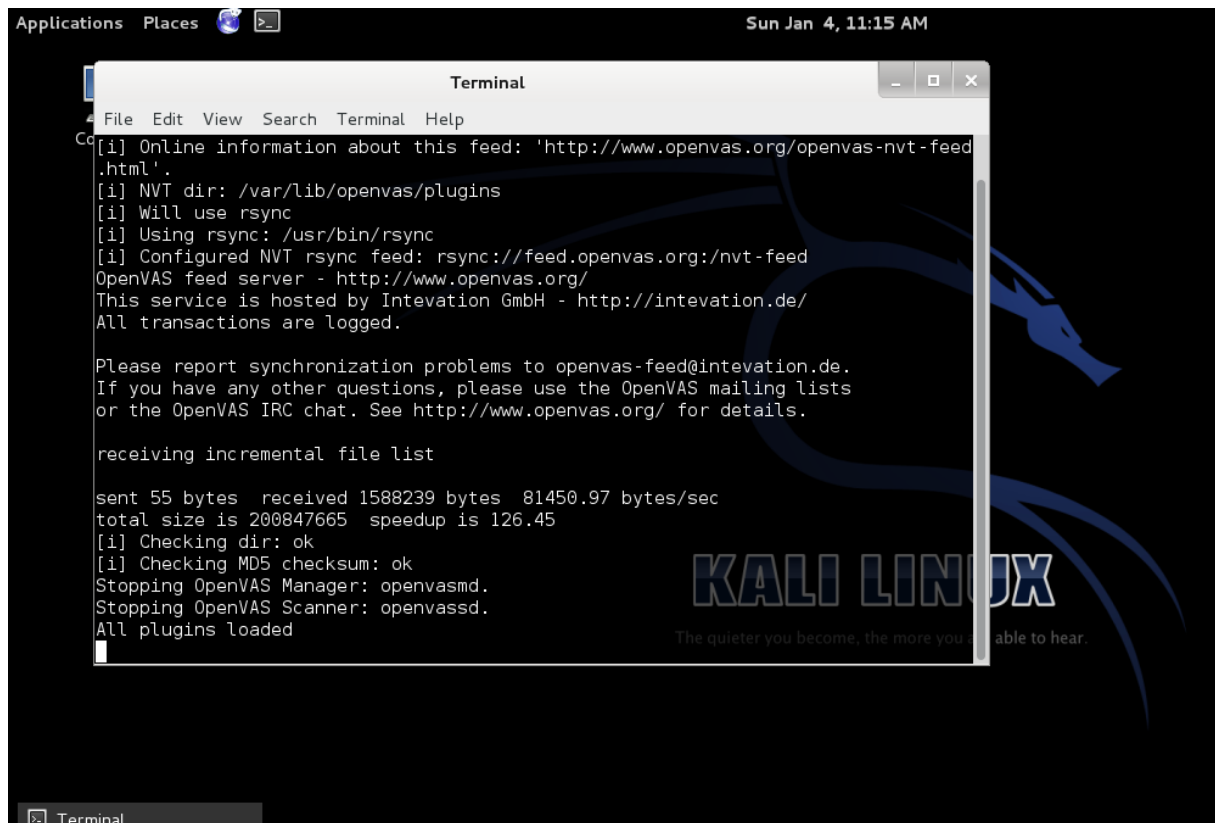
W prezentacji wykorzystano **Kali-Linux-1.0.9-vm-amd64..**

Pierwszym krokiem jest pobranie pluginów do OpenVas.

Applications > Kali Linux > Vulnerability Analysis > OpenVAS > OpenVas Initial Setup



Po uruchomieniu **OpenVas** pobierze wszystkie potrzebne dodatki. Domyślny użytkownik to: **admin**, natomiast hasło należy ustawić.

A screenshot of a Kali Linux desktop environment. The top bar shows 'Applications', 'Places', and the date 'Sun Jan 4, 11:15 AM'. A terminal window titled 'Terminal' is open, displaying the following text:

```
File Edit View Search Terminal Help
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /var/lib/openvas/plugins
[i] Will use rsync
[i] Using rsync: /usr/bin/rsync
[i] Configured NVT rsync feed: rsync://feed.openvas.org:/nvt-feed
OpenVAS feed server - http://www.openvas.org/
This service is hosted by Intevation GmbH - http://intevation.de/
All transactions are logged.

Please report synchronization problems to openvas-feed@intevation.de.
If you have any other questions, please use the OpenVAS mailing lists
or the OpenVAS IRC chat. See http://www.openvas.org/ for details.

receiving incremental file list

sent 55 bytes received 1588239 bytes 81450.97 bytes/sec
total size is 200847665 speedup is 126.45
[i] Checking dir: ok
[i] Checking MD5 checksum: ok
Stopping OpenVAS Manager: openvasmd.
Stopping OpenVAS Scanner: openvasd.
All plugins loaded
```

Po pobraniu wszystkich dodatków i ustawieniu hasła, uruchamiamy przeglądarkę i przechodzimy na adres **https://127.0.0.1:9392** albo **https://localhost:9392**. Pojawi się komunikat: **To połączenie jest niezaufane** wystarczy dodać wyjątek.

W oknie logowania wpisujemy:

Login: **admin**

Hasło: to które podaliśmy wcześniej

Applications Places Sun Jan 4, 11:24 AM root

Greenbone Security Assistant - Iceweasel


File Edit View History Bookmarks Tools Help

Greenbone Security Assistant

<https://127.0.0.1:9392/login/Login.html>

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

Greenbone Security Assistant



Username

Password

[root@kali: ~] Greenbone Security A...

Po zalogowaniu pokaże się Asystent skanowania. W tym widzimy stany naszych skanów oraz możemy zeskanować szybko cel.

The screenshot shows the Greenbone Security Assistant web interface in a browser window. The browser address bar shows the URL: `https://127.0.0.1:9392/omp?cmd=get_tasks&overrides=1&token=c5b29b0d-fada-4dca-97b0-56fdb64721b`. The interface displays a table of scan tasks and a 'Quick start' section.

Name	Status	Total	Reports		Threat	Trend	Actions
			First	Last			
localhost	Done	1		Dec 27 2014	Medium		
N.A.S.A. (wan scan)	Done	1		Dec 27 2014	High		
router	Done	1		Dec 28 2014	Low		

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

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.
For more detailed information on

Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

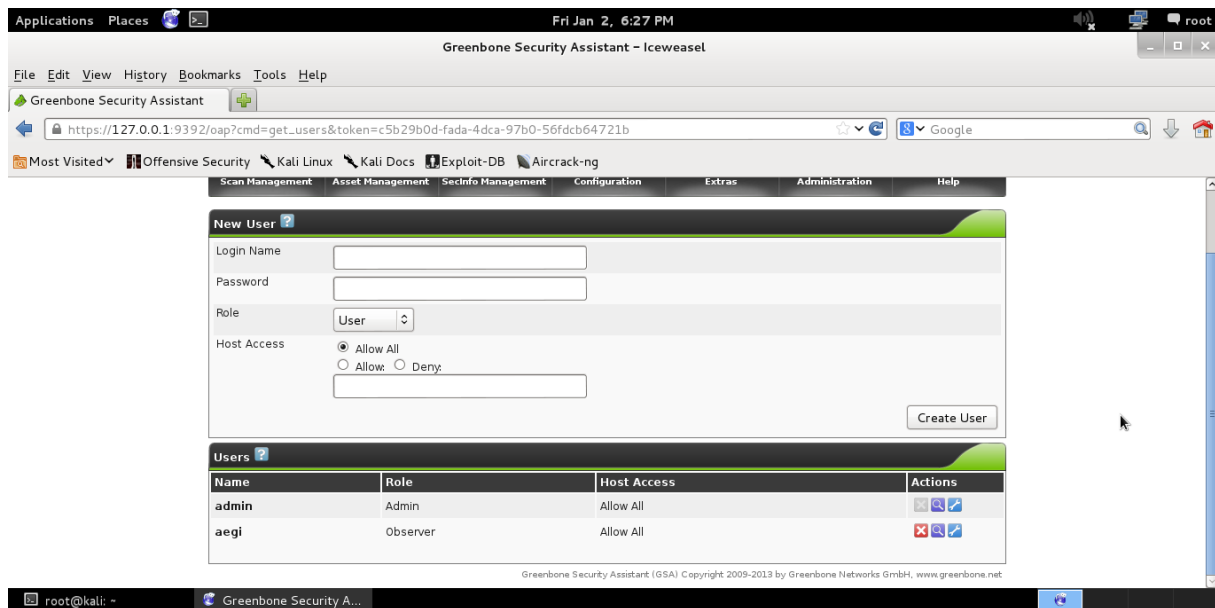
Najważniejszą rzeczą przed rozpoczęciem skanowania jest uaktualnienie NVT Feed.
Administration > NVT Feed

The screenshot shows a web browser window titled "Greenbone Security Assistant - Iceweasel" with the URL `https://127.0.0.1:9392/oap?cmd=get_feed&token=c5b29b0d-fada-4dca-97b0-56fdcb64721b`. The page is logged in as Admin admin and shows the "Administration" menu. The "NVT Feed Management" section displays the "OpenVAS NVT Feed" with version 201412300733. A "Synchronize with Feed now" button is visible, along with a link to learn about side effects of feed synchronization.

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net

Wybrane opcje:

- Dodawanie użytkownika - **Administration > Users**







The screenshot displays the Greenbone Security Assistant web interface. The browser address bar shows the URL: `https://127.0.0.1:9392/oap?cmd=get_users&token=c5b29b0d-fada-4dca-97b0-56fdb64721b`. The interface includes a navigation menu with options like Scan Management, Asset Management, and Administration. The 'Administration' section is active, showing a 'New User' form and a 'Users' table.

New User Form:

- Login Name:
- Password:
- Role:
- Host Access: Allow All, Allow, Deny
-

Users Table:

Name	Role	Host Access	Actions
admin	Admin	Allow All	 
aegi	Observer	Allow All	 

Poza podstawowymi polami takimi jak Login name i Passowrd jest także rola jaką może dostać nowy użytkownik a są nimi: Admin, User i Observer, możemy także ustawić dostęp dla danego użytkownika: Allow All, Allow oraz Deny.

- Dodawanie celu - **Configuration > Targets**

Greenbone Security Assistant - Iceweasel

Logged in as Admin admin | Logout
Fri Jan 2 23:28:02 2015 UTC

Scan Management | Asset Management | **SecInfo Management** | Configuration | Extras | Administration | Help

Targets 1 - 4 of 4 (total: 4) Nowy cel

Filter: rows=10 first=1 sort=name

Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions
192.168.100.5 (pierwszy skan)	192.168.100.5	1	All IANA assigned TCP 2012-02-10			[Icons]
localhost	localhost	1	OpenVAS Default			[Icons]
N.A.S.A. (wan scan)	192.168.100.2	1	All IANA assigned TCP 2012-02-10			[Icons]
router	192.168.100.252	1	All IANA assigned TCP 2012-02-10			[Icons]

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

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net

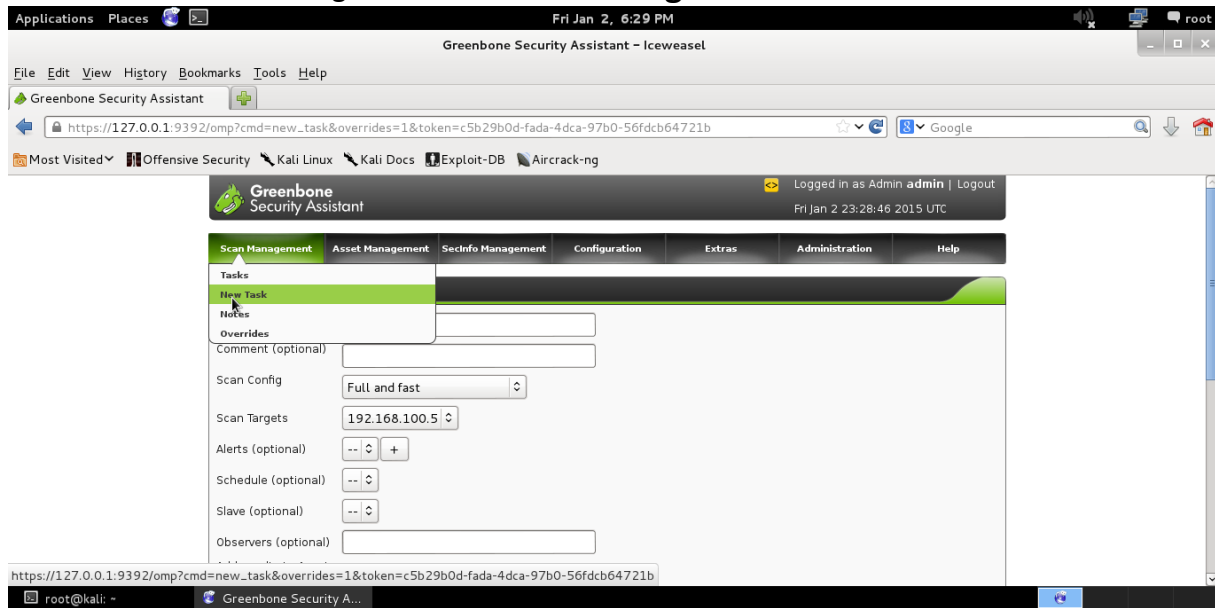
Aby dodać nowy cel należy przycisnąć przyciski z białą gwiazdką. W kolejnym oknie uzupełniamy:

Name: nazwa skanu

Hosts: możemy wpisać albo wybrać z pliku (liczba hostów nie jest ograniczona do 1)

Port List: porty do skanowania. Ustawienia można zmieniać w - **Configuration > Port Lists**

- Dodawanie nowego zadania - **Scan Management > New Task**



W tym oknie tworzymy nowe zadanie.

Name: nazwa zadania

Scan Config: w tym polu możemy wybrać konfiguracje skanowania

Scan Targets: nazwa naszego celu

Alerts: tu możemy wybrać rodzaj alarmu - **Configuration > Alerts**

Schedule: wybór zaplanowanego czasu skanowania- **Configuration > Schedules**

Po uzupełnieniu wystarczy wcisnąć **Create Task**

Aktywne oraz zakończone skany można podglądać w oknie Scan Management > Tasks

The screenshot shows the Greenbone Security Assistant web interface. The main content area displays a table of scan tasks. The table has columns for Name, Status, Total, Reports (First, Last, Threat), Trend, and Actions. Three tasks are listed: localhost, N.A.S.A. (wan scan), and router. All tasks have a status of 'Done'. The 'Threat' column shows 'Medium' for localhost, 'High' for N.A.S.A., and 'Low' for router. Below the table, there is a 'Welcome dear new user!' section with a 'Quick start: Immediately scan an IP address' button and a 'Start Scan' button.

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
localhost	Done	1	Dec 27 2014		Medium		
N.A.S.A. (wan scan)	Done	1	Dec 27 2014		High		
router	Done	1	Dec 28 2014		Low		

Pasek statusu będzie się uaktualniał co 10, 30, 60 sek. aż dojdzie do 100%, jeśli odpowiednio zmienimy opcje z **No auto-refresh** oraz wciśnięciu zielonego przycisku odśwież aby zapisać zmiany.

Po zakończeniu skanowania pojawią się w:

Status: napis **Done** zamiast procentów

Total: liczba przeprowadzonych skanów

Last: data ostatniego skanowana

Threat: poziom zagrożenia

Aby obejrzeć raport ze skanowania danego celu klikamy na datę ostatniego skanowania.

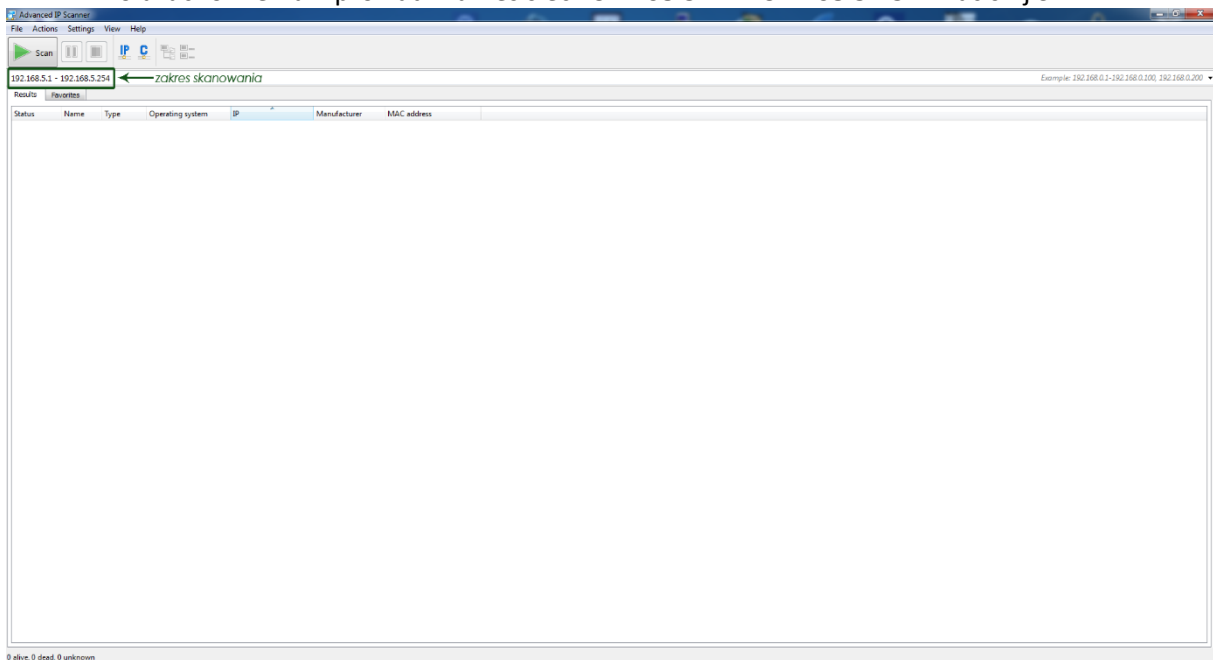
The top screenshot shows the Greenbone Security Assistant interface. The browser address bar displays the URL: `https://127.0.0.1:9392/omp?cmd=get_report&report_id=3b694917-fc9b-4761-a979-b6a33838d1f0¬es=1&overrides=1&re`. The main content area shows a 'Report Summary' for a scan of 'localhost' that started on 'Sat Dec 27 19:11:55 2014' and ended on 'Sat Dec 27 19:14:29 2014'. Below the summary is a table with columns for severity levels (Critical, Medium, Low, Info, Error, Total), 'Run Alert', and 'Download'. The 'Full report' row shows 14 total results, with 2 Medium severity results. The 'Download' column contains a 'PDF' icon and a download arrow.

The bottom screenshot shows the 'Filtered Results 1 - 2 of 2' section. It contains a table with columns: Host, OS, Start, End, Critical, Medium, Low, Info, Error, Total. The first row shows results for '127.0.0.1 (localhost)' with 2 Medium severity results. Below the table is a 'Port summary for 127.0.0.1' section, which lists a service 'otp (9390/tcp)' with a 'Medium' threat level. Underneath, 'Security Issues reported for 127.0.0.1' are listed, including a 'Medium (CVSS: 4.3)' issue: 'NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)'. The issue details show 'Weak ciphers offered by this service: SSL3_RSA_RC4_128_SHA, TLS1_RSA_RC4_128_SHA'. A 'Click to switch to "Workspace 2"' button is visible in the bottom right corner.

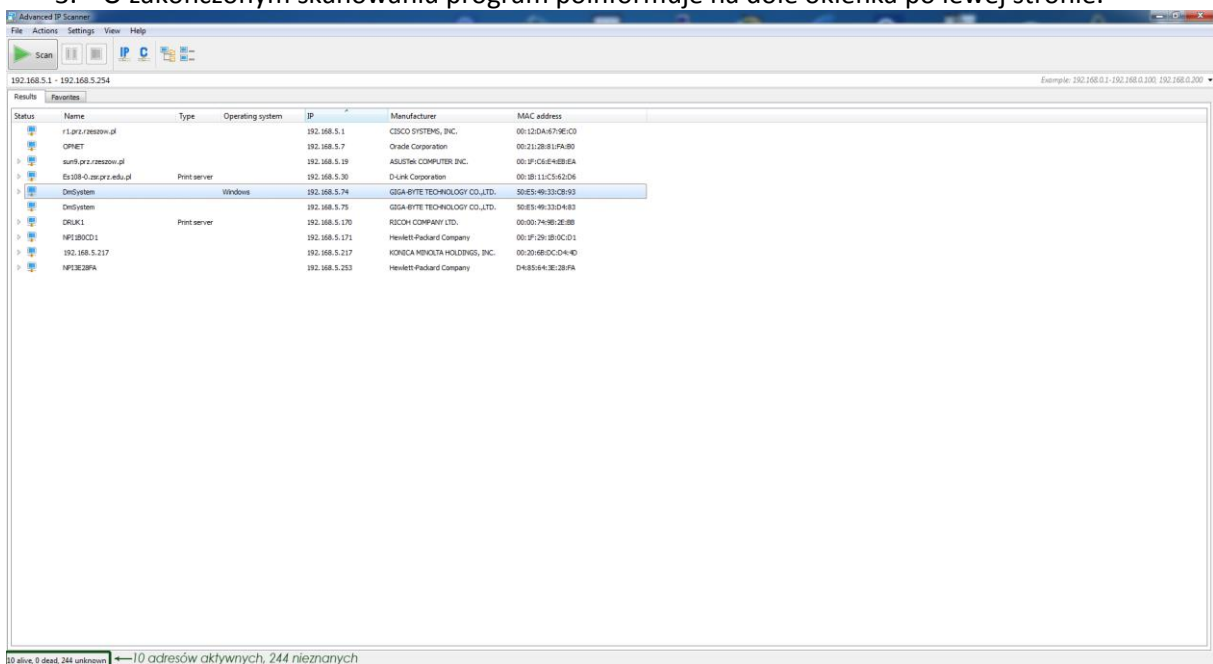
Każdy raport można pobrać i zapisać w wielu formatach.

Skanowanie sieci za pomocą Advanced IP Scanner

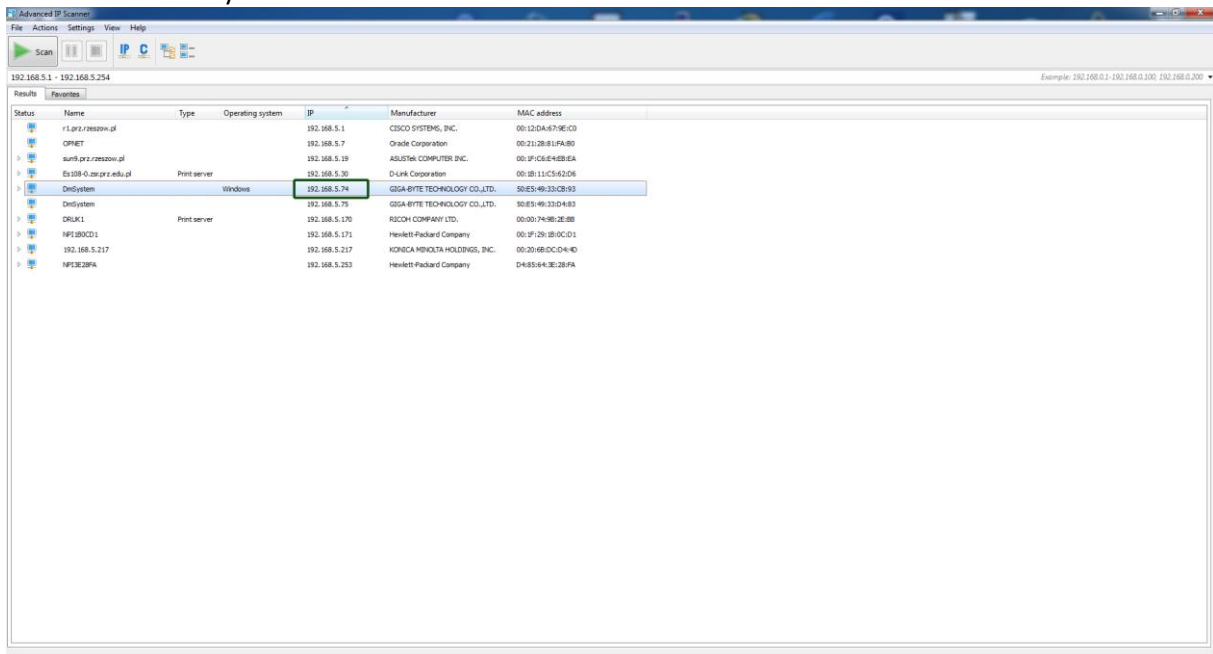
1. Uruchom Advanced IP Scanner.
2. Po uruchomieniu wprowadź zakres sieć **192.168.5.1 – 192.168.5.254** i naciśnij **SKAN**



3. O zakończonym skanowaniu program poinformuje na dole okienka po lewej stronie.

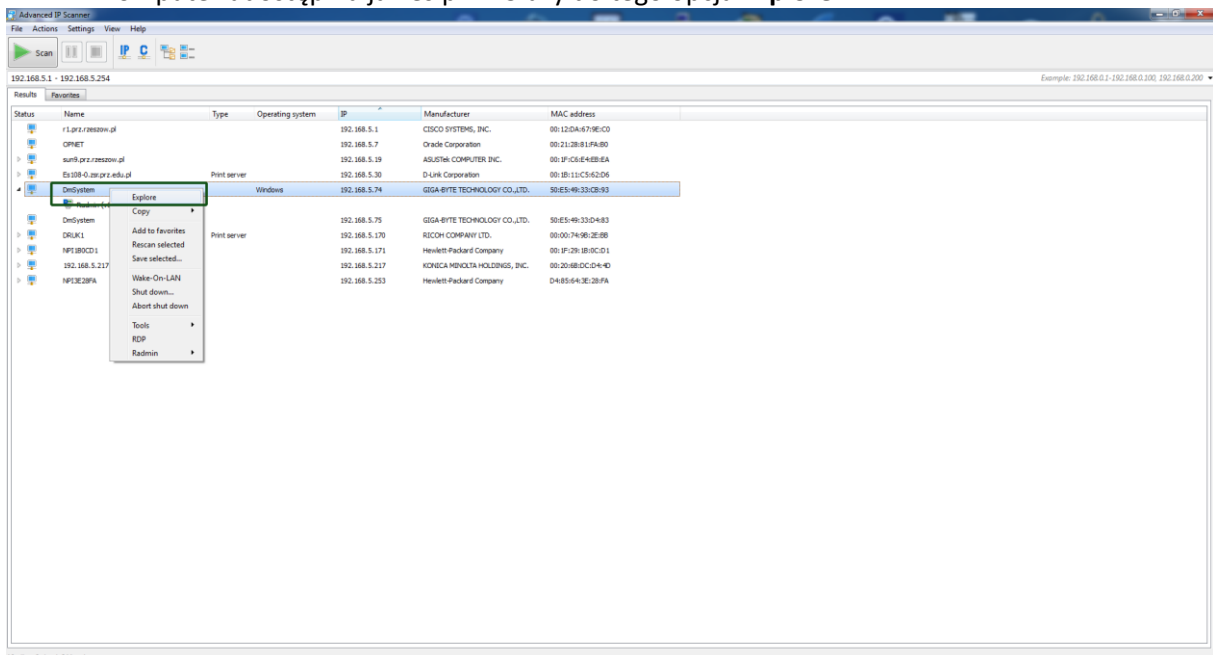


- Na liście znajdź adres **192.168.5.74**, odczytaj informacje na temat systemu operacyjnego oraz adres karty MAC.



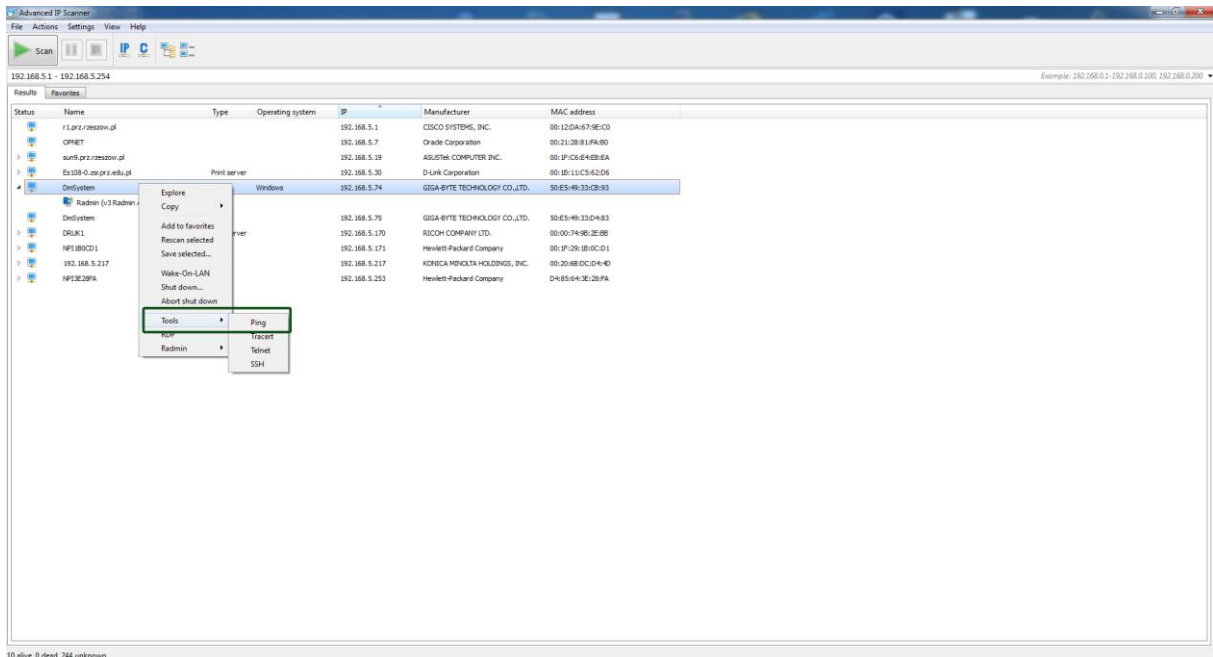
10 alive, 0 dead, 244 unknown

- Kliknij prawym przyciskiem myszy na nazwę znalezionej adresu i sprawdź czy dany komputer udostępnia jakieś pliki. Służy do tego opcja **Explore**.

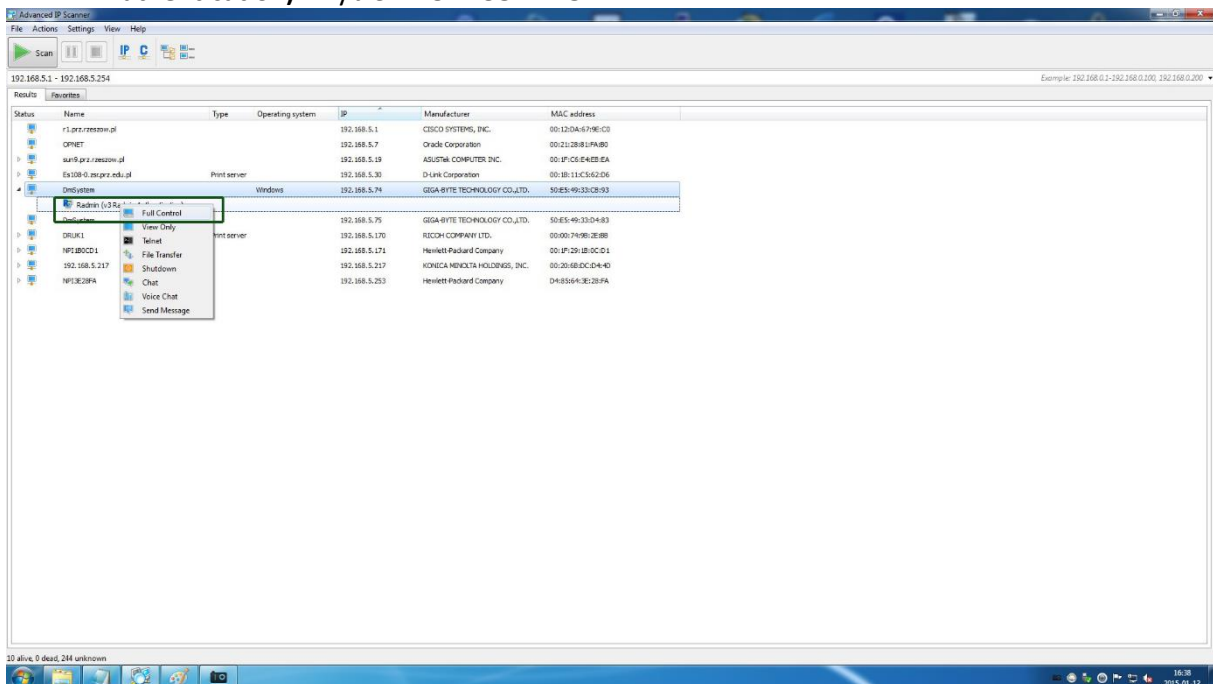


10 alive, 0 dead, 244 unknown

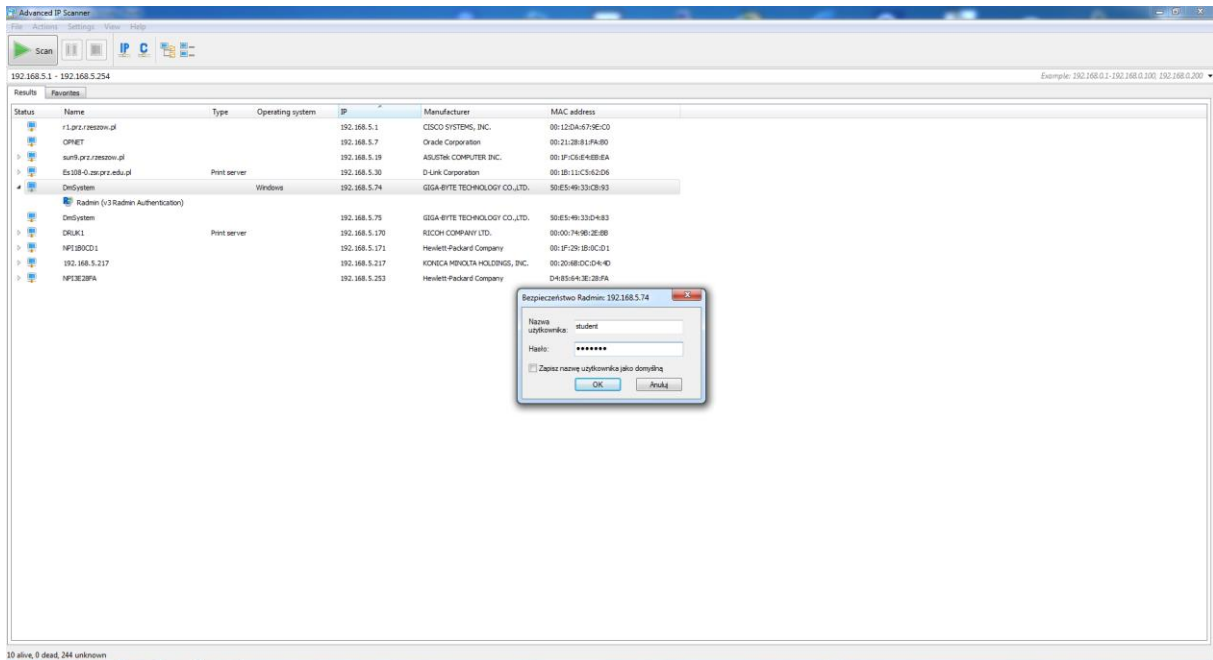
- Kliknij ponownie PPM i z **TOOLS** wybierz opcje **PING**.



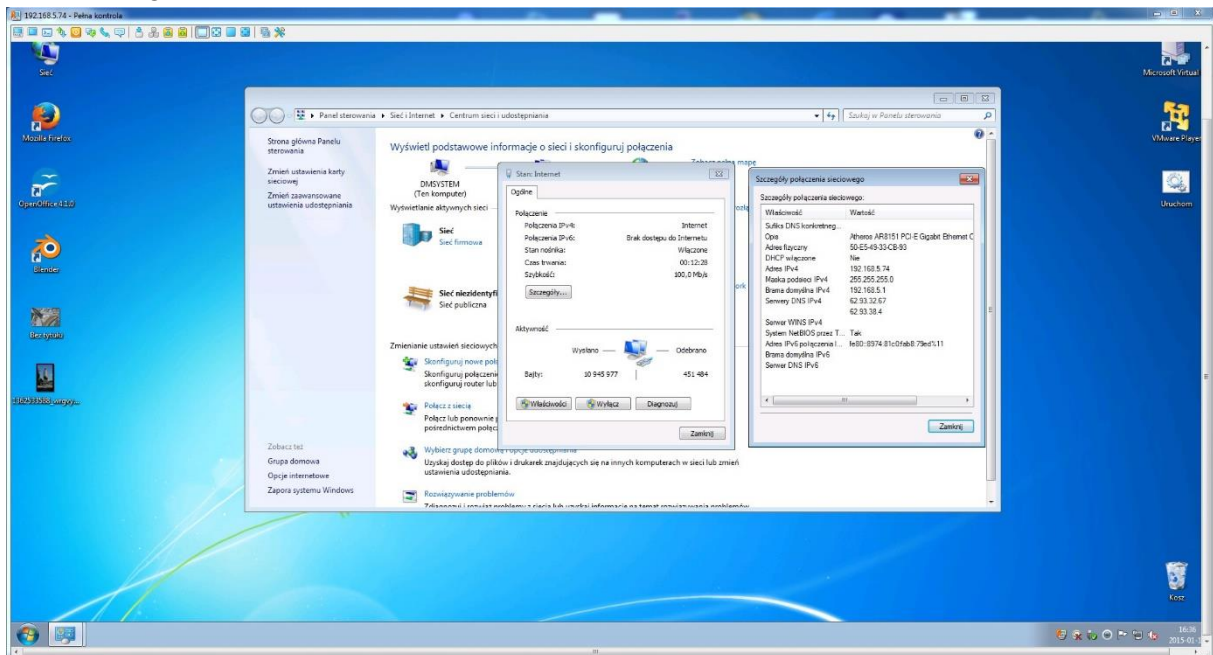
7. Przejmij pełną kontrolę nad komputerem z adresem ip: **192.168.5.74**, aby tego dokonać kliknij na trójkąt obok ikony komputera naszego celu i rozwiń menu, w którym znajduje się dodatkowe oprogramowanie pod nazwą **RADMIN**. Kliknij PPM na **Radmin (v3 Radmin Authentication)** i wybierz **FULL CONTROL**.



8. Wpisz login: student i hasło: student.

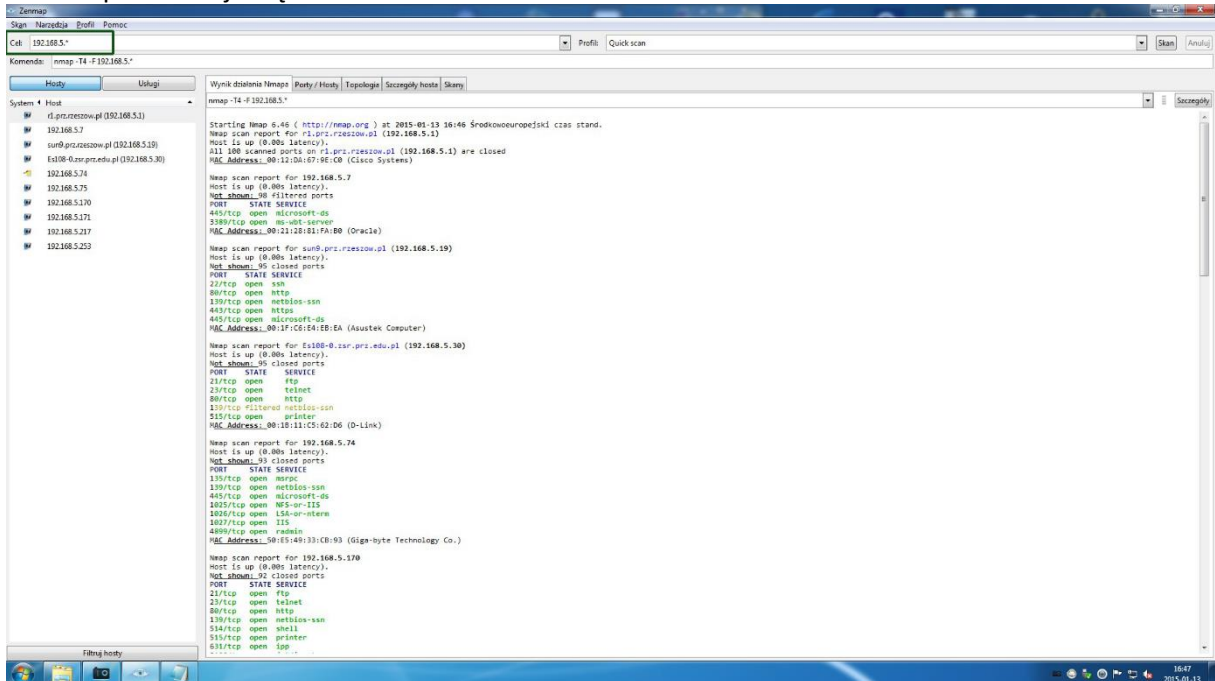


9. Po podłączeniu uruchom **Szczegóły połączenia sieciowego** i sprawdź czy zgadza się adres MAC



Skanowanie sieci za pomocą Nmap - Zenmap GUI

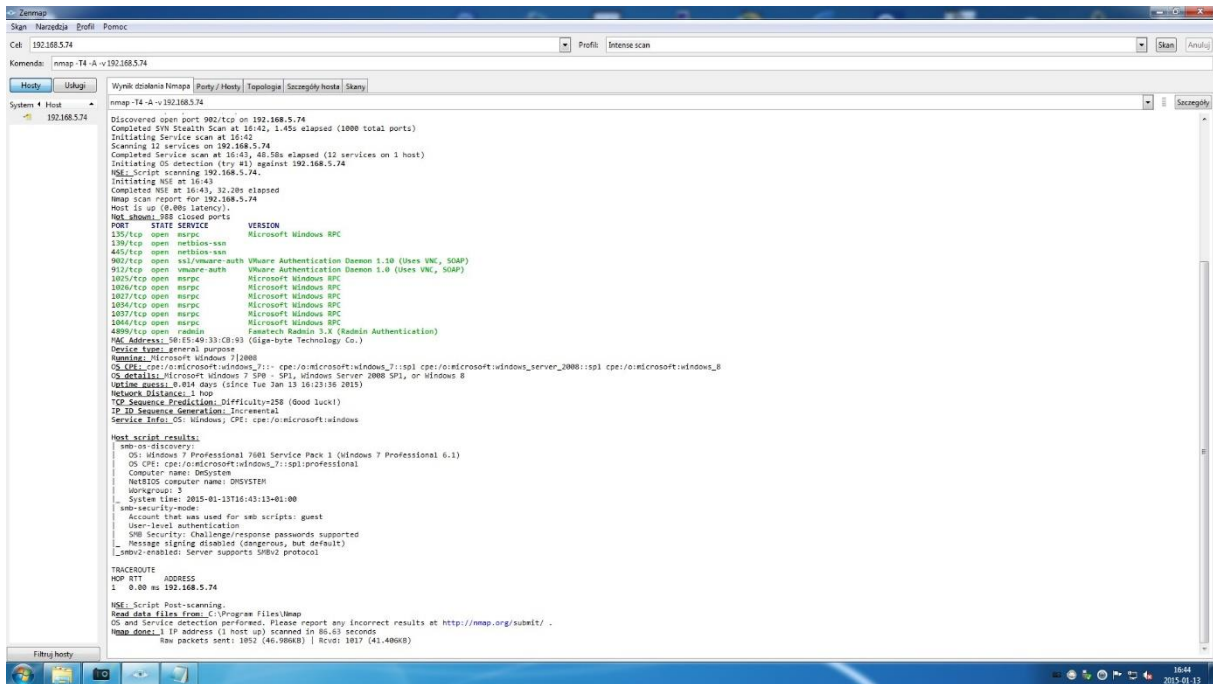
1. Uruchom Nmap - Zenmap GUI w pole Cel: wpisz **192.168.5.*** i wybierz w Profile: **Quick Skan**, przeskanuj całą sieć.



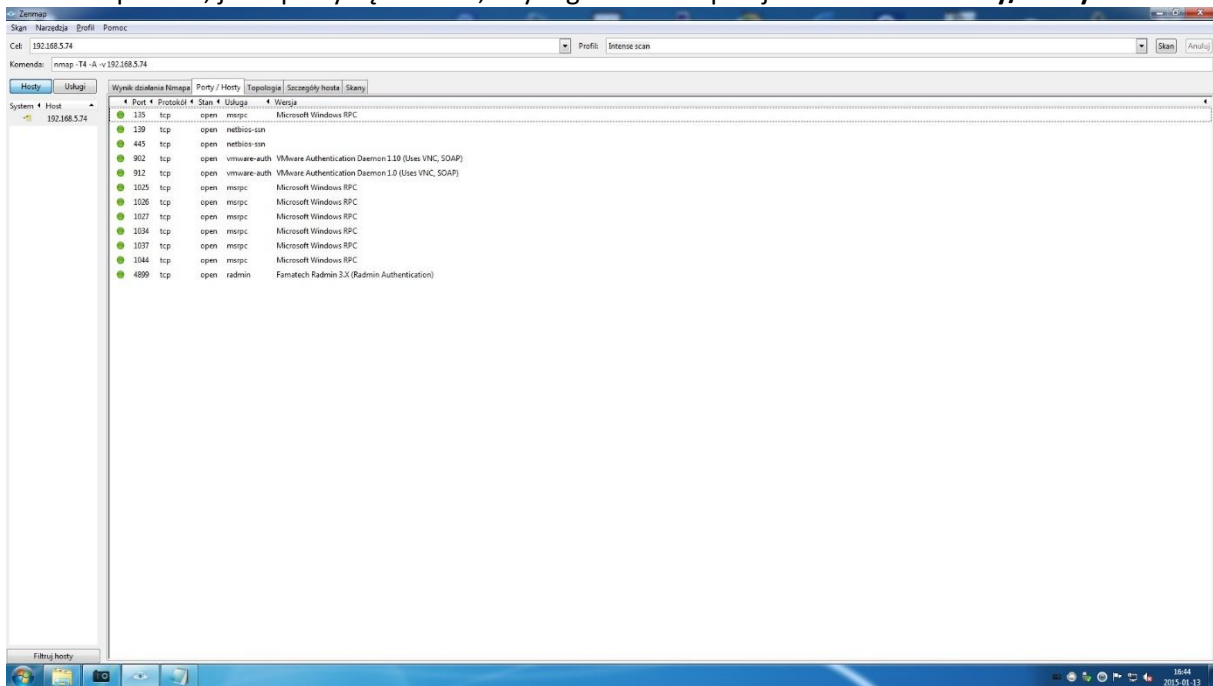
2. Sprawdź czy na liście po lewej znajdują się adres: **192.168.5.74** i czy ma otwarte porty.



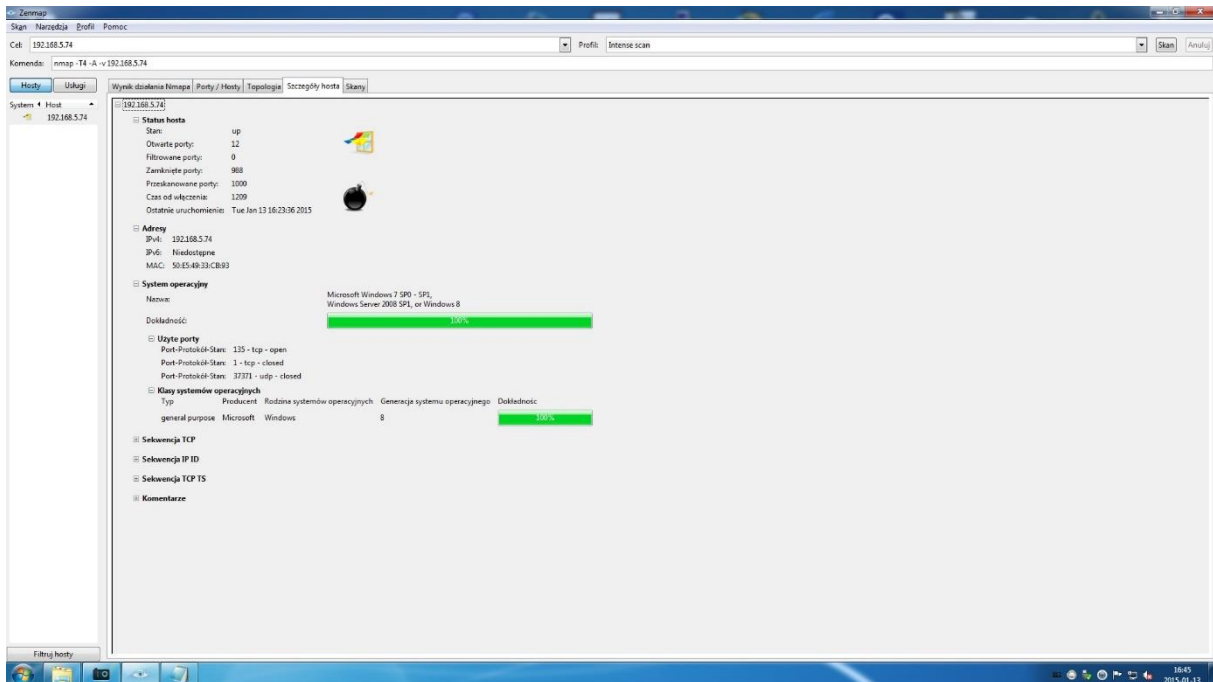
3. Przeskanuj adres: **192.168.5.74** w Profile: wybierz **Intense scan**.



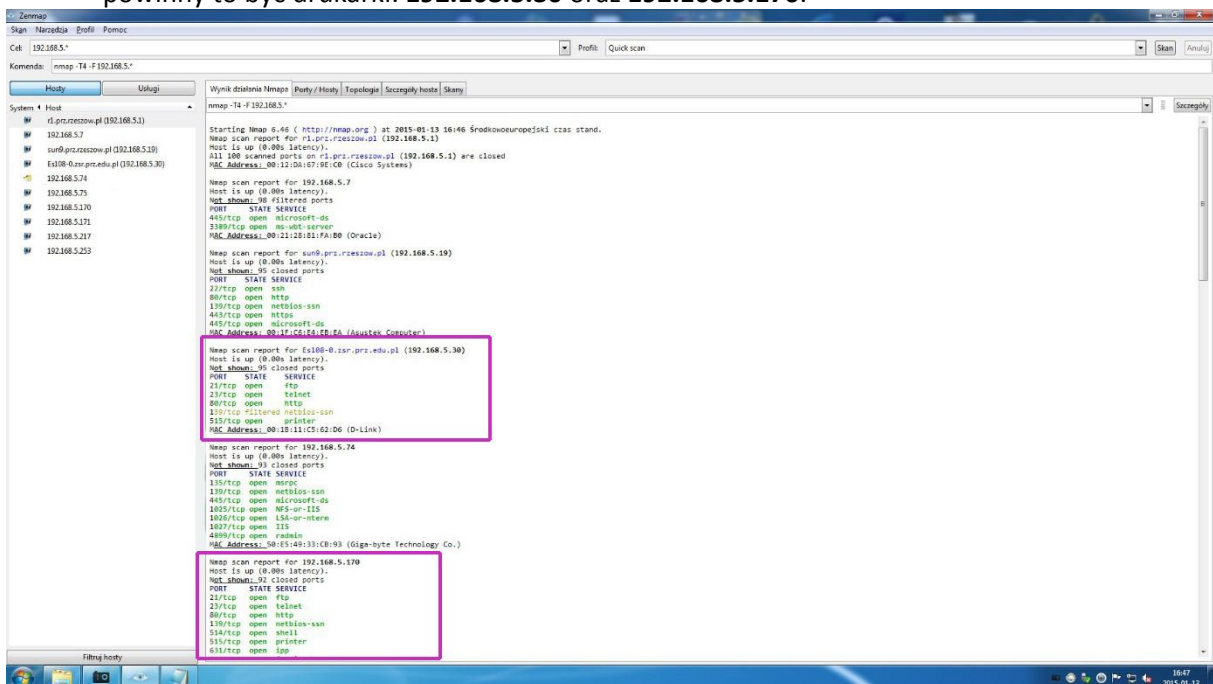
4. Sprawdź, jakie porty są otwarte, aby tego dokonać przejdź do zakładki **Porty/Hosty**.



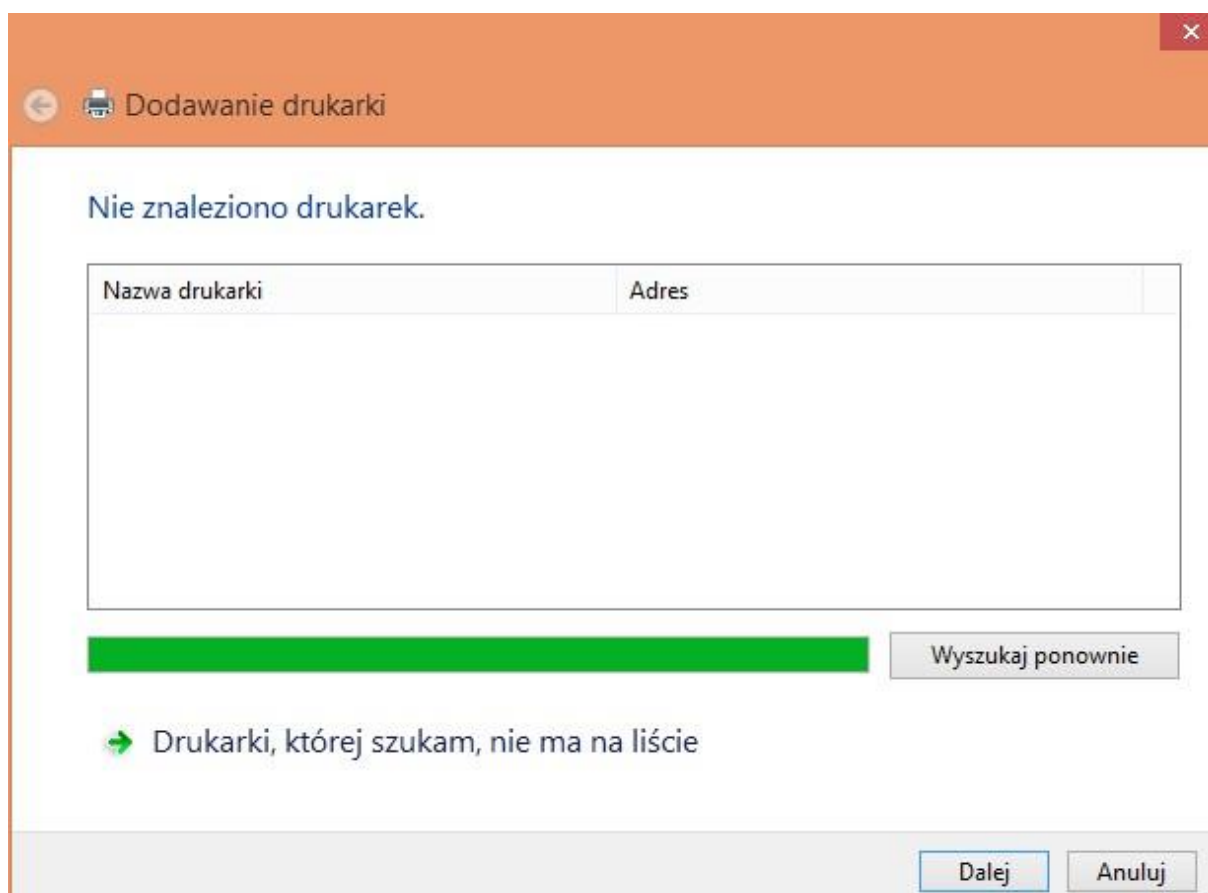
5. W zakładce **Szczegóły hosta** sprawdź ile portów przeskanował program, jaki adres karty MAC komputera.



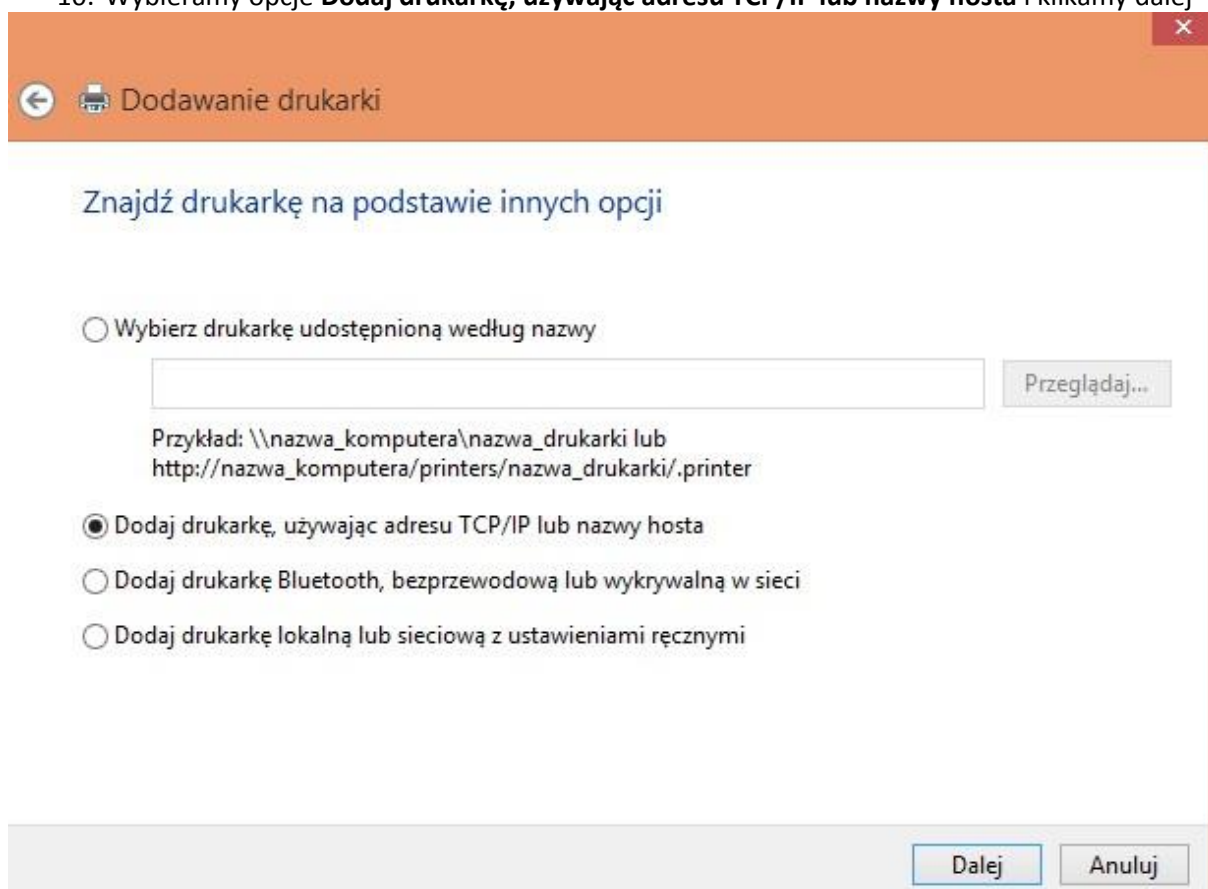
6. Dla tego samego adresu wykonaj skanowanie jeszcze raz, ale w Profile: wybierz **Intense scan plus UDP**. Porównaj wyniki.
7. Ze skanowania dostaliśmy informacje o tym, że 2 adresy posiadają otwarte porty **515** czyli powinny to być drukarki: **192.168.5.30** oraz **192.168.5.170**.



8. Dodamy te adresy do naszego komputera, aby można było z nich korzystać, aby tego dokonać należy przejść do Panel sterowania > Sprzęt i dźwięk > Urządzenia i drukarki.
9. Używamy opcji Dodaj drukarkę, następnie **Drukarki, której szukam, nie ma na liście**



10. Wybieramy opcje **Dodaj drukarkę, używając adresu TCP/IP lub nazwy hosta** i klikamy dalej



11. W kolejnym oknie ustawiamy:
 - a) Typ urządzenia zmieniamy na Urządzenie TCP/IP
 - b) Nazwa hosta drukarki lub adres: 192.168.5.30
 - c) Nazwa Portu: 515 i klikamy dalej

← Dodawanie drukarki

Wpisz nazwę hosta drukarki lub adres IP

Typ urządzenia:

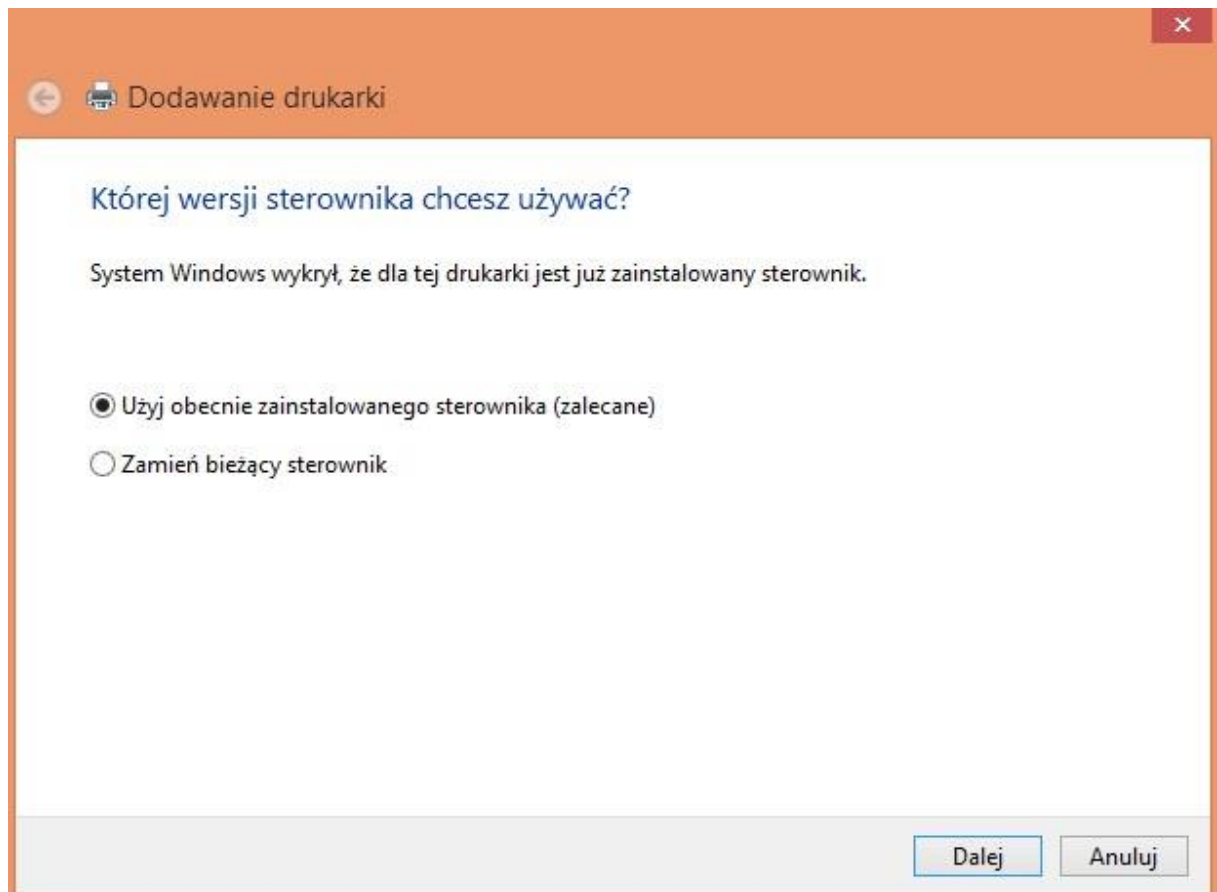
Nazwa hosta drukarki lub adres IP:

Nazwa portu:

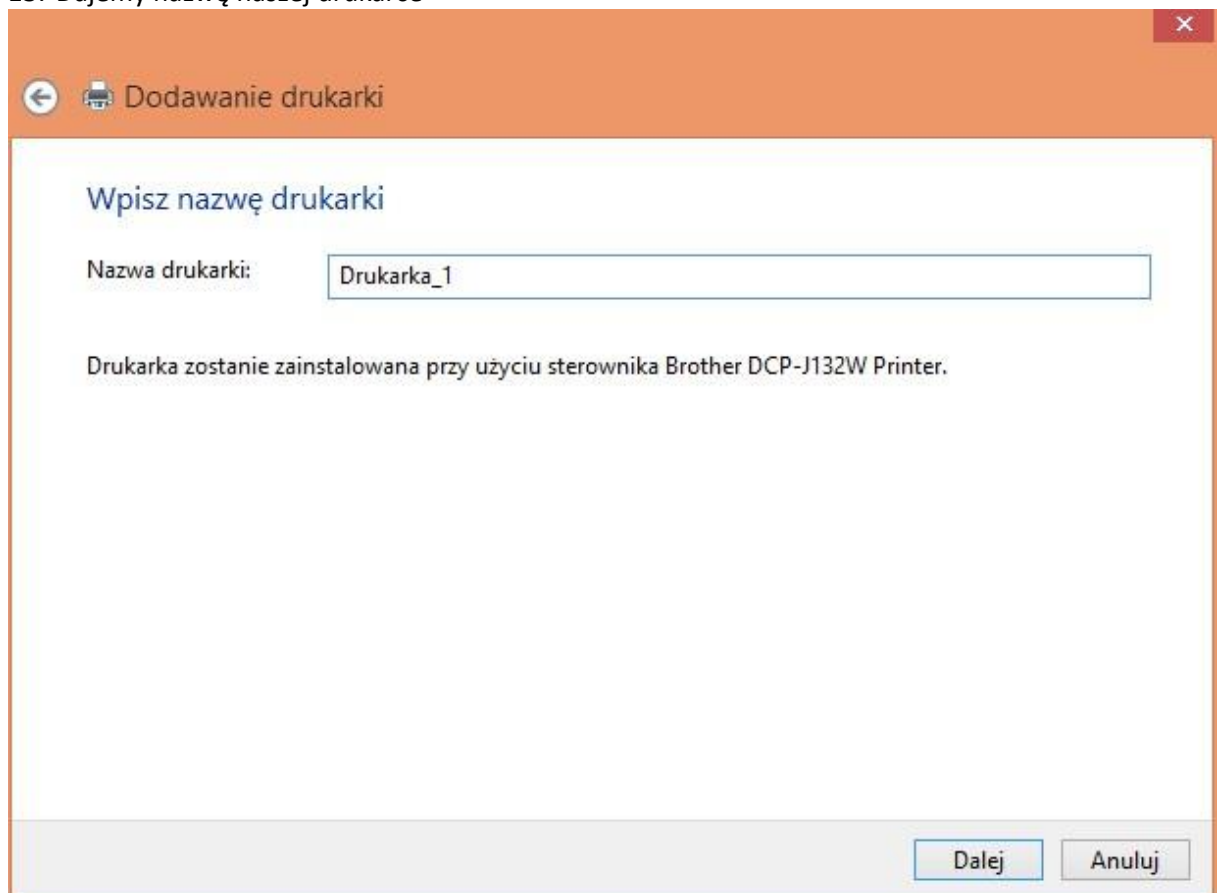
Sprawdź drukarkę i automatycznie wybierz sterownik do użycia

Dalej Anuluj

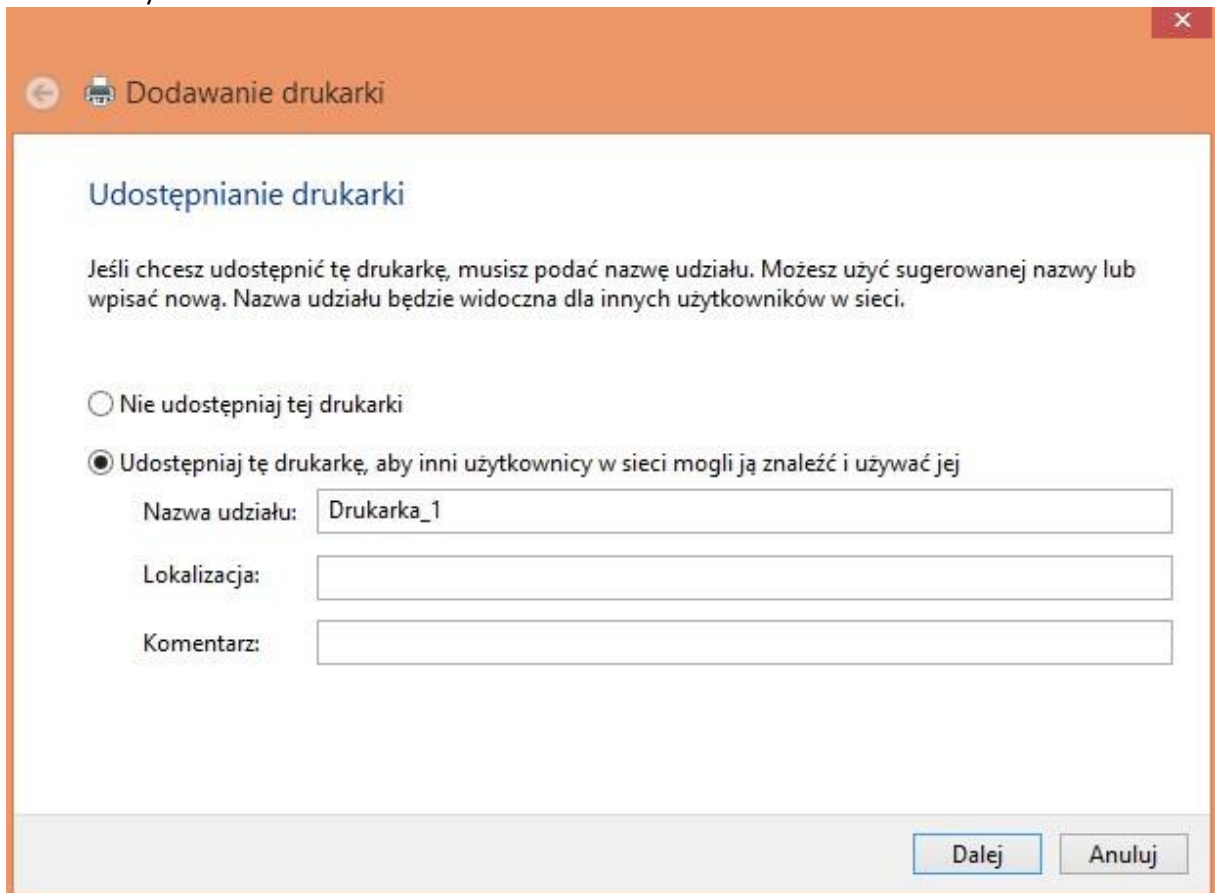
12. Jeśli jest możliwość to wybieramy **Użyj obecnie zainstalowanego sterownika**, a jeśli nie ma trzeba pobrać sterowniki do drukarki



13. Dajemy nazwę naszej drukarce



14. Udostępniamy drukarkę i drukarka została dodana teraz możemy za jej pomocą wydrukować dowolny tekst.



The image shows a Windows dialog box titled "Dodawanie drukarki" (Adding a printer). The main heading is "Udostępnianie drukarki" (Sharing a printer). Below the heading, there is a paragraph of text: "Jeśli chcesz udostępnić tę drukarkę, musisz podać nazwę udziału. Możesz użyć sugerowanej nazwy lub wpisać nową. Nazwa udziału będzie widoczna dla innych użytkowników w sieci." (If you want to share this printer, you must provide a share name. You can use the suggested name or enter a new one. The share name will be visible to other users on the network.)

There are two radio button options:

- Nie udostępniaj tej drukarki (Do not share this printer)
- Udostępniaj tę drukarkę, aby inni użytkownicy w sieci mogli ją znaleźć i używać jej (Share this printer so that other users on the network can find and use it)

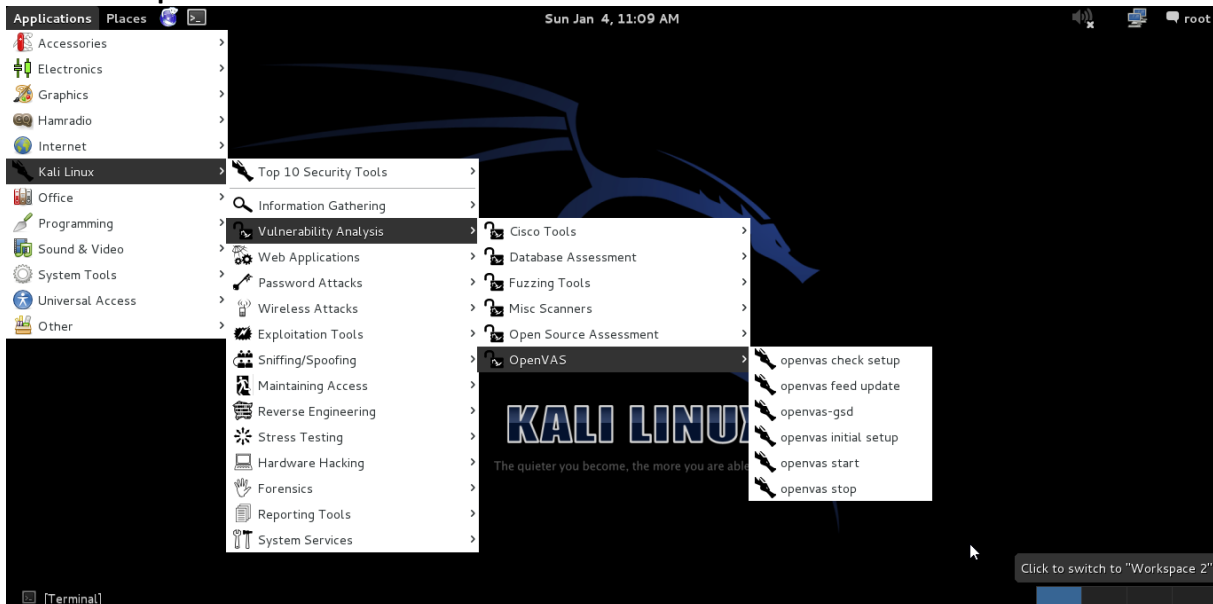
Below the options are three text input fields:

- Nazwa udziału: Drukarka_1
- Lokalizacja: (empty)
- Komentarz: (empty)

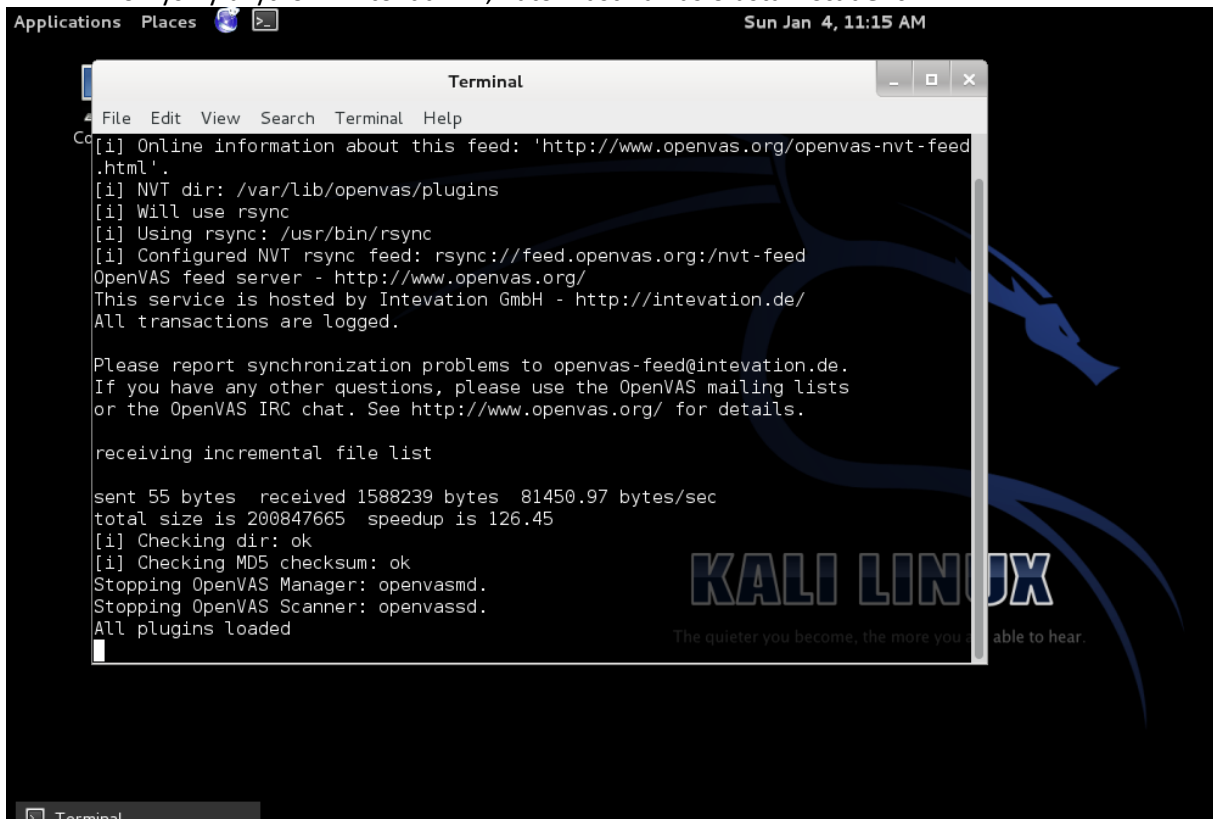
At the bottom right, there are two buttons: "Dalej" (Next) and "Anuluj" (Cancel).

Skanowanie podatności OpenVas

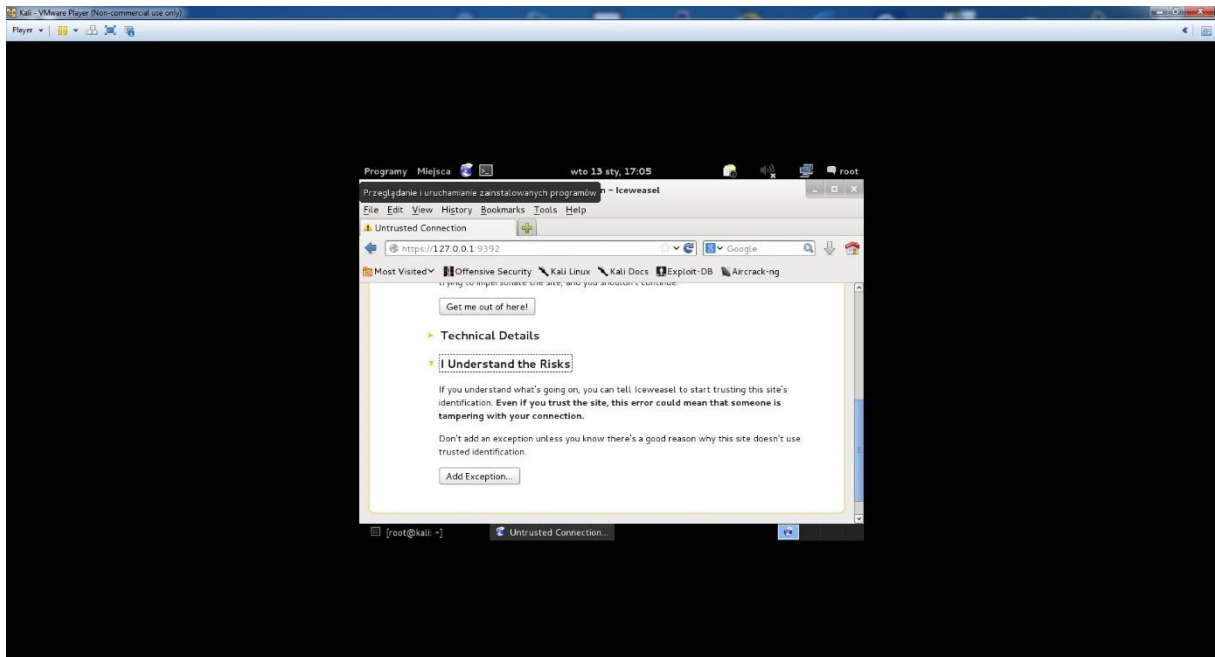
1. Uruchom **VMware Player** i wybierz **Kali**.
login: root
hasło: student
2. Z menu **Programy** wybierz **Kali Linux > Vulnerability Analysis > OpenVAS > OpenVas Initial Setup**



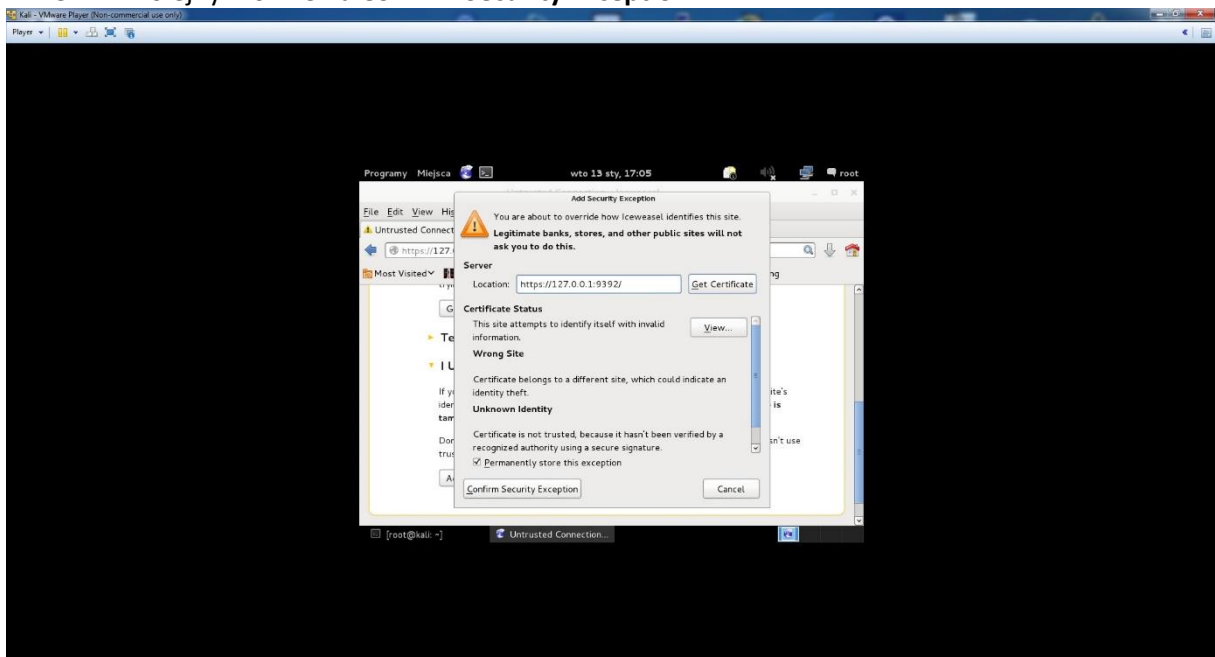
3. Po uruchomieniu OpenVas pobierze wszystkie potrzebne dodatki może to potrwać chwilę.
Domyślny użytkownik to: **admin**, natomiast na hasło ustaw **student**.



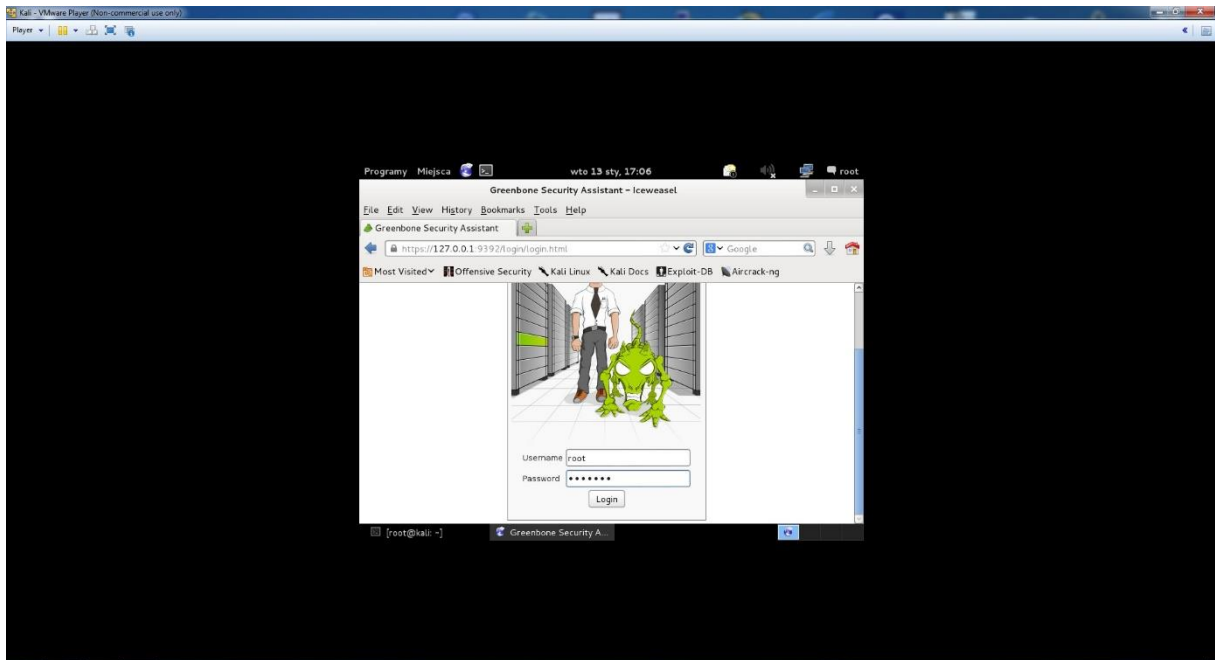
4. Uruchom przeglądarkę **Iceweasel** i wpisz **https://127.0.0.1:9392**. Kliknij na **I Understand the Risk** a następnie **Add Exception**



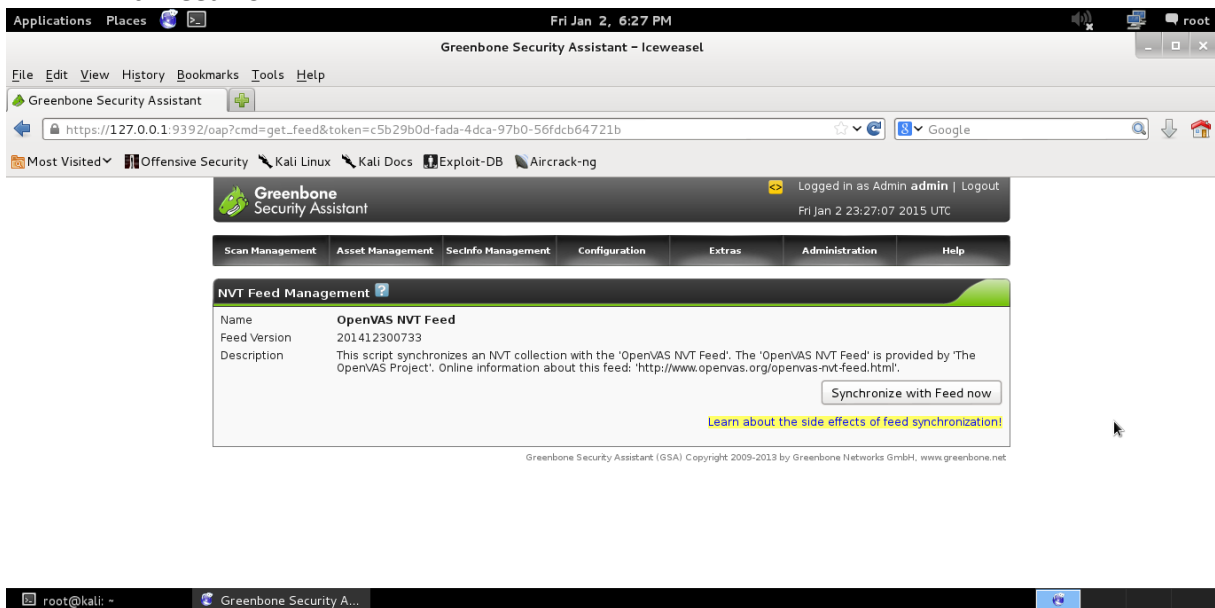
5. W kolejnym oknie na **Confirm Security Exception**



6. Zaloguj się za pomocą login: **admin**, hasło: **student**



7. Przejdź do zakładki **Administration**, wybierz **NVT Feed** a następnie kliknij na **Synchronize with Feed now**



8. Przejdź do zakładki **Configuration**, wybierz **Targets** a następnie kliknij na białą gwiazdkę.

Greenbone Security Assistant - Iceweasel

https://127.0.0.1:9392/omp

Logged in as Admin admin | Logout
Wed Jan 14 18:40:41 2015 UTC

Scan Management | Asset Management | Secinfo Management | Configuration | Extras | Administration | Help

TARGETS 1 - 1 of 1 (total: 1) [No auto-refresh]

Filter: rows=10 first=1 sort=name **nowy cel**

Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions
Localhost	localhost	1	OpenVAS Default			[Actions]

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

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net

9. Wpisz adres: **192.168.5.74** i wciśnij **Create Target**.

Greenbone Security Assistant - Iceweasel

https://127.0.0.1:9392/omp?cmd=new_target&filter=rows%3D10 first%3D1 sort%3Dname&filt_id=&token=592a9ac4-c507-427

Scan Management | Asset Management | Secinfo Management | Configuration | Extras | Administration | Help

New Target

Name: pierwsze skanowanie

Hosts: Manual 192.168.5.74
 From file Browse... No file selected.

Comment (optional):

Port List: All IANA assigned TCP 2012-02-10

SSH Credential (optional): on port 22

SMB Credential (optional):

Create Target

Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net

10. Przejdź do zakładki **Scan Management**, wybierz **New Task**. W pole name: wpisz adres **192.168.5.74**, a w **Scan Targets** wybierz **pierwsze skanowanie** a następnie kliknij **Create Task**

Greenbone Security Assistant - Iceweasel

https://127.0.0.1:9392/omp?cmd=new_task&overrides=1&token=592a9ac4-c507-427b-a68d-4f23c82b458e

Scan Management | Asset Management | Secinfo Management | Configuration | Extras | Administration | Help

New Task

Name: 192.168.5.74

Comment (optional):

Scan Config: Full and fast

Scan Targets: pierwsze skanowanie

Alerts (optional):

Schedule (optional):

Slave (optional):

Observers (optional):

Add results to Asset Management: yes no

Scan Intensity

Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Create Task

11. W kolejnym oknie kliknij zielony przycisk **PLAY**, aby uruchomić skanowanie.

Greenbone Security Assistant - Iceweasel


Greenbone Security Assistant

Logged in as Admin admin | Logout
Wed Jan 14 18:54:29 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 1 of 1 (total: 1) | No auto-refresh | Apply overrides

Filter: apply_overrides=1 first=1 rows=10 sort=name

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
192.168.5.74	New						

uruchom skanowanie

Welcome dear new user!

Quick start: Immediately scan an IP address

IP address or hostname:

Start Scan

For this short-cut I will do the following for you:

- Create a new Target with default Port List
- Create a new Task using this target with default Scan

12. Po paru minutach Status z **New** zmieni się na **Done**. Po zakończonym skanowaniu kliknij na datę ostatniego skanowania, aby zobaczyć raport.

Greenbone Security Assistant - Iceweasel


Greenbone Security Assistant

Logged in as Admin admin | Logout
Wed Jan 14 19:20:58 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 1 of 1 (total: 1) | Refresh every 30 Sec. | Apply overrides

Filter: apply_overrides=1 first=1 rows=10 sort=name

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
192.168.5.74	Done	1		Jan 14 2015	Medium		

ostatnie skanowanie

Welcome dear new user!

Quick start: Immediately scan an IP address

IP address or hostname:

Start Scan

For this short-cut I will do the following for you:

- Create a new Target with default Port List
- Create a new Task using this target with default Scan

13. W kolejnym oknie zapisz **Full report** do pliku PDF.

Greenbone Security Assistant - Iceweasel

Greenbone Security Assistant

Logged in as Admin admin | Logout
Wed Jan 14 19:20:58 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Report Summary | Apply overrides










Result of Task: 192.168.5.74

Order of results: by host

Scan started: Wed Jan 14 19:01:01 2015

Scan ended: Wed Jan 14 19:16:57 2015

Scan status: Done

	Critical	Medium	Low	Log	Follow Up	Total	Run Alert	Download
Full report:	0	2	3	25	0	30		  pobierz plik
All filtered results:	0	2	0	0	0	2		 
Filtered results 1 - 2:	0	2	0	0	0	2		 

Result Filtering

Sorting: port ascending | port descending | threat ascending | threat descending

14. Otwórz plik PDF i sprawdź wyniki skanowania.

Host scan start Wed Jan 14 19:16:15 2015 UTC
Host scan end Wed Jan 14 19:16:57 2015 UTC

Service (Port)	Threat Level
epmap (135/tcp)	Medium
ideafarm-chat (902/tcp)	Low
unknown (5357/tcp)	Low
epmap (135/tcp)	Log
ideafarm-chat (902/tcp)	Log
unknown (5357/tcp)	Log
apex-mesh (912/tcp)	Log
blackjack (1025/tcp)	Log
cap (1026/tcp)	Log
exosee (1027/tcp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/tcp	Log
iad1 (1030/tcp)	Log
iad2 (1031/tcp)	Log