

1. Napisz skrypt, który pobiera listę adresów IP (z pliku lub argumentów wejściowych), a następnie sprawdza reputację każdego z nich, korzystając z API AbuseIPDB. Wyniki zapisz do pliku CSV

```
1  #!/bin/bash
2  ARGS=("ipAddress" "abuseConfidenceScore" "countryName" "domain" "totalReports")
3
4  if [ -f "$1" ]; then
5      IP=$(cat $1)
6  else
7      IP="$@"
8  fi
9
10 echo "IP,ConfidenceScore,Country,Domain,TotalReports" > raport.csv
11
12 function check(){
13     ip=$1
14     QUERY=$(curl -s -G https://api.abuseipdb.com/api/v2/check \
15 --data-urlencode "ipAddress=$ip" \
16 -d maxAgeInDays=90 \
17 -d verbose \
18 -H "Key: acca343895ec6dd4a5ef26d155dd9dbebc7b2d978fe9e5752c3f53ada892f6177d6b280af23c81d6" \
19 -H "Accept: application/json"
20 )
21     results=""
22     for argu in ${ARGS[@]}; do
23         results+="$(echo "$QUERY" | jq -r ".data.$argu"),"
24     done
25     results="${results%},"
26     echo $results >> raport.csv
27 }
28
29 for ip in ${IP[@]}; do
30     echo "Trwa sprawdzanie ip: $ip"
31     check $ip
32 done
33
```

```
(kali㉿kali)-[~/Documents/Programowanie_skryptowe/lab9]  
$ ./abuse1.sh ip_addr.txt
```

```
Trwa sprawdzanie ip: 103.108.94.19  
Trwa sprawdzanie ip: 196.251.70.87  
Trwa sprawdzanie ip: 115.116.64.144  
Trwa sprawdzanie ip: 80.240.252.168  
Trwa sprawdzanie ip: 121.229.0.135
```

```
(kali㉿kali)-[~/Documents/Programowanie_skryptowe/lab9]  
$ cat raport.csv
```

```
IP,ConfidenceScore,Country,Domain,TotalReports  
103.108.94.19,0,New Zealand,intergrid.com.au,0  
196.251.70.87,100,Netherlands,cheapy.host,4824  
115.116.64.144,0,India,tatacommunications.com,0  
80.240.252.168,100,Russian Federation,rt.ru,1916  
121.229.0.135,100,China,chinatelecom.cn,922
```

```
(kali㉿kali)-[~/Documents/Programowanie_skryptowe/lab9]  
$ ./abuse1.sh 103.108.94.19 121.229.0.135 80.240.252.168
```

```
Trwa sprawdzanie ip: 103.108.94.19  
Trwa sprawdzanie ip: 121.229.0.135  
Trwa sprawdzanie ip: 80.240.252.168
```

```
(kali㉿kali)-[~/Documents/Programowanie_skryptowe/lab9]  
$ cat raport.csv
```

```
IP,ConfidenceScore,Country,Domain,TotalReports  
103.108.94.19,0,New Zealand,intergrid.com.au,0  
121.229.0.135,100,China,chinatelecom.cn,922  
80.240.252.168,100,Russian Federation,rt.ru,1916
```

2. Napisz skrypt, który wyświetli podstawowe dane i listę otwartych portów dla podanego adresu IP przez API Shodan (zoomeye).

```

$ shodan.sh
1  #!/bin/bash
2
3  api_key="j52H0U"
4  if [ -f "$1" ]; then
5      IP=$(cat $1)
6  else
7      IP="$@"
8  fi
9
10 function checkIP(){
11     request=$(curl -s -X GET "https://api.shodan.io/shodan/host/$1?key=$api_key" )
12     echo "Organisation: $(echo "$request" | jq -r '.org' )"
13     echo "ISP: $(echo "$request" | jq -r '.isp' )"
14     echo "Country: $(echo "$request" | jq -r '.country_code' )"
15     echo "City: $(echo "$request" | jq -r '.data[0].location.city' )"
16     echo "Hostnames: $(echo "$request" | jq -r '.data[0].hostnames[]' )"
17     echo "OS: $(echo "$request" | jq -r '.data[1].cpe23[1]' )"
18     echo "Open ports: $(echo "$request" | jq -r '.ports' )"
19     echo ""
20     echo ""
21 }
22
23 for ip in ${IP[@]}; do
24     echo "Checking $ip..."
25     checkIP $ip
26 done

```

```

(kali㉿kali)-[~/Documents/Programowanie_skryptowe/lab9]
$ ./shodan.sh ip_addr.txt
Checking 196.251.70.87 ...
Organisation: internet-security-cheapyhost
ISP: cheapy.host LLC
Country: NL
City: Amsterdam
Hostnames:
OS: null
Open ports: [
  22
]

Checking 121.229.0.135 ...
Organisation: CHINANET jiangsu province network
ISP: CHINANET-BACKBONE
Country: CN
City: Shanghai
Hostnames:
OS: cpe:2.3:o:debian:debian_linux
Open ports: [
  123,
  21,
  22
]

```