

Testy Penetracyjne Lab 4

Julia Sadecka, Cyberbezpieczeństwo

1. Wykonanie procedury globalnego ustawienia RHOST i RPORT na adres 192.168.2.4 (Windows XP)

```
root@kali:~# ifconfig
root: flags=4099<UP,BROADCAST,LOOPBACK> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:79:69:c0:2b type tunneled (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.4 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::20c:29ff:fe73:bc01 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:20:c2:9f type tunneled (Ethernet)
    RX packets 215 bytes 171457 (221.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 118 bytes 29149542 (27.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ifconfig lo
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop=[ metasploit v6.1.4-dev Loopback ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 8 evasion bytes 52919 (51.6 KiB) ]
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

root@kali:~# msf6
msf6 > set RHOST 192.168.2.4
RHOST => 192.168.2.4
msf6 > set RPORT 80
RPORT => 80
msf6 >
```

2. Exiftool

Zdjęcie własnym telefonem z lokalizacją

```
(julia@kali)-[~/Desktop]
$ exiftool phone.jpg
ExifTool Version Number      : 12.57
File Name                    : phone.jpg
Directory                    : .
File Size                     : 3.5 MB
File Modification Date/Time   : 2023:12:09 08:05:25-05:00
File Access Date/Time        : 2023:12:09 08:05:25-05:00
File Inode Change Date/Time   : 2023:12:09 08:05:37-05:00
File Permissions              : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Big-endian (Motorola, MM)
Make                         : samsung
Camera Model Name             : SM-G780G
Orientation                   : Rotate 90 CW
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Modify Date                   : 2023:12:08 20:04:33
Y Cb Cr Positioning           : Centered
Exposure Time                 : 1/25
F Number                      : 1.8
Exposure Program              : Program AE
ISO                           : 1000
Exif Version                  : 0220
Date/Time Original            : 2023:12:08 20:04:33
Create Date                   : 2023:12:08 20:04:33
Offset Time                   : +01:00
Offset Time Original          : +01:00
Components Configuration     : Y, Cb, Cr, -
Shutter Speed Value           : 1/25
Aperture Value                : 1.8
Brightness Value              : -1.98
Exposure Compensation         : 0
Max Aperture Value            : 1.8
Metering Mode                 : Center-weighted average
Flash                         : No Flash
Focal Length                  : 5.4 mm
Sub Sec Time                  : 946205
Sub Sec Time Original         : 946205
Sub Sec Time Digitized        : 946205
Flashpix Version              : 0100
Color Space                   : sRGB
```

```

Sub Sec Time           : 946205
Sub Sec Time Original  : 946205
Sub Sec Time Digitized : 946205
Flashpix Version       : 0100
Color Space            : sRGB
Exif Image Width       : 4032
Exif Image Height      : 3024
Interoperability Index : R98 - DCF basic file (sRGB)
Interoperability Version : 0100
Sensing Method         : Not defined
Scene Type             : Directly photographed
Exposure Mode          : Auto
White Balance          : Auto
Focal Length In 35mm Format : 26 mm
Scene Capture Type     : Standard
GPS Longitude Ref      : East
GPS Altitude Ref       : Above Sea Level
GPS Time Stamp         : 00:00:00
GPS Date Stamp         : 1970:01:01
Compression            : JPEG (old-style)
Thumbnail Offset       : 1064
Thumbnail Length       : 32995
Image Width            : 4032
Image Height           : 3024
Encoding Process       : Baseline DCT, Huffman coding
Bits Per Sample        : 8
Color Components       : 3
Y Cb Cr Sub Sampling  : YCbCr4:2:0 (2 2)
Time Stamp             : 2023:12:08 14:04:33.237-05:00
MCC Data               : Poland
Aperture               : 1.8
Image Size             : 4032x3024
Megapixels             : 12.2
Scale Factor To 35 mm Equivalent: 4.8
Shutter Speed          : 1/25
Create Date            : 2023:12:08 20:04:33.946205
Date/Time Original     : 2023:12:08 20:04:33.946205+01:00
Modify Date            : 2023:12:08 20:04:33.946205+01:00
Thumbnail Image        : (Binary data 32995 bytes, use -b option to extract)
GPS Altitude           : 0 m Above Sea Level
GPS Date/Time          : 1970:01:01 00:00:00Z
GPS Longitude          : 0 deg 0' 0.00" E
Circle Of Confusion    : 0.006 mm
Field Of View          : 69.4 deg
Focal Length           : 5.4 mm (35 mm equivalent: 26.0 mm)
Hyperfocal Distance    : 2.60 m
Light Value            : 3.0

```

1. **Rozmiar:** 3.5MB
2. **Data Utworzenia:** 2023:12:08 20:04:33
3. **Urządzenie, które wykonało zdjęcie:** samsung, SM-G780G
4. **Rotate:** Rotate 90CW
5. **Czy flash był użyty:** Nie
6. **Rozdzielczość:** 4032x3024 px
7. **Przysłona urządzenia:** 1.8
8. **Lokalizacja:** dane GPS wskazują na brak konkretnej informacji o lokalizacji (długość geograficzna i wysokość nad poziomem morza są ustawione na zerowe wartości), a data i czas są ustawione na 1970-01-01 00:00:00 UTC, co może być wartością domyślną lub sygnalizować brak dostępnych danych czasowych.

Jedynie co wiemy to, że długość geograficzna znajduje się na wschodniej półkuli

```
GPS Longitude Ref      : East
GPS Altitude Ref      : Above Sea Level
GPS Time Stamp        : 00:00:00
GPS Date Stamp        : 1970:01:01
```

```
GPS Altitude          : 0 m Above Sea Level
GPS Date/Time         : 1970:01:01 00:00:00Z
GPS Longitude         : 0 deg 0' 0.00" E
```

9. Obiektywy urządzenia: Brak

Zdjęcie własnym telefonem bez lokalizacji

```
(julia@kali)-[~/Desktop]
$ exiftool phone-photo.jpg
ExifTool Version Number      : 12.57
File Name                    : phone-photo.jpg
Directory                    : .
File Size                     : 4.3 MB
File Modification Date/Time   : 2023:12:08 08:48:36-05:00
File Access Date/Time        : 2023:12:08 08:48:36-05:00
File Inode Change Date/Time   : 2023:12:08 08:49:19-05:00
File Permissions              : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Little-endian (Intel, II)
Make                         : samsung
Camera Model Name             : SM-G780G
Orientation                   : Rotate 90 CW
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Software                     : G780GXXS7EWH8
Modify Date                   : 2023:10:16 21:48:57
Y Cb Cr Positioning           : Centered
Exposure Time                 : 1/50
F Number                      : 1.8
Exposure Program              : Program AE
ISO                           : 400
Exif Version                  : 0220
Date/Time Original            : 2023:10:16 21:48:57
Create Date                   : 2023:10:16 21:48:57
Offset Time                   : +02:00
Offset Time Original          : +02:00
Shutter Speed Value           : 1
Aperture Value                : 1.8
Brightness Value              : 0.48
Exposure Compensation         : 0
Max Aperture Value            : 1.8
Metering Mode                 : Center-weighted average
Flash                         : No Flash
Focal Length                  : 5.4 mm
Sub Sec Time                  : 942
Sub Sec Time Original         : 942
Sub Sec Time Digitized        : 942
```

```
Color Space           : sRGB
Exif Image Width      : 4032
Exif Image Height     : 3024
Exposure Mode         : Auto
White Balance         : Auto
Digital Zoom Ratio    : 1
Focal Length In 35mm Format : 26 mm
Scene Capture Type    : Standard
Image Unique ID       : X12QSD02PM
Compression           : JPEG (old-style)
Thumbnail Offset      : 850
Thumbnail Length      : 58842
Image Width           : 4032
Image Height          : 3024
Encoding Process      : Baseline DCT, Huffman coding
Bits Per Sample       : 8
Color Components      : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Time Stamp            : 2023:10:16 15:48:58.042-04:00
MCC Data              : Poland
Aperture              : 1.8
Image Size            : 4032x3024
Megapixels            : 12.2
Scale Factor To 35 mm Equivalent: 4.8
Shutter Speed         : 1/50
Create Date           : 2023:10:16 21:48:57.942
Date/Time Original    : 2023:10:16 21:48:57.942+02:00
Modify Date           : 2023:10:16 21:48:57.942+02:00
Thumbnail Image       : (Binary data 58842 bytes, use -b option to extract)
Circle Of Confusion   : 0.006 mm
Field Of View         : 69.4 deg
Focal Length          : 5.4 mm (35 mm equivalent: 26.0 mm)
Hyperfocal Distance   : 2.60 m
Light Value           : 5.3
```

1. **Rozmiar:** 4.3MB
2. **Data Utworzenia:** 2023:10:16 21:48:57
3. **Urządzenie, które wykonało zdjęcie:** samsung SM-G780G
4. **Rotate:** X: 72, Y:72, Rotate 90 CW
5. **Czy flash był użyty:** nie
6. **Rozdzielczość:** 4032x3024 px
7. **Przysłona urządzenia:** 1.8
8. **Lokalizacja:** Brak, widoczne jest tylko MCC data: Polska
9. **Obiektywy urządzenia:** Brak

Zdjęcie otrzymane przez WhatsApp

Zdjęcie zostało przesłane przez Whatsapp. W danych jest niewiele informacji, Jedyna data, którą widać to data przesłania zdjęcia na komputer. Z interesujących informacji w danych znajdziemy jedynie wielkość zdjęcia, a także nazwę.


```
(julia@kali)-[~/Desktop]
$ exiftool whatsapp-photo.jpg
ExifTool Version Number      : 12.57
File Name                    : whatsapp-photo.jpg
Directory                   : .
File Size                    : 165 kB
File Modification Date/Time  : 2023:12:08 08:48:42-05:00
File Access Date/Time       : 2023:12:08 08:48:42-05:00
File Inode Change Date/Time  : 2023:12:08 08:49:34-05:00
File Permissions             : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : None
X Resolution                 : 1
Y Resolution                 : 1
Image Width                 : 1080
Image Height                : 1920
Encoding Process            : Progressive DCT, Huffman coding
Bits Per Sample             : 8
Color Components            : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                  : 1080x1920
Megapixels                  : 2.1
```

1. **Rozmiar:** 165 kB
2. **Data Utworzenia:** Brak
3. **Urządzenie, które wykonało zdjęcie:** Brak
4. **Rotate:** Brak
5. **Czy flash był użyty:** Brak informacji
6. **Rozdzielczość:** 1080x1920 px
7. **Przysłona urządzenia:** Brak informacji
8. **Lokalizacja:** Brak
9. **Obiektywy urządzenia:** Brak informacji

Zdjęcie z Google Grafika

Przebadane zdjęcie pochodzi ze strony Wikimedia Commons. Znajduje się tu data utworzenia, a także wiele informacji na temat profili i kolorów obrazu

```
(julia@kali)-[~/Desktop]
$ exiftool Lion_d\'Afrique.jpg
ExifTool Version Number      : 12.57
File Name                    : Lion_d\'Afrique.jpg
Directory                   : .
File Size                    : 1448 kB
File Modification Date/Time  : 2023:12:08 09:18:44-05:00
File Access Date/Time       : 2023:12:08 09:18:45-05:00
File Inode Change Date/Time  : 2023:12:08 09:18:44-05:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
Profile CMM Type             : Little CMS
Profile Version              : 2.1.0
Profile Class                : Display Device Profile
Color Space Data             : RGB
Profile Connection Space     : XYZ
Profile Date Time            : 2012:01:25 03:41:57
Profile File Signature       : acsp
Primary Platform             : Apple Computer Inc.
CMM Flags                    : Not Embedded, Independent
Device Manufacturer         :
Device Model                 :
Device Attributes            : Reflective, Glossy, Positive, Color
Rendering Intent             : Perceptual
Connection Space Illuminant  : 0.9642 1 0.82491
Profile Creator              : Little CMS
Profile ID                   : 0
Profile Description          : c2
Profile Copyright            : FB
Media White Point            : 0.9642 1 0.82491
Media Black Point            : 0.01205 0.0125 0.01031
Red Matrix Column            : 0.43607 0.22249 0.01392
Green Matrix Column          : 0.38515 0.71687 0.09708
Blue Matrix Column           : 0.14307 0.06061 0.7141
Red Tone Reproduction Curve  : (Binary data 64 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 64 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 64 bytes, use -b option to extract)
Image Width                  : 1879
Image Height                 : 2048
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1879x2048
Megapixels                   : 3.8
```

1. **Rozmiar:** 1448 kB
2. **Data Utworzenia:** 2012:01:25 03:41:57
3. **Urządzenie, które wykonało zdjęcie:** Brak, widzimy jedynie informację, że pierwotną platformą, na której został utworzony lub przetworzony plik był komputer Mac (Apple Computer Inc.)
4. **Rotate:** Brak
5. **Czy flash był użyty:** Brak informacji
6. **Rozdzielczość:** 1879x2048 px
7. **Przysłona urządzenia:** Brak informacji
8. **Lokalizacja:** Brak,

9. **Obiektywy urządzenia:** Brak informacji