



Politechnika Wrocławska

SPRAWOZDANIE Z ZAJĘĆ LABORATORYJNYCH  
CYBERBEZPIECZEŃSTWO

---

**Lab 10**  
**Open source intelligence**

---

Tomasz Mroczko, 266604

January 12, 2024

# 1 Zadania

## Zadanie I

Wybierz jedną dobrze znaną domenę (np. [www.pwr.edu.pl](http://www.pwr.edu.pl)) Spróbuj zebrać bardziej szczegółowe informacje o domenie i jej właścicielu: na przykład kto zarejestrował domenę i kiedy, do kiedy jest ona ważna, czy używa cloudflare lub innej ochrony DDOS,

Wybrana została witryna <http://www.polkowicka.pl/menu.html>. Jest to strona internetowa jednej z niewielu restauracji w moim rodzinnym mieście - Polkowicach.

## Zadanie II

Przepytaj bazę whois `whois example.com`

```
DOMAIN NAME:          polkowicka.pl
registrant type:      organization
nameservers:          dns107.ovh.net.
                     ns107.ovh.net.
created:              2016.06.30 09:40:05
last modified:        2023.05.23 12:13:15
renewal date:         2024.06.30 09:40:05

no option

dnssec:               Unsigned

REGISTRAR:
Consulting Service Sp. z o.o.
ul. Jerzego Iwanowa-Szajnowicza 7 lok. U3
02-796 Warszawa
Polska/Poland
+48.221238080
domeny@ConsultingService.pl

WHOIS database responses: https://dns.pl/en/whois
WHOIS displays data with a delay not exceeding 15 minutes in relation to the .pl Registry system
```

Komenda `whois` dostarczyła sporo informacji na temat domeny. Została ona zarejestrowana przez organizację i utworzona 30 czerwca 2016 roku. Ostatnia modyfikacja wykonana została 23 maja 2023 roku, a domena wygasa 30 czerwca 2024 roku. Serwery nazw (DNS) to `dns107.ovh.net` oraz `ns107.ovh.net`. Rejestrat to Consulting Service, z siedzibą w Warszawie. Można skontaktować się z nimi poprzez nr telefonu: +48.221238080 lub adres email: `domeny@ConsultingService.pl`.

## Zadanie III

Zbierz informacje o serwerach DNS i odpowiednich rekordach domeny docelowej:

- Użyj narzędzia wiersza poleceń, aby wyszukać adres IP hosta na serwerze DNS
  - `host www.example.pl`

```
sejsmo@DESKTOP-00J23TV: /usr/share/nmap/scripts$ host polkowicka.pl
polkowicka.pl has address 87.98.239.3
polkowicka.pl mail is handled by 10 mx3.mail.ovh.net.
polkowicka.pl mail is handled by 1 mx4.mail.ovh.net.
```

Adres na serwerze DNS to 87.98.239.3

- Użyj programu `dig` w celu przepytania DNS

- *dig polkowicka.pl any*

```
>>> dig 9.18.12-0ubuntu0.22.04.3-Ubuntu <<<> polkowicka.pl any @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 22013
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;polkowicka.pl.                IN      ANY

;; ANSWER SECTION:
polkowicka.pl. 3600 IN SOA dns107.ovh.net. tech.ovh.net. 2020120400 86400 3600 3600000 300
polkowicka.pl. 3600 IN NS dns107.ovh.net.
polkowicka.pl. 3600 IN NS ns107.ovh.net.
polkowicka.pl. 3600 IN MX 1 mx4.mail.ovh.net.
polkowicka.pl. 3600 IN MX 10 mx3.mail.ovh.net.
polkowicka.pl. 3600 IN A 87.98.239.3
polkowicka.pl. 3600 IN TXT "i|www.polkowicka.pl"

;; Query time: 80 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (TCP)
;; WHEN: Thu Jan 11 16:01:24 CET 2024
;; MSG SIZE rcvd: 224
```

To polecenie wykonuj zapytanie DNS do serwera 8.8.8.8 (bez podania adresu ip serwera DNS, pojawiał się timeout). Zwraca ono wszystkie rekordy DNS dla domeny polkowicka.pl.

- *dig -x 8.8.8.8*

```
>>> dig 9.18.12-0ubuntu0.22.04.3-Ubuntu <<<> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 34099
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.        IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa. 0 IN PTR dns.google.

;; Query time: 10 msec
;; SERVER: 172.18.208.1#53(172.18.208.1) (UDP)
;; WHEN: Thu Jan 11 16:02:10 CET 2024
;; MSG SIZE rcvd: 82
```

To polecenie wykonuje odwrotne wyszukiwanie DNS. Pozwala ono uzyskać nazwę domenową dla konkretnego adresu IP. W tym wypadku pokazano że 8.8.8.8 to adres IP serwera DNS firmy Google.

- *dig @8.8.8.8 polkowicka.pl MX*

```
$ dig @8.8.8.8 polkowicka.pl MX
; <<>> DiG 9.19.17-1-Debian <<>> @8.8.8.8 polkowicka.pl MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 6549
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;polkowicka.pl.                IN      MX

;; ANSWER SECTION:
polkowicka.pl. 3600 IN MX 1 mx4.mail.ovh.net.
polkowicka.pl. 3600 IN MX 10 mx3.mail.ovh.net.

;; Query time: 52 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Thu Jan 11 16:41:37 CET 2024
;; MSG SIZE rcvd: 94
```

Komedna pobiera rekordy Mail Exchange (MX) podanej domeny. Są one odpowiedzialne za obsługę email domeny.

- *dig polkowicka.pl +trace* Polecenie to wykonuje śledzenie trasy pakietów zapytania DNS dla domeny.

- Określ primary DNS dla danej domeny

```
(kali@kali)-[~]  
$ host -t soa polkowicka.pl  
polkowicka.pl has SOA record dns107.ovh.net. tech.ovh.net. 2020120400  
86400 3600 3600000 300
```

Znaleziono dwa serwery DNS dla domeny polkowicka.pl. Są to: dns107.ovh.net oraz ns107.ovh.net.

- Dowiedz się jak jest wartość TTL i czy żądana domena została zapisana w pamięci podręcznej DNS.

```
(kali@kali)-[~]  
$ dig @dns107.ovh.net polkowicka.pl +noall +answer  
polkowicka.pl.      3600    IN      A       87.98.239.3
```

Wartość TTL (Time To Live) na primary DNS wynosi 3600 sekund.

- Dowiedz się, jak dawno dana domena była żądana w niektórych DNS (np. 1.1.1.1, 8.8.8.8, lokalny DNS, ...)

Nie udało mi się wykonać tego zadania.

## Zadanie IV

Użyj polecenia `dnsenum`

- `dnsenum polkowicka.pl`

```
$ dnsenum polkowicka.pl
dnsenum VERSION:1.2.6

----- polkowicka.pl -----

Host's addresses:

polkowicka.pl.          3600    IN      A       87.9
8.239.3

Name Servers:

dns107.ovh.net.         1559    IN      A       213.
251.188.151
ns107.ovh.net.          2797    IN      A       213.
251.128.151

Mail (MX) Servers:

mx4.mail.ovh.net.       60      IN      A       178.
32.124.207
mx3.mail.ovh.net.       60      IN      A       91.1
21.53.175

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for polkowicka.pl on dns107.ovh.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for polkowicka.pl on ns107.ovh.net ...
AXFR record query failed: REFUSED

Brute forcing with /usr/share/dnsenum/dns.txt:

test.polkowicka.pl.     3600    IN      A       87.9
8.239.3
www.polkowicka.pl.     3600    IN      A       87.9
8.239.3

polkowicka.pl class C netranges:

87.98.239.0/24
```

Polecenie *dnsenum* ujawniło wiele informacji na temat domeny. Adres IP hosta, serwery nazw, serwery pocztowe oraz wiele innych. Narzędzie przeprowadziło również atak typu "brute force" na subdomeny przy użyciu słownika dostępnego w lokalizacji */usr/share/dnsenum/dns.txt* (domyślna lokalizacja). Odnaleziono subdomeny *test.polkowicka.pl* i *www.polkowicka.pl* z przypisanym adresem IP 87.98.239.3.

- *dnsenum -f dns.txt polkowicka.pl* Opcja ta pozwala podać własny plik z listą subdomen do przeszukania.

## Zadanie V

*Znajdź wszystkie adresy IP i nazwy domenowe dla danego celu*

```

NS: dns.pwr.wroc.pl. dns2.pwr.wroc.pl. ns2.net.icm.edu.pl. ns1.net.icm.edu.pl.
SOA: dns.pwr.wroc.pl. (156.17.18.10)
Zone: failure
Wildcard: failure
Found: ad.pwr.edu.pl. (156.17.70.205)
Nearby:
{'156.17.70.200': '200-70-17-156.pwr.wroc.pl.',
'156.17.70.201': '201-70-17-156.pwr.wroc.pl.',
'156.17.70.202': '202-70-17-156.pwr.wroc.pl.',
'156.17.70.203': '203-70-17-156.pwr.wroc.pl.',
'156.17.70.204': '204-70-17-156.pwr.wroc.pl.',
'156.17.70.205': '205-70-17-156.pwr.wroc.pl.',
'156.17.70.206': '206-70-17-156.pwr.wroc.pl.',
'156.17.70.207': '207-70-17-156.pwr.wroc.pl.',
'156.17.70.208': '208-70-17-156.pwr.wroc.pl.',
'156.17.70.209': 'adcs.pwr.wroc.pl.',
'156.17.70.210': 'credens.pwr.wroc.pl.'}
Found: ae.pwr.edu.pl. (156.17.193.59)
Nearby:
{'156.17.193.58': 'vm-icewarp.wcss.wroc.pl.',
'156.17.193.59': 'vm-webmin2.wcss.wroc.pl.',
'156.17.193.62': 'gw-v119.wask.wroc.pl.'}
Found: ai.pwr.edu.pl. (104.198.14.52)
Nearby:
{'104.198.14.47': '47.14.198.104.bc.googleusercontent.com.',
'104.198.14.48': '48.14.198.104.bc.googleusercontent.com.',
'104.198.14.49': '49.14.198.104.bc.googleusercontent.com.',
'104.198.14.50': '50.14.198.104.bc.googleusercontent.com.',
'104.198.14.51': '51.14.198.104.bc.googleusercontent.com.',
'104.198.14.52': '52.14.198.104.bc.googleusercontent.com.',
'104.198.14.53': '53.14.198.104.bc.googleusercontent.com.',
'104.198.14.54': '54.14.198.104.bc.googleusercontent.com.',
'104.198.14.55': '55.14.198.104.bc.googleusercontent.com.',
'104.198.14.56': '56.14.198.104.bc.googleusercontent.com.',
'104.198.14.57': '57.14.198.104.bc.googleusercontent.com.'}

```

Figure 1: Część wyników polecenia *fierce* dla domeny *pwr.edu.pl*

Polecenie wykonane zostało dla domeny *polkowicka.pl* oraz *pwr.edu.pl*. Jeśli chodzi o wyniki dla małej domeny *polkowicka.pl*, to nie udało się znaleźć żadnych adresów IP. W przypadku *pwr.edu.pl* znaleziono wiele adresów oraz nazw domenowych.

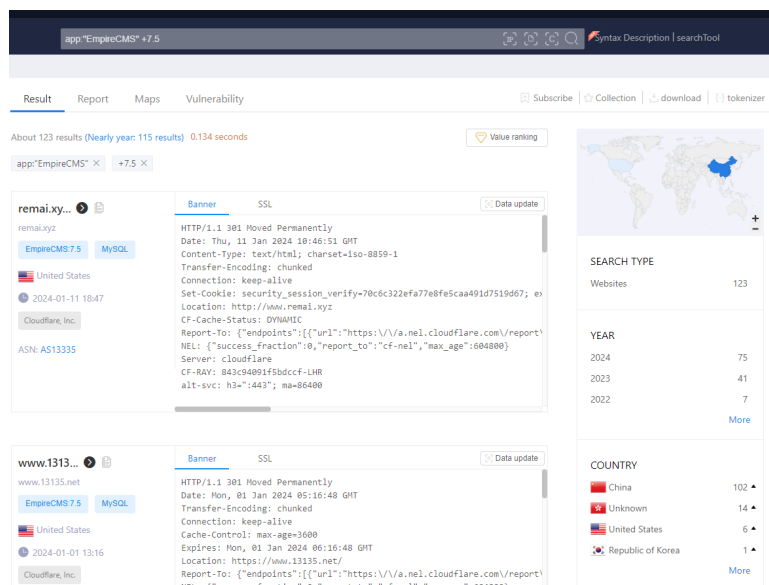
## Zadanie X

Korzystając z <https://nvd.nist.gov/vuln/search> wyszukaj luki w zabezpieczeniach jakiegoś typu usługi (ssh, ftp, ssl, apache, qnap, western digital. . .) oraz w kolejnym zapytaniu dotyczącym jakiegoś urządzenia ( np. router bezprzewodowy, router bezprzewodowy asus, tp-link). Znajdź konkretny problem związany z tą usługą (urządzeniem) - jest on opisany jako CVE - numer roku. Znajdź krytyczne luki w zabezpieczeniach. Opisz lukę. Znajdź link do strony internetowej z exploitem i / lub szczegółowym opisem luki.

- **Usługa narażona na atak: EmpireCMS, wersja 7.5**  
 EmpireCMS v7.5, posiada lukę w zabezpieczeniach podczas konfigurowania haseł FTP. Jest to luka typu SQL Injection.  
 Link do opisu luki [CVE-2023-50073](#)  
 Link do exploitu <https://github.com/leadscloud/EmpireCMS/issues/7>
- **Urządzenie narażone na atak: Gra Nintendo "Mario Kart Wii"**  
 Podatność typu buffer overflow pozwala może być wykorzystana przez klienta geometry do wykonania kodu na maszynie za pomocą spreparowanego pakietu.  
 Link do opisu luki [CVE-2023-35856](#)  
 Link do exploitu <https://github.com/MikelsAStar/Mario-Kart-Wii-Remote-Code-Execution>

## Zadanie XI

Korzystając z wyników z poprzedniego punktu (np. Openssh 7.7 jest podatny) wyszukaj systemy z tą podatnością (z punktu X)



Wyszukiwanie na stronie [zoomeye.org](https://zoomeye.org) pokazało że 123 systemy używają EmpireCMS w wersji 7.5. Zdecydowanie najwięcej systemów jest w Chinach (102), ale są też systemy w Stanach Zjednoczonych (6), Korei (1).

## 2 Pytania

### Pytanie I

*Jak możliwe jest tworzenie odcisków palców systemu operacyjnego?*

Cyfrowe odciski palców pozwalają na identyfikację systemu operacyjnego na podstawie zebranych informacji. Zbierane są informacje takie jak właściwości sprzętowe, charakterystyka środowiska, informacje o nagłówkach pakietów sieciowych, informacje o systemie plików, informacje o procesach, informacje o zainstalowanych pakietach. Tworzenie odcisków palca polega na analizie tych cech i identyfikacji systemu operacyjnego na podstawie zebranych danych. Niektóre z metod wykorzystywanych do tworzenia odcisków palców to:

- **Narzędzia do skanowania systemu i zbierania informacji**
- **Analiza ruchu sieciowego i nagłówków pakietów**
- **Analiza cech sprzętu**

Narzędzia takie jak *dig*, *whois*, *host* mogą być pomocne do tworzenia cyfrowych odcisków palców. Są one legalne i pozwalają zebrać znaczną ilość danych.

### Pytanie II

*Dlaczego pobieranie odcisków palców systemu operacyjnego może być ważne dla bezpieczeństwa?*

Pobieranie odcisków palców może być ważne, ponieważ pozwala na identyfikację użytkowników, systemów, urządzeń, aplikacji. Pozwala to na zwiększenie bezpieczeństwa poprzez identyfikację i weryfikację. Dzięki temu można ograniczyć dostępne treści tylko dla wybranych użytkowników, zablokować dostęp do systemu dla nieznanych.

Analiza pozwala także na monitorowanie bezpieczeństwa systemu i wykrywanie niepożądanych zmian.

### **Pytanie III**

*Jaka jest różnica między pasywnym i aktywnym tworzeniem odcisku palca systemu operacyjnego?*

Aktywne tworzenie odcisku palca polega na jawnym, planowanym gromadzeniu informacji o systemie operacyjnym, zwykle przy pomocy specjalnych narzędzi. Pasywne tworzenie odcisku palca polega na gromadzeniu informacji w tle, bez dodatkowych akcji użytkownika, często bez jego wiedzy.

### **Pytanie IV**

*Czy można chronić systemy przed pobieraniem odcisków palców systemu operacyjnego?*

Można zwiększyć bezpieczeństwo systemu poprzez zmniejszenie ilości informacji dostępnych dla osób trzecich. Należy na bieżąco aktualizować oprogramowanie, dbanie o prywatność oraz korzystanie z zaufanych narzędzi. Przydatne może być korzystanie z usługi VPN, która pozwala na ukrycie adresu IP.

### **Pytanie V**

*Czy można oszukać intruza i pokazać mu, że twój system nie jest dostępny?*

Korzystanie z firewalla może pomóc ukryć system przed intruzami.

### **Pytanie VI**

*Co to jest transfer stref DNS i jakie jest ryzyko związane z tym mechanizmem?*

Transfer stref DNS to proces synchronizacji danych pomiędzy serwerami DNS. Pozwala on na przeniesienie danych z jednego serwera na drugi. Ryzyko związane z tym mechanizmem to możliwość uzyskania nieautoryzowanego dostępu do danych przez osobę trzecią.

<https://kb.wedos.com/pl/dns-pl/teoria-dns/domeny-i-dns/protokol-dns-axfr-transfer-strefy/>

### **Pytanie VII**

*Czy używanie metod OSINT w celu uzyskania poufnych informacji jest legalne?*

Teoretycznie używanie metod OSINT, jak sama nazwa wskazuje, jest legalne. Informacje które można pozyskać powinny być dostępne do publicznego wglądu. Jendak używanie metod OSINT w celu wykonywania nielegalnych czynności jest wątpliwe etycznie.

### **Pytanie VIII**

*Jakie jest największe zagrożenie w kontekście metod bezpieczeństwa i OSINT?*

Dużym zagrożeniem OSINT jest dostęp do ogromnych ilości danych osobowych. Może to prowadzić do poważnych problemów oraz wycieków prywatności. Napięcia pomiędzy Stanami Zjednoczonymi a Iranem były podsycane wykorzystaniem analizy OSINT. Analiza była używana do śledzenia ruchów militarnych obu stron. Hakerzy mogą wykorzystać OSINT do pozyskiwania adresów, numerów telefonów, a nawet danych finansowych i haseł.

<https://www.secjuice.com/the-dark-side-of-osint/>



## Pytanie IX

*Jak chronić poufne dane przed wyszukiwaniem OSINT?*

Aby chronić poufne dane należy starannie zarządzać danymi publikowanymi w internecie. Należy ograniczyć je do minimum i udostępniać tylko te dane, które są niezbędne. Pliki powinny być szyfrowane, a serwisy z których korzystamy godne zaufania. Należy również korzystać z VPN, aby ukryć adres IP.