Patryk Gozdera, 277185

**BOT –   
Laboratorium 1**

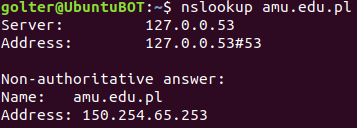
**Rekonesans i skanowanie**

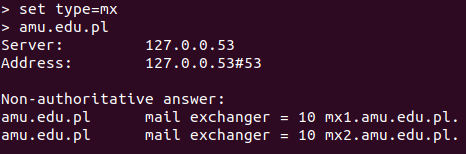
# Część pierwsza – rekonesans

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.

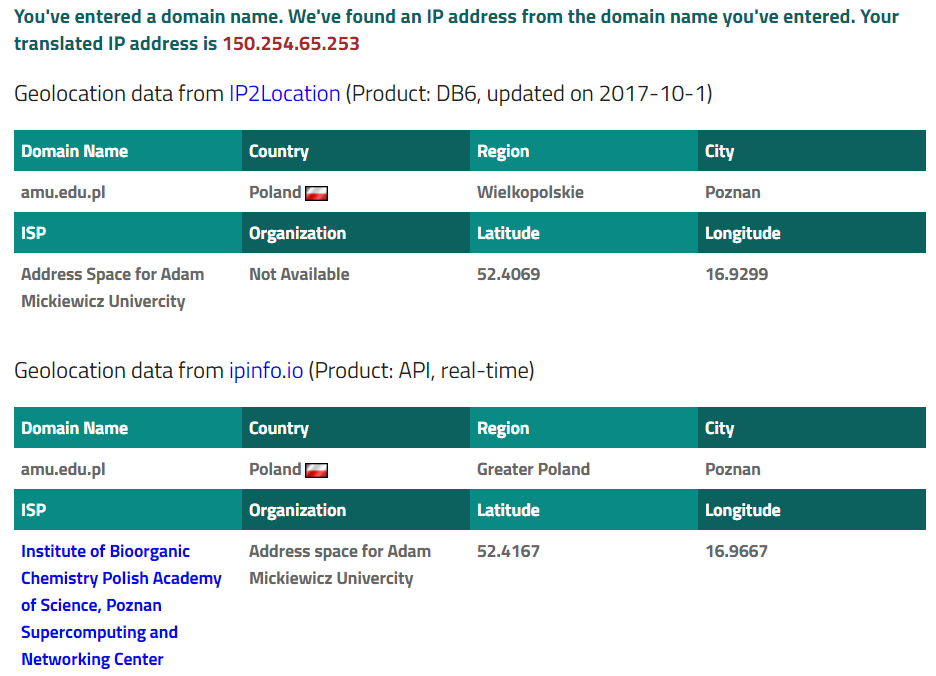
Poniżej zostaną przedstawione zgromadzone informacje z poszczególnych narzędzi (z widocznymi na screen’ach komendami).

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





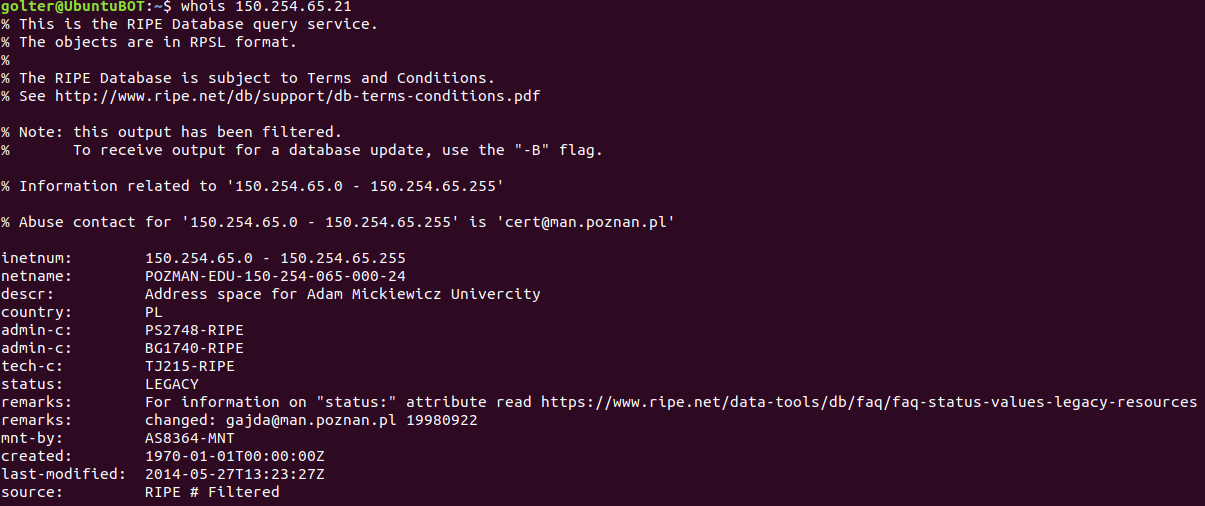
* Lokalizacja geograficzna – korzystając ze strony <https://www.iplocation.net/> , ustaliłem lokalizację:

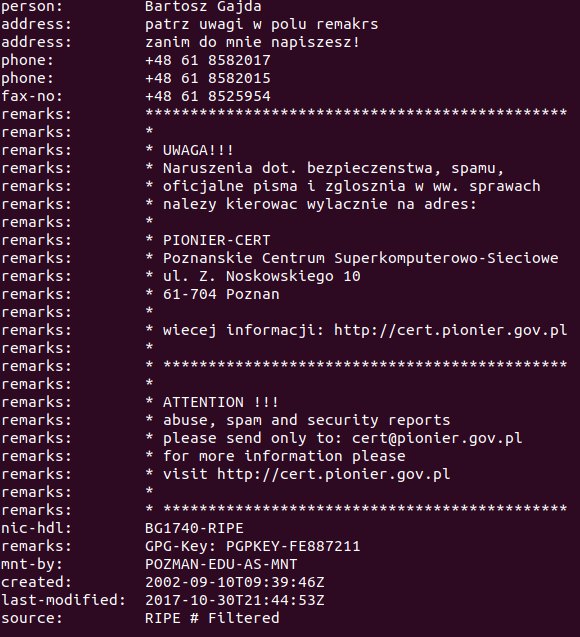
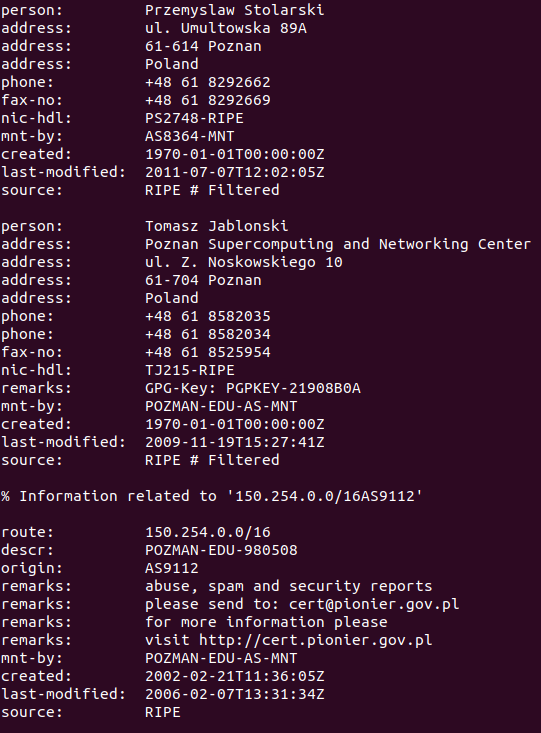


* Whois – narzędzie umożliwiające dostarczenie takich informacji jak dane o serwerach DNS, adresy IP, daty związane z utworzeniem lub modyfikacją, jak również dane kontaktowe i adresowe:



Po odpytaniu pierwszego z wyszukanych serwerów DNS:

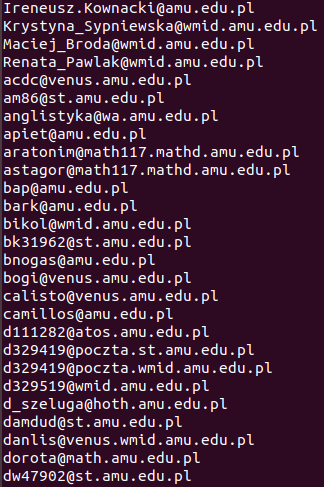




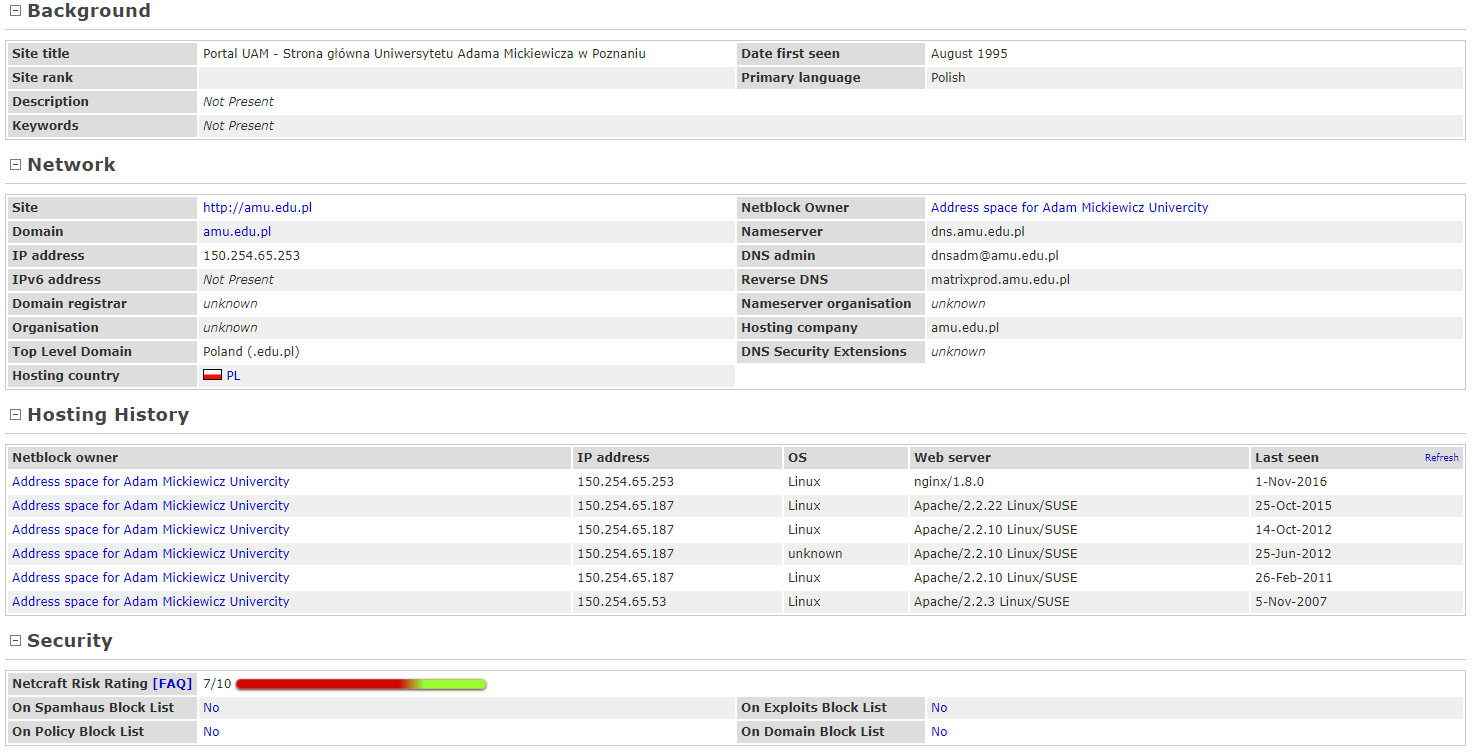
* The Harvester – narzędzie pozwalające na masowe zbieranie adresów e-mail, nazw użytkowników oraz hostów związanych z interesującą domeną. Dane te są wyszukiwane na podstawie publicznych źródeł, takich jak przeglądarki, serwery PGP, czy serwis LinkedIn.

Za jego pomocą udało się uzyskać około 150 adresów email i wiele nazw hostów związanych z UAM.



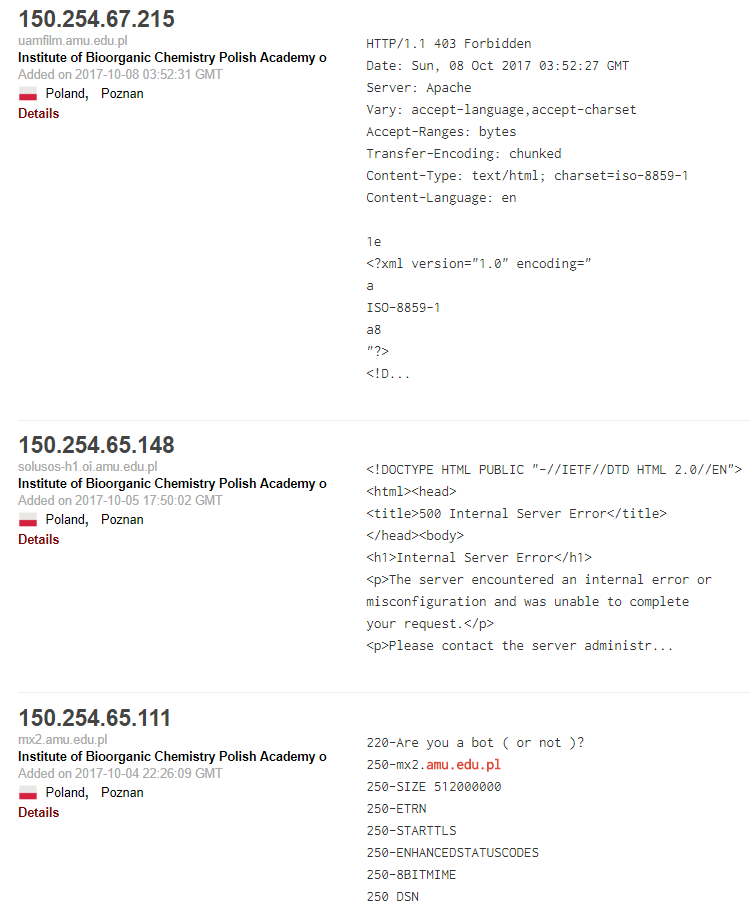


* Netcraft – uzyskane informacje o witrynie UAM znajdują się poniżej. Zawierają one m.in. wiadomości o pełnym tytule strony, dacie pierwszego ‘kontaktu’ ze stroną, języku, adresie IP i wiele innych. Wartym uwagi jest wskazana wartość „Netcraft Risk Rating”, która osiąga wysoką, negatywną wartość, ocenioną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



* 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.

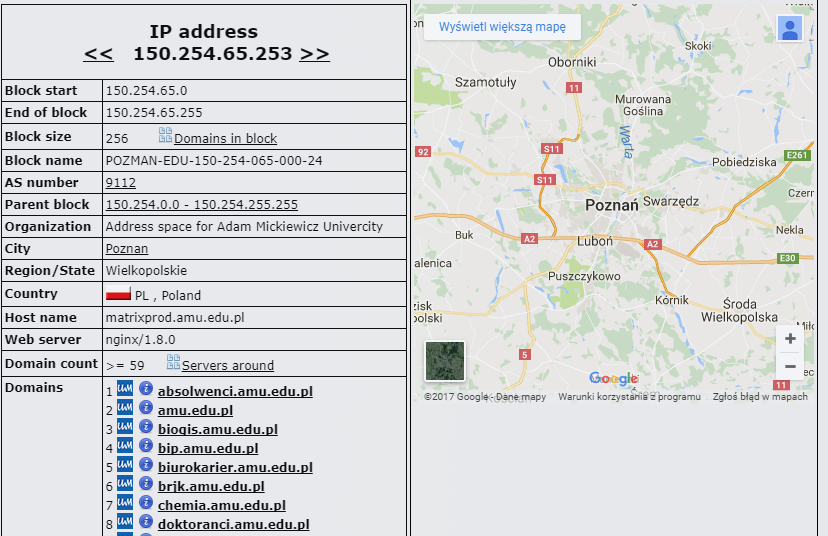




* Archiwalna wersja strony z 1997 roku, zawierające dane osób pracujących w tych latach na profilowanej uczelni.



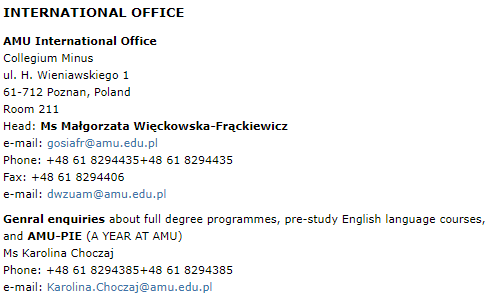
* Ipv4info.com – informacje o witrynie, zawierające m.in. nazwę hosta, web server, czy lokalizację:



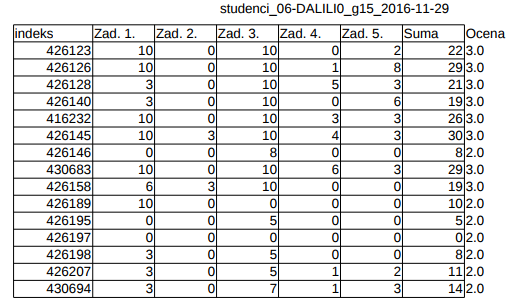
* Dyrektywy gogle

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



* site:amu.edu.pl intext:wyniki (algebra nie poszła najlepiej ☺)



Zakwalifikowani do programu MOST (mała część listy osób):

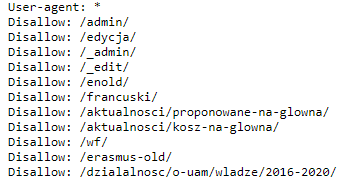


* site:amu.edu.pl intext:lista studentów

Fragment listy przyjętych na filologię angielską

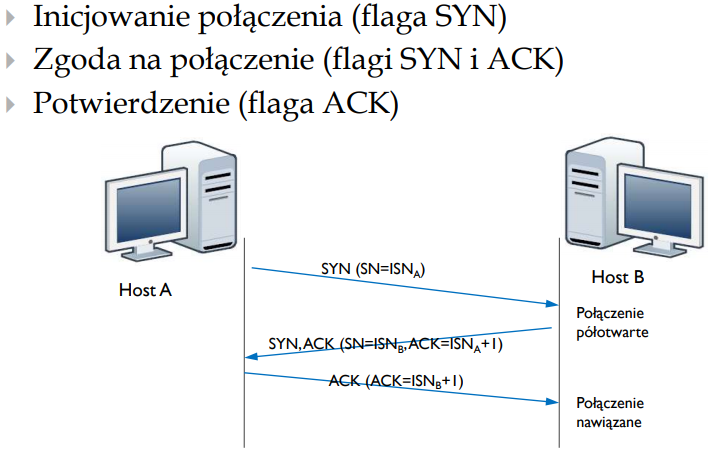


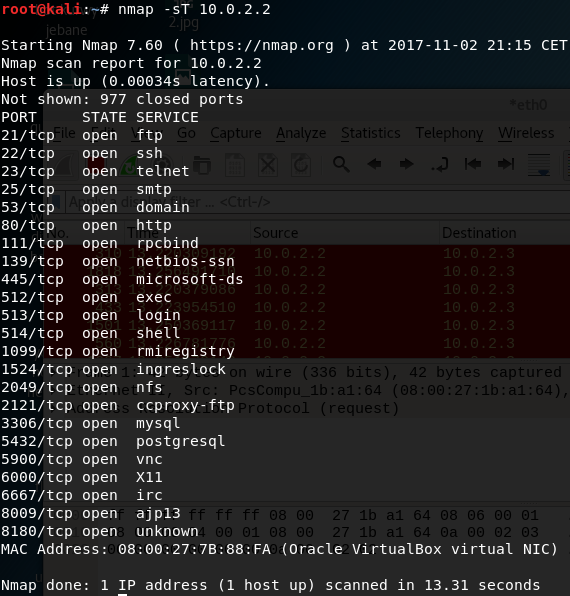
* site:amu.edu.pl inurl:robots.txt



# Część druga – skanowanie i analiza metadanych

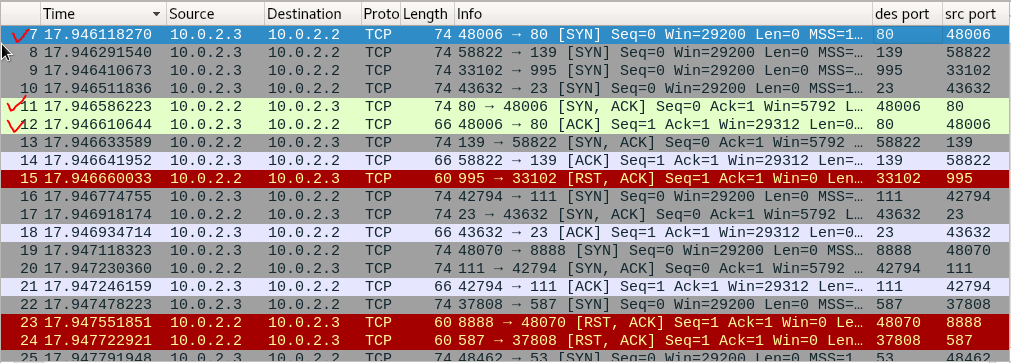
## Skanowanie i wykrywanie systemu operacyjnego – nMap

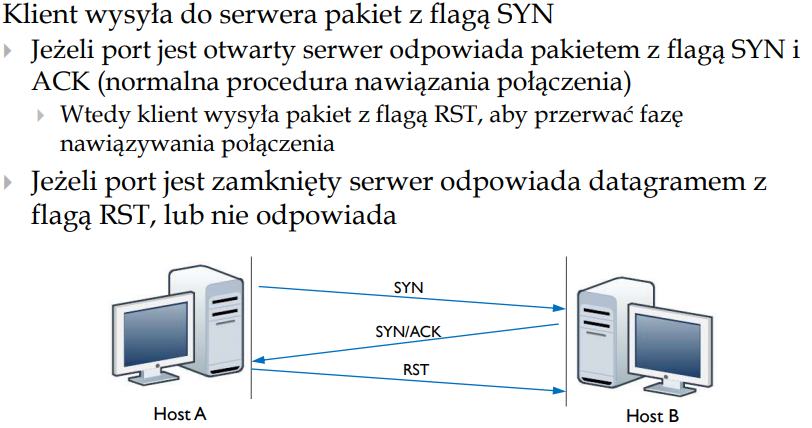
* Skanowanie TCP

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.

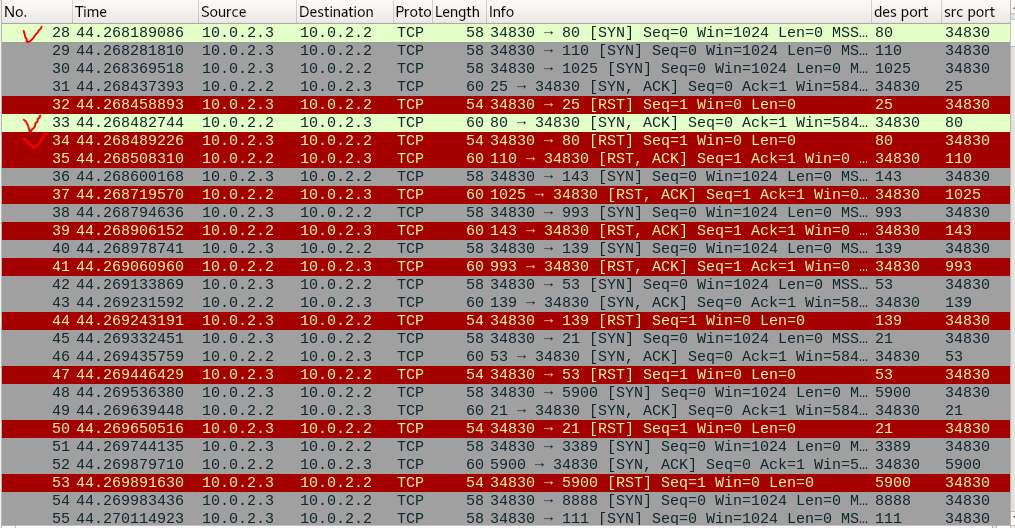
Najpierw Kali wysyła do Meta pakiet z flagą SYN (następuje zainicjowanie połączenia). Następnie Meta odsyła SYN ACK (zgoda na połączenie), aby ostatecznie Kali wysłał ACK (stanowiące potwierdzenie).



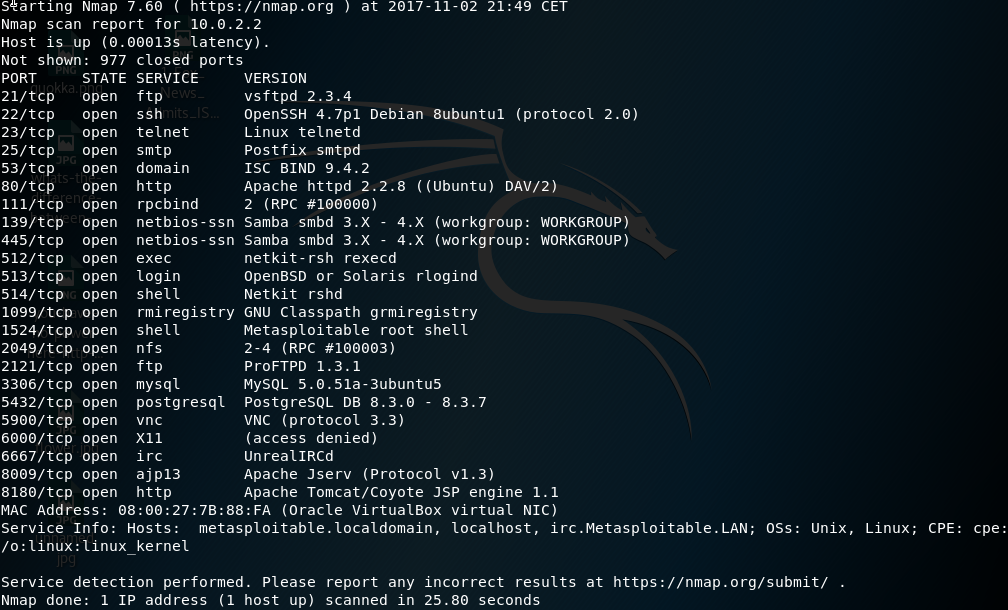
* Skanowanie stealh

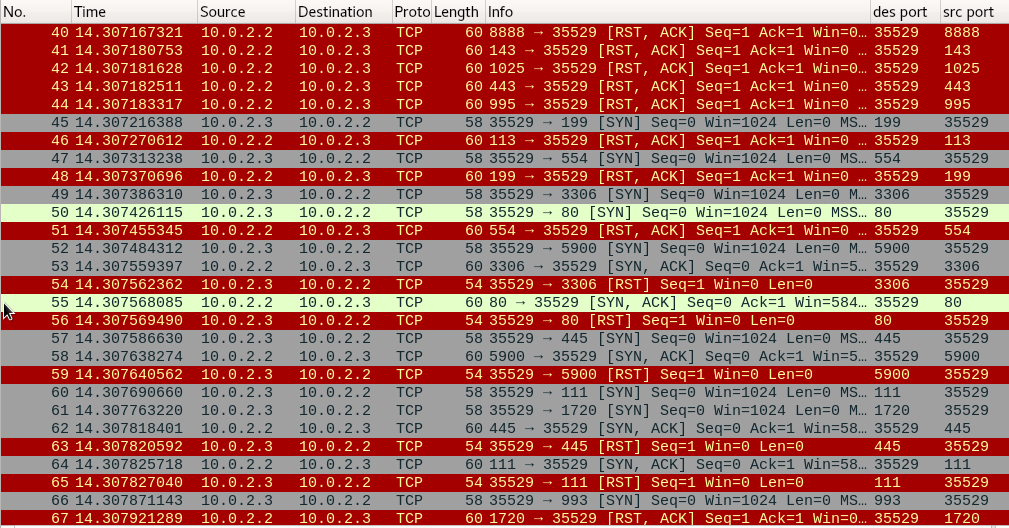


Widzimy poniżej, że port 80 jest otwarty, występuje sytuacja opisana i zilustrowana powyżej – najpierw wysłanie pakietu z flagą SYN, następnie odpowiedź od portu 34830 SYN i ACK, a następnie RST od klienta w celu przerwania nawiązywania połączenia.

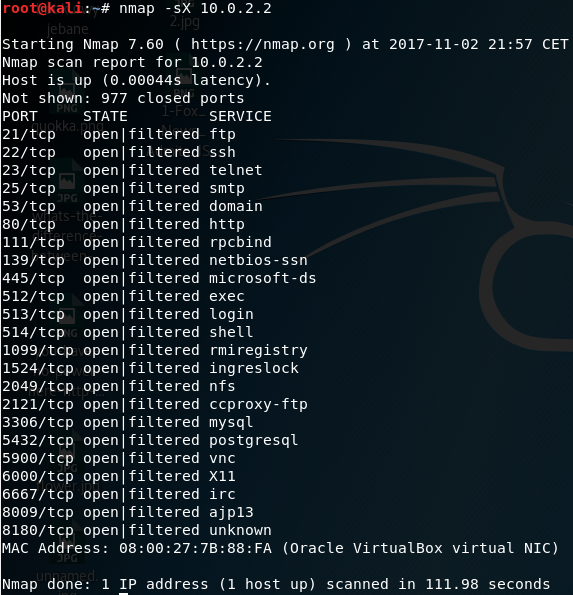
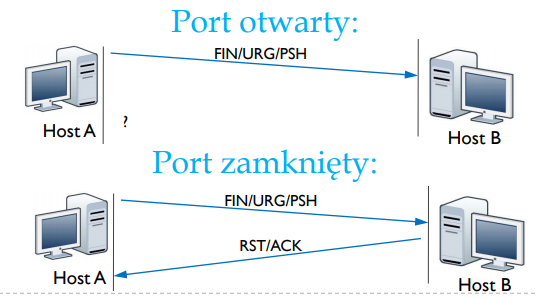


* Skanowanie wersji

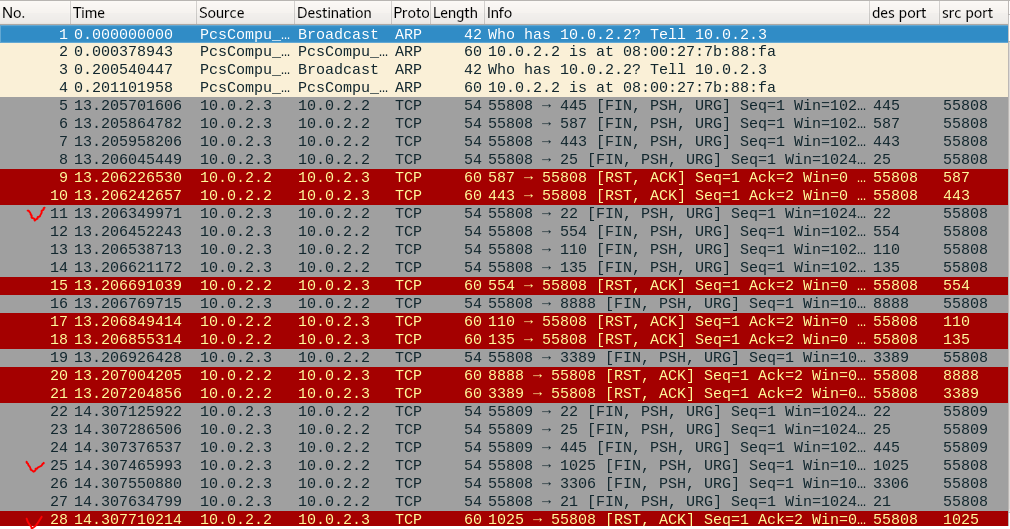


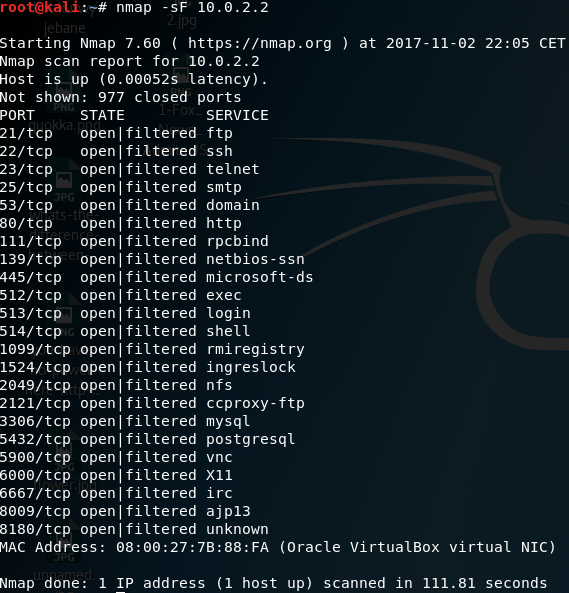
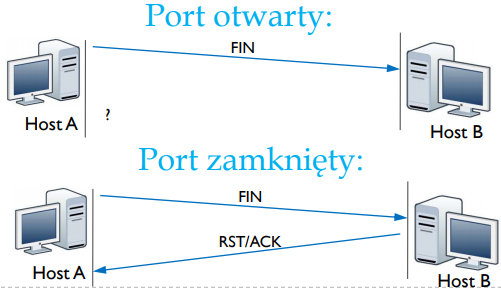


W przypadku tego skanowania, możemy uzyskać wiedzę na temat wersji systemu dla danego portu.

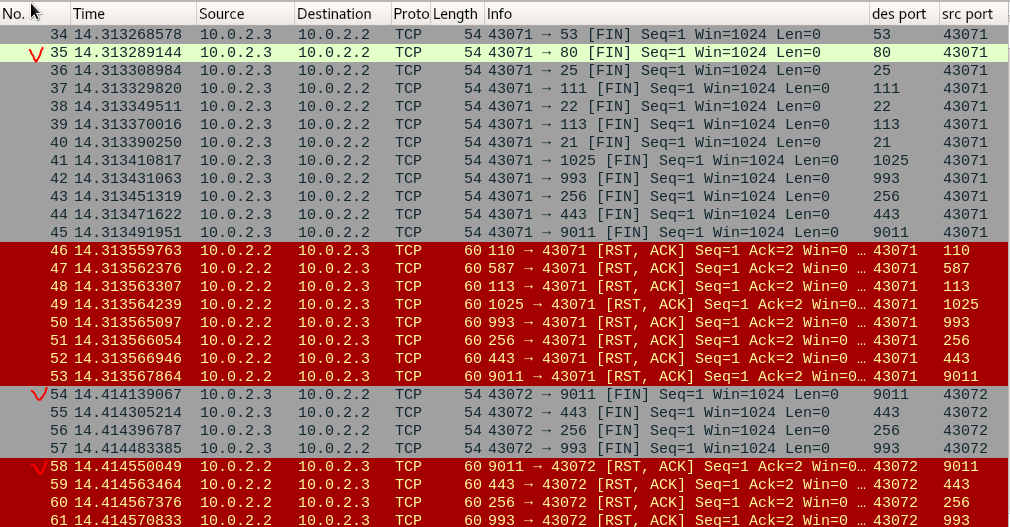
* Skanowanie Xmas

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

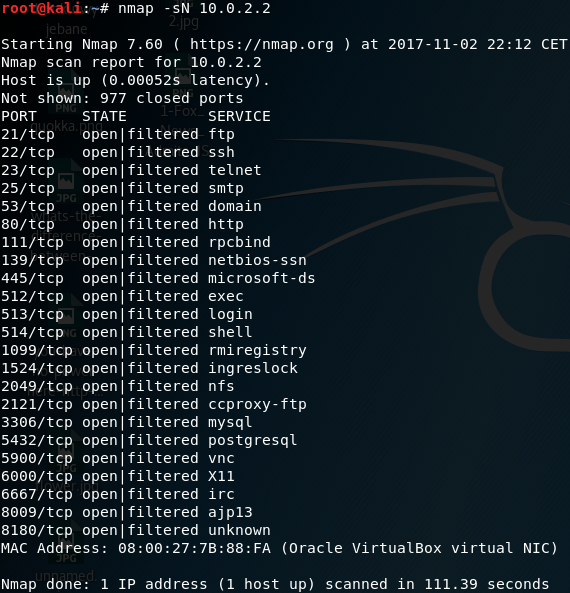


* Skanowanie Fin

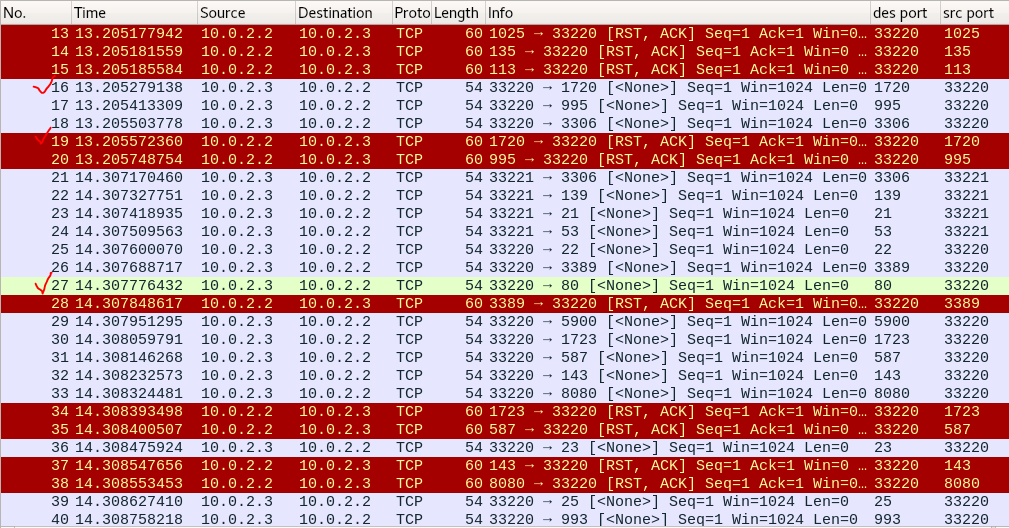
Zaznaczone na poniższym screen’ie logi potwierdzają powyższy rysunek – port 80 jest otwarty, natomiast port 9011 zamknięty.



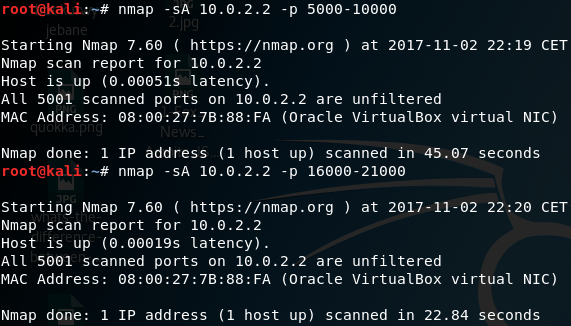
* Skanowanie Null

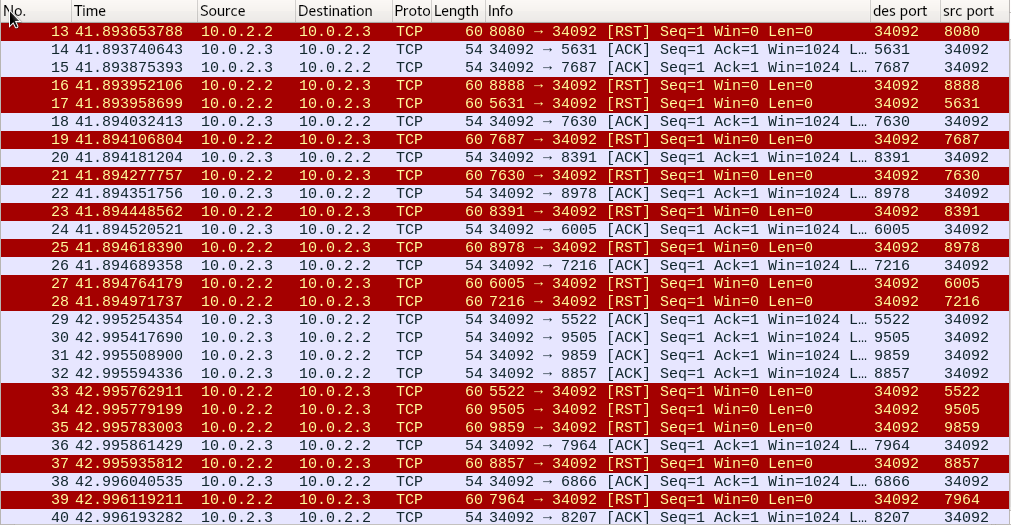


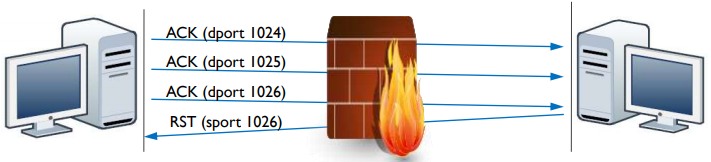
Zaznaczone na poniższym screen’ie logi potwierdzają powyższy rysunek – port 80 jest otwarty, natomiast port 33220 zamknięty.



* Skanowanie Ack

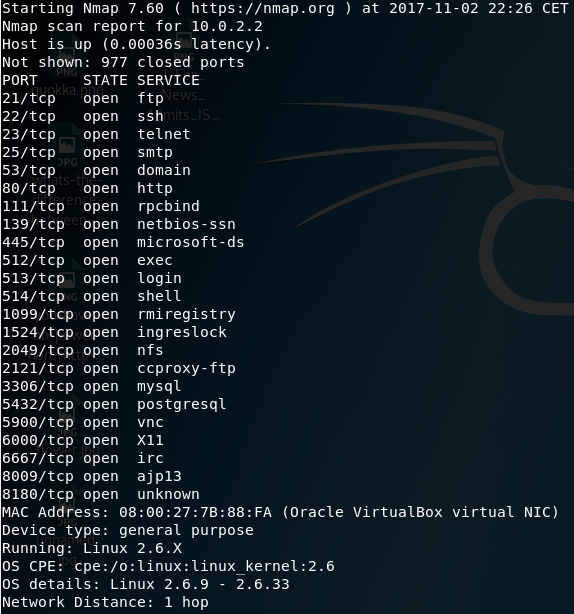


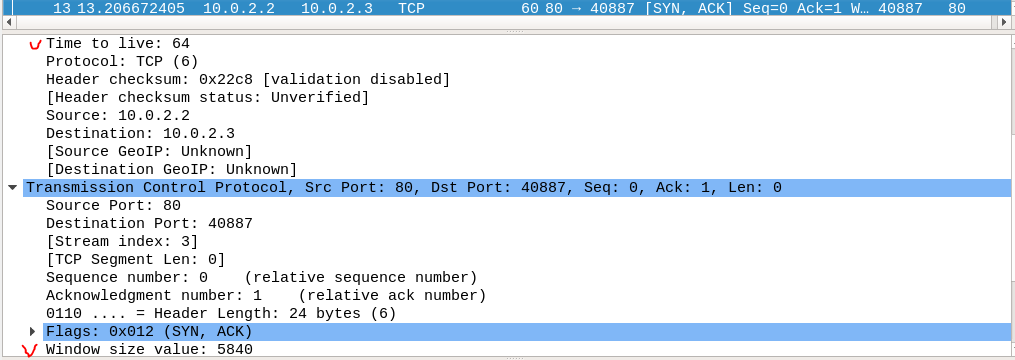


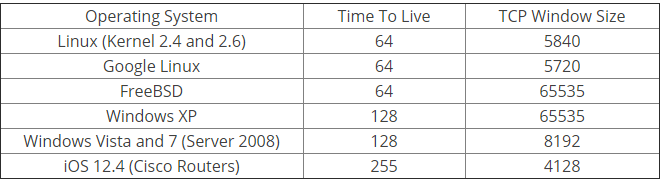


Jak widać, otrzymujemy kolejne pakiety RST, będące odpowiedzią na wysłane pakiety z flagą ACK – porty niefiltrowane przez firewalla.

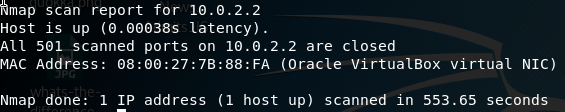
* Rozpoznawanie systemu

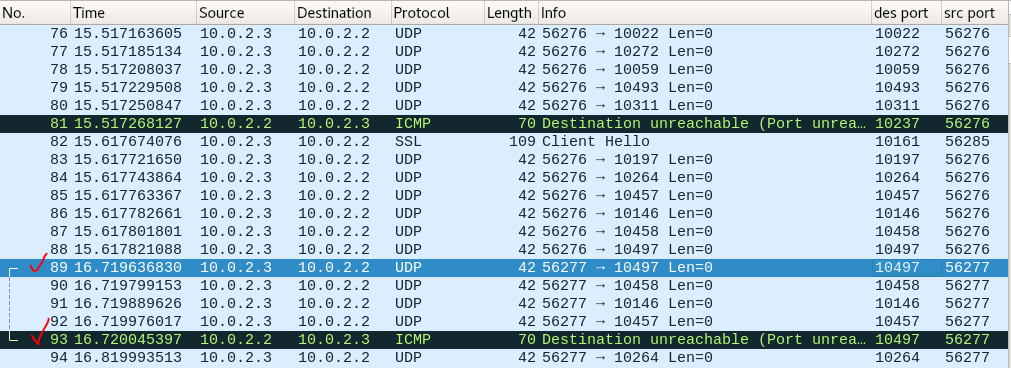


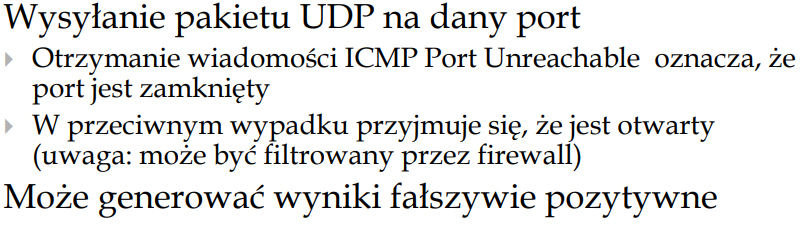


Jak widać, na podstawie wartości TTL oraz TCP WS, rozpoznany system to Linux.

* Skanowanie UDP





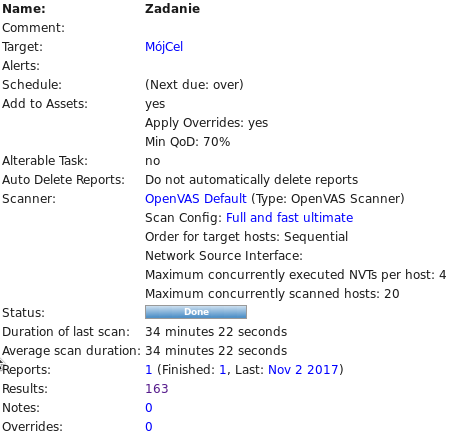


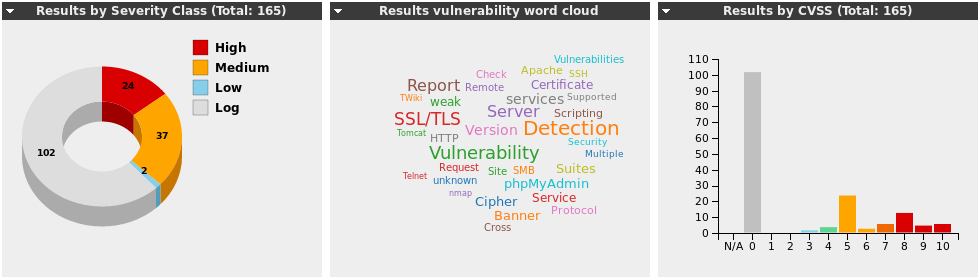
Zgodnie z informacją widoczną w konsoli, wszystkie skanowane porty są zamknięte. Potwierdza to zrzut z Wiresharka – otrzymujemy kolejne wiadomości ICMP Port Unreachable.

### Podsumowanie

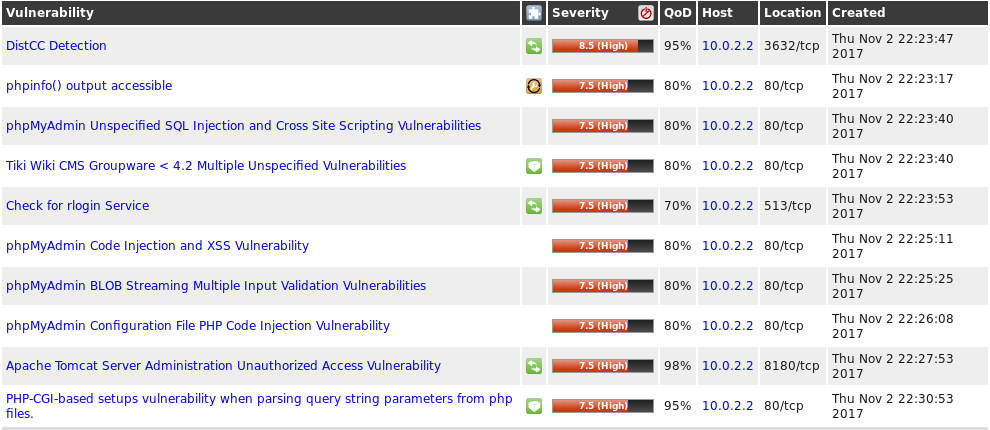
Każda z użytych metod dostarczyła wielu cennych informacji, potwierdzających wiedzę teoretyczną odnośnie danego typu skanowania. Z pewnością cennymi okazać się mogą informacje zdobyte na temat systemu operacyjnego badanej maszyny, jej otwartych, jak również zamkniętych portów, czy wreszcie stopień ich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

## Skanowanie podatności – OpenVAS









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-ExifTool-10.65# exiftool -s euro.jpg

ExifToolVersion : 10.65

FileName : euro.jpg

Directory : .

**FileSize : 147 kB**

**FileModifyDate : 2017:11:02 23:56:25+01:00**

**FileAccessDate : 2017:11:02 23:55:32+01:00**

**FileInodeChangeDate : 2017:11:02 23:56:25+01:00**

FilePermissions : rw-r--r--

FileType : JPEG

FileTypeExtension : jpg

MIMEType : image/jpeg

JFIFVersion : 1.01

ExifByteOrder : Big-endian (Motorola, MM)

**Make : NIKON CORPORATION**

**Model : NIKON D5200**

Orientation : Horizontal (normal)

XResolution : 300

YResolution : 300

ResolutionUnit : inches

Software : Ver.1.02

**ModifyDate : 2017:08:24 18:14:57**

YCbCrPositioning : Co-sited

ExposureTime : 1/60

FNumber : 5.6

ExposureProgram : Not Defined

ISO : 720

ExifVersion : 0230

**DateTimeOriginal : 2017:08:24 18:14:57**

**CreateDate : 2017:08:24 18:14:57**

ComponentsConfiguration : Y, Cb, Cr, -

CompressedBitsPerPixel : 2

ExposureCompensation : 0

MaxApertureValue : 4.0

MeteringMode : Multi-segment

Flash : Auto, Did not fire

FocalLength : 25.0 mm

MakerNoteVersion : 2.11

Quality : Normal

WhiteBalance : Auto

FocusMode : AF-A

WB\_RBLevels : 2.1953125 1.71484375 1 1

Compression : JPEG (old-style)

PreviewImageStart : 19478

PreviewImageLength : 24291

ISOSetting : 720

ImageBoundary : 0 0 4496 3000

CropHiSpeed : Off (6036x4020 cropped to 6036x4020 at pixel 0,0)

SerialNumber : 4522370

VRInfoVersion : 0100

VibrationReduction : On

VRMode : Normal

ActiveD-Lighting : Auto

PictureControlVersion : 0100

PictureControlName : Standard

PictureControlBase : Standard

PictureControlAdjust : Default Settings

Brightness : Normal

HueAdjustment : None

**TimeZone : +01:00**

DaylightSavings : No

DateDisplayFormat : Y/M/D

ISOExpansion : Off

ISO2 : 713

ISOExpansion2 : Off

AutoDistortionControl : Off

HDRInfoVersion : 0200

HDR : Off

HDRLevel : Auto

LensType : G VR

Lens : 18-105mm f/3.5-5.6

FlashMode : Did Not Fire

ShootingMode : Single-Frame, Auto ISO

ShotInfoVersion : 0226

FirmwareVersion : 1.02

NoiseReduction : Off

ColorBalanceVersion : 0218

LensDataVersion : 0204

ExitPupilPosition : 97.5 mm

AFAperture : 3.9

FocusPosition : 0x05

FocusDistance : 5.62 m

LensIDNumber : 158

LensFStops : 5.33

MinFocalLength : 18.3 mm

MaxFocalLength : 106.8 mm

MaxApertureAtMinFocal : 3.6

MaxApertureAtMaxFocal : 5.7

MCUVersion : 160

EffectiveMaxAperture : 4.0

RetouchHistory : None

ImageDataSize : 3476694

ShutterCount : 39412

FlashInfoVersion : 0105

VariProgram : Food

MultiExposureVersion : 0100

MultiExposureAutoGain : Off

HighISONoiseReduction : Normal

PowerUpTime : 0000:00:00 00:00:00

AFInfo2Version : 0100

AFAreaMode : Single Area

PhaseDetectAF : On (39-point)

PrimaryAFPoint : C6 (Center)

AFPointsUsed : C6

ContrastDetectAFInFocus : No

FileInfoVersion : 0100

DirectoryNumber : 101

FileNumber : 0770

RetouchInfoVersion : 0200

RetouchNEFProcessing : Off

SubSecTime : 10

SubSecTimeOriginal : 10

SubSecTimeDigitized : 10

FlashpixVersion : 0100

ColorSpace : sRGB

ExifImageWidth : 4496

ExifImageHeight : 3000

InteropVersion : 0100

SensingMethod : One-chip color area

FileSource : Digital Camera

SceneType : Directly photographed

CFAPattern : [Red,Green][Green,Blue]

CustomRendered : Normal

ExposureMode : Auto

DigitalZoomRatio : 1

FocalLengthIn35mmFormat : 37 mm

SceneCaptureType : Standard

GainControl : Low gain up

Contrast : Normal

Saturation : Normal

Sharpness : Normal

SubjectDistanceRange : Unknown

OffsetSchema : 4100

SensitivityType : Recommended Exposure Index

Padding : (Binary data 2060 bytes, use -b option to extract)

ThumbnailOffset : 44304

ThumbnailLength : 8517

About : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b

CreatorTool : Ver.1.02

ImageWidth : 730

ImageHeight : 487

EncodingProcess : Baseline DCT, Huffman coding

BitsPerSample : 8

ColorComponents : 3

YCbCrSubSampling : YCbCr4:2:2 (2 1)

Aperture : 5.6

AutoFocus : On

BlueBalance : 1.714844

ImageSize : 730x487

LensID : AF-S DX VR Zoom-Nikkor 18-105mm f/3.5-5.6G ED

LensSpec : 18-105mm f/3.5-5.6 G VR

Megapixels : 0.356

PreviewImage : (Binary data 24291 bytes, use -b option to extract)

RedBalance : 2.195313

ScaleFactor35efl : 1.5

ShutterSpeed : 1/60

SubSecCreateDate : 2017:08:24 18:14:57.10

SubSecDateTimeOriginal : 2017:08:24 18:14:57.10

SubSecModifyDate : 2017:08:24 18:14:57.10

ThumbnailImage : (Binary data 8517 bytes, use -b option to extract)

CircleOfConfusion : 0.020 mm

DOF : inf (2.79 m - inf)

FOV : 51.7 deg (5.45 m)

FocalLength35efl : 25.0 mm (35 mm equivalent: 37.0 mm)

HyperfocalDistance : 5.50 m

LightValue : 8.0

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.