



BOT – Laboratorium 1

Rekonesans i skanowanie

Patryk Gozdera, 277185

Część pierwsza – rekonesans

Po zapoznaniu się z dostępnymi narzędziami, umożliwiającymi przeprowadzenie rekonesansu, przeszedłem do tworzenia profilu przydzielonej mi instytucji (**Uniwersytet Adama Mickiewicza w Poznaniu**), na podstawie zebranych z sieci danych.

Poniżej zostaną przedstawione zgromadzone informacje z poszczególnych narzędzi (z widocznymi na screen'ach komendami).

- Nslookup – wyszukanie informacji odnoszących się do serwerów DNS włączając adres IP poszczególnych komputerów, nazwę domeny. Poniżej zostały umieszczone screeny wynikowe:

```
golter@UbuntuBOT:~$ nslookup amu.edu.pl
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   amu.edu.pl
Address: 150.254.65.253


> set type=mx
> amu.edu.pl
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
amu.edu.pl   mail exchanger = 10 mx1.amu.edu.pl.
amu.edu.pl   mail exchanger = 10 mx2.amu.edu.pl.
```


- Lokalizacja geograficzna – korzystając ze strony <https://www.iplocation.net/>, ustaliłem lokalizację:

You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is **150.254.65.253**

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2017-10-1)

Domain Name	Country	Region	City
amu.edu.pl	Poland 	Wielkopolskie	Poznan
ISP	Organization	Latitude	Longitude
Address Space for Adam Mickiewicz University	Not Available	52.4069	16.9299

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

Domain Name	Country	Region	City
amu.edu.pl	Poland 	Greater Poland	Poznan
ISP	Organization	Latitude	Longitude
Institute of Bioorganic Chemistry Polish Academy of Science, Poznan Supercomputing and Networking Center	Address space for Adam Mickiewicz University	52.4167	16.9667

- Whois – narzędzie umożliwiające dostarczenie takich informacji jak dane o serwerach DNS, adresy IP, daty związane z utworzeniem lub modyfikacją, jak również dane kontaktowe i adresowe:

```
golter@UbuntuBOT:~$ whois amu.edu.pl

DOMAIN NAME:          amu.edu.pl
registrant type:      organization
nameservers:          dns.amu.edu.pl. [150.254.65.21]
                     dns2.amu.edu.pl. [150.254.65.22]
                     dns3.amu.edu.pl. [164.132.111.99]
created:              1995.01.01 12:00:00
last modified:        2017.10.18 16:59:00
renewal date:         2017.12.31 13:00:00

no option

dnssec:               Unsigned

REGISTRAR:
home.pl S.A.
ul. Zbożowa 4
70-653 Szczecin
Polska/Poland
+48.914325555
+48.504502500
https://home.pl/kontakt

WHOIS database responses: http://www.dns.pl/english/opiskomunikatow_en.html

WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry system
Registrant data available at http://dns.pl/cgi-bin/en_whois.pl
```

Po odpytaniu pierwszego z wyszukanych serwerów DNS:

```
golter@UbuntuBOT:~$ whois 150.254.65.21
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '150.254.65.0 - 150.254.65.255'

% Abuse contact for '150.254.65.0 - 150.254.65.255' is 'cert@man.poznan.pl'

inetnum:          150.254.65.0 - 150.254.65.255
netname:          POZMAN-EDU-150-254-065-000-24
descr:            Address space for Adam Mickiewicz University
country:          PL
admin-c:          PS2748-RIPE
admin-c:          BG1740-RIPE
tech-c:           TJ215-RIPE
status:           LEGACY
remarks:          For information on "status:" attribute read https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources
mnt-by:           AS8364-MNT
created:          1970-01-01T00:00:00Z
last-modified:    2014-05-27T13:23:27Z
source:           RIPE # Filtered
```

```

person:      Bartosz Gajda
address:     patrz uwagi w polu remakrs
address:     zanim do mnie napiszesz!
phone:       +48 61 8582017
phone:       +48 61 8582015
fax-no:      +48 61 8525954
remarks:     *****
remarks:     *
remarks:     * UWAGA!!!
remarks:     * Naruszenia dot. bezpieczeństwa, spamu,
remarks:     * oficjalne pisma i zgłoszenia w ww. sprawach
remarks:     * należy kierować wyłącznie na adres:
remarks:     *
remarks:     * PIONIER-CERT
remarks:     * Poznańskie Centrum Superkomputerowo-Sieciowe
remarks:     * ul. Z. Noskowskiego 10
remarks:     * 61-704 Poznań
remarks:     *
remarks:     * więcej informacji: http://cert.pionier.gov.pl
remarks:     *
remarks:     * *****
remarks:     *
remarks:     * ATTENTION !!!
remarks:     * abuse, spam and security reports
remarks:     * please send only to: cert@pionier.gov.pl
remarks:     * for more information please
remarks:     * visit http://cert.pionier.gov.pl
remarks:     *
remarks:     * *****
nic-hdl:     BG1740-RIPE
remarks:     GPG-Key: PGPKEY-FE887211
mnt-by:      POZMAN-EDU-AS-MNT
created:     2002-09-10T09:39:46Z
last-modified: 2017-10-30T21:44:53Z
source:      RIPE # Filtered

```

```

person:      Przemysław Stolarski
address:     ul. Umultowska 89A
address:     61-614 Poznań
address:     Poland
phone:       +48 61 8292662
fax-no:      +48 61 8292669
nic-hdl:     PS2748-RIPE
mnt-by:      AS8364-MNT
created:     1970-01-01T00:00:00Z
last-modified: 2011-07-07T12:02:05Z
source:      RIPE # Filtered

person:      Tomasz Jablonski
address:     Poznań Supercomputing and Networking Center
address:     ul. Z. Noskowskiego 10
address:     61-704 Poznań
address:     Poland
phone:       +48 61 8582035
phone:       +48 61 8582034
fax-no:      +48 61 8525954
nic-hdl:     TJ215-RIPE
remarks:     GPG-Key: PGPKEY-21908B0A
mnt-by:      POZMAN-EDU-AS-MNT
created:     1970-01-01T00:00:00Z
last-modified: 2009-11-19T15:27:41Z
source:      RIPE # Filtered

% Information related to '150.254.0.0/16AS9112'

route:       150.254.0.0/16
descr:       POZMAN-EDU-980508
origin:      AS9112
remarks:     abuse, spam and security reports
remarks:     please send to: cert@pionier.gov.pl
remarks:     for more information please
remarks:     visit http://cert.pionier.gov.pl
mnt-by:      POZMAN-EDU-AS-MNT
created:     2002-02-21T11:36:05Z
last-modified: 2006-02-07T13:31:34Z
source:      RIPE

```

- The Harvester – narzędzie pozwalające na masowe zbieranie adresów e-mail, nazw użytkowników oraz hostów związanych z interesującą domeną. Dane te są wyszukiwane na podstawie publicznych źródeł, takich jak przeglądarki, serwery PGP, czy serwis LinkedIn. Za jego pomocą udało się uzyskać około 150 adresów email i wiele nazw hostów związanych z UAM.

```

golter@UbuntuBOT: /opt/theHarvester/trunk$ python theHarvester.py -d amu.edu.pl -b all
*****
*
*  THE HARVESTER  *
*  THE HARVESTER  *
*
* TheHarvester Ver. 2.7.1
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Full harvest..
[-] Searching in Google..
    Searching 0 results...
    Searching 100 results...
[-] Searching in PGP Key server..
200
OK
[-] Searching in Netcraft server..
    Searching Netcraft results..
[-] Searching in CRTSH server..
    Searching CRT.sh results..
[-] Searching in Virustotal server..
    Searching CRT.sh results..
[-] Searching in Bing..
    Searching 50 results...
    Searching 100 results...
[-] Searching in Exalead..
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...

```

Ireneusz.Kownacki@amu.edu.pl
Krystyna_Sypniewska@wmid.amu.edu.pl
Maciej_Broda@wmid.amu.edu.pl
Renata_Pawlak@wmid.amu.edu.pl
acdc@venus.amu.edu.pl
am86@st.amu.edu.pl
anglistyka@wa.amu.edu.pl
apiet@amu.edu.pl
aratonim@math117.mathd.amu.edu.pl
astagor@math117.mathd.amu.edu.pl
bap@amu.edu.pl
bark@amu.edu.pl
bikol@wmid.amu.edu.pl
bk31962@st.amu.edu.pl
bnogas@amu.edu.pl
bogi@venus.amu.edu.pl
calisto@venus.amu.edu.pl
camillos@amu.edu.pl
d111282@atos.amu.edu.pl
d329419@poczta.st.amu.edu.pl
d329419@poczta.wmid.amu.edu.pl
d329519@wmid.amu.edu.pl
d_szeluga@hoth.amu.edu.pl
damdud@st.amu.edu.pl
danlis@venus.wmid.amu.edu.pl
dorota@math.amu.edu.pl
dw47902@st.amu.edu.pl

150.254.65.40:rejestracja.amu.edu.pl
150.254.65.79:rekrutacja.amu.edu.pl
150.254.65.110:reporting.amu.edu.pl
150.254.65.83:repozytorium.amu.edu.pl
150.254.65.44:rience2.amu.edu.pl
150.254.65.42:rkn.amu.edu.pl
150.254.65.177:rzym.amu.edu.pl
150.254.65.42:schoolpl.amu.edu.pl
150.254.65.178:simplesamlphp.amu.edu.pl
150.254.65.253:siw.amu.edu.pl
150.254.65.253:sj.amu.edu.pl
91.185.185.73:sknf.fizyka.amu.edu.pl
150.254.65.67:smtp.amu.edu.pl
150.254.65.42:snjo.amu.edu.pl
150.254.65.177:socjologia.amu.edu.pl
150.254.65.177:sons.amu.edu.pl
150.254.65.53:sp.amu.edu.pl
150.254.65.177:sp9.home.amu.edu.pl
150.254.65.177:spacer.amu.edu.pl
150.254.78.114:spire.wmi.amu.edu.pl
150.254.65.42:spktjn.amu.edu.pl
150.254.65.178:srs.amu.edu.pl
150.254.65.110:st.amu.edu.pl
150.254.65.253:starter.amu.edu.pl
150.254.65.177:stasim.home.amu.edu.pl
150.254.65.253:stowarzyszenieabsolwentow.amu.edu.pl
150.254.65.253:studenci.amu.edu.pl
150.254.65.67:sun.amu.edu.pl
150.254.65.126:sun.st.amu.edu.pl
150.254.65.177:swfis.amu.edu.pl
150.254.65.177:swfis.home.amu.edu.pl
150.254.65.253:teologia.amu.edu.pl
150.254.65.189:testyjezykowe.amu.edu.pl
150.254.65.253:transferkompetencji.amu.edu.pl

- Netcraft – uzyskane informacje o witrynie UAM znajdują się poniżej. Zawierają one m.in. wiadomości o pełnym tytule strony, dacie pierwszego ‘kontaktu’ ze stroną, języku, adresie IP i wiele innych. Wartym uwagi jest wskazana wartość „Netcraft Risk Rating”, która osiąga wysoką, negatywną wartość, ocenioną na 7 punktów w tej skali.

Background

Site title	Portal UAM - Strona główna Uniwersytetu Adama Mickiewicza w Poznaniu	Date first seen	August 1995
Site rank		Primary language	Polish
Description	Not Present		
Keywords	Not Present		

Network

Site	http://amu.edu.pl	Netblock Owner	Address space for Adam Mickiewicz University
Domain	amu.edu.pl	Nameserver	dns.amu.edu.pl
IP address	150.254.65.253	DNS admin	dnsadm@amu.edu.pl
IPv6 address	Not Present	Reverse DNS	matrixprod.amu.edu.pl
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	amu.edu.pl
Top Level Domain	Poland (.edu.pl)	DNS Security Extensions	unknown
Hosting country	PL		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Address space for Adam Mickiewicz University	150.254.65.253	Linux	nginx/1.8.0	1-Nov-2016	
Address space for Adam Mickiewicz University	150.254.65.187	Linux	Apache/2.2.22 Linux/SUSE	25-Oct-2015	
Address space for Adam Mickiewicz University	150.254.65.187	Linux	Apache/2.2.10 Linux/SUSE	14-Oct-2012	
Address space for Adam Mickiewicz University	150.254.65.187	unknown	Apache/2.2.10 Linux/SUSE	25-Jun-2012	
Address space for Adam Mickiewicz University	150.254.65.187	Linux	Apache/2.2.10 Linux/SUSE	26-Feb-2011	
Address space for Adam Mickiewicz University	150.254.65.53	Linux	Apache/2.2.3 Linux/SUSE	5-Nov-2007	

Security

Netcraft Risk Rating [FAQ]	7/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

- Shodan – narzędzie odpowiedzialne za wyszukiwanie i identyfikację hostów (komputery, serwery, routery, itd.). Uzyskuje o nich wiedzę, poprzez skanowanie portów – permanentne przeszukiwanie kolejnych zakresów adresów IP i indeksowanie zawartości wyłuskanych w ten sposób banerów.

150.254.67.215
uamfilm.amu.edu.pl
Institute of Bioorganic Chemistry Polish Academy of Sciences
Added on 2017-10-08 03:52:31 GMT
Poland, Poznan
[Details](#)

```
HTTP/1.1 403 Forbidden
Date: Sun, 08 Oct 2017 03:52:27 GMT
Server: Apache
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
Content-Language: en
```


```
1e
<?xml version="1.0" encoding="
a
ISO-8859-1
a8
"?>
<!D...
```

150.254.65.148

solusos-h1.oi.amu.edu.pl

Institute of Bioorganic Chemistry Polish Academy o

Added on 2017-10-05 17:50:02 GMT

 Poland, Poznan

[Details](#)


```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administr...
```

150.254.65.111

mx2.amu.edu.pl

Institute of Bioorganic Chemistry Polish Academy o

Added on 2017-10-04 22:26:09 GMT

 Poland, Poznan

[Details](#)

```
220-Are you a bot ( or not )?
250-mx2.amu.edu.pl
250-SIZE 512000000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

- Archiwalna wersja strony z 1997 roku, zawierające dane osób pracujących w tych latach na profilowanej uczelni.

INTERNET ARCHIVE
Wayback Machine

<http://www.amu.edu.pl/80/> Go JAN FEB 25 MAY 1997 1998
1,229 captures
25 Feb 1997 - 25 Oct 2017

UNIWERSYTET ADAMA MICKIEWICZA

STRUKTURA

- wydziały
- władze
- ośrodki
- instytuty
- inne jednostki
- organizacyjne
- obiekty

NAUKA

- konferencje
- programy
- badawcze

DYDAKTYKA

- rekrutacja
- doręczy
- studenckie

ENGLISH

WŁADZE

Rektor
prof. dr hab. Stefan Jurga

tel.: (+48 61) 526425, 536251 ext. 392, 308
fax: (+48 61) 536711
e-mail: rectorof@vm.amu.edu.pl



Collegium Minus

Prorektor d/s Nauki i współpracy z Zagranicą
prof. dr hab. Marek Kreglewski

tel.: (+48 61) 536835, 536251 ext. 367, 307
fax: (+48 61) 536711
e-mail: mkreg@rovib.amu.edu.pl

Prorektor d/s Nauczycieli Akademickich
prof. dr hab. Stanisław Lorenc

tel.: (+48 61) 536835, 536251 ext. 367, 307
fax: (+48 61) 536711
e-mail: rectorof@vm.amu.edu.pl

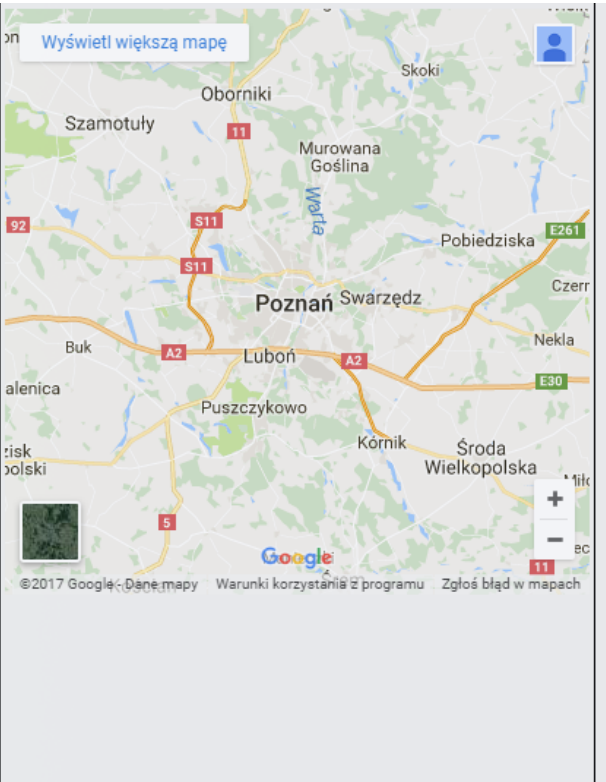
Prorektor d/s Studenckich
prof. dr hab. Joachim Cieślak

tel.: (+48 61) 536835, 536251 ext. 367, 307
fax: (+48 61) 536711
e-mail: cieślak@hum.amu.edu.pl

Poznańskie Zasoby Słowne Szukajcie Informacji AMU-NET Informator Poznański Polskie Serwery WWW

- Ipv4info.com – informacje o witrynie, zawierające m.in. nazwę hosta, web server, czy lokalizację:

IP address << 150.254.65.253 >>	
Block start	150.254.65.0
End of block	150.254.65.255
Block size	256 Domains in block
Block name	POZMAN-EDU-150-254-065-000-24
AS number	9112
Parent block	150.254.0.0 - 150.254.255.255
Organization	Address space for Adam Mickiewicz University
City	Poznań
Region/State	Wielkopolskie
Country	PL , Poland
Host name	matrixprod.amu.edu.pl
Web server	nginx/1.8.0
Domain count	>= 59 Servers around
Domains	<ol style="list-style-type: none"> absolwenci.amu.edu.pl amu.edu.pl biois.amu.edu.pl bip.amu.edu.pl biurokarier.amu.edu.pl brik.amu.edu.pl chemia.amu.edu.pl doktoranci.amu.edu.pl



- Dyrektywy google
Niestety za ich pomocą nie udało uzyskać się nr telefonów, bądź nr PESEL studentów. Poniżej znajdują się przykładowe wyniki wyszukiwań:

➤ +48 site:amu.edu.pl

INTERNATIONAL OFFICE

AMU International Office

Collegium Minus

ul. H. Wieniawskiego 1

61-712 Poznań, Poland

Room 211

Head: **Ms Małgorzata Więckowska-Frąckiewicz**

e-mail: gosiafr@amu.edu.pl

Phone: +48 61 8294435+48 61 8294435

Fax: +48 61 8294406

e-mail: dwzuam@amu.edu.pl

Genral enquiries about full degree programmes, pre-study English language courses, and **AMU-PIE** (A YEAR AT AMU)

Ms Karolina Choczaj

Phone: +48 61 8294385+48 61 8294385

e-mail: Karolina.Choczaj@amu.edu.pl

- [site.amu.edu.pl intext:wyniki](http://site.amu.edu.pl/intext:wyniki) (algebra nie poszła najlepiej ☹)

studenci_06-DALILIO_g15_2016-11-29

indeks	Zad. 1.	Zad. 2.	Zad. 3.	Zad. 4.	Zad. 5.	Suma	Ocena
426123	10	0	10	0	2	22	3.0
426126	10	0	10	1	8	29	3.0
426128	3	0	10	5	3	21	3.0
426140	3	0	10	0	6	19	3.0
416232	10	0	10	3	3	26	3.0
426145	10	3	10	4	3	30	3.0
426146	0	0	8	0	0	8	2.0
430683	10	0	10	6	3	29	3.0
426158	6	3	10	0	0	19	3.0
426189	10	0	0	0	0	10	2.0
426195	0	0	5	0	0	5	2.0
426197	0	0	0	0	0	0	2.0
426198	3	0	5	0	0	8	2.0
426207	3	0	5	1	2	11	2.0
430694	3	0	7	1	3	14	2.0

Zakwalifikowani do programu MOST (mała część listy osób):

Program MOST 2013/2014 – kwalifikacja na semestr zimowy oraz cały rok akademicki

	IMIĘ	NAZWISKO	UCZ. MACIERZ	UCZ. PRZYJM	STUDIA_NAZWA	OKRES
1.	Honorata	Brzuchala	KUL	UWR	Prawo, studia jednolite magisterskie, stacjonarne	rok akademicki
2.	Michał	Dzierżak	KUL	UWR	Dziennikarstwo i komunikacja społeczna, studia II stopnia, stacjonarne Kulturoznawstwo, studia II stopnia, stacjonarne	semestr zimowy
3.	Natalia	Galecka	KUL	UG	Psychologia, studia jednolite magisterskie, stacjonarne	rok akademicki
4.	Paweł	Gawryszczak	KUL	UJ	sociologia, studia II stopnia, stacjonarne	semestr zimowy
5.	Klaudia	Hadala	KUL	UJ	prawo, studia jednolite magisterskie	rok akademicki
6.	Edyta	Ilczuk	KUL	UW	Ekonomia - Wydział Nauk Ekonomicznych, studia I stopnia, stacjonarne	rok akademicki
7.	Marek	Klupczyński	KUL	UAM	prawo, studia jednolite magisterskie, stacjonarne	rok akademicki
8.	Sofiya	Kostyuk	KUL	UJ	sociologia, studia II stopnia, stacjonarne	semestr zimowy
9.	Iryna	Maksymova	KUL	UPJPII	dziennikarstwo i komunikacja społeczna, studia I stopnia, stacjonarne	semestr zimowy
10.	Kamil	Mazurek	KUL	UJ	historia, studia II stopnia, stacjonarne	semestr zimowy
11.	Filip	Pastuszka	KUL	UG	Psychologia, studia jednolite magisterskie, stacjonarne	rok akademicki

- [site.amu.edu.pl intext:lista](http://site.amu.edu.pl/intext:lista) studentów

Fragment listy przyjętych na filologię angielską

Lp	Nazwisko	Imię
1	Adamczyk	Julita Anna
2	Adamski	Paweł Zygmunt
3	Andrzejewski	Piotr Michał
4	Aperliński	Grzegorz Ryszard
5	Banach	Katarzyna Barbara
6	Baranowska	Katarzyna Maria
7	Barański	Marcin Łukasz
8	Bartkowiak	Barbara
9	Bartlewska	Aleksandra Elżbieta
10	Ben Amer	Sara Stella

➤ site:amu.edu.pl inurl:robots.txt

```
User-agent: *  
Disallow: /admin/  
Disallow: /edycja/  
Disallow: /_admin/  
Disallow: /_edit/  
Disallow: /enold/  
Disallow: /francuski/  
Disallow: /aktualnosci/proponowane-na-glowna/  
Disallow: /aktualnosci/kosz-na-glowna/  
Disallow: /wf/  
Disallow: /erasmus-old/  
Disallow: /dzialalnosc/o-uam/wladze/2016-2020/
```

Część druga – skanowanie i analiza metadanych

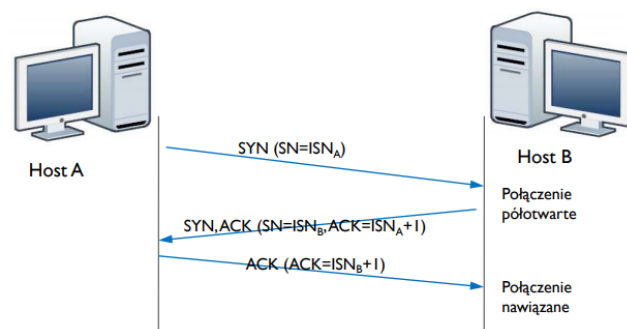
Skanowanie i wykrywanie systemu operacyjnego – nMap

- Skanowanie TCP

```
Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 10.0.2.2
Host is up (0.00034s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7B:88:FA

Nmap done: 1 IP address (1 host)
```

- Inicjowanie połączenia (flaga SYN)
- Zgoda na połączenie (flagi SYN i ACK)
- Potwierdzenie (flaga ACK)



Jak widać na poniższym zrzucie z Wiresharka, port 80 jest otwarty (potwierdza to wynik z nmap'a).

Występuje sytuacja analogiczna do tej, przedstawionej na ilustracji.

10.0.2.3 jest adresem maszyny z Kali Linuxem, natomiast 10.0.2.2 to host Metasploitable.

Najpierw Kali wysyła do Meta pakiet z flagą SYN (następuje zainicjowanie połączenia). Następnie Meta odsyła SYN ACK (zgoda na połączenie), aby ostatecznie Kali wysłał ACK (stanowiące potwierdzenie).

	Time	Source	Destination	Proto	Length	Info	des port	src port
✓	7	17.946118270	10.0.2.3	10.0.2.2	TCP	74 48006 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1...	80	48006
	8	17.946291540	10.0.2.3	10.0.2.2	TCP	74 58822 → 139 [SYN] Seq=0 Win=29200 Len=0 MSS=...	139	58822
	9	17.946410673	10.0.2.3	10.0.2.2	TCP	74 33102 → 995 [SYN] Seq=0 Win=29200 Len=0 MSS=...	995	33102
	10	17.946511836	10.0.2.3	10.0.2.2	TCP	74 43632 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1...	23	43632
✓	11	17.946586223	10.0.2.2	10.0.2.3	TCP	74 80 → 48006 [SYN, ACK] Seq=0 Ack=1 Win=5792 L...	48006	80
✓	12	17.946610644	10.0.2.3	10.0.2.2	TCP	66 48006 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0...	80	48006
	13	17.946633589	10.0.2.2	10.0.2.3	TCP	74 139 → 58822 [SYN, ACK] Seq=0 Ack=1 Win=5792 ...	58822	139
	14	17.946641952	10.0.2.3	10.0.2.2	TCP	66 58822 → 139 [ACK] Seq=1 Ack=1 Win=29312 Len=...	139	58822
	15	17.946660033	10.0.2.2	10.0.2.3	TCP	60 995 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=...	33102	995
	16	17.946774755	10.0.2.3	10.0.2.2	TCP	74 42794 → 111 [SYN] Seq=0 Win=29200 Len=0 MSS=...	111	42794
	17	17.946918174	10.0.2.2	10.0.2.3	TCP	74 23 → 43632 [SYN, ACK] Seq=0 Ack=1 Win=5792 L...	43632	23
	18	17.946934714	10.0.2.3	10.0.2.2	TCP	66 43632 → 23 [ACK] Seq=1 Ack=1 Win=29312 Len=0...	23	43632
	19	17.947118323	10.0.2.3	10.0.2.2	TCP	74 48070 → 8888 [SYN] Seq=0 Win=29200 Len=0 MSS=...	8888	48070
	20	17.947230360	10.0.2.2	10.0.2.3	TCP	74 111 → 42794 [SYN, ACK] Seq=0 Ack=1 Win=5792 ...	42794	111
	21	17.947246159	10.0.2.3	10.0.2.2	TCP	66 42794 → 111 [ACK] Seq=1 Ack=1 Win=29312 Len=...	111	42794
	22	17.947478223	10.0.2.3	10.0.2.2	TCP	74 37808 → 587 [SYN] Seq=0 Win=29200 Len=0 MSS=...	587	37808
	23	17.947551851	10.0.2.2	10.0.2.3	TCP	60 8888 → 48070 [RST, ACK] Seq=1 Ack=1 Win=0 Le...	48070	8888
	24	17.947722921	10.0.2.2	10.0.2.3	TCP	60 587 → 37808 [RST, ACK] Seq=1 Ack=1 Win=0 Len=...	37808	587
	25	17.947791948	10.0.2.3	10.0.2.2	TCP	74 48462 → 53 [SYN] Seq=0 Win=29200 Len=0 MSS=1...	53	48462

- Skanowanie stealth

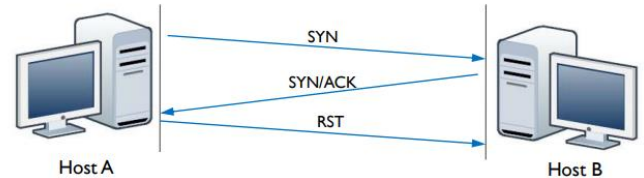
```
Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 10.0.2.2
Host is up (0.000084s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7B:88:FA
Nmap done: 1 IP address (1 host)
```

Klient wysyła do serwera pakiet z flagą SYN

▶ Jeżeli port jest otwarty serwer odpowiada pakietem z flagą SYN i ACK (normalna procedura nawiązania połączenia)

▶ Wtedy klient wysyła pakiet z flagą RST, aby przerwać fazę nawiązywania połączenia

▶ Jeżeli port jest zamknięty serwer odpowiada datagramem z flagą RST, lub nie odpowiada



Widzimy poniżej, że port 80 jest otwarty, występuje sytuacja opisana i zilustrowana powyżej – najpierw wysłanie pakietu z flagą SYN, następnie odpowiedź od portu 34830 SYN i ACK, a następnie RST od klienta w celu przerwania nawiązywania połączenia.

No.	Time	Source	Destination	Proto	Length	Info	dest port	src port
✓ 28	44.268189086	10.0.2.3	10.0.2.2	TCP	58	34830 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS...	80	34830
29	44.268281810	10.0.2.3	10.0.2.2	TCP	58	34830 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS...	110	34830
30	44.268369518	10.0.2.3	10.0.2.2	TCP	58	34830 → 1025 [SYN] Seq=0 Win=1024 Len=0 M...	1025	34830
31	44.268437393	10.0.2.2	10.0.2.3	TCP	60	25 → 34830 [SYN, ACK] Seq=0 Ack=1 Win=584...	34830	25
32	44.268458893	10.0.2.3	10.0.2.2	TCP	54	34830 → 25 [RST] Seq=1 Win=0 Len=0	25	34830
✓ 33	44.268482744	10.0.2.2	10.0.2.3	TCP	60	80 → 34830 [SYN, ACK] Seq=0 Ack=1 Win=584...	34830	80
✓ 34	44.268489226	10.0.2.3	10.0.2.2	TCP	54	34830 → 80 [RST] Seq=1 Win=0 Len=0	80	34830
35	44.268508310	10.0.2.2	10.0.2.3	TCP	60	110 → 34830 [RST, ACK] Seq=1 Ack=1 Win=0 ...	34830	110
36	44.268600168	10.0.2.3	10.0.2.2	TCP	58	34830 → 143 [SYN] Seq=0 Win=1024 Len=0 MS...	143	34830
37	44.268719570	10.0.2.2	10.0.2.3	TCP	60	1025 → 34830 [RST, ACK] Seq=1 Ack=1 Win=0...	34830	1025
38	44.268794636	10.0.2.3	10.0.2.2	TCP	58	34830 → 993 [SYN] Seq=0 Win=1024 Len=0 MS...	993	34830
39	44.268906152	10.0.2.2	10.0.2.3	TCP	60	143 → 34830 [RST, ACK] Seq=1 Ack=1 Win=0 ...	34830	143
40	44.268978741	10.0.2.3	10.0.2.2	TCP	58	34830 → 139 [SYN] Seq=0 Win=1024 Len=0 MS...	139	34830
41	44.269060960	10.0.2.2	10.0.2.3	TCP	60	993 → 34830 [RST, ACK] Seq=1 Ack=1 Win=0 ...	34830	993
42	44.269133869	10.0.2.3	10.0.2.2	TCP	58	34830 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS...	53	34830
43	44.269231592	10.0.2.2	10.0.2.3	TCP	60	139 → 34830 [SYN, ACK] Seq=0 Ack=1 Win=58...	34830	139
44	44.269243191	10.0.2.3	10.0.2.2	TCP	54	34830 → 139 [RST] Seq=1 Win=0 Len=0	139	34830
45	44.269332451	10.0.2.3	10.0.2.2	TCP	58	34830 → 5900 [SYN] Seq=0 Win=1024 Len=0 MS...	5900	34830
46	44.269435759	10.0.2.2	10.0.2.3	TCP	60	53 → 34830 [SYN, ACK] Seq=0 Ack=1 Win=584...	34830	53
47	44.269446429	10.0.2.3	10.0.2.2	TCP	54	34830 → 53 [RST] Seq=1 Win=0 Len=0	53	34830
48	44.269536380	10.0.2.3	10.0.2.2	TCP	58	34830 → 5900 [SYN] Seq=0 Win=1024 Len=0 M...	5900	34830
49	44.269639448	10.0.2.2	10.0.2.3	TCP	60	21 → 34830 [SYN, ACK] Seq=0 Ack=1 Win=584...	34830	21
50	44.269650516	10.0.2.3	10.0.2.2	TCP	54	34830 → 21 [RST] Seq=1 Win=0 Len=0	21	34830
51	44.269744135	10.0.2.3	10.0.2.2	TCP	58	34830 → 3389 [SYN] Seq=0 Win=1024 Len=0 M...	3389	34830
52	44.269879710	10.0.2.2	10.0.2.3	TCP	60	5900 → 34830 [SYN, ACK] Seq=0 Ack=1 Win=5...	34830	5900
53	44.269891630	10.0.2.3	10.0.2.2	TCP	54	34830 → 5900 [RST] Seq=1 Win=0 Len=0	5900	34830
54	44.269983436	10.0.2.3	10.0.2.2	TCP	58	34830 → 8888 [SYN] Seq=0 Win=1024 Len=0 M...	8888	34830
55	44.270114923	10.0.2.3	10.0.2.2	TCP	58	34830 → 111 [SYN] Seq=0 Win=1024 Len=0 MS...	111	34830

- Skanowanie wersji

```

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-02 21:49 CET
Nmap scan report for 10.0.2.2
Host is up (0.00013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7B:88:FA (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.80 seconds

```

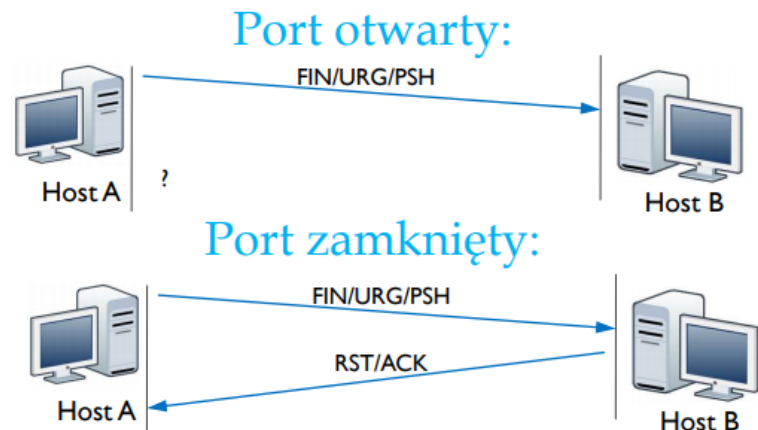
No.	Time	Source	Destination	Proto	Length	Info	des port	src port
40	14.307167321	10.0.2.2	10.0.2.3	TCP	60	8888 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0...	35529	8888
41	14.307180753	10.0.2.2	10.0.2.3	TCP	60	143 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0 ...	35529	143
42	14.307181628	10.0.2.2	10.0.2.3	TCP	60	1025 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0...	35529	1025
43	14.307182511	10.0.2.2	10.0.2.3	TCP	60	443 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0 ...	35529	443
44	14.307183317	10.0.2.2	10.0.2.3	TCP	60	995 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0 ...	35529	995
45	14.307216388	10.0.2.3	10.0.2.2	TCP	58	35529 → 199 [SYN] Seq=0 Win=1024 Len=0 MS...	199	35529
46	14.307270612	10.0.2.2	10.0.2.3	TCP	60	113 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0 ...	35529	113
47	14.307313238	10.0.2.3	10.0.2.2	TCP	58	35529 → 554 [SYN] Seq=0 Win=1024 Len=0 MS...	554	35529
48	14.307370696	10.0.2.2	10.0.2.3	TCP	60	199 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0 ...	35529	199
49	14.307386310	10.0.2.3	10.0.2.2	TCP	58	35529 → 3306 [SYN] Seq=0 Win=1024 Len=0 M...	3306	35529
50	14.307426115	10.0.2.3	10.0.2.2	TCP	58	35529 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS...	80	35529
51	14.307455345	10.0.2.2	10.0.2.3	TCP	60	554 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0 ...	35529	554
52	14.307484312	10.0.2.3	10.0.2.2	TCP	58	35529 → 5900 [SYN] Seq=0 Win=1024 Len=0 M...	5900	35529
53	14.307559397	10.0.2.2	10.0.2.3	TCP	60	3306 → 35529 [SYN, ACK] Seq=0 Ack=1 Win=5...	35529	3306
54	14.307562362	10.0.2.3	10.0.2.2	TCP	54	35529 → 3306 [RST] Seq=1 Win=0 Len=0	3306	35529
55	14.307568085	10.0.2.2	10.0.2.3	TCP	60	80 → 35529 [SYN, ACK] Seq=0 Ack=1 Win=584...	35529	80
56	14.307569490	10.0.2.3	10.0.2.2	TCP	54	35529 → 80 [RST] Seq=1 Win=0 Len=0	80	35529
57	14.307586630	10.0.2.3	10.0.2.2	TCP	58	35529 → 445 [SYN] Seq=0 Win=1024 Len=0 MS...	445	35529
58	14.307638274	10.0.2.2	10.0.2.3	TCP	60	5900 → 35529 [SYN, ACK] Seq=0 Ack=1 Win=5...	35529	5900
59	14.307640562	10.0.2.3	10.0.2.2	TCP	54	35529 → 5900 [RST] Seq=1 Win=0 Len=0	5900	35529
60	14.307690660	10.0.2.3	10.0.2.2	TCP	58	35529 → 111 [SYN] Seq=0 Win=1024 Len=0 MS...	111	35529
61	14.307763220	10.0.2.3	10.0.2.2	TCP	58	35529 → 1720 [SYN] Seq=0 Win=1024 Len=0 M...	1720	35529
62	14.307818401	10.0.2.2	10.0.2.3	TCP	60	445 → 35529 [SYN, ACK] Seq=0 Ack=1 Win=58...	35529	445
63	14.307820592	10.0.2.3	10.0.2.2	TCP	54	35529 → 445 [RST] Seq=1 Win=0 Len=0	445	35529
64	14.307825718	10.0.2.2	10.0.2.3	TCP	60	111 → 35529 [SYN, ACK] Seq=0 Ack=1 Win=58...	35529	111
65	14.307827040	10.0.2.3	10.0.2.2	TCP	54	35529 → 111 [RST] Seq=1 Win=0 Len=0	111	35529
66	14.307871143	10.0.2.3	10.0.2.2	TCP	58	35529 → 993 [SYN] Seq=0 Win=1024 Len=0 MS...	993	35529
67	14.307921289	10.0.2.2	10.0.2.3	TCP	60	1720 → 35529 [RST, ACK] Seq=1 Ack=1 Win=0...	35529	1720

W przypadku tego skanowania, możemy uzyskać wiedzę na temat wersji systemu dla danego portu.

- Skanowanie Xmas

```
Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 10.0.2.2
Host is up (0.00044s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:7B:88:FA (Oracle VM VirtualBox)

Nmap done: 1 IP address (1 host up)
```



Zaznaczone na poniższym screen'ie logi potwierdzają powyższy rysunek – port 22 jest otwarty, natomiast port 1025 zamknięty.

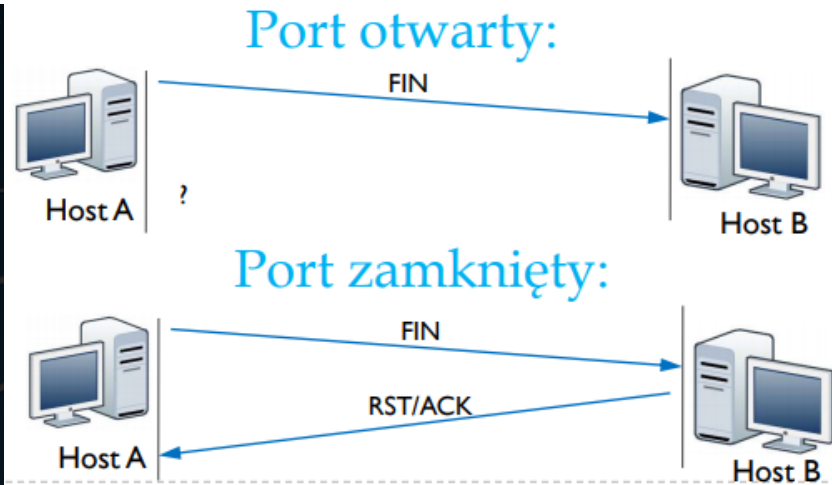


No.	Time	Source	Destination	Proto	Length	Info	des port	src port
1	0.000000000	PcsCompu...	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.3		
2	0.000378943	PcsCompu...	PcsCompu...	ARP	60	10.0.2.2 is at 08:00:27:7b:88:fa		
3	0.200540447	PcsCompu...	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.3		
4	0.201101958	PcsCompu...	PcsCompu...	ARP	60	10.0.2.2 is at 08:00:27:7b:88:fa		
5	13.205701606	10.0.2.3	10.0.2.2	TCP	54	55808 → 445 [FIN, PSH, URG] Seq=1 Win=102...	445	55808
6	13.205864782	10.0.2.3	10.0.2.2	TCP	54	55808 → 587 [FIN, PSH, URG] Seq=1 Win=102...	587	55808
7	13.205958206	10.0.2.3	10.0.2.2	TCP	54	55808 → 443 [FIN, PSH, URG] Seq=1 Win=102...	443	55808
8	13.206045449	10.0.2.3	10.0.2.2	TCP	54	55808 → 25 [FIN, PSH, URG] Seq=1 Win=102...	25	55808
9	13.206226530	10.0.2.2	10.0.2.3	TCP	60	587 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0 ...	55808	587
10	13.206242657	10.0.2.2	10.0.2.3	TCP	60	443 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0 ...	55808	443
✓ 11	13.206349971	10.0.2.3	10.0.2.2	TCP	54	55808 → 22 [FIN, PSH, URG] Seq=1 Win=102...	22	55808
12	13.206452243	10.0.2.3	10.0.2.2	TCP	54	55808 → 554 [FIN, PSH, URG] Seq=1 Win=102...	554	55808
13	13.206538713	10.0.2.3	10.0.2.2	TCP	54	55808 → 110 [FIN, PSH, URG] Seq=1 Win=102...	110	55808
14	13.206621172	10.0.2.3	10.0.2.2	TCP	54	55808 → 135 [FIN, PSH, URG] Seq=1 Win=102...	135	55808
15	13.206691039	10.0.2.2	10.0.2.3	TCP	60	554 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0 ...	55808	554
16	13.206769715	10.0.2.3	10.0.2.2	TCP	54	55808 → 8888 [FIN, PSH, URG] Seq=1 Win=10...	8888	55808
17	13.206849414	10.0.2.2	10.0.2.3	TCP	60	110 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0 ...	55808	110
18	13.206855314	10.0.2.2	10.0.2.3	TCP	60	135 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0 ...	55808	135
19	13.206926428	10.0.2.3	10.0.2.2	TCP	54	55808 → 3389 [FIN, PSH, URG] Seq=1 Win=10...	3389	55808
20	13.207004205	10.0.2.2	10.0.2.3	TCP	60	8888 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0...	55808	8888
21	13.207204856	10.0.2.2	10.0.2.3	TCP	60	3389 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0...	55808	3389
22	14.307125922	10.0.2.3	10.0.2.2	TCP	54	55809 → 22 [FIN, PSH, URG] Seq=1 Win=102...	22	55809
23	14.307286506	10.0.2.3	10.0.2.2	TCP	54	55809 → 25 [FIN, PSH, URG] Seq=1 Win=102...	25	55809
24	14.307376537	10.0.2.3	10.0.2.2	TCP	54	55809 → 445 [FIN, PSH, URG] Seq=1 Win=102...	445	55809
✓ 25	14.307465993	10.0.2.3	10.0.2.2	TCP	54	55808 → 1025 [FIN, PSH, URG] Seq=1 Win=10...	1025	55808
26	14.307550880	10.0.2.3	10.0.2.2	TCP	54	55808 → 3306 [FIN, PSH, URG] Seq=1 Win=10...	3306	55808
27	14.307634799	10.0.2.3	10.0.2.2	TCP	54	55808 → 21 [FIN, PSH, URG] Seq=1 Win=102...	21	55808
✓ 28	14.307710214	10.0.2.2	10.0.2.3	TCP	60	1025 → 55808 [RST, ACK] Seq=1 Ack=2 Win=0...	55808	1025

- Skanowanie Fin

```
Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 10.0.2.2
Host is up (0.00052s latency).
Not shown: 977 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:7B:88:FA (Oracle VM VirtualBox)

Nmap done: 1 IP address (1 host up)
```



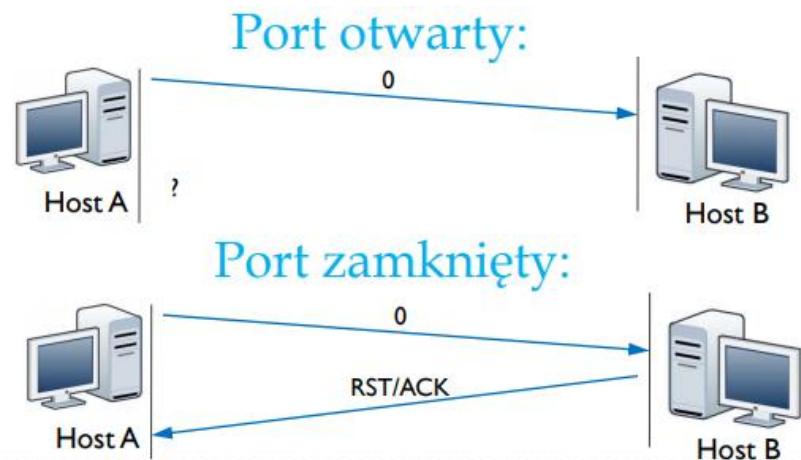
Zaznaczone na poniższym screen'ie logi potwierdzają powyższy rysunek – port 80 jest otwarty, natomiast port 9011 zamknięty.

No.	Time	Source	Destination	Proto	Length	Info	des port	src port
34	14.313268578	10.0.2.3	10.0.2.2	TCP	54	43071 → 53 [FIN] Seq=1 Win=1024 Len=0	53	43071
✓ 35	14.313289144	10.0.2.3	10.0.2.2	TCP	54	43071 → 80 [FIN] Seq=1 Win=1024 Len=0	80	43071
36	14.313308984	10.0.2.3	10.0.2.2	TCP	54	43071 → 25 [FIN] Seq=1 Win=1024 Len=0	25	43071
37	14.313329820	10.0.2.3	10.0.2.2	TCP	54	43071 → 111 [FIN] Seq=1 Win=1024 Len=0	111	43071
38	14.313349511	10.0.2.3	10.0.2.2	TCP	54	43071 → 22 [FIN] Seq=1 Win=1024 Len=0	22	43071
39	14.313370016	10.0.2.3	10.0.2.2	TCP	54	43071 → 113 [FIN] Seq=1 Win=1024 Len=0	113	43071
40	14.313390250	10.0.2.3	10.0.2.2	TCP	54	43071 → 21 [FIN] Seq=1 Win=1024 Len=0	21	43071
41	14.313410817	10.0.2.3	10.0.2.2	TCP	54	43071 → 1025 [FIN] Seq=1 Win=1024 Len=0	1025	43071
42	14.313431063	10.0.2.3	10.0.2.2	TCP	54	43071 → 993 [FIN] Seq=1 Win=1024 Len=0	993	43071
43	14.313451319	10.0.2.3	10.0.2.2	TCP	54	43071 → 256 [FIN] Seq=1 Win=1024 Len=0	256	43071
44	14.313471622	10.0.2.3	10.0.2.2	TCP	54	43071 → 443 [FIN] Seq=1 Win=1024 Len=0	443	43071
45	14.313491951	10.0.2.3	10.0.2.2	TCP	54	43071 → 9011 [FIN] Seq=1 Win=1024 Len=0	9011	43071
46	14.313559763	10.0.2.2	10.0.2.3	TCP	60	110 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	110
47	14.313562376	10.0.2.2	10.0.2.3	TCP	60	587 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	587
48	14.313563307	10.0.2.2	10.0.2.3	TCP	60	113 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	113
49	14.313564239	10.0.2.2	10.0.2.3	TCP	60	1025 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	1025
50	14.313565097	10.0.2.2	10.0.2.3	TCP	60	993 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	993
51	14.313566054	10.0.2.2	10.0.2.3	TCP	60	256 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	256
52	14.313566946	10.0.2.2	10.0.2.3	TCP	60	443 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	443
53	14.313567864	10.0.2.2	10.0.2.3	TCP	60	9011 → 43071 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43071	9011
✓ 54	14.414139067	10.0.2.3	10.0.2.2	TCP	54	43072 → 9011 [FIN] Seq=1 Win=1024 Len=0	9011	43072
55	14.414305214	10.0.2.3	10.0.2.2	TCP	54	43072 → 443 [FIN] Seq=1 Win=1024 Len=0	443	43072
56	14.414396787	10.0.2.3	10.0.2.2	TCP	54	43072 → 256 [FIN] Seq=1 Win=1024 Len=0	256	43072
57	14.414483385	10.0.2.3	10.0.2.2	TCP	54	43072 → 993 [FIN] Seq=1 Win=1024 Len=0	993	43072
✓ 58	14.414550049	10.0.2.2	10.0.2.3	TCP	60	9011 → 43072 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43072	9011
59	14.414563464	10.0.2.2	10.0.2.3	TCP	60	443 → 43072 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43072	443
60	14.414567376	10.0.2.2	10.0.2.3	TCP	60	256 → 43072 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43072	256
61	14.414570833	10.0.2.2	10.0.2.3	TCP	60	993 → 43072 [RST, ACK] Seq=1 Ack=2 Win=0 ...	43072	993

- Skanowanie Null

```
Starting Nmap 7.60 ( https://nmap.org )
Nmap scan report for 10.0.2.2
Host is up (0.00052s latency).
Not shown: 977 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:7B:88:FA (Oracle VM VirtualBox)

Nmap done: 1 IP address (1 host up)
```



Zaznaczone na poniższym screen'ie logi potwierdzają powyższy rysunek – port 80 jest otwarty, natomiast port 33220 zamknięty.

No.	Time	Source	Destination	Proto	Length	Info	des port	src port
13	13.205177942	10.0.2.2	10.0.2.3	TCP	60	1025 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0...	33220	1025
14	13.205181559	10.0.2.2	10.0.2.3	TCP	60	135 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0 ...	33220	135
15	13.205185584	10.0.2.2	10.0.2.3	TCP	60	113 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0 ...	33220	113
✓ 16	13.205279138	10.0.2.3	10.0.2.2	TCP	54	33220 → 1720 [<None>] Seq=1 Win=1024 Len=0	1720	33220
17	13.205413309	10.0.2.3	10.0.2.2	TCP	54	33220 → 995 [<None>] Seq=1 Win=1024 Len=0	995	33220
18	13.205503778	10.0.2.3	10.0.2.2	TCP	54	33220 → 3306 [<None>] Seq=1 Win=1024 Len=0	3306	33220
✓ 19	13.205572360	10.0.2.2	10.0.2.3	TCP	60	1720 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0...	33220	1720
20	13.205748754	10.0.2.2	10.0.2.3	TCP	60	995 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0 ...	33220	995
21	14.307170460	10.0.2.3	10.0.2.2	TCP	54	33221 → 3306 [<None>] Seq=1 Win=1024 Len=0	3306	33221
22	14.307327751	10.0.2.3	10.0.2.2	TCP	54	33221 → 139 [<None>] Seq=1 Win=1024 Len=0	139	33221
23	14.307418935	10.0.2.3	10.0.2.2	TCP	54	33221 → 21 [<None>] Seq=1 Win=1024 Len=0	21	33221
24	14.307509563	10.0.2.3	10.0.2.2	TCP	54	33221 → 53 [<None>] Seq=1 Win=1024 Len=0	53	33221
25	14.307600070	10.0.2.3	10.0.2.2	TCP	54	33220 → 22 [<None>] Seq=1 Win=1024 Len=0	22	33220
26	14.307688717	10.0.2.3	10.0.2.2	TCP	54	33220 → 3389 [<None>] Seq=1 Win=1024 Len=0	3389	33220
✓ 27	14.307776432	10.0.2.3	10.0.2.2	TCP	54	33220 → 80 [<None>] Seq=1 Win=1024 Len=0	80	33220
28	14.307848617	10.0.2.2	10.0.2.3	TCP	60	3389 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0...	33220	3389
29	14.307951295	10.0.2.3	10.0.2.2	TCP	54	33220 → 5900 [<None>] Seq=1 Win=1024 Len=0	5900	33220
30	14.308059791	10.0.2.3	10.0.2.2	TCP	54	33220 → 1723 [<None>] Seq=1 Win=1024 Len=0	1723	33220
31	14.308146268	10.0.2.3	10.0.2.2	TCP	54	33220 → 587 [<None>] Seq=1 Win=1024 Len=0	587	33220
32	14.308232573	10.0.2.3	10.0.2.2	TCP	54	33220 → 143 [<None>] Seq=1 Win=1024 Len=0	143	33220
33	14.308324481	10.0.2.3	10.0.2.2	TCP	54	33220 → 8080 [<None>] Seq=1 Win=1024 Len=0	8080	33220
34	14.308393498	10.0.2.2	10.0.2.3	TCP	60	1723 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0...	33220	1723
35	14.308400507	10.0.2.2	10.0.2.3	TCP	60	587 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0 ...	33220	587
36	14.308475924	10.0.2.3	10.0.2.2	TCP	54	33220 → 23 [<None>] Seq=1 Win=1024 Len=0	23	33220
37	14.308547656	10.0.2.2	10.0.2.3	TCP	60	143 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0 ...	33220	143
38	14.308553453	10.0.2.2	10.0.2.3	TCP	60	8080 → 33220 [RST, ACK] Seq=1 Ack=1 Win=0...	33220	8080
39	14.308627410	10.0.2.3	10.0.2.2	TCP	54	33220 → 25 [<None>] Seq=1 Win=1024 Len=0	25	33220
40	14.308758218	10.0.2.3	10.0.2.2	TCP	54	33220 → 993 [<None>] Seq=1 Win=1024 Len=0	993	33220

- Skanowanie Ack

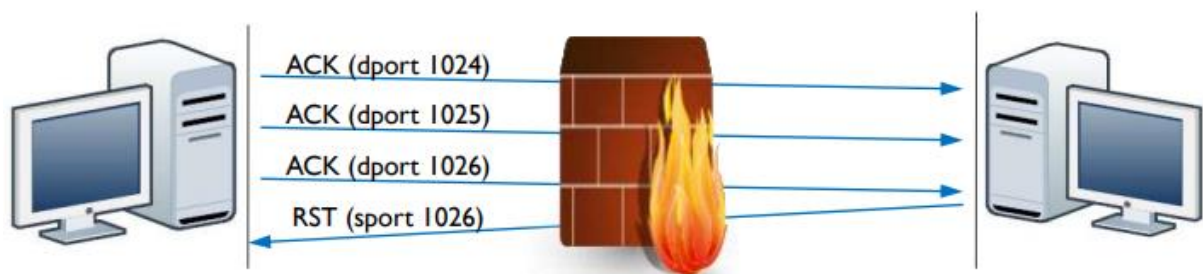
```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-02 22:19 CET
Nmap scan report for 10.0.2.2
Host is up (0.00051s latency).
All 5001 scanned ports on 10.0.2.2 are unfiltered
MAC Address: 08:00:27:7B:88:FA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 45.07 seconds
root@kali:~# nmap -sA 10.0.2.2 -p 16000-21000

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-02 22:20 CET
Nmap scan report for 10.0.2.2
Host is up (0.00019s latency).
All 5001 scanned ports on 10.0.2.2 are unfiltered
MAC Address: 08:00:27:7B:88:FA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.84 seconds
```

No.	Time	Source	Destination	Proto	Length	Info	des port	src port
13	41.893653788	10.0.2.2	10.0.2.3	TCP	60	8080 → 34092 [RST] Seq=1 Win=0 Len=0	34092	8080
14	41.893740643	10.0.2.3	10.0.2.2	TCP	54	34092 → 5631 [ACK] Seq=1 Ack=1 Win=1024 L...	5631	34092
15	41.893875393	10.0.2.3	10.0.2.2	TCP	54	34092 → 7687 [ACK] Seq=1 Ack=1 Win=1024 L...	7687	34092
16	41.893952106	10.0.2.2	10.0.2.3	TCP	60	8888 → 34092 [RST] Seq=1 Win=0 Len=0	34092	8888
17	41.893958699	10.0.2.2	10.0.2.3	TCP	60	5631 → 34092 [RST] Seq=1 Win=0 Len=0	34092	5631
18	41.894032413	10.0.2.3	10.0.2.2	TCP	54	34092 → 7630 [ACK] Seq=1 Ack=1 Win=1024 L...	7630	34092
19	41.894106804	10.0.2.2	10.0.2.3	TCP	60	7687 → 34092 [RST] Seq=1 Win=0 Len=0	34092	7687
20	41.894181204	10.0.2.3	10.0.2.2	TCP	54	34092 → 8391 [ACK] Seq=1 Ack=1 Win=1024 L...	8391	34092
21	41.894277757	10.0.2.2	10.0.2.3	TCP	60	7630 → 34092 [RST] Seq=1 Win=0 Len=0	34092	7630
22	41.894351756	10.0.2.3	10.0.2.2	TCP	54	34092 → 8978 [ACK] Seq=1 Ack=1 Win=1024 L...	8978	34092
23	41.894448562	10.0.2.2	10.0.2.3	TCP	60	8391 → 34092 [RST] Seq=1 Win=0 Len=0	34092	8391
24	41.894520521	10.0.2.3	10.0.2.2	TCP	54	34092 → 6005 [ACK] Seq=1 Ack=1 Win=1024 L...	6005	34092
25	41.894618390	10.0.2.2	10.0.2.3	TCP	60	8978 → 34092 [RST] Seq=1 Win=0 Len=0	34092	8978
26	41.894689358	10.0.2.3	10.0.2.2	TCP	54	34092 → 7216 [ACK] Seq=1 Ack=1 Win=1024 L...	7216	34092
27	41.894764179	10.0.2.2	10.0.2.3	TCP	60	6005 → 34092 [RST] Seq=1 Win=0 Len=0	34092	6005
28	41.894971737	10.0.2.2	10.0.2.3	TCP	60	7216 → 34092 [RST] Seq=1 Win=0 Len=0	34092	7216
29	42.995254354	10.0.2.3	10.0.2.2	TCP	54	34092 → 5522 [ACK] Seq=1 Ack=1 Win=1024 L...	5522	34092
30	42.995417690	10.0.2.3	10.0.2.2	TCP	54	34092 → 9505 [ACK] Seq=1 Ack=1 Win=1024 L...	9505	34092
31	42.995508900	10.0.2.3	10.0.2.2	TCP	54	34092 → 9859 [ACK] Seq=1 Ack=1 Win=1024 L...	9859	34092
32	42.995594336	10.0.2.3	10.0.2.2	TCP	54	34092 → 8857 [ACK] Seq=1 Ack=1 Win=1024 L...	8857	34092
33	42.995762911	10.0.2.2	10.0.2.3	TCP	60	5522 → 34092 [RST] Seq=1 Win=0 Len=0	34092	5522
34	42.995779199	10.0.2.2	10.0.2.3	TCP	60	9505 → 34092 [RST] Seq=1 Win=0 Len=0	34092	9505
35	42.995783003	10.0.2.2	10.0.2.3	TCP	60	9859 → 34092 [RST] Seq=1 Win=0 Len=0	34092	9859
36	42.995861429	10.0.2.3	10.0.2.2	TCP	54	34092 → 7964 [ACK] Seq=1 Ack=1 Win=1024 L...	7964	34092
37	42.995935812	10.0.2.2	10.0.2.3	TCP	60	8857 → 34092 [RST] Seq=1 Win=0 Len=0	34092	8857
38	42.996040535	10.0.2.3	10.0.2.2	TCP	54	34092 → 6866 [ACK] Seq=1 Ack=1 Win=1024 L...	6866	34092
39	42.996119211	10.0.2.2	10.0.2.3	TCP	60	7964 → 34092 [RST] Seq=1 Win=0 Len=0	34092	7964
40	42.996193282	10.0.2.3	10.0.2.2	TCP	54	34092 → 8207 [ACK] Seq=1 Ack=1 Win=1024 L...	8207	34092



Jak widać, otrzymujemy kolejne pakiety RST, będące odpowiedzią na wysłane pakiety z flagą ACK – porty niefiltrowane przez firewalla.

- Rozpoznawanie systemu

```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-02 22:26 CET
Nmap scan report for 10.0.2.2
Host is up (0.00036s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7B:88:FA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

13 13.206672405 10.0.2.2 10.0.2.3 TCP 60 80 → 40887 [SYN, ACK] Seq=0 Ack=1 W... 40887 80

✓ Time to live: 64
 Protocol: TCP (6)
 Header checksum: 0x22c8 [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.0.2.2
 Destination: 10.0.2.3
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 40887, Seq: 0, Ack: 1, Len: 0
 Source Port: 80
 Destination Port: 40887
 [Stream index: 3]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 0110 = Header Length: 24 bytes (6)
 ▶ Flags: 0x012 (SYN, ACK)
 ✓ Window size value: 5840

Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128

Jak widać, na podstawie wartości TTL oraz TCP WS, rozpoznany system to Linux.

- Skanowanie UDP

```
Nmap scan report for 10.0.2.2
Host is up (0.00038s latency).
All 501 scanned ports on 10.0.2.2 are closed
MAC Address: 08:00:27:7B:88:FA (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 553.65 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info	des port	src port
76	15.517163605	10.0.2.3	10.0.2.2	UDP	42	56276 → 10022 Len=0	10022	56276
77	15.517185134	10.0.2.3	10.0.2.2	UDP	42	56276 → 10272 Len=0	10272	56276
78	15.517208037	10.0.2.3	10.0.2.2	UDP	42	56276 → 10059 Len=0	10059	56276
79	15.517229508	10.0.2.3	10.0.2.2	UDP	42	56276 → 10493 Len=0	10493	56276
80	15.517250847	10.0.2.3	10.0.2.2	UDP	42	56276 → 10311 Len=0	10311	56276
81	15.517268127	10.0.2.2	10.0.2.3	ICMP	70	Destination unreachable (Port unrea...	10237	56276
82	15.617674076	10.0.2.3	10.0.2.2	SSL	109	Client Hello	10161	56285
83	15.617721650	10.0.2.3	10.0.2.2	UDP	42	56276 → 10197 Len=0	10197	56276
84	15.617743864	10.0.2.3	10.0.2.2	UDP	42	56276 → 10264 Len=0	10264	56276
85	15.617763367	10.0.2.3	10.0.2.2	UDP	42	56276 → 10457 Len=0	10457	56276
86	15.617782661	10.0.2.3	10.0.2.2	UDP	42	56276 → 10146 Len=0	10146	56276
87	15.617801801	10.0.2.3	10.0.2.2	UDP	42	56276 → 10458 Len=0	10458	56276
88	15.617821088	10.0.2.3	10.0.2.2	UDP	42	56276 → 10497 Len=0	10497	56276
89	16.719636830	10.0.2.3	10.0.2.2	UDP	42	56277 → 10497 Len=0	10497	56277
90	16.719799153	10.0.2.3	10.0.2.2	UDP	42	56277 → 10458 Len=0	10458	56277
91	16.719889626	10.0.2.3	10.0.2.2	UDP	42	56277 → 10146 Len=0	10146	56277
92	16.719976017	10.0.2.3	10.0.2.2	UDP	42	56277 → 10457 Len=0	10457	56277
93	16.720045397	10.0.2.2	10.0.2.3	ICMP	70	Destination unreachable (Port unrea...	10497	56277
94	16.819993513	10.0.2.3	10.0.2.2	UDP	42	56277 → 10264 Len=0	10264	56277

Wysyłanie pakietu UDP na dany port

- ▶ Otrzymanie wiadomości ICMP Port Unreachable oznacza, że port jest zamknięty
- ▶ W przeciwnym wypadku przyjmuje się, że jest otwarty (uwaga: może być filtrowany przez firewall)

Zgodnie z informacją widoczną w konsoli, wszystkie skanowane porty są zamknięte. Potwierdza to zrzut z Wiresharka – otrzymujemy kolejne wiadomości ICMP Port Unreachable.

Podsumowanie

Każda z użytych metod dostarczyła wielu cennych informacji, potwierdzających wiedzę teoretyczną odnośnie danego typu skanowania. Z pewnością cennymi okazać się mogą informacje zdobyte na temat systemu operacyjnego badanej maszyny, jej otwartych, jak również zamkniętych portów, czy wreszcie stopień ich filtrowania przez systemowego firewall'a.

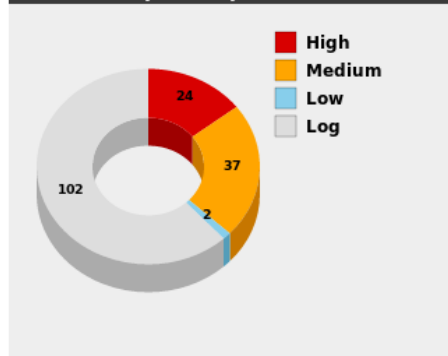
Zdradliwą metodą może okazać się natomiast skanowanie UDP, ze względu na fakt, iż występuje w tym przypadku prawdopodobieństwo generowania wyników przekłamanych (fałszywie pozytywnych).

Ponadto metody XMAS, FIN, oraz NULL działają jedynie w przypadku systemów operacyjnych implementujących RFC 793.

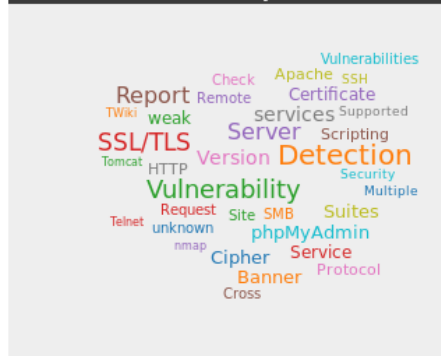
Skowanie podatności – OpenVAS

Name:	Zadanie
Comment:	
Target:	MójCel
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and fast ultimate
	Order for target hosts: Sequential
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 4
	Maximum concurrently scanned hosts: 20
Status:	Done
Duration of last scan:	34 minutes 22 seconds
Average scan duration:	34 minutes 22 seconds
Reports:	1 (Finished: 1 , Last: Nov 2 2017)
Results:	163
Notes:	0
Overrides:	0

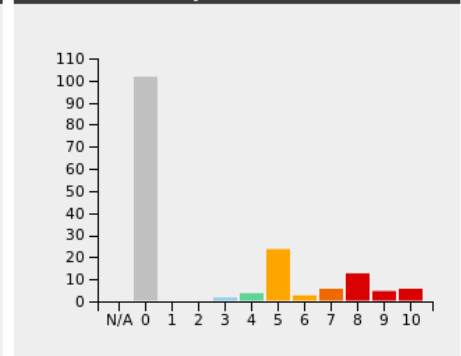
Results by Severity Class (Total: 165)



Results vulnerability word cloud



Results by CVSS (Total: 165)



Vulnerability		Severity	QoD	Host	Location	Created
Check for rexecd Service		10.0 (High)	80%	10.0.2.2	512/tcp	Thu Nov 2 22:25:20 2017
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:25:26 2017
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	10.0.2.2	8787/tcp	Thu Nov 2 22:29:47 2017
Possible Backdoor: Ingreslock		10.0 (High)	99%	10.0.2.2	1524/tcp	Thu Nov 2 22:31:50 2017
OS End Of Life Detection		10.0 (High)	80%	10.0.2.2	general/tcp	Thu Nov 2 22:49:35 2017
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	10.0.2.2	3632/tcp	Thu Nov 2 22:26:24 2017
MySQL / MariaDB weak password		9.0 (High)	95%	10.0.2.2	3306/tcp	Thu Nov 2 22:28:21 2017
PostgreSQL weak password		9.0 (High)	99%	10.0.2.2	5432/tcp	Thu Nov 2 22:29:12 2017
VNC Brute Force Login		9.0 (High)	95%	10.0.2.2	5900/tcp	Thu Nov 2 22:29:36 2017
SSH Brute Force Logins With Default Credentials Reporting		9.0 (High)	95%	10.0.2.2	22/tcp	Thu Nov 2 22:49:35 2017

Vulnerability		Severity	QoD	Host	Location	Created
DistCC Detection		8.5 (High)	95%	10.0.2.2	3632/tcp	Thu Nov 2 22:23:47 2017
phpinfo() output accessible		7.5 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:23:17 2017
phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities		7.5 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:23:40 2017
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:23:40 2017
Check for rlogin Service		7.5 (High)	70%	10.0.2.2	513/tcp	Thu Nov 2 22:23:53 2017
phpMyAdmin Code Injection and XSS Vulnerability		7.5 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:25:11 2017
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities		7.5 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:25:25 2017
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	80%	10.0.2.2	80/tcp	Thu Nov 2 22:26:08 2017
Apache Tomcat Server Administration Unauthorized Access Vulnerability		7.5 (High)	98%	10.0.2.2	8180/tcp	Thu Nov 2 22:27:53 2017
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	10.0.2.2	80/tcp	Thu Nov 2 22:30:53 2017

Stworzony przeze mnie target otrzymał host 10.0.2.2 do skanowania, na wszystkich portach TCP, z opcją Scan Config Default do weryfikacji czy maszyna działa.

Jak widać na załączonych screenach, program OpenVAS dostarczył nam wiedzy o wielu licznych lukach na płaszczyźnie bezpieczeństwa. Widocznych jest dużo pozycji o wysokiej podatności na niebezpieczeństwo.

Zagłębiając się w poszczególne wpisy programu, możemy dowiedzieć się m.in., że 'backdoor' jest zainstalowany na zdalnym hoście, co potencjalny atakujący może wykorzystać dowolne polecenia w danej aplikacji, działające na naszą niekorzyść.

Widnieje również informacja, iż system operacyjny na hoście zdalnym zakończył swoje działanie (życie) i nie powinien być już używany.

Kolejnym poważnym błędem w materii bezpieczeństwa jest komunikat z MySQL-a, mówiący, że do danej bazy danych można było się zalogować z pustym hasłem, a winnym miejscu wystarczyło użyć jawnego hasła „postgres”.

Jak widać, używany program OpenVAS jest narzędziem chwilami nieocenionym przy pomocy w wykrywaniu podatności na niebezpieczeństwo, szczegółowych informacji o nich, jak również sposobów naprawy takich luk. Dostarcza nam wiedzy na temat poziomu zagrożenia, kieruje, czym należy zająć się w pierwszej kolejności.

Metadane



Mistrzostwa Europy w Siatkówce Halowej, Polska 2017

root@kali:~/Downloads/Image-	ExposureProgram	: Not	SerialNumber	: 4522370
ExifTool-10.65# exiftool -s euro.jpg	Defined		VRInfoVersion	: 0100
ExifToolVersion : 10.65	ISO : 720		VibrationReduction	: On
FileName : euro.jpg	ExifVersion : 0230		VRMode	: Normal
Directory : .	DateTimeOriginal	:	ActiveD-Lighting	: Auto
FileSize : 147 kB	2017:08:24 18:14:57		PictureControlVersion	: 0100
FileModifyDate : 2017:11:02	CreateDate : 2017:08:24		PictureControlName	: Standard
23:56:25+01:00	18:14:57		PictureControlBase	: Standard
FileAccessDate : 2017:11:02	ComponentsConfiguration : Y, Cb,		PictureControlAdjust	: Default
23:55:32+01:00	Cr, -		Settings	
FileinodeChangeDate :	CompressedBitsPerPixel : 2		Brightness	: Normal
2017:11:02 23:56:25+01:00	ExposureCompensation : 0		HueAdjustment	: None
FilePermissions : rw-r--r--	MaxApertureValue : 4.0		TimeZone	: +01:00
FileType : JPEG	MeteringMode : Multi-		DaylightSavings	: No
FileTypeExtension : jpg	segment		DateDisplayFormat	: Y/M/D
MIMEType : image/jpeg	Flash : Auto, Did not fire		ISOExpansion	: Off
JFIFVersion : 1.01	FocalLength : 25.0 mm		ISO2	: 713
ExifByteOrder : Big-endian	MakerNoteVersion : 2.11		ISOExpansion2	: Off
(Motorola, MM)	Quality : Normal		AutoDistortionControl	: Off
Make : NIKON	WhiteBalance : Auto		HDRInfoVersion	: 0200
CORPORATION	FocusMode : AF-A		HDR	: Off
Model : NIKON D5200	WB_RBLevels : 2.1953125		HDRLevel	: Auto
Orientation : Horizontal	1.71484375 1 1		LensType	: G VR
(normal)	Compression : JPEG (old-		Lens	: 18-105mm f/3.5-
XResolution : 300	style)		FlashMode	: Did Not Fire
YResolution : 300	PreviewImageStart : 19478		ShootingMode	: Single-
ResolutionUnit : inches	PreviewImageLength : 24291		Frame, Auto ISO	
Software : Ver.1.02	ISOSetting : 720		ShotInfoVersion	: 0226
ModifyDate : 2017:08:24	ImageBoundary : 0 0 4496		FirmwareVersion	: 1.02
18:14:57	3000		NoiseReduction	: Off
YCbCrPositioning : Co-sited	CropHiSpeed : Off		ColorBalanceVersion	: 0218
ExposureTime : 1/60	(6036x4020 cropped to 6036x4020 at		LensDataVersion	: 0204
FNumber : 5.6	pixel 0,0)			

ExitPupilPosition	: 97.5 mm	FlashpixVersion	: 0100	EncodingProcess	: Baseline
AFAperture	: 3.9	ColorSpace	: sRGB	DCT, Huffman coding	
FocusPosition	: 0x05	ExifImageWidth	: 4496	BitsPerSample	: 8
FocusDistance	: 5.62 m	ExifImageHeight	: 3000	ColorComponents	: 3
LensIDNumber	: 158	InteropVersion	: 0100	YCbCrSubSampling	:
LensFStops	: 5.33	SensingMethod	: One-chip	YCbCr4:2:2 (2 1)	
MinFocalLength	: 18.3 mm	color area		Aperture	: 5.6
MaxFocalLength	: 106.8 mm	FileSource	: Digital Camera	AutoFocus	: On
MaxApertureAtMinFocal	: 3.6	SceneType	: Directly	BlueBalance	: 1.714844
MaxApertureAtMaxFocal	: 5.7	photographed		ImageSize	: 730x487
MCUVersion	: 160	CFAPattern	:	LensID	: AF-S DX VR
EffectiveMaxAperture	: 4.0	[Red,Green][Green,Blue]		Zoom-Nikkor 18-105mm f/3.5-5.6G ED	
RetouchHistory	: None	CustomRendered	: Normal	LensSpec	: 18-105mm
ImageDataSize	: 3476694	ExposureMode	: Auto	f/3.5-5.6 G VR	
ShutterCount	: 39412	DigitalZoomRatio	: 1	Megapixels	: 0.356
FlashInfoVersion	: 0105	FocalLengthIn35mmFormat	: 37	PreviewImage	: (Binary data
VariProgram	: Food	mm		24291 bytes, use -b option to extract)	
MultiExposureVersion	: 0100	SceneCaptureType	: Standard	RedBalance	: 2.195313
MultiExposureAutoGain	: Off	GainControl	: Low gain up	ScaleFactor35efl	: 1.5
HighISONoiseReduction	: Normal	Contrast	: Normal	ShutterSpeed	: 1/60
PowerUpTime	: 0000:00:00	Saturation	: Normal	SubSecCreateDate	:
00:00:00		Sharpness	: Normal	2017:08:24 18:14:57.10	
AFInfo2Version	: 0100	SubjectDistanceRange	:	SubSecDateTimeOriginal	:
AFAreaMode	: Single Area	Unknown		2017:08:24 18:14:57.10	
PhaseDetectAF	: On (39-	OffsetSchema	: 4100	SubSecModifyDate	:
point)		SensitivityType	:	2017:08:24 18:14:57.10	
PrimaryAFPoint	: C6 (Center)	Recommended Exposure Index		ThumbnailImage	: (Binary
AFPointsUsed	: C6	Padding	: (Binary data	data 8517 bytes, use -b option to	
ContrastDetectAFInFocus	: No	2060 bytes, use -b option to extract)		extract)	
FileInfoVersion	: 0100	ThumbnailOffset	: 44304	CircleOfConfusion	: 0.020 mm
DirectoryNumber	: 101	ThumbnailLength	: 8517	DOF	: inf (2.79 m - inf)
FileNumber	: 0770	About	: uuid:faf5bdd5-	FOV	: 51.7 deg (5.45 m)
RetouchInfoVersion	: 0200	ba3d-11da-ad31-d33d75182f1b		FocalLength35efl	: 25.0 mm
RetouchNEFProcessing	: Off	CreatorTool	: Ver.1.02	(35 mm equivalent: 37.0 mm)	
SubSecTime	: 10	ImageWidth	: 730	HyperfocalDistance	: 5.50 m
SubSecTimeOriginal	: 10	ImageHeight	: 487	LightValue	: 8.0
SubSecTimeDigitized	: 10				

Ze zgromadzonych informacji możemy dowiedzieć się m.in. kiedy zdjęcie zostało wykonane, kiedy była jego ostatnia modyfikacja, jakim modelem aparatu zostało zrobione, w jakiej strefie czasowej, czy jaką posiada wielkość.

Czasami można znaleźć nawet informację o osobie tworzącej daną fotografię i towarzyszącej temu zdarzeniu lokalizacji, co daje duże możliwości weryfikacyjne. Można bowiem w łatwy sposób określić, czy data, osoba, miejsce i wreszcie zawartość zdjęcia, układają się jedną, spójną całość, czy może ktoś tymi danymi manipulował.