

# Projekt\_WCYB

Marcin Dadura nr: 303\_688

---

Organizacja - Politechnika Gdańska

---

## Zadanie 1 - OSINT (3p.)

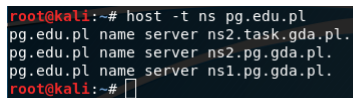
Dla wytypowanej organizacji należy zebrać informacje dostępne w Internecie, w szczególności te udostępniane przez wyszukiwarkę Google oraz za pomocą narzędzi do rekonesansu. Jakie informacje nas interesują?

a) infrastruktura posiadana przez podmiot (serwery, ich adresy IP, prawdopodobna lokalizacja geograficzna), b) ostatnie informacje o problemach bezpieczeństwa, c) ostatni restart serwerów, d) usługi oferowane przez serwery, e) posiadane domeny i subdomeny, f) informacje w cache'u wyszukiwarki Google, g) numery telefonów, PESEL itp. oraz inne istotne informacje, które mogą zostać wykorzystane np. w socjotechnice oraz ogólnie w przeprowadzeniu udanych testów penetracyjnych.

---

a) infrastruktura posiadana przez podmiot (serwery, ich adresy IP, prawdopodobna lokalizacja geograficzna),

Serwery:



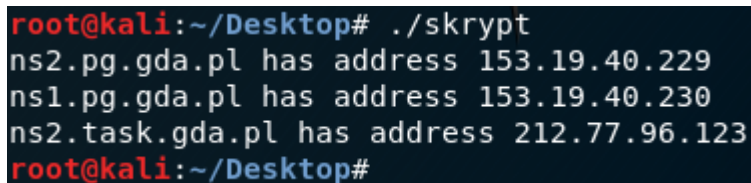
```
root@kali:~# host -t ns pg.edu.pl
pg.edu.pl name server ns2.task.gda.pl.
pg.edu.pl name server ns2.pg.gda.pl.
pg.edu.pl name server ns1.pg.gda.pl.
root@kali:~#
```

Adresy ip serwerów:

(skrypt:

```
#!/bin/bash

for x in $(host -t ns pg.edu.pl | cut -d " " -f 4 | rev | cut -c2- | rev) ; do host $x | grep "has address"; done
```




```
root@kali:~/Desktop# ./skrypt
ns2.pg.gda.pl has address 153.19.40.229
ns1.pg.gda.pl has address 153.19.40.230
ns2.task.gda.pl has address 212.77.96.123
root@kali:~/Desktop#
```


Prawdopodobna lokalizacja geograficzna

(strona <https://www.iplocation.net/>)


Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-1-1)

Domain Name	Country	Region	City
pg.edu.pl	Poland 	Pomorskie	Gdansk
ISP	Organization	Latitude	Longitude
Technical University of Gdansk Academic Computer Center Task	Not Available	54.3521	18.6464

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

Domain Name	Country	Region	City
pg.edu.pl	Poland 	Pomerania	Gdańsk
ISP	Organization	Latitude	Longitude
<a href="#">Technical University of Gdansk, Academic Computer Center TASK</a>	TASK Academic Computer Network ( <a href="#">gda.pl</a> )	54.3731	18.6187

Geolocation data from [DB-IP](#) (Product: Full, 2020-1-1)

Domain Name	Country	Region	City
pg.edu.pl	Poland 	Mazovia	Warsaw
ISP	Organization	Latitude	Longitude
Technical University of Gdansk	Task PG	52.2297	21.0122

(strona <https://pg.edu.pl/uczelnia/kontakt>)

## Adres

Politechnika Gdańska

ul. Gabriela Narutowicza 11/12

80-233 Gdańsk

Polska

---

### b) Ostatnie informacje o problemach bezpieczeństwa.

- Wyciek danych studnetów z pewnej strony promotora. (1/10/2018  
<https://niebezpiecznik.pl/post/prywatne-serwisy-wykladowcow-z-danymi-osobowymi->

[czyli-uczelnianych-wpadek-czesc-v/](#))

Przedmiot: [REDACTED]								
Nr albumu	Nazwisko	Imię	Aktywność	Kol1	Kol2	Suma	Egz1	
Grupa dziekańska [REDACTED]								
1[REDACTED]1	[REDACTED]	Aleksander		26	14	40	spr. poprawkowy	
1[REDACTED]2	[REDACTED]	Agnieszka		24	24	48	EGZAMIN	
1[REDACTED]3	[REDACTED]	Małgorzata		9	17	26	spr. poprawkowy	
1[REDACTED]7	[REDACTED]	Angelika		44	45	89	EGZAMIN	
1[REDACTED]2	[REDACTED]	Weronika		25	24	49	EGZAMIN	
1[REDACTED]6	[REDACTED]	Paulina		7		7	spr. poprawkowy	
1[REDACTED]2	[REDACTED]	Kinga		10	33	43	EGZAMIN	
1[REDACTED]8	[REDACTED]	Karolina	1	11	38	50	EGZAMIN	
1[REDACTED]2	[REDACTED]	Oliwia		30	34	64	EGZAMIN	
1[REDACTED]2	[REDACTED]	Marta		2	3	5	spr. poprawkowy	
1[REDACTED]5	[REDACTED]	Kuba		19	29	48	EGZAMIN	
1[REDACTED]8	[REDACTED]	Marcelina		29	21	50	EGZAMIN	
1[REDACTED]7	[REDACTED]	Klaudia		33	25	58	EGZAMIN	
1[REDACTED]7	[REDACTED]	Daria		32	41	73	EGZAMIN	
1[REDACTED]3	[REDACTED]	Patrycja				0	spr. poprawkowy	
1[REDACTED]9	[REDACTED]	Julia		9	0	9	spr. poprawkowy	
1[REDACTED]8	[REDACTED]	Jan				0	spr. poprawkowy	
1[REDACTED]6	[REDACTED]	Michał		1	15	16	spr. poprawkowy	
1[REDACTED]6	[REDACTED]	Szymon		17	43	60	EGZAMIN	
1[REDACTED]2	[REDACTED]	Paweł		20		20	spr. poprawkowy	

- Opublikowanie przez Anonymous baz danych wydziałów PG (Studenckiego Klubu Turystycznego Politechniki Gdańskiej, Wydziału Architektury Politechniki Gdańskiej, witrynie Katedry Chemii Nieorganicznej Politechniki Gdańskiej) (30.03.2012 <https://niebezpiecznik.pl/post/anonymous-polska-bazy-sadow-i-prokuratur/>)

---

c) ostatni restart serwerów

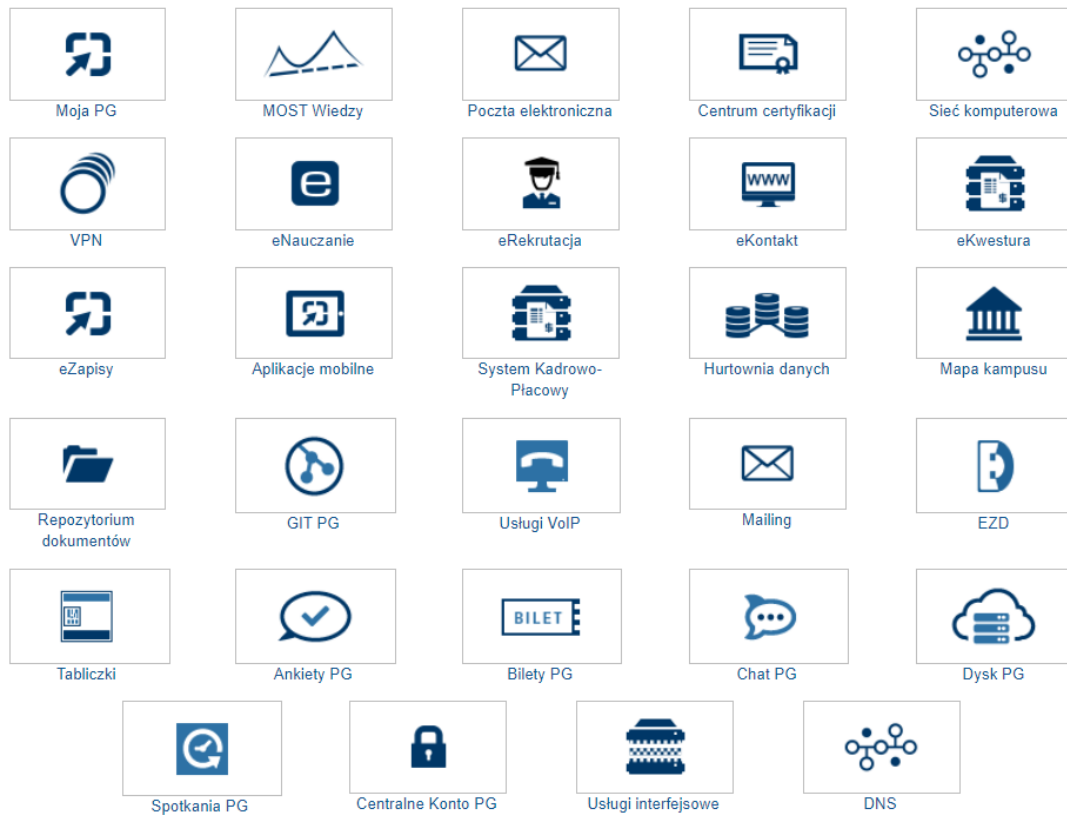
**NAPISZ COS**

---

d) Usługi oferowane przez serwery.

<https://cui.pg.edu.pl/>

## Centrum Usług Informatycznych PG udostępnia poniższe usługi



### e) Posiadane domeny i subdomeny.

Użyłem komendy `dnsrecon -d pg.edu.pl`

```
root@kali:~# dnsrecon -d pg.edu.pl
[*] Performing General Enumeration of Domain: pg.edu.pl
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to pg.edu.pl
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for pg.edu.pl
[*] SOA ns1.pg.gda.pl 153.19.40.230
[*] NS ns1.pg.gda.pl 153.19.40.230
[*] Bind Version for 153.19.40.230 Just go away.
[*] NS ns1.pg.gda.pl 2001:4070:10:4000::230
[*] NS ns2.task.gda.pl 212.77.96.123
[*] Bind Version for 212.77.96.123 :o)
[*] NS ns2.pg.gda.pl 153.19.40.229
[*] Bind Version for 153.19.40.229 Just go away.
[*] NS ns2.pg.gda.pl 2001:4070:10:4000::229
[*] MX smtp.pg.edu.pl 153.19.40.251
[*] MX smtp.pg.edu.pl 2001:4070:10:4000::251
[*] A pg.edu.pl 153.19.40.170
[*] TXT pg.edu.pl v=spf1 ip4:153.19.32.0/19 ip6:2001:4070:10:4000::0/118 -all
[*] TXT pg.edu.pl google-site-verification=Y5dxT1f2ERr8NXs-1szaGEmN-eQzYzIbJYNeE8eDjr4
[*] TXT _domainkey.pg.edu.pl v=spf1 ip4:153.19.32.0/19 ip6:2001:4070:10:4000::0/118 -all
[*] TXT _domainkey.pg.edu.pl google-site-verification=Y5dxT1f2ERr8NXs-1szaGEmN-eQzYzIbJYNeE8eDjr4
[*] Enumerating SRV Records
[-] No SRV Records Found for pg.edu.pl
[+] 0 Records Found
root@kali:~#
```

Do wylistowania subdomen użyłem narzędzia sublist3r . Użyłem komendy: `python sublist3r.py -d pg.edu.pl -o subdomains.txt`

```
root@kali:~/Desktop/Sublister/Sublist3r# python sublist3r.py -d pg.edu.pl -o subdomains.txt
```

```
#!
Intelij
OpenStuck
skryp
Sublist3r
Main.java
10.c
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for pg.edu.pl
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Saving results to file: subdomains.txt
[-] Total Unique Subdomains Found: 187
www.pg.edu.pl
akademiki.pg.edu.pl
ankieta.pg.edu.pl
ankieta.pg.edu.pl<BR>www.ankieta.pg.edu.pl
ankiety.pg.edu.pl
arch.pg.edu.pl
www.arch.pg.edu.pl
```

```
www.pg.edu.pl
akademiki.pg.edu.pl
ankieta.pg.edu.pl
ankiety.pg.edu.pl
arch.pg.edu.pl
arch.pg.edu.pl
rekrutacja.awf.pg.edu.pl
bg.pg.edu.pl
han.bg.pg.edu.pl
login.han.bg.pg.edu.pl
katalog.bg.pg.edu.pl
bilety.pg.edu.pl
biuletyn.pg.edu.pl
biuletyn.pg.edu.pl
budzetobywatelski.pg.edu.pl
campus.pg.edu.pl
cdn.pg.edu.pl
chat.pg.edu.pl
chem.pg.edu.pl
fmch.chem.pg.edu.pl
leki.chem.pg.edu.pl
chor.pg.edu.pl
cjo.pg.edu.pl
cjo.pg.edu.pl
mediateka.cjo.pg.edu.pl
clickmeeting.pg.edu.pl
```

cmtm.pg.edu.pl  
cnm.pg.edu.pl  
cnm-srv.pg.edu.pl  
csa.pg.edu.pl  
ctwit-crm.pg.edu.pl  
ctwt.pg.edu.pl  
cui.pg.edu.pl  
domki.pg.edu.pl  
drive.pg.edu.pl  
dzp.pg.edu.pl  
dzp.pg.edu.pl  
ects.pg.edu.pl  
eduroam.pg.edu.pl  
eia.pg.edu.pl  
chmura.eia.pg.edu.pl  
eka.pg.edu.pl  
eka.pg.edu.pl  
enauczanie.pg.edu.pl  
energia2015.pg.edu.pl  
etee2015.pg.edu.pl  
eti.pg.edu.pl  
sis.eti.pg.edu.pl  
ezd.pg.edu.pl  
ezd-prod-app1.pg.edu.pl  
ezd-prod-db1.pg.edu.pl  
festiwal.pg.edu.pl  
forum.pg.edu.pl  
ftims.pg.edu.pl  
git.pg.edu.pl  
help.pg.edu.pl  
imap.pg.edu.pl  
kampus.pg.edu.pl  
kp.pg.edu.pl  
kube-prod-front1.pg.edu.pl  
kube-prod-front2.pg.edu.pl  
kube-prod-front3.pg.edu.pl  
kube-prod-front4.pg.edu.pl  
kube-prod-http.pg.edu.pl  
logowanie.pg.edu.pl  
smtprelay.mailing.pg.edu.pl  
mba.pg.edu.pl  
mech.pg.edu.pl  
media.pg.edu.pl  
meteo.pg.edu.pl  
mif.pg.edu.pl  
mobile.pg.edu.pl  
moja.pg.edu.pl  
pg.moja.pg.edu.pl  
nextcloud.pg.edu.pl  
oio.pg.edu.pl  
piksel.oio.pg.edu.pl  
pixel.oio.pg.edu.pl

synertech.oio.pg.edu.pl  
okno.pg.edu.pl  
pg.pg.edu.pl  
phplist.pg.edu.pl  
platnosci.pg.edu.pl  
poczta.pg.edu.pl  
pomoc.pg.edu.pl  
position.pg.edu.pl  
praca.pg.edu.pl  
pub.pg.edu.pl  
rekrutacja.pg.edu.pl  
repos.pg.edu.pl  
roundcube.pg.edu.pl  
samorzad.pg.edu.pl  
sk.pg.edu.pl  
sklep.pg.edu.pl  
smtp.pg.edu.pl  
smtplist.pg.edu.pl  
spotkania.pg.edu.pl  
student.pg.edu.pl  
imap.student.pg.edu.pl  
smtp.student.pg.edu.pl  
chat.szko1.pg.edu.pl  
ezd-szkol-app1.szko1.pg.edu.pl  
kube-szkol-http.szko1.pg.edu.pl  
logowanie.szko1.pg.edu.pl  
pg.moja.szko1.pg.edu.pl  
techem9.pg.edu.pl  
platnosci.test.pg.edu.pl  
repos.test.pg.edu.pl  
webmail.test.pg.edu.pl  
vcenter.pg.edu.pl  
voip.pg.edu.pl  
vpn.pg.edu.pl  
vpn1.pg.edu.pl  
vpn2.pg.edu.pl  
webapps.pg.edu.pl  
webinar.pg.edu.pl  
webmail.pg.edu.pl  
ext.webmail.pg.edu.pl  
wilis.pg.edu.pl  
wilis.pg.edu.pl  
wit.pg.edu.pl  
wzie.pg.edu.pl  
xn--wili-o5a.pg.edu.pl  
zadania.pg.edu.pl  
zapisy.pg.edu.pl  
zgloszenia.pg.edu.pl  
zie.pg.edu.pl  
crk.zie.pg.edu.pl  
ekonomia-kultura-wartosci.zie.pg.edu.pl  
imap.zie.pg.edu.pl

kizo.zie.pg.edu.pl  
mail.zie.pg.edu.pl  
marketinfo.zie.pg.edu.pl  
mx.zie.pg.edu.pl  
pop3.zie.pg.edu.pl  
smtp.zie.pg.edu.pl  
zlecenia.pg.edu.pl

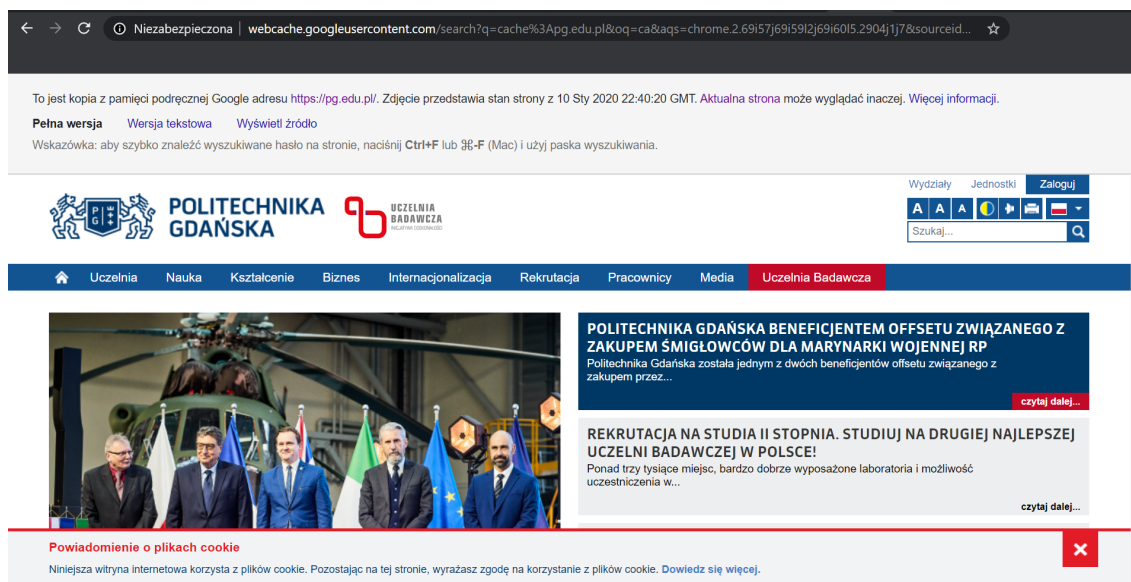
## f) Informacje w cache'u wyszukiwarki Google.

Aby dostać się do cashe wyszukiwarki googla należu wpisać: `cache:pg.edu.pl`

Pojawia się następujące informacje:

To jest kopia z pamięci podręcznej Google adresu <https://pg.edu.pl/>. Zdjęcie przedstawia stan strony z 10 Sty 2020 22:40:20 GMT

- ostatnia aktualizacja pamieci cashe to 10 styczani 2020, 22.40.20 GMT
- czas dostępu 13.01.2020, 18.06 GMT



Strona nie zapisuje cashe-u na dysku hosta który korzysta ze strony  
(<https://www.shodan.io/host/153.19.40.170>):



## Services

80	HTTP/1.1 301 Moved Permanently
tcp	content-length: 0
http	location: https://pg.edu.pl/



443
tcp
https



HTTP/1.1 200 OK  
set-cookie: EKSESSIONID=E32682DE0DF8216DB30B19EE56D9718B; Domain=.pg.edu.pl; Path=/  
expires: Thu, 01 Jan 1970 00:00:00 GMT  
cache-control: private, no-cache, no-store, must-revalidate  
pragma: no-cache  
set-cookie: GUEST\_LANGUAGE\_ID=pl\_PL; Expires=Tue, 12-Jan-2021 07:47:09 GMT; Path=/  
set-cookie: COOKIE\_SUPPORT=true; Expires=Tue, 12-Jan-2021 07:47:09 GMT; Path=/  
content-type: text/html; charset=UTF-8  
date: Mon, 13 Jan 2020 07:47:11 GMT  
vary: Accept-Encoding  
age: 0  
etag: W/"2d03f577"  
x-varnish-cache: MISS

**g) Numery telefonów, PESEL itp. oraz inne istotne informacje, które mogą zostać wykorzystane np. w socjotechnice oraz ogólnie w przeprowadzeniu udanych testów penetracyjnych.**

**Dane kontaktowe oraz adres organizacji wraz z NIP oraz REGON**

## Dane kontaktowe

### Adres

Politechnika Gdańska  
ul. Gabriela Narutowicza 11/12  
80-233 Gdańsk  
Polska

 [zobacz lokalizację na mapie](#)

NIP: 5840203593, REGON: 000001620

---

## Wydziały Politechniki Gdańskiej

## Jednostki organizacyjne Politechniki Gdańskiej

---

### Informacja o numerach telefonów w Politechnice Gdańskiej

tel.: +48 58 347 11 00

### Informacja o pracownikach

<https://moja.pg.edu.pl/app/addressBook/>

### Informacja o rekrutacji

pon.–pt. 7.30–15.30

tel.: +48 58 348 67 00

<https://pg.edu.pl/rekrutacja>

[rekrutacja@pg.edu.pl](mailto:rekrutacja@pg.edu.pl)

### Kontakt dla mediów

tel.: +48 58 347 29 99

[biuro.prasowe@pg.edu.pl](mailto:biuro.prasowe@pg.edu.pl)

### Webmaster

tel.: +48 58 348 63 37

[webmaster@pg.edu.pl](mailto:webmaster@pg.edu.pl)

nr albumu studentów



site:pg.edu.pl intext:"album"



...konkursu jest przedstawienie najlepszych, najciekawszych ...

## [PDF] Wykład 5 Tworzenie zaawansowanych aplikacji w środowisku ...

pg.edu.pl › documents › Translate this page

Model View Controller how. Album. AlbumView. ViewController update notify update user actions. Tworzenie zaawansowanych aplikacji w środowisku iOS.

## [XLS] Report

eia.pg.edu.pl › documents › sem\_1\_AiR › Translate this page

2014/15. 2. Grupa dziekańska 1, Grupa dziekańska 2, Grupa dziekańska 3. 3. Lp. Nazwisko, Imię, Album, Lp. Nazwisko, Imię, Album, Lp. Nazwisko, Imię, Album.

## Simon Laks In Between – powrót wielkiego kompozytora ...

https://pg.edu.pl › sgold › asset\_publisher › content › ot... › Translate this page

Simon Laks In Between to muzyczny album, który przybliży fascynującą, zapomnianą postać i twórczość polsko-żydowskiego kompozytora. Koncertowa ...

Podział na grupy sem. I r.ak. 2014/15			Grupa dziekańska 1			Grupa dziekańska 2			Grupa dziekańska 3		
Lp.	Nazwisko	Imię	Album	Lp.	Nazwisko	Imię	Album	Lp.	Nazwisko	Imię	Album
1	CZERNIOWSKI	MICHAŁ	1	1	BARANIA	MICHAŁ	1	1	BARANIA	MICHAŁ	1
2	DĄBKOWSKI	MATEUSZ	2	2	BERENY	PAWEŁ	2	2	DEBICKI	MACEJ	2
3	DOBROWOLSKI	KAROL	3	3	BOBKOWSKI	WOLCIECH	3	3	DOMACHOWSKI	SZYMON	3
4	FLISZCZAK	ROMAN	4	4	BOGDAŃ	BEATA	4	4	DOBROWOLSKI	KAROL	4
5	GRZYBOWSKI	DARIUSZ	5	5	BORAWSKI	KRZYSZTOF	5	5	DOBROWOLSKI	KAROL	5
6	HOLYSE	SEBASTYAN	6	6	BOUZY	MACEJ	6	6	DOBROWOLSKI	KAROL	6
7	JAKUBOWSKI	MIKOŁAJ	7	7	BRONIAK	MIKOŁAJ	7	7	DOBROWOLSKI	KAROL	7
8	KŁOSIŃSKI	TOMASZ	8	8	BRONIAK	MIKOŁAJ	8	8	DOBROWOLSKI	KAROL	8
9	KOCOR	MIKOŁAJ	9	9	BULCZAK	MIKOŁAJ	9	9	DOBROWOLSKI	KAROL	9
10	KOLAROWSKA	JULIA	10	10	BRUTECZKI	SZYMON	10	10	DOBROWOLSKI	KAROL	10
11	KULIŃSKI	KRZYSZTOF	11	11	CEBARK	KATARZYNA	11	11	DOBROWOLSKI	KAROL	11
12	LADACH	KRZYSZTOF	12	12	CELEŃSKI	ADRIAN	12	12	DOBROWOLSKI	KAROL	12
13	LEBENT	PAWEŁ	13	13	CICHOCKI	OSKAR	13	13	DOBROWOLSKI	KAROL	13
14	MACIOWSKI	MATEUSZ	14	14	CZAPUR	ADAM	14	14	DOBROWOLSKI	KAROL	14
15	MILCZAK	MICHAŁ	15	15	CZERNIOWSKI	MIKOŁAJ	15	15	DOBROWOLSKI	KAROL	15
16	MILCZAK	MATEUSZ	16	16	CZYŻEWSKI	MATEUSZ	16	16	DOBROWOLSKI	KAROL	16
17	MILCZAK	MATEUSZ	17	17	DANIELEWSKI	RAFAŁ	17	17	DOBROWOLSKI	KAROL	17
18	PARZYCKI	JAN	18	18	DANIELEWSKI	RAFAŁ	18	18	DOBROWOLSKI	KAROL	18
19	PŁOCIN	PAWEŁ	19	19	DĄBKOWSKI	HUBERT	19	19	DOBROWOLSKI	KAROL	19
20	PŁOCIN	PAWEŁ	20	20	DEBICKI	MACEJ	20	20	DOBROWOLSKI	KAROL	20
21	PŁOCIN	PAWEŁ	21	21	DEBICKI	MACEJ	21	21	DOBROWOLSKI	KAROL	21
22	PŁOCIN	PAWEŁ	22	22	DEBICKI	MACEJ	22	22	DOBROWOLSKI	KAROL	22
23	PŁOCIN	PAWEŁ	23	23	DEBICKI	MACEJ	23	23	DOBROWOLSKI	KAROL	23
24	PŁOCIN	PAWEŁ	24	24	DEBICKI	MACEJ	24	24	DOBROWOLSKI	KAROL	24
25	PŁOCIN	PAWEŁ	25	25	DEBICKI	MACEJ	25	25	DOBROWOLSKI	KAROL	25
26	PŁOCIN	PAWEŁ	26	26	DEBICKI	MACEJ	26	26	DOBROWOLSKI	KAROL	26
27	PŁOCIN	PAWEŁ	27	27	DEBICKI	MACEJ	27	27	DOBROWOLSKI	KAROL	27
28	PŁOCIN	PAWEŁ	28	28	DEBICKI	MACEJ	28	28	DOBROWOLSKI	KAROL	28
29	PŁOCIN	PAWEŁ	29	29	DEBICKI	MACEJ	29	29	DOBROWOLSKI	KAROL	29
30	PŁOCIN	PAWEŁ	30	30	DEBICKI	MACEJ	30	30	DOBROWOLSKI	KAROL	30
31	PŁOCIN	PAWEŁ	31	31	DEBICKI	MACEJ	31	31	DOBROWOLSKI	KAROL	31
32	PŁOCIN	PAWEŁ	32	32	DEBICKI	MACEJ	32	32	DOBROWOLSKI	KAROL	32