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).

2						Advanced IP Scanner			- 🗆 🗙						
File Ac	tions Settings	View H	lelp												
► s	seen Zakres skanowania														
192.168.	192168.10.0.1 · 192168.10.254 Example: 192168.0.1 · 192168.0.10 · 192168.0.200 ·														
Results	Aesults Favorites														
Status	Name	Туре	Operating system	IP	Manufacturer	MAC address									
0 alive, 0 d	ead, 0 unknown														

(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).

2						Adva	anced IP Scanner			- 🗆 🗙
File Actio	ons Settings View	Help								
Sca	n II 🔳 📕	P Ç								
192.168.10	00.1 - 192.168.100.25	4						adros ka	du MAC	Example: 192.168.0.1-192.168.0.100, 192.168.0.200 👻
Results	Favorites				S	system operacy	/jny	dures ku	ITY MAC	
Status	Name			Туре	Operating system	IP	Manufacturer	MAC address		
	BRW3423874E886E					192.168.100.9	Hon Hai Precision In	34:23:87:4E:88:6E		
4 💻	AEGIS				Windows	192.168.100.2	Hon Hai Precision In	4C:0F:6E:11:8F:55		
	📳 Radmin (v3 Rad	lmin Authe	entication)		dodatek Radn	nin				
	🗀 Users 🗲		udostęp	niany f	older					
	192.168.100.71					192.168.100.71	Samsung Electronics	78:1F:DB:C6:04:0A		
-	192.168.100.10					192.168.100.10	HTC Corporation	50:2E:5C:4E:40:73		
	192.168.100.45					192.168.100.45	Nokia Corporation	54:44:08:3B:11:64		
L										
5 alive, 1 dea	ad, 248 unknown									

W oknie można zauważyć, że w obecnej sieci znajduję 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. 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).

Główna 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.

•	Ze	nmap	- 🗆 🗙
Sk <u>a</u> n Narzędz <u>i</u> a <u>P</u> rofil	Pomoc		
Cel:	V Profil:	Intense scan	Skan Anuluj
Komenda: nmap -T4 -A	-v	Intense scan	
Hosty Usługi System I Host I	Wynik działania Nmapa	Intense scan, all TCP ports Intense scan, no ping Ping scan Quick scan Quick scan plus Quick traceroute Regular scan Slow comprehensive scan	osta Skany
Filtruj hosty			

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

-P0: Traktuj wszystkie hosty jako dosępne - 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

-sl <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>: Podmieniaj 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>: Podmieniaj 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 grepowalnym

-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).

•	Zenmap		- 1	0 ×
Sk <u>a</u> n Narzędzja <u>P</u> rofil Pomoc				
Cel: 192.168.100.*	V Profit: Intense scan	~	Skar	Anuluj
Komenda: nmap -T4 -A -v 192.168	100.*			
Hosty Usługi	Wynik działania Nmapa Porty / Hosty Topologia Szczegóły hosta Skany			
System 4 Host	nmap -T4 -A -v 192.168.100.*	~		Szczegóły
I92.168.100.2				~
192.168.100.4	Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-27 18:07 Środkowoeuropejski czas stand.			
103 100 100 5	N <u>SE:</u> Loaded 118 Scripts for Scanning. NSE: Script Pre-scanning			
192.108.100.5	Initiating ARP Ping Scan at 18:07			
192.168.100.45	Scanning 255 hosts [1 port/host]			
International	Completed AKY Fing Scan at 10:07, 3.315 elapsed (255 total nosts) Initiating Parallel DNS resolution of 255 hosts, at 18:07			
192-190-1902-22	Hmap scan report for 192.168.100.0 [host down]         Nmap scan report for 192.168.100.1 [host down]         Nmap scan report for 192.168.100.3 [host down]         Nmap scan report for 192.168.100.7 [host down]         Nmap scan report for 192.168.100.8 [host down]         Nmap scan report for 192.168.100.7 [host down]         Nmap scan report for 192.168.100.8 [host down]         Nmap scan report for 192.168.100.1 [host down]         Nmap scan report for 192.168.100.2 [host down]			
Filtruj hosty	<pre>mmp scall reput: tou: 192.108.100.20 [lost down] hmap scan report for 192.108.100.27 [lost down] hmap scan report for 192.108.100.28 [lost down] hmap scan report for 192.108.100.29 [lost down] hmap scan report for 192.108.100.30 [lost down] hmap scan report for 192.108.100.32 [lost down]</pre>			~

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

•							Zenmap		- 0	×	
Sk <u>a</u> n N	arzędzja <u>P</u> rofil Pomoc										
Cel: 19	2.168.100.*						V Profit: Intense scan	~	Skan	Anuluj	
Komenda	: nmap -T4 -A -v 192.168.10	00.*									
Ho	sty Usługi	Wyr	iik działa	nia Nmapa	Porty / I	losty Topologia	Szczegóły hosta   Skany				
System 4	Host 🔺		Port 4	Protokół •	Stan	<ul> <li>Usługa</li> </ul>	Wersja			4	
۲	192.168.100.2		135	tcp	open	msrpc	Microsoft Windows RPC				
- 5	192.168.100.4		139	tcp	open	netbios-ssn					
	192.168.100.5		445	tcp	open	netbios-ssn					
	192.168.100.45		554	tcp	open	rtsp					
	192.168.100.71		2869	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)				
	192.168.100.252		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)				
			6646	tcp	open	unknown					
			10243	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)				
			49152	tcp	open	msrpc	Microsoft Windows KPC				
			49153	tcp	open	msrpc	Microsoft Windows RPC				
			49104	tcp	open	msrpc	Microsoft Windows RPC				
			49155	tcp	open	msrpc	Microsoft Windows KPC				
		•	49161	tcp	open	msrpc	Microsoft Windows RPC				
	Filtruj hosty										

• topologia - graficzny podgląd sieci



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

- Zenmap	- 1	×
Sk <u>a</u> n Narzędzja <u>P</u> rofil Pomoc		
Cel: 192.168.100.* V Profil: Intense scan	✓ Skan	Anuluj
Komenda: nmap -T4 -A -v 192.168.100.*		
Hosty Usługi Wynik działania Nmapa Porty / Hosty   Topologia Szczegóły hosta Skany		
System 4 Host 🔺 🖂 192.168.100.4		^
192.168.100.2 E Status hosta		
192.168.100.4 Stan: up		
92.168.100.5 Otwarte porty: 13		
192.168.100.45 Phillowale ports: 967		
192.168.100.71      Przeskanowane porty: 1000		
192.168.100.252     Czas od właczenia: 2693		
Ostatnie uruchomienie: Sat Dec 27 17:30:10 2014		
Advan		
IPv4: 192.168.100.4		
IPv6: Niedostępne		
MAC: 24:FD:52:FF:CD:AF		
System operacyiny		
Nazwa: Microsoft Windows 7 Professional or Win	ndows 8	
Dokładność: 1	100%	
⊖ Użyte porty     Port-Protokói-Stan: 135 - tcp - open		
Klasy systemów operacyjnych		
Typ Producent Rodzina systemów operacyjnych Generacja systemu o	operacyjnego Dokładnośc	
general purpose Microsoft Windows 8	100%	
🕀 Sekwencja TCP		
Sekwencja IP ID		
Sekwencja TCP TS		
Filtruj hosty		~

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.



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



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



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



🗵 root@kali: ~ 🦉 Greenbone Security A...

Wybrane opcje:

• Dodawanie użytkownika - Administration > Users

Applications Places ổ 돈			Fri Jan 2, 6:27 PM		4	🖌 🚅 🖣 root
		Greenbone S	Security Assistant – Iceweasel			_ 🗆 ×
<u>File Edit View History Book</u>	kmarks <u>T</u> ools <u>H</u> elp					
left Security Assistant	-					
https://127.0.0.1:9392	?/oap?cmd=get_users&	token=c5b29b0d-fada-4dca-97	7b0-56fdcb64721b	ି 🗸 🕑 🚺 🖌 ଜ	oogle	🔍 🕹 🐔
👼 Most Visited 🗸 👖 Offensive	Security 🌂 Kali Linux	🔨 Kali Docs  🕕 Exploit-DB	Aircrack-ng			
	Scan Management	Asset Management SecInfo Manage	ment Configuration Extras	Administration H	lelp	^
	New User <table-cell></table-cell>					
	Login Name					_
	Password					
	Role	User 🗘				
	Host Access	Allow All				
		O Allow: O Deny:				
				Crea	ite User	k i
	Users <table-cell></table-cell>					
	Name	Role	Host Access	Actio	ns	
	admin	Admin	Allow All	$\times$	J 📶	
	aegi	Observer	Allow All	× 🛛		
	r@		Greenbone Security Assistant (GSA) Copyright 2009-20	)13 by Greenbone Networks GmbH, www.ç	jreenbone.net	<b>v</b>
🖭 root@kali: ~	Greenbone Security	/ A				

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.



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** 

Applications Places	籆 🛌 Fri Jan 2, 6:29 PM	📢 🚅 🗬 root
	Greenbone Security Assistant – Iceweasel	_ <b>_</b> ×
<u>File Edit View History</u>	Bookmarks Tools Help	
left Ass	sistant 🗣	
https://127.0.0.1	1:9392/omp?cmd=new_task&overrides=1&token=c5b29b0d-fada-4dca-97b0-56fdcb64721b 🗘 ♥ 🕑 関 ♥ Google	🧟 🕹 🐔
offe≣Most Visited ✓ MOffe	ansive Security 🥆 Kali Linux 🌂 Kali Docs 🛄 Exploit-DB 🐚 Aircrack-ng	
	Greenbone     O     Logged in as Admin admin   Logout       Security Assistant     Fri Jan 2 23:28:46 2015 UTC	
	Scan Management Asset Management SecInfo Management Configuration Extras Administration Help	
	Tasks	=
	Notes	
	Overrides	
	Comment (optional)	
	Scan Config Full and fast	
	Scan Targets 192.168.100.5	
	Alerts (optional) 🗘 +	
	Schedule (optional) 🗘	
	Slave (optional) 🗘	
	Observers (optional)	

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 podglądnąć w oknie **Scan Management > Tasks**



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:

Stanus: 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.



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.

Advanced	IP Scanner						-	200	-	-	 	- 6 - X-
File Actio	ns Settings View Help											
Scar												
192.168.5.1	- 192.168.5.254										Example: 192.168.0.1	-192 168 0 100 192 168 0 200 -
Results	Favorites											
Status	Name	Type Op	erating system	IP .	Manufacturer	MAC address						
	r1.prz.rzeszow.pl			192.168.5.1	CISCO SYSTEMS, INC.	00:12:DA:67:9E:C0						
	OPNET			192.168.5.7	Orade Corporation	00:21:28:81:FA:80						
> 🖳	sun9.prz.rzeszow.pl			192.168.5.19	ASUSTek COMPUTER INC.	00:1F:C6:E4:EB:EA						
5 🖷	Es108-0.zsr.prz.edu.pl	Print server		192.168.5.30	D-Link Corporation	00:18:11:C5:62:D6						
> 💻	DmSystem	Win	dows	192.168.5.74	GIGA-BYTE TECHNOLOGY CO., LTD.	50:E5:49:33:C8:93						
	DmSystem			192.168.5.75	GIGA-BYTE TECHNOLOGY CO., LTD.	\$0:E5:49:33:D4:83						
> 👳	DRUK1	Print server		192.168.5.170	RICOH COMPANY LTD.	00:00:74:98:22:88						
> 💻	NPI180CD1			192.168.5.171	Hewlett-Packard Company	00:1F:29:18:0C:D1						
> 💵	192.168.5.217			192.168.5.217	KONECA MINOLTA HOLDINGS, INC.	00:20:68:DC:D4:4D						
2 💻	NP13E28FA			192.168.5.253	Hewlett-Packard Company	D4:85:64:3E:28:FA						
	10/	adrosów aktuw	nuch 244 n	ieznanych								
av anve, u dea	ad, 2++ dhknown	au sour uniyw	17011/2441	in an in the second								

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

File Action	s Settings View Help						-	~ ~	
- ACTION									
Scan									
103 169 5 1	102 149 5 254								
192.108.3.1	192.108.3.234								
Results F	avontes								
Status	Name	Type	Operating system	IP	Manufacturer	MAC address			
	r1.prz.rzeszow.pl			192.168.5.1	CISCO SYSTEMS, INC.	00:12:DA:67:9E:C0			
1	OPNET			192.168.5.7	Orade Corporation	00:21:28:81:FA:80			
> 🕎	sun9.prz.rzeszow.pl			192.168.5.19	ASUSTER COMPUTER INC.	00:1F:C6:E4:E8:EA			
> <u>*</u>	Es108-0.zsr.prz.edu.pl	Print server		192.168.5.30	D-Link Corporation	00:18:11:C5:62:D6			
>	DmSystem		Windows	192.168.5.74	GIGA-BYTE TECHNOLOGY CO., LTD.	50:E5:49:33:C8:93			
+	DmSystem			192.168.5.75	GIGA-BYTE TECHNOLOGY CO., LTD.	50:E5:49:33:D4:83			
> =	DRUK1	Print server		192.168.5.170	RICOH COMPANY LTD.	00:00:74:98:22:88			
2 -	NPI180CD1			192, 168, 5, 171	Hewlett-Packard Company	00:1F:29:18:0C:D1			
2 4	192.168.5.217			192.168.5.217	KONECA MENOLTA HOLDINGS, INC.	00:20:68:DC:D4:4D			
2. 🖳	NP13E28FA			192.168.5.253	Hewlett-Packard Company	D4:85:64:3E:28:FA			

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

File Actio	ns Settings View	Help				<u> </u>	_
Sca		₽ <b>₽ 1</b> :					
192.168.5.	• 192.168.5.254						
Results	Favorites						
Status	Name		Type	Operating system	p ^	Manufacturer	MAC address
	r1.prz.rzeszow.pl				192.168.5.1	CISCO SYSTEMS, INC.	00:12:DA:67:9E:C0
	OPNET				192.168.5.7	Oracle Corporation	00:21:28:81:FA:80
> 📮	sun9.prz.rzeszow.	pl			192.168.5.19	ASUSTH: COMPUTER INC.	00:1F:C6:E4:EB:EA
> 👳	Es 108-0.zsr.prz.ed	lu.pl	Print server		192.168.5.30	D-Link Corporation	00:1B:11:C5:62:D6
4 🖳	DmSystem	for the second s		Windows	192.168.5.74	GIGA-BITE TECHNOLOGY CO., LTD.	50:E5:49:33:C8:93
	<b>B</b> Autor (1	Conv	1				
	DmSystem	copy			192.168.5.75	GIGA-BYTE TECHNOLOGY CO., LTD.	50:E5:49:33:D4:83
> 📮	DRUK1	Add to favorites	Print server		192.168.5.170	RECOH COMPANY LTD.	00:00:74:98:25:68
> 📮	NPI 1B0CD 1	Rescan selected			192.168.5.171	Hewlett-Packard Company	00: 1F:29: 1B:0C:D1
▶ 📮	192.168.5.217				192.168.5.217	KONICA MINOLTA HOLDINGS, INC.	00:20:68:DC:D4:4D
▶ 📮	NP13E28FA	Wake-On-LAN			192.168.5.253	Hewlett-Packard Company	D4:85:64:3E:28:FA
		Abort shut down					
		RDP					
		Radmin +					
			1				
10 - 5 - 0 - 4	1.244						

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

Advanced	IP Scanner						A	-	
File Action	s Settings View Help								
Scan		18 2:							
192.168.5.1	- 192.168.5.254								Example: 192.168.0.1-192.168.0.100.192.168.0.200 -
Results	avorites								
Status	Name r1.prz.rzeszow.pl	Туре	Operating system	IP 192.168.5.1	Manufacturer CISCO SYSTEMS, INC.	MAC address 00:12:DA:67:9E:C0			
-	OPNET			192.168.5.7	Orade Corporation	00:21:28:81:FA:80			
≥ ₩	sun9.prz.rzeszow.pl			192.168.5.19	ASUSTER COMPUTER INC.	00: 1F:C6:E4:EB:EA			
1	Es 108-0.zsr.prz.edu.pl	Print ser	ver	192.168.5.30	D-Unk Corporation	00:18:11:C5:62:D6	i i		
-	DmSystem	Explore	Windows	192.168.5.74	GEGA-BYTE TECHNOLOGY CO.,LTD.	50:E5:49:33:08:93	1		
	DmSystem	Copy +		192, 168, 5, 75	GEGA-BYTE TECHNOLOGY CO.,LTD.	50:65:49:33:D4:83			
2 📮	DRUK1	Rescan selected	ver	192.168.5.170	RECOH COMPANY LTD.	00:00:74:98:25:68			
2 🖤	NPI180CD1	Save selected		192.168.5.171	Hewlett-Packard Company	00: 1F:29: 18:0C:D 1			
2 🕎	192.168.5.217			192.168.5.217	KONICA MINOLTA HOLDINGS, INC.	00:20:68:DC:D4:4D			
2 🖉	NPI3E28FA	Shut down		192.168.5.253	Hewlett-Packard Company	D4:85:64:3E:28:FA			
		Abort shut down							
	Г								
	L	Tools •	Ping						
		Row	Tracert						
	_	Neamin	Telnet SSM						
			3311						
10 alive, 0 dea	d, 244 unknown								

 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.

File Actions Settings	View Help							
Scan II III	] ₩ ₩ वि 🖦							
192.168.5.1 - 192.168.5.25	54							Example: 192.168.0.1-192.168.0.100, 192.168.0.2
Results Favorites								
Status Name		Type Or	perating system	1p ^	Manufacturer	MAC address		
r1.prz.rzeszo	w.pl			192.168.5.1	CISCO SYSTEMS, INC.	00:12:0A:67:9E:C0		
P OPNET				192.168.5.7	Oracle Corporation	00:21:28:81:FA:80		
b 📮 sun9.prz.rzes	zow.pl			192.168.5.19	ASUSTER COMPUTER INC.	00:1F:C6:E4:EB:EA		
) 📮 Es108-0.250p	vz.edu.pl	Print server		192.158.5.30	D-Link Corporation	00:18:11:C5:62:D6		
🖌 💻 DmSystem		Wa	ndows	192.158.5.74	GIGA-BYTE TECHNOLOGY CO., LTD.	50:E5:49:33:C8:93		
🐯 Radmin (	v3Re							
DesGystem	Full Control	-		192.168.5.75	GIGA-BYTE TECHNOLOGY CO., LTD.	50:E5:49:33:04:83		
DRUK1	2 Teinet	mint server		192, 168, 5, 170	RECOH COMPANY LTD.	00:00:74:96:26:88		
NP1BOCD1	4. File Transfer			192.168.5.171	Henlett-Packard Company	00:1F:29:18:0C:D1		
▶ 📮 192.168.5.21	17 🚺 Shutdown			192, 168, 5, 217	KONECA MINOLTA HOLDINGS, INC.	00:20:68:DC:D4:40		
P 📮 NPI3E28FA	🍕 Chat			192.168.5.253	Hewlett-Packard Company	D4:85:64:3E:28:FA		
	Voice Chat							
	Send Message							
0 alive. 0 dead. 244 unknown	1							
	1 1 1 1	tro.						16:38

8. Wpisz login: student i hasło: student.

Advanced 1	P Scanner					<u> </u>		
File Action	Settings View Help							
Scan								
192.168.5.1	192.168.5.254							Example: 192.168.0.1-192.168.0.100, 192.168.0.200 💌
Results B	svorites							
Status	Name	Type	Operating system	p .	Manufacturer	MAC address		
	rl.or.resow.ol			192, 168, 5, 1	CISCO SYSTEMS, INC.	00:12:D4:67:9E:C0		
100	OPNET			192.168.5.7	Oracle Corporation	00:21:28:81:FA:80		
> 10	sur9.prz.rzeszow.pł			192, 168, 5, 19	ASUSTER COMPUTER INC.	00: 1F=C6:E4:EB=EA		
5 B	Es108-0.zs.orz.edu.ol	Print server		192, 168, 5, 30	D-Link Corporation	00:18:11:C5:62:D6		
	DmSystem		Windows	192.168.5.74	GIGA-BYTE TECHNOLOGY CO.,LT	D. 50:E5:49:33:C8:93		
	Radmin (v3 Radmin Authentication)							
	DmSystem			192.168.5.75	GEGA-BYTE TECHNOLOGY CO.,LT	D. 50:E5:+9:33:D4:83		
> 🖷	DRUK1	Print server		192.168.5.170	RICOH COMPANY LTD.	00:00:74:98:22:88		
> 🜉	NPI1B0CD1			192.168.5.171	Hewlett-Packard Company	00: 1F:29: 1B:0C:D 1		
2 10	192.168.5.217			192.168.5.217	KONECA MINOLTA HOLDINGS, IN	C. 00:20:68:DC:D4:40		
> 💻	NPI3E28FA			192.168.5.253	Hewlett-Packard Company	D4:85:64:3E:28:FA		
						Respicentitus Radmin 192165.74		
10 alive 0 dear	1.244 unknown							
Av ante, o ueau	, see all seense	_					 	

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

192.168.5.74 - Pełna kontrola					_		X
E = C 1 2 3 4 7 5 8 8 8 1 2 3	1 🗃   🗟 💥						
Siel .							Microsoft Virtual
~							
- <u></u>	Panel sterowani	s ► SiećiInternet ► Centrum sieciiu	dostępniania		• 4 Szukaj w Panelu sterowa	niu 🔎	
Mozilla Firefox	Strona główna Panelu	Wyświetl podstawowe info	rmacje o sieci i skonfiguruj połączenia			0 ^	VMware Player
	Zmień urtawienia kartu	<b>A</b>	and Zahara ada	mape			
ar -	sieciowej	DIMSYSTEM	Star: Internet	Szczegóły	połączenia sieciowego		Q
OpenAlifice (1912)	Zmień zaawansowane ustawienia udostępniania	(Ten komputer) Wyświetlanie aktywnych sieci –	ugone	Szczegół)	polączenia sieciowego:		Uruchom
		<b>6</b>	Polączenia IPv4: Internet	Suffice D	osc Watosc NS konkretneg		
1		Sieć firmowa	Połączenia IPv6: Brak dostępu do Internetu Etno opóska	Opis Adres fiz	Atheros AR8151 PCI-E Giga rozny 50-E5-49-33-CB-93	bit Bhemet C	
			Cras trvenia: 00:12:28	DHCP w	laczone Nie 192 102 5 74		
Clarker			Szybkość: 100,0 Mb/s	Maska p	odsieci IPv4 255.255.255.0		
		Sieć niezidentyfi Sieć publiczna	Szczegoły	Servery	DNS IPv4 62 93 32 67		
			Aldunadd	Server \	62.93.38.4 VINS IPv4		
Bern syntax		Zmienianie ustawień sieciowych		System I Adres IP	letBIOS przez T Tak v6 polączenia I le80:8974.81c0 fab8.79ed	an	
_		🙀 Skonfiguruj nowe pols	wysiano — 🚽 — Odebrano	Brama d Server B	omyálna IPv6 DNS IPv6		
		Skonfiguruj połączeni skonfiguruj router lub	Sajty: 10 945 977 451 484				
Hill-Hilling and parts		Polacz z siecia	Wiladowości 😵 Wyłącz Diagnozuj	× 📖	<i>H</i>		
		Polącz lub ponownie p			1	Zamirri	
	7 object tet	posicialicawin polic	Zaminij				
	Grupa domowa	Uzyskaj dostęp do plików	i drukarek znajdujących się na innych komputerach w sieci lub zm	vień			
	Opcje internetowe	ustawienia udostepniania	L.				
	Zapora systemu Windows	Rozwiązywanie problemó	w danu z ciacia lub uzorkaj informacio na temat consiste suspija suspija	lemóu		-	
				_			Kosz
							😌 😪 to \ominus 🏲 🖯 🕼 🕺 🚺 📩
							- Kog

## 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.





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

and free second		
Cel: 192.168.5.74	Profile Intense scan	Skan Anuluj
Komenda: nmap -T4 -A -v	192.168.5.74	
Hosty Usługi	Wynik ddialania Nimapa Porty / Hosty   Topologia   Szczegóły hosta   Skany	
System 4 Host 🔺	nnap-14-A-v192168.5.74	
192.168.5.74	Discovered gene port 92/LTG on 192.184.5.74 Outries 20 % Stark 15 and 11 (11, 14, 164 scienced (12) services on 1 host) Somming 13 services on 183.184.578 Somming 13 services on 183.184.578 Digitation for the source of 18.184 scienced (12) services on 1 host) Digitation for the source of 18.184.578 Digitation for the	
	91/16p gen vmare wifn Wuare Anthenticiation Disson 1.8 (Dec WC, SGMP) 91/16p gen vmare wifn Wuare Anthenticiation Disson 1.8 (Dec WC, SGMP) 102/16p gen vmare Microsoft Hindows SWC 102/16p gen vmare Microsoft Hindows Microsoft Hindows Hindows SWC 102/16p gen Vmare Microsoft Hindows Microsoft Hindows	
	Data and Licenser; Dividious Treferesions 1/001 Service Fack 1 (Windows 7 Professional 6.1) Dividious 7 Professional 1/001 Service Fack 1 (Windows 7 Professional 6.1) Dividious 7 Professional International Int	

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

🗢 Zen

Skan Narzedzja Brofil I	Pomoc		
Cel: 192.168.5.74		Profil: Intense scan	Skan Anufuj
Komenda: nmap -T4 -A -v	v 192.168.5.74		
Horty Uskuni	March destants Marcas Data Clast Transform Constraints And		
nong onogi	A Dext & Dextel/of A Star & Hohers A Wards		
System 4 Host *	135 tra para mene Microsoft Vindous RPC		
192.168.5.74	120 tra som ather ra		
	Soz top open vinware-auti vitware Authenboation Daemon 110 (Oses Vinc, SOAP)		
	912 tcp open vmware-auto vivware Autoenocation Daemon 1.0 (Uses vivc, SOAP)		
	U23 tcp open msrpc Niticrosoft Windows RPC		
	1020 tcp open msrpc Microsoft Windows KPC		
	9 1027 tcp open msrpc Microsoft Windows RPC		
	9 1034 tcp open msrpc Microsoft Windows RPC		
	1037 tcp open msrpc Microsoft Windows RPC		
	1044 tcp open msrpc Microsoft Windows RPC		
	4899 tcp open radmin Famatech Radmin 3.X (Radmin Authentication)		
Filtruj hosty			
A 19 m		and the second	1644
			2015-01-13
E 1	W zakładco <b>Szczogółu bosta</b> spi	rowdź ilo portów przeckopował r	aragram jaki adroc kary NAAC

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

🔹 Zenmap				-		_	-	100	-	-	
Skan Narz	eedzja <u>Profil</u> P	Pomoc									
Cel: 192.1	68.5.74					Profil: Intense scar	1				Skan Anufuj
Komenda:	nmap ·T4 ·A ·v	192.168.5.74									
Hosty	Usługi	Wynik działania Nmapa Porty / Hosty Topologia Szczegó	ly hosta Skany								
Sustan 4 H	inst +	192 168 5 24									
-1 1	192.168.5.74	E Status hosta									
		Stan: up									
		Otwarte porty: 12	- 10 C								
		Filtrowane porty: 0									
		Zamknięte porty: 988									
		Przeskanowane porty: 1000	<b>A</b> -								
		Ortethia unuchamianiar Tuo Iao 12 16 22/26 2015									
		E Adresy 19:4: 192.168.5.74									
		IPv6: Niedostępne									
		MAC: 50:E5:49:33:CB:93									
		🗄 System operacyjny									
		Nazwa:	Microsoft Windows 7 SP0 - SP1, Windows Server 2018 SP1, or Win	idows 8							
		Dokładność:		100%							
		E librte norte									
		Port-Protokól-Stan: 135 - top - open									
		Port-Protokół-Starc 1 - tcp - closed									
		Port-Protokół-Stan: 37371 - udp - closed									
		<ul> <li>Klasy systemów operacyjnych Typ Producent Rodzine system</li> </ul>	nów operacyjnych – Generacja syster	nu operacyjnego	Dokładnośc						
		general purpose Microsoft Windows	8		100%						
		🗄 Sekwencja TCP									
		🗟 Sekwencja IP ID									
		🗟 Sekwencja TCP TS									
		Komentarze									
Eilter	(heat)										
Fatro	g moty				_						1645
											🔤 😋 🥡 🕑 🏲 📮 🤚 2015-01-13

- 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**.

2enmap		
Skan Narzędzja <u>P</u> rofil Pomoc		
Cel: 192.168.5.*	Profit Quick scan	Skan Anufuj
Komenda: nmap -T4 -F 192.168.5.*		
Master Dahari		
Hosty Usrugi	Wynik dhalinia Nimapa   Party / Hosty   Topologia   Szczegóły hosta   Skany	
System 4 Host	uumab - 14 - 4 187100'3'.	• Szczegoły
Internetwork         (122,108,51)           102,108,57         (120,08,51)           103,008,57         (120,08,53)           103,008,573         (120,08,57)           103,008,573         (120,08,53)           103,008,573         (120,08,53)           103,008,573         (120,08,53)           103,008,574         (120,08,53)           103,008,574         (120,08,52)           102,008,574         (120,08,52)           102,008,574         (120,08,52)           102,008,574         (120,08,52)	<pre>starting https://dx.j/res.j/res.j/it.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.stoff.</pre>	
Filmá Soto	NGL_Address_0         0:10:11:11:01:00         0:Link           Negs contrapped for 192:1485.74         Ness contrapped for 192:1485.74           Ness contrapped for 192:1485.74         Ness contrapped for 192:1485.74           115/frag deem merge         115/frag deem merge           120/frag deem merge         120/frag deem merge	
risty		
		16:47 🐽 📥 🙆 🖛 🖛 16:47

- 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

		Wyszukaj po	nownie
Drukarki, której szukar	n, nie ma na liście		
. Wybieramy opcje <b>Dodaj druk</b>	arkę, używając adresu TCP/IP lul	Dalej b nazwy hosta i kl	Anı ikamy
. Wybieramy opcje <b>Dodaj druk</b> Dodawanie drukarki Znajdź drukarkę na podstav	arkę, używając adresu TCP/IP lul vie innych opcji	Dalej b nazwy hosta i kl	Anı
. Wybieramy opcje <b>Dodaj druk</b> Dodawanie drukarki Znajdź drukarkę na podstav Wybierz drukarkę udostępnioną v	arkę, używając adresu TCP/IP lul vie innych opcji redług nazwy	Dalej b nazwy hosta i kl	ikamy
<ul> <li>Wybieramy opcje Dodaj druka</li> <li>Dodawanie drukarki</li> <li>Znajdź drukarkę na podstav</li> <li>Wybierz drukarkę udostępnioną v</li> <li>Przykład: \\nazwa_komputera http://nazwa_komputera/prin</li> </ul>	arkę, używając adresu TCP/IP lul vie innych opcji vedług nazwy \nazwa_drukarki lub ters/nazwa_drukarki/.printer	Dalej b nazwy hosta i kl	Anı ikamy
<ul> <li>Wybieramy opcje Dodaj druka</li> <li>Dodawanie drukarki</li> <li>Znajdź drukarkę na podstav</li> <li>Wybierz drukarkę udostępnioną v</li> <li>Przykład: \\nazwa_komputera http://nazwa_komputera/prin</li> <li>Dodaj drukarkę, używając adresu</li> </ul>	arkę, używając adresu TCP/IP lul vie innych opcji vedług nazwy \nazwa_drukarki lub ters/nazwa_drukarki/.printer TCP/IP lub nazwy hosta	Dalej b nazwy hosta i kl	eglądaj
<ul> <li>Wybieramy opcje Dodaj druka</li> <li>Dodawanie drukarki</li> <li>Znajdź drukarkę na podstav</li> <li>Wybierz drukarkę udostępnioną v</li> <li>Przykład: \\nazwa_komputera http://nazwa_komputera/prin</li> <li>Dodaj drukarkę, używając adresu</li> <li>Dodaj drukarkę Bluetooth, bezprz</li> </ul>	arkę, używając adresu TCP/IP lul vie innych opcji vedług nazwy \nazwa_drukarki lub ters/nazwa_drukarki/.printer TCP/IP lub nazwy hosta ewodową lub wykrywalną w sieci	Dalej b nazwy hosta i kl	eglądaj

×

- 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 dale	ej
----------	---------------------------	----

<b>2</b>		
Typ urządzenia:	Urządzenie TCP/IP	
Nazwa hosta drukarki lub adres IP:	192.168.5.30	
Nazwa portu:	515	
✓ Sprawdź drukarkę i automatyc	znie wybierz sterownik do użycia	

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

			×
📄 🖶 Dodawanie	drukarki		
Której wersji s	terownika chcesz używać?		
System Windows v	vykrył, że dla tej drukarki jest już zainstalowany sterownik	<b>.</b> .	
🖲 Użyj obecnie za	instalowanego sterownika (zalecane)		
🔿 Zamień bieżący	sterownik		
		Dalei	Anului
Daiomy pazwo pac			
Dajettiy nazwę nas			×
🖶 Dodawanie	drukarki		
Wpisz nazwę o	Irukarki		
Nazwa drukarki:	Drukarka_1		
Drukarka zostanie :	zainstalowana przy użyciu sterownika Brother DCP-1132V	V Drinter	
	unistalowana przy użycia sterownika biotner ber 31524	- Thiten	

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

🕞 🖶 Dodawanie dr	ukarki
Udostepnianie d	rukarki
Jeśli chcesz udostępni wpisać nową. Nazwa i	ć tę drukarkę, musisz podać nazwę udziału. Możesz użyć sugerowanej nazwy lub udziału będzie widoczna dla innych użytkowników w sieci.
🔿 Nie udostępniaj tej	drukarki
Udostępniaj tę drul	karkę, aby inni użytkownicy w sieci mogli ją znaleźć i używać jej
Nazwa udziału:	Drukarka_1
Lokalizacja:	
Komentarz:	
	Dalej Anuluj

# Skanowanie podatności OpenVas

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



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

Kali - VMware Player (Non-commercial use only)			_		-	-	-			x
Player 👻 🔛 🖛 🖼 🦷									*	
	Programy Miejsca 😨 🔙 Przegłądanie i uruchamianie zari Elle Edit Vjew Higtory Boc	w istalowanych progra ikmarks <u>I</u> ools <u>H</u> e	vto 13 sty, 17:05 mów n – Iceweaso Plp	ei	44 <u>)</u>	e root				
	L Untrusted Connection	4				_				
	https://127.0.0.1 939	2		ି <b>~ ୯</b> ୩ 🔂 ~ Ge	oogle	🗠 🖖 😤				
	Most Visited Difference Differenc	Security Nati Li source use are and of here! Details and the Risks and what's going on Even if you trust t ith your connectio exception unless you fication. on	nux 🔪 Kali Docs o you snourone cor n, you can tell icew che site, this error n. u know there's a gr	Veasel to start trusti r could mean that s	larcrack⇒ng ing this site's iomeone is site doesn't use	2				
	🗊 [root@kali: -]	C Untrusted Conn	ection		6					

5. W kolejnym oknie na Confirm Security Exception

won-commercial use only/				-	_	
2 18						٠ (
Programy Miejsca	i 😨 🛌 🦷 wto 13 sty, 2	17:05	× =	root		
	Add Security E	ception		× 1		
<u>File</u> Edit <u>View</u> H	You are about to override how li	ceweasel identifies this site.				
A Untrusted Connec	🖞 🧀 Legitimate banks, stores, and	other public sites will not				
	ask you to do this.		Q 4	<b>1</b>		
🛅 Most Visited 🗸 🚦	Server		ng			
	Location: https://127.0.0.1:9392/	Get Certificate		1		
	G Certificate Status					
	This site attempts to identify itself w	ith invalid View				
• T	e information.					
*1	wrong site					
	Certificate belongs to a different site	, which could indicate an				
lf - ide	/ identity theft.		ite's			
ta	Unknown Identity					
Pr	Certificate is not trusted, because it i	nasn't been verified by a	sn't use			
tru	recognized authority using a secure s	ignature. 💟		12		
	<u>rermanently store this exception</u>					
	Confirm Security Exception	Cancel				
	C Hatavated Connection			V		
[root@kau: ^]	Contrusted Connection					

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

Applications Places 🔕 돈		Fri Jan 2, 6:27 PM	(c))	<u> </u>	🗬 root
		Greenbone Security Assistant - Iceweasel		-	• ×
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookn	narks <u>T</u> ools <u>H</u> elp				
left for the security Assistant left for the security Assistant left for the security Assistant left for the security assists and the security ass	4				
https://127.0.0.1:9392/d	pap?cmd=get_feed&	ktoken=c5b29b0d-fada-4dca-97b0-56fdcb64721b 🗇 ♥ 🕲 🛛 Google		Q,	J 😚
🛅 Most Visited 🌱 👖 Offensive Se	ecurity 🥆 Kali Linu	x 🍾 Kali Docs 🚦 Exploit-DB 📡 Aircrack-ng			
	🝌 Greenbor	ie Logged in as Admin admin   Logout			
	🤣 Security As	sistant Fri Jan 2 23:27:07 2015 UTC			
	Scan Management	Asset Management SecInfo Management Configuration Extras Administration Help			
	NVT Feed Manag	gement 🛛			
	Name	OpenVAS NVT Feed			
	Feed Version Description	201412300733 This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'. The 'OpenVAS NVT Feed' is provided by 'The			
		OpenVAS Project'. Online information about this feed: 'http://www.openvas.org/openvas.nvt.feed.html'.			
		Synchronize with Feed now			
		Learn about the side effects of feed synchronization!	)	÷	
		Greenbone Security Assistant (GSA) Copyright 2009-2013 by Greenbone Networks GmbH, www.greenbone.net			
🗵 root@kali: ~	Greenbone Secur	ty A			

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

Applications Places 🔞 돈		Green	Wed Jan 14, 1:	41 PM		•)
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ool	kmarks <u>T</u> ools <u>H</u> elp	Green	Some Security Assistant -	iceweaser		
left Greenbone Security Assistant	<b>-</b>					
https://127.0.0.1:9392	!/omp				☆ ✔ ኛ 😵 Google	٩ 4
Most Visited 🗸 👖 Offensive :	Security 🌂 Kali Linux	🔨 Kali Docs  🔝 Exploit	-DB 📡 Aircrack-ng			
	Security Assis	stant		<mark>% </mark>	Logged in as Admin admin   Logout Wed Jan 14 18:40:41 2015 UTC	
	Scan Management	Asset Management Secinfo	Management Configuration	n Extras	Administration Help	
	Targets 1 - 1 of 1 (	total: 1) 🛛 🗷 🗐 🛛 🛡	√No auto-refresh 🛛 🗘 🕄			_
	Filter: rows=10 first	=1 sort=name	<ul> <li>nowy cel</li> </ul>	2	E 0 2 E	
	Name         Hos           Localhost         local           (Applied filter: rows=10 first)         local	ts IPs Port Lis host 1 OpenVAS =1 sort=name)	it SSH Crede	ntial SMB Creder	tial Actions	
			Great don't d'actuality roadier	n (COP) Copyright 200-2020 o		~
9. Whisz ac	™ root@kall: ~ dres: <b>192.16</b>	8.5.74 i wci	śnii <b>Create Ta</b>	rget.		<u>G</u>
Applications Places 👸 🗏			Wed Jan 14, 1:	44 PM		•)
		Green	bone Security Assistant -	lceweasel		- 6
<u>File Edit View History Bool</u>	kmarks <u>T</u> ools <u>H</u> elp					
Greenbone Security Assistant	2/omp2cmd=new_target	&filter=rows%3D10 firs	t%3D1 sort%3Dname&filt	id=&token=592a9ac4-c5	07-427 ☆ ✔ @ [ <b>장 ×</b> Google	
Most Visited	Security 🌂 Kali Linux	Kali Docs	-DB NAircrack-ng	a acoren sseasaches		
	Scan Management A	sset Management Secinfo	Management Configuration	Extras	Administration Help	
	New Target 🔋 🗏					
	Name	pierwsze skanow	anie			
	Hosts	Manual 192.	.168.5.74			
		O From file Bro	wse No file selected.			
	Comment (optional)					
	Port List	All IANA assigne	d TCP 2012-02-10	•		
	SSH Credential (option	al) 🗘 on port 22				k
	SMB Credential (option	nal) 🗢				
					Create Target	
			Greenbone Security Assista	nt (GSA) Copyright 2009-2013 by	Greenbone Networks GmbH, www.greenbone.ne	t
🗯 Greenbone Security A	🗵 root@kali: ~			-		<b>@</b>
10. Przejdź o	do zakładki s	Scan <b>Manag</b>	<b>ement</b> , wybie	erz <b>New Task</b>	. W pole name: w	pisz adres
192.168	<b>.5.74</b> , a w <b>S</b>	can Targets	wybierz pierv	vsze skanow	anie a następnie l	diknij <b>Create T</b> a
		Greent	oone Security Assistant -	Iceweasel		
File Edit View History Book	marks <u>T</u> ools <u>H</u> elp					
Greenbone Security Assistant	l'ann à mais teals a		-04 -507 4276 -694 46	22-02-450-		
Most Visited	Security 🌋 Kali Linuw	Kali Docs EFviloit	-DB Aircrack-ng	2323207302		
Concepted - Manual - Ma Manual - Manual - Manua - Manual - Manual	Name	192168 5 74				
	Comment (optional)	192.168.5.74				
	Scan Config	Eull and fact				
	Scan Targete	nierwsze skapowanie 🛆				
	Alerts (optional)	0 +				
	Schedule (optional)					
	Slave (optional)	\$				
	Observers (optional)					
	Add results to Asset Management	● yes ○ no				
	Scan Intensity					
	Maximum concurrently	executed NVTs per bost				
	. asimum concurrently	sites and a set to set	4			
	Maximum concurrently	scanned hosts	20			
					Create Task	

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

	_ 0 ×		
<u>File Edit View History</u>	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		
left for the security Assis left for the security Assis left for the security Assis left for the security and the security as	tant		
https://127.0.0.1:9	392/omp?cmd=get_tasks&overrides=1&token=592a9ac4-c	507-427b-a68d-4f23c82b458e 🗇 📽 🚱 Google	Q 🕹 😤
Most Visited ✓      Most Visited ✓	sive Security 🌂 Kali Linux 🌂 Kali Docs  🗊 Exploit-DB 🐚	Aircrack-ng	
	A Greenbone	😞 Logged in as Admin admin   Logout	<u>_</u>
	Security Assistant	Wed Jan 14 18:54:29 2015 UTC	
	Scan Management Asset Management SecInfo Managem	ent Configuration Fetras Administration Help	
	ocantalogenene roosertelogenene oceano tonogen		
	Tasks 1 - 1 of 1 (total: 1) 🛛 🗮 🔳 🛛 🚺	lo auto-refresh   ≎] vApply overrides   ≎] 🖸	
	Filter: apply_overrides=1 first=1 rows=10 sort=name	2	=
	Name Status	Total Reports First Last Threat Trend Actions	
	192.168.5.74 New		
	(Applied filter: apply_overrides=1 first=1 rows=10 sort=name)	uruchom skanowanie	
	Welcome dear new user!	/ Quick start: Immediately scan an IP address	
	To explore this powerful application and to	IP address or hostname:	
	time, I am here to assist you with some	Start Scan	
	I will appear automatically in areas where	For this short-cut I will do the following for you:	
	you have created no or only a few objects. And disappear when you have more than 3 miles	<ol> <li>Create a new Target with default Port List</li> <li>Create a new Task using this target with default Scan</li> </ol>	

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



14. Otwórz plik PDF i sprawdź wyniki skanowania.

герог	t-721b60da-d387-4555-a4f5-18fa	a3d95902-1.pdf	 u x
File Edit View Go Bookmarks Help			
The Previous Vext 2 (2 of 14) Fit Page Width V			
HOST Stan Start WCu 3	an 14 13.01.10 2019 UTC		
Host scan end Wed J	an 14 19:16:57 2015 UTC		- 11
			1
	Service (Port)	Threat Level	- 14
	epmap (135/tcp)	Medium	- 11
	ideafarm-chat $(902/tcp)$	Low	- 11
	unknown (5357/tcp)	Low	- 11
	epmap (135/tcp)	Log	- 11
	ideafarm-chat (902/tcp)	Log	- 11
	unknown (5357/tcp)	Log	- 11
	apex-mesh $(912/tcp)$	Log	- 11
	blackjack (1025/tcp)	Log	- 11
	cap (1026/tcp)	Log	- 11
	exosee $(1027/tcp)$	Log	- 11
	general/CPE-T	Log	- 11
	general/HOST-T	Log	- 11
	general/tcp	Log	
	iad1 (1030/tcp)	Log	- 11
	iad2 (1031/tcp)	Log	- 11