Michał Dziarkowski,
Aleksandra Rząca,
Szymon Szkarłat

Testy Penetracyjne

Laboratorium 3

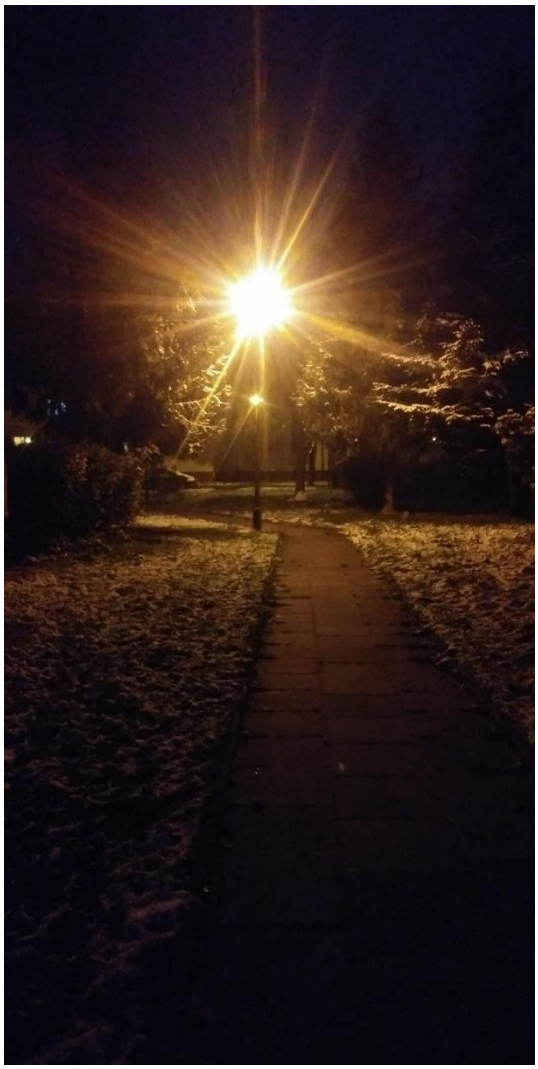
Spis treści

Zadanie 1

Narzędzie Exiftool

Exiftool jest to narzędzie działające za pomocą terminala, gdyż nie posiada GUI (interfejsu graficznego użytkownika), dostępne w systemie Kali Linux. Program ten pozwala na wyświetlanie, czyszczenie oraz edycje metadanych.

Wykonane zdjęcia



Efekty wywołania narzędzia Exiftool na oryginalnych plikach zdjęć.

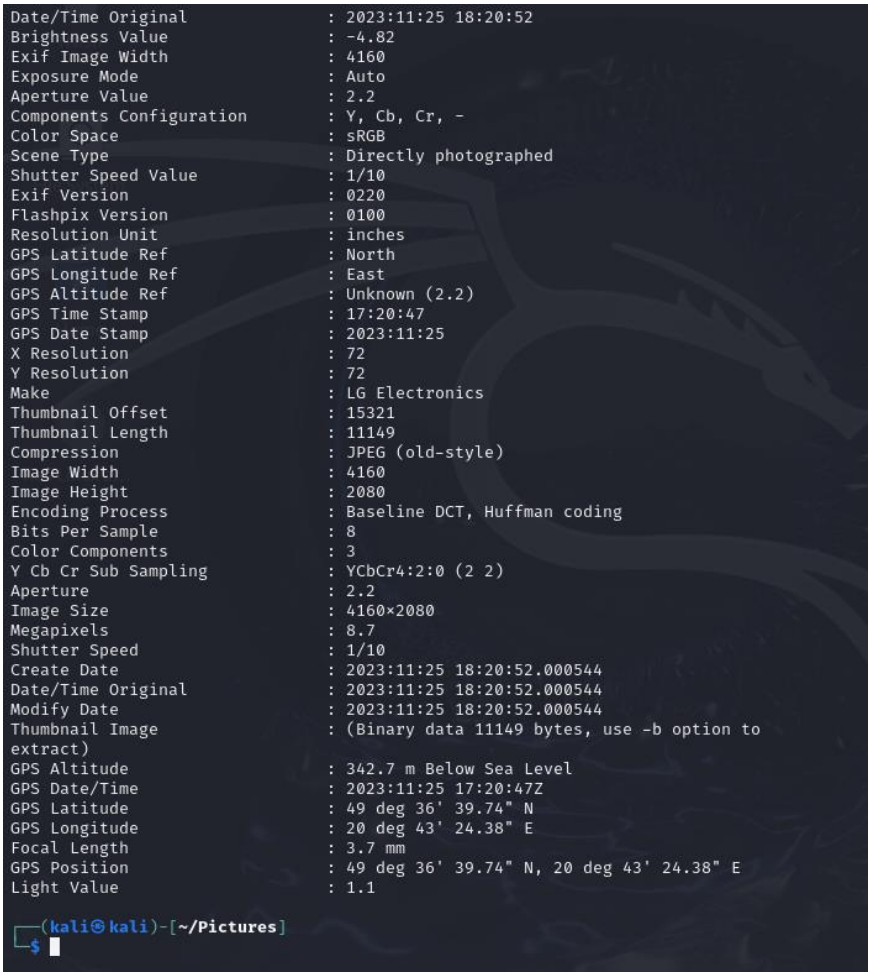
```
┌──(arzaca㉿kali)-[~/Desktop]
└─$ exiftool IMG_20240210_121931.jpg
ExifTool Version Number         : 12.76
File Name                       : IMG_20240210_121931.jpg
Directory                       : .
File Size                       : 4.7 MB
File Modification Date/Time     : 2024:02:10 12:19:33+01:00
File Access Date/Time           : 2024:11:02 01:02:51+01:00
File Inode Change Date/Time     : 2024:11:02 01:02:50+01:00
File Permissions                : -rwxrw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```

```
┌──(arzaca㉿kali)-[~/Desktop]
└─$ exiftool -a -G -gps* IMG_20240210_121931.jpg
[EXIF]          GPS Latitude                    : 49 deg 29' 32.59"
[EXIF]          GPS Altitude                    : 791.1253 m
[EXIF]          GPS Latitude Ref                : North
[EXIF]          GPS Speed                       : 1.332
[EXIF]          GPS Altitude Ref                : Above Sea Level
[EXIF]          GPS Processing Method           : gps
[EXIF]          GPS Speed Ref                   : km/h
[EXIF]          GPS Longitude Ref               : East
[EXIF]          GPS Time Stamp                  : 11:19:22
[EXIF]          GPS Longitude                   : 20 deg 42' 25.71"
[EXIF]          GPS Date Stamp                  : 2024:02:10
[Composite]     GPS Altitude                    : 791.1 m Above Sea Level
[Composite]     GPS Date/Time                   : 2024:02:10 11:19:22Z
[Composite]     GPS Latitude                    : 49 deg 29' 32.59" N
[Composite]     GPS Longitude                   : 20 deg 42' 25.71" E
[Composite]     GPS Position                    : 49 deg 29' 32.59" N, 20 deg 42' 25.71" E
```

```
┌──(kali㉿kali)-[~/Pictures]
└─$ exiftool photo1.jpg
ExifTool Version Number         : 12.76
File Name                       : photo1.jpg
Directory                       : .
File Size                       : 2.3 MB
File Modification Date/Time     : 2024:10:31 05:26:40-05:00
File Access Date/Time           : 2024:10:31 05:30:56-05:00
File Inode Change Date/Time     : 2024:10:31 05:30:56-05:00
File Permissions                : -rwxrw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Camera Model Name               : LG-M700
Orientation                     : Rotate 90 CW
Modify Date                     : 2023:11:25 18:20:52
Y Cb Cr Positioning             : Centered
Warning                         : [minor] Unrecognized MakerNotes
ISO                             : 2200
Exposure Program                : Not Defined
F Number                        : 2.2
Exposure Time                   : 1/10
Sensing Method                  : One-chip color area
Sub Sec Time Digitized          : 000544
Sub Sec Time Original           : 000544
Sub Sec Time                    : 000544
Focal Length                    : 3.7 mm
Flash                           : Off, Did not fire
Metering Mode                   : Center-weighted average
Scene Capture Type              : Standard
User Comment                    : 0  FM0 CR0 Prmid2 mxDrkA5.27 mxBrtA0.07 mxP
kNSat0.80 dr77.16 br1.25 wdr43.40 wbr0.83 sbr0.56 ldr79.55 lp60.0 [f0] 011011
111bfalic 00000
Interoperability Index          : R98 - DCF basic file (sRGB)
Interoperability Version        : 0100
Create Date                     : 2023:11:25 18:20:52
Exposure Compensation           : 0
Digital Zoom Ratio              : 1
Exif Image Height               : 2080
White Balance                   : Auto
```

Z wyników możemy odczytać takie parametry jak:

- File Name - Nazwa zdjęcia (photo1.jpg)
- File Size – Rozmiar pliku (2.3 MB)
- File Modification Date – Ostatnia data modyfikacji pliku (31.10.2024)
- File Permissions – Uprawnienia do pliku (-rwxrw-rw-)
- File Type oraz File Type Extension – typ pliku oraz rozszerzenie pliku (jpg – format popularny dla zdjęć)
- Camera Model Name – Nazwa modelu aparatu, którym było wykonywane zdjęcie (telefon LG)
- Orientation – informacja czy zdjęcie zostało wykonane pionowo czy poziomo (w tym przypadku zostało ono wykonane pionowo)
- Dodatkowe parametry opisujące zdjęcie (czy jest wycentrowane, czy użyto lampy błyskowej – flasha)
- Modify Date – Data ostatniej modyfikacji zdjęcia (zdjęcie to nie było modyfikowane, edytowane, ponieważ data jego wykonania oraz modyfikacji są takie same)
- Create Date – Data utworzenia pliku (2023:11:25 o godzinie 18:20)

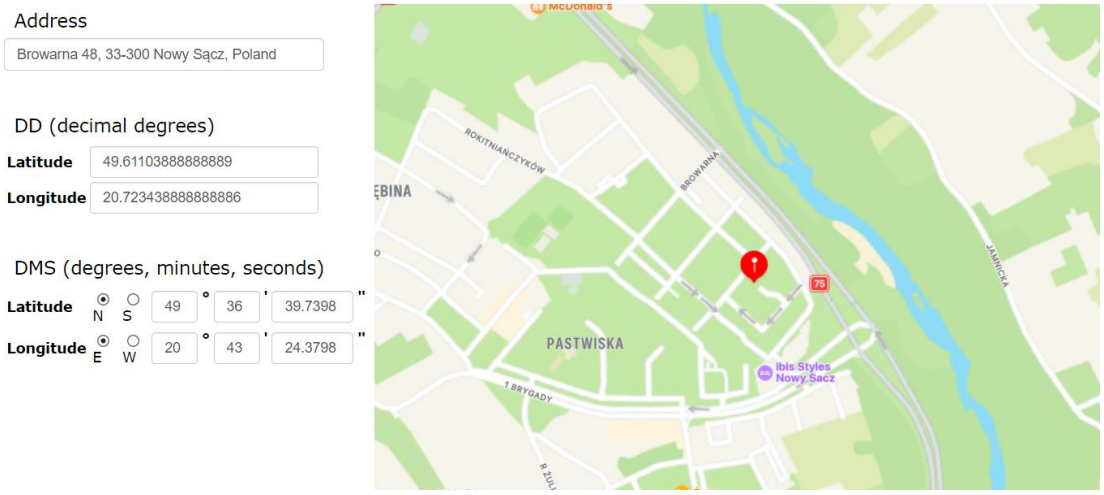


```
Date/Time Original              : 2023:11:25 18:20:52
Brightness Value                : -4.82
Exif Image Width                : 4160
Exposure Mode                   : Auto
Aperture Value                  : 2.2
Components Configuration        : Y, Cb, Cr, -
Color Space                     : sRGB
Scene Type                      : Directly photographed
Shutter Speed Value             : 1/10
Exif Version                    : 0220
Flashpix Version                : 0100
Resolution Unit                 : inches
GPS Latitude Ref                : North
GPS Longitude Ref               : East
GPS Altitude Ref                : Unknown (2.2)
GPS Time Stamp                  : 17:20:47
GPS Date Stamp                  : 2023:11:25
X Resolution                    : 72
Y Resolution                    : 72
Make                            : LG Electronics
Thumbnail Offset                : 15321
Thumbnail Length                : 11149
Compression                     : JPEG (old-style)
Image Width                     : 4160
Image Height                    : 2080
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 2.2
Image Size                      : 4160×2080
Megapixels                      : 8.7
Shutter Speed                   : 1/10
Create Date                     : 2023:11:25 18:20:52.000544
Date/Time Original              : 2023:11:25 18:20:52.000544
Modify Date                     : 2023:11:25 18:20:52.000544
Thumbnail Image                 : (Binary data 11149 bytes, use -b option to
extract)
GPS Altitude                    : 342.7 m Below Sea Level
GPS Date/Time                   : 2023:11:25 17:20:47Z
GPS Latitude                    : 49 deg 36' 39.74" N
GPS Longitude                   : 20 deg 43' 24.38" E
Focal Length                    : 3.7 mm
GPS Position                    : 49 deg 36' 39.74" N, 20 deg 43' 24.38" E
Light Value                     : 1.1

┌──(kali㉿kali)-[~/Pictures]
└─$
```

Dane lokalizacyjne informują, że:

- zdjęcie wykonano 342.7 m nad poziom morza.
- dane z GPS zostały pobrane o godz. 17:20, dnia 25.11.2023
- dokładne parametry lokalizacji to: 49 deg 36' 39.74" N, 20 deg 43' 24.38" E

Wprowadzając współrzędne do narzędzia online (https://gps-coordinates.org) sprawdzamy czy są poprawne. Porównujemy otrzymane wartości z lokalizacją, w której zostało wykonane zdjęcie. Można stwierdzić, że wartości się zgadzają.



Po wysłaniu tych samych zdjęć przez jeden z komunikatorów (facebook messenger) ponownie wykonujemy na nich polecenie exiftool:

```
┌──(arzaca㉿kali)-[~/Desktop]
└─$ exiftool download.jpg
ExifTool Version Number         : 12.76
File Name                       : download.jpg
Directory                       : .
File Size                       : 66 kB
File Modification Date/Time     : 2024:11:02 01:04:55+01:00
File Access Date/Time           : 2024:11:02 01:05:00+01:00
File Inode Change Date/Time     : 2024:11:02 01:04:58+01:00
File Permissions                : -rwxrw-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
```

```
┌──(arzaca㉿kali)-[~/Desktop]
└─$ exiftool -a -G -gps* download.jpg

┌──(arzaca㉿kali)-[~/Desktop]
└─$
```

```
┌──(kali㉿kali)-[~/Pictures]
└─$ exiftool photo2.jpeg
ExifTool Version Number         : 12.76
File Name                       : photo2.jpeg
Directory                       : .
File Size                       : 88 kB
File Modification Date/Time     : 2024:10:31 05:28:08-05:00
File Access Date/Time           : 2024:10:31 05:30:56-05:00
File Inode Change Date/Time     : 2024:10:31 05:30:56-05:00
File Permissions                : -rwxrw-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                     : 1024
Image Height                    : 2048
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                      : 1024×2048
Megapixels                      : 2.1

┌──(kali㉿kali)-[~/Pictures]
└─$
```

Danych, które wykryło narzędzie jest o wiele mniej. Przede wszystkim:

- Plik jest zdecydowanie lżejszy, waży zaledwie 88 kB. Jest to spowodowane za pewne faktem, że zawiera o wiele mniejszą ilość danych – nie posiada danych lokalizacyjnych.
- Są dane o ostatnich modyfikacjach pliku (np. data skopiowania pliku). Nie ma jednak informacji o dacie wykonania zdjęcia.
- Nie ma informacji o sprzęcie, przy pomocy którego wykonane zostało zdjęcie oraz o brak informacji o sposobie jego wykonania (np. orientacja w jakiej wykonano zdjęcie).
- Konkretnie dane dotyczące lokalizacji zostały całkowicie wykasowane.

Wnioski

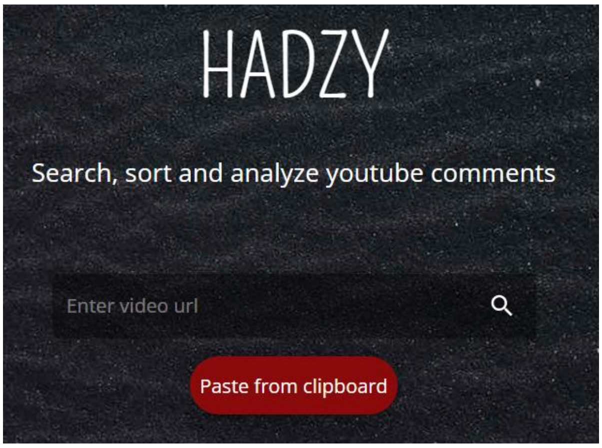
Metadane to szczegółowy zbiór informacji, który opisuje dane. W przypadku pliku są to między innymi dane o czasie wykonania go, sposobie jego wykonania czy lokalizacji. Metadane różnią się w zależności od rodzaju pliku. Dla prezentowanego przykładu są to dane o urządzeniu, którym wykonano zdjęcie, data wykonania zdjęcia, sposób jego wykonania oraz lokalizacja, w której zdjęcie zostało wykonane.
W porównaniu do drugiego wywołania programu exiftool można dojść do wniosku, że taki komunikator jak Messenger usuwa metadane z pliku, który przesyłamy. Zatem na podstawie zdjęcia pobranego z Messengera nie jesteśmy w stanie ustalić między innymi lokalizacji, w której wykonano zdjęcie.

Współczesne komunikatory w większości usuwają metadane zdjęć ze względów bezpieczeństwa, ale też np. aby możliwie zmniejszyć objętość danych (często widać to też po stracie na jakości zdjęcia). Warto mieć jednak na uwadze, że nie każdy portal czy komunikator musi usuwać metadane plików.

Zadanie 2

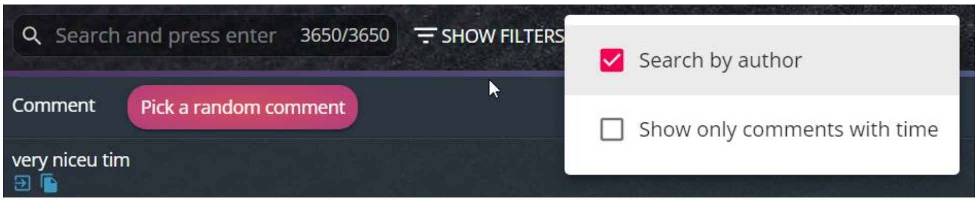
Istniejące narzędzie

https://www.hadzy.com



Zastosowanie:

1. Podajemy URL do interesującego nas wideo.
2. Klikamy Load Data a następnie View Comments.
3. W domyśle wyszukiwarka filtruje komentarze po treści, klikając w opcję Show Filters należy zaznaczyć opcję Search by author.



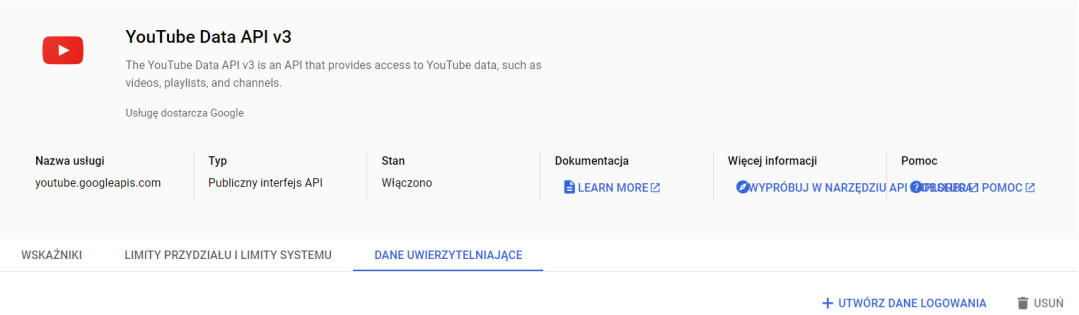
Program Python

Kod źródłowy:

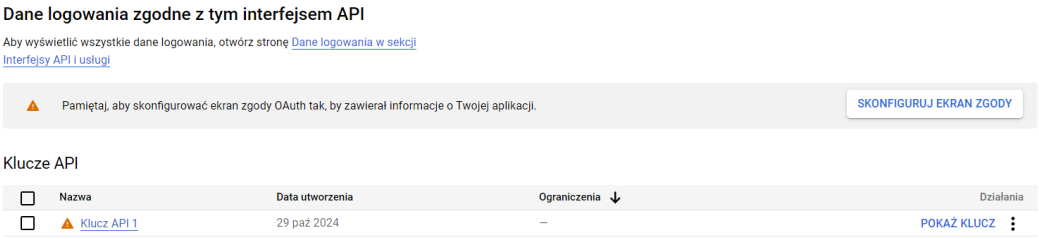
```python
import requests


# Settings
API_KEY = [redacted]
VIDEO_ID = 'M8ELgzg7SAo'
USER_NICK = '@KazSurma'


# Function for downloading comments
def get_comments(video_id, api_key):
    comments = []
    url = f'https://www.googleapis.com/youtube/v3/commentThreads'
    params = {
        'part': 'snippet',
        'videoId': video_id,
        'key': api_key,
        'textFormat': 'plainText',
        'maxResults': 100
    }

    while True:
        response = requests.get(url, params=params).json()
        for item in response['items']:
            comment = item['snippet']['topLevelComment']['snippet']
            comments.append({
                'author': comment['authorDisplayName'],
                'text': comment['textDisplay']
            })

        if 'nextPageToken' in response:
            params['pageToken'] = response['nextPageToken']
        else:
            break

    return comments


if __name__ == '__main__':
    all_comments = get_comments(VIDEO_ID, API_KEY)
    user_comments = [c for c in all_comments if c['author'] == USER_NICK]


    # Print results
    for comment in user_comments:
        print(f"{comment['author']}: {comment['text']}")

```

Opis działania:

1. Na początku podajemy klucz API, który został wygenerowany na stronie Google Cloud Platform.



Wygenerowany klucz API, który umieściłem w programie Python.



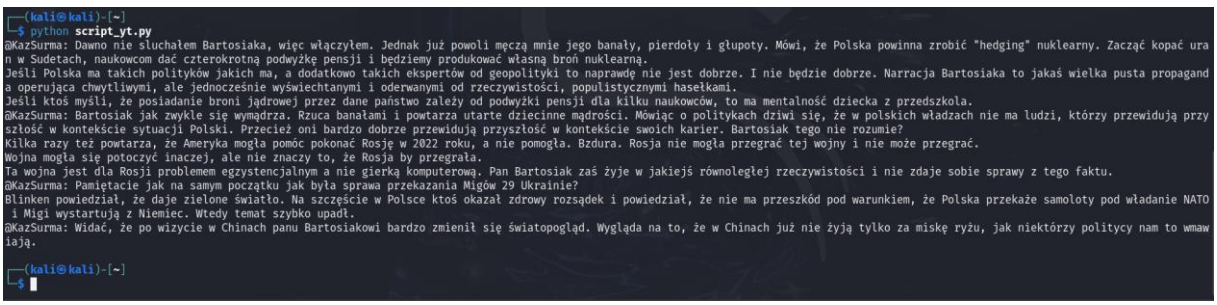
2. Poza kluczem API podajemy również id filmu na YouTube oraz nick użytkownika, którego komentarze chcemy wyświetlić.

3. Funkcja get_comments odpowiedzialna, jest za pobranie wszystkich komentarzy dla podanego filmu na platformie YouTube. Funkcja zwraca listę zebranych komentarzy.

4. Następnie zebrane komentarze, dla danego filmu są analizowane i dopasowywane dla konkretnego użytkownika, którego nick podaliśmy wcześniej. Komentarze tego użytkownika umieszczane są w liście, a następnie wyświetlane w odpowiedni sposób.

Wynik działania programu

Dla wybranego przeze mnie filmu, tj. https://www.youtube.com/watch?v=M8ELgzg7SAo oraz wybranego użytkownika o nicku: @KazSurma wynikiem działania programu są następujące cztery zaprezentowane komentarze, których treść umieszczam poniżej w postaci screena.



Zadanie 3

Do zadania wykorzystano środowisko laboratoryjne przygotowane na potrzeby Laboratorium 1.

Próba pierwsza

Maszyna wirtualna z systemem Windows 10, jak przedstawiono na rysunku technicznym posiada adres IP: 192.168.158.136, co więcej nie jest podatna na usługę SMB, co dowodzi poniższy screen.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script smb-vuln* -p 445 192.168.158.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 10:39 CDT
Nmap scan report for 192.168.158.136
Host is up (0.00066s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:5D:0D:48 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 6.03 seconds
```

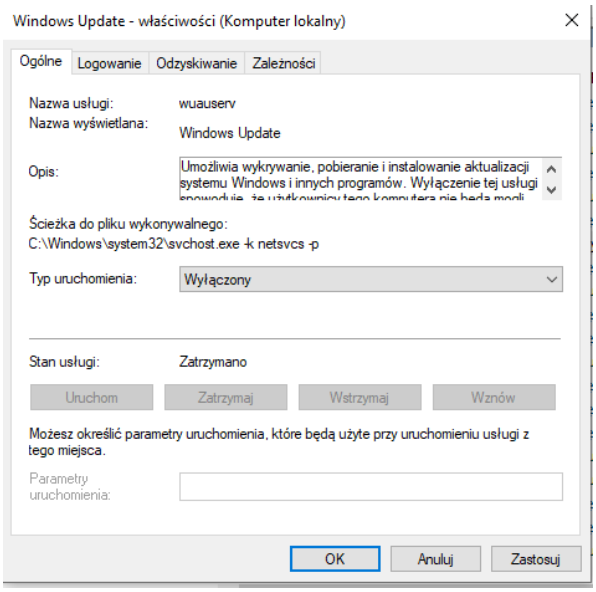
Zatem podjęto próbę konfiguracji systemu Windows, w taki sposób, aby maszyna była podatna.

1. Na początku uruchamiamy usługę SMBv1 i wyłączamy SMBv2, która jest domyślnie dostępna, w tej wersji systemu Windows 10, w tym celu wykorzystano PowerShella z uprawnieniami administratora.

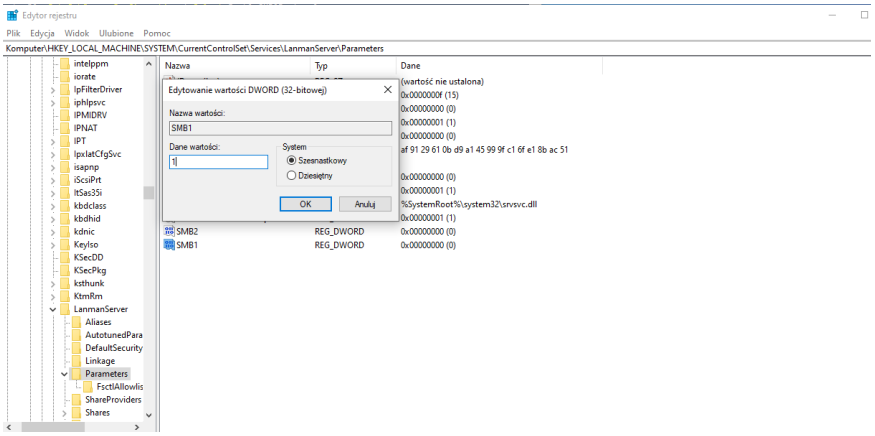
```
PS C:\Windows\system32> Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart


Path          :
Online        : True
RestartNeeded : False



PS C:\Windows\system32>
```

```
PS C:\Windows\system32> Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol

EnableSMB1Protocol EnableSMB2Protocol
------------------ ------------------
              True              False


PS C:\Windows\system32>
```

2. Kolejno wyłączamy aktualizacje w systemie Windows.



3. Dodajemy odpowiedni wpis w rejestrze, dotyczący wersji pierwszej usługi SMB.



4. Wynik wykonania polecenia jest trochę inny. Jednak maszyna z Windows 10 w dalszym ciągu nie jest podatna.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script smb-vuln* -p 445 192.168.158.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 11:05 CDT
Nmap scan report for 192.168.158.136
Host is up (0.00060s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:5D:0D:48 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 5.35 seconds
```

Próba druga

1. Sprawdzenie dostępu do usługi SMB na Windows Server 2022 (IPv4 192.168.189.133) z poziomu Kali Linux (IPv4 192.168.189.130).

Protokół SMB domyślnie używa portów 445 oraz 139. Otrzymany wynik skanowania za pomocą nmap pokazuje, że te porty na serwerze Windows Server 2022 są w stanie filtered, co oznacza, że są filtrowane przez zaporę. Można tymczasowo dezaktywować zaporę na Windowsie lub dodać regułę która zezwoli na ruch SMB i następnie ponowić skan.

```
┌──(arzaca㉿kali)-[~]
└─$ sudo nmap -p 445,139 192.168.189.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 13:24 CET
Nmap scan report for 192.168.189.133
Host is up (0.00068s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:2B:87:55 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

2. Wykrywanie podatności SMB przy pomocy skryptów nmap.

Wynik skanowania pokazuje, że skrypty smb-vuln-ms10-061 i smb-vuln-ms10-054 nie wykryły żadnych podatności ani nie udało się im nawiązać pełnego połączenia.

```
┌──(arzaca㉿kali)-[~]
└─$ nmap -Pn -p 139,445 --script=smb-vuln* 192.168.189.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 13:27 CET
Nmap scan report for 192.168.189.133
Host is up (0.00080s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 5.18 seconds
```

Wynik skryptu smb-protocols pokazuje, że serwer obsługuje nowsze wersje protokołu SMB: SMBv2 i SMBv3, które są bezpieczniejsze i lepiej chronione przed większością znanych podatności.

```
┌──(arzaca㉿kali)-[~]
└─$ sudo nmap -p 445 --script smb-protocols 192.168.189.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 13:36 CET
Nmap scan report for 192.168.189.133
Host is up (0.00039s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:2B:87:55 (VMware)

Host script results:
| smb-protocols:
|   dialects:
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|_    3:1:1

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

3. Konfiguracja SMBv1.

Na Windows Server 2022 uruchamiamy komendę w PowerShell: *Enable-WindowsOptionalFeature -Online -FeatureName smb1protocol -NoRestart* i restartujemy maszynę. Następnie ponawiamy skanowanie za pomocą nmap.

```
PS C:\Users\Administrator> Get-WindowsOptionalFeature -Online -FeatureName smb1protocol


FeatureName      : SMB1Protocol
DisplayName      : SMB 1.0/CIFS File Sharing Support
Description      : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.
RestartRequired  : Possible
State            : Enabled
CustomProperties :
                   ServerComponent\Description : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer
                   Browser protocol.
                   ServerComponent\DisplayName : SMB 1.0/CIFS File Sharing Support
                   ServerComponent\Id : 487
                   ServerComponent\Type : Feature
                   ServerComponent\UniqueName : FS-SMB1
                   ServerComponent\Deploys\Update\Name : SMB1Protocol
```

Mimo to, nmap nie wykazuje znaleznienia podatności ze względu na brak dostępnych użytkowników. Konfigurujemy przykładowe konto na Windowsie.

```
PS C:\Users\Administrator> New-LocalUser -Name

Name     Enabled Description
----     ------- -----------
testuser True    User for SMB access
```

```
└─$ nmap -Pn -p 139,445 --script=smb-vuln* 192.168.189.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 13:45 CET
Nmap scan report for 192.168.189.133
Host is up (0.00065s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: No accounts left to try
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 6.25 seconds
```

```
└─$ smbclient //192.168.189.133/IPC$ -U testuser

Password for [WORKGROUP\testuser]:
Try "help" to get a list of possible commands.
smb: \>
```

Po utworzeniu dodatkowego użytkownika komunikat przy użyciu nmap się zmienia, ale wciąż podatność nie jest wykryta.

```
└─$ nmap -Pn -p 139,445 --script=smb-vuln* 192.168.189.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 14:09 CET
Nmap scan report for 192.168.189.133
Host is up (0.00057s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

```
└─$ nmap -p 139,445 --script=smb-enum-shares,smb-enum-users --script-args user=testuser,password=Password123! 192.168.189.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 14:15 CET
Nmap scan report for 192.168.189.133
Host is up (0.00072s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\192.168.189.133\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.189.133\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.189.133\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Podsumowanie pierwszych dwóch prób

Testy podatności na SMBv1 przeprowadzone na dwóch różnych środowiskach laboratoryjnych, zarówno na systemach Windows 10 oraz Windows Server 2022 nie przyniosły oczekiwanego wyniku. Pomimo różnych kroków konfiguracji, takich jak wymuszenie aktywacji SMBv1, wyłączenie zapory oraz dodanie konta użytkownika, nie udało się uzyskać podatności na SMBv1.

Oba systemy korzystają domyślnie z nowszych wersji protokołów, takich jak SMBv2 i SMBv3, które są bardziej zabezpieczone. Ponad to, filtracja portów (445 i 139) przez zaporę w środowisku Windows Server 2022 ograniczała dostępność usługi SMB z zewnętrznych hostów. Wyłączenie zapory lub dodanie odpowiednich reguł było niezbędne do umożliwienia pełnego skanowania.

Podatna usługa SMB w systemie Windows 7

Jak wynika chociażby z tego źródła https://msrc.microsoft.com/blog/2017/05/customer-guidance-for-wannacrypt-attacks/, ale i wielu innych (https://sekurak.pl/wyciek-z-nsa-nowy-ransomware-blyskawicznie-atakujacy-kolejne-kraje-wana-decrypt0r-2-0/, https://kapitanhack.pl/2020/02/27/nieskategoryzowane/czym-jest-protokol-smbv1-i-dlaczego-powinienes-go-wylaczyc/), w 2017 roku system Windows 10 doczekał się aktualizacji, która naprawiła podatność związaną z nieprawidłowym działaniem SMB. Zatem postanowiliśmy zainstalować system Windows 7, który nie zawierał takowej aktualizacji dla usługi SMB, aby sprawdzić, czy faktycznie system Windows 7 posiada podatność związaną z usługą SMB.

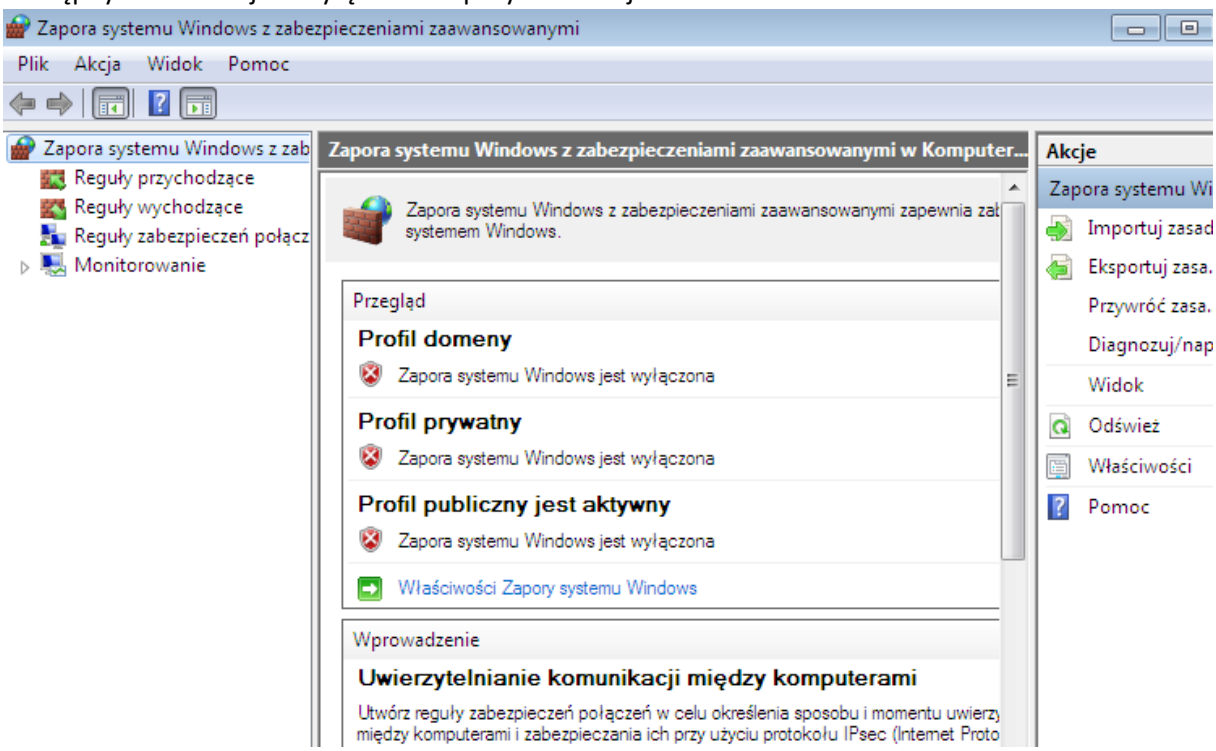
Adres IP maszyny wirtualnej w środowisku testowym.

```
C:\Windows\system32>ipconfig

Konfiguracja IP systemu Windows


Karta Ethernet Połączenie lokalne:

   Sufiks DNS konkretnego połączenia : localdomain
   Adres IPv6 połączenia lokalnego . : fe80::6d8d:e6a4:efb8:528%11
   Adres IPv4. . . . . . . . . . . . : 192.168.158.144
   Maska podsieci. . . . . . . . . . : 255.255.255.0
   Brama domyślna. . . . . . . . . . : 192.168.158.2

Karta tunelowa isatap.localdomain:

   Stan nośnika . . . . . . . . . . .: Nośnik odłączony
   Sufiks DNS konkretnego połączenia : localdomain

C:\Windows\system32>_
```

Poniżej zaprezentowano wprowadzone zmiany, które mają na celu uruchomienie SMBv1.

```
C:\Windows\system32>sc config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20
/nsi
[SC] ChangeServiceConfig SUKCES

C:\Windows\system32>sc config mrxsmb10 start= auto
[SC] ChangeServiceConfig SUKCES

C:\Windows\system32>sc qc lanmanserver
[SC] QueryServiceConfig SUKCES

SERVICE_NAME: lanmanserver
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\system32\svchost.exe -k netsvcs
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Serwer
        DEPENDENCIES       : SamSS
                           : Srv
        SERVICE_START_NAME : LocalSystem

C:\Windows\system32>_
```

Następnym krokiem jest wyłączenie zapory sieciowej.



Poniżej zaprezentowano wyniki skanowania stacji z systemem Windows 7. Skanowanie miało na celu sprawdzenie czy stacja ma podatną usługę SMB. Okazało się, że Windows 7 jest podatny, co przedstawia poniższy zrzut ekranu.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script smb-vuln* -p 445 192.168.158.144
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-06 07:44
 CST
Nmap scan report for 192.168.158.144
Host is up (0.00089s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:B1:FB:1E (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 ser
vers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists
in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/cu
stomer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-201
7-0143
|_      https://technet.microsoft.com/en-us/library/security/m
s17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds
```