

AUDYT CYBERBEZPIECZEŃSTWA

PROJEKT ZALICZENIOWY

Zestaw programów wsadowych realizujących rozpoznanie OSINT wybranego obiektu/firmy/organizacji

Wykonali:  
Radosław Lesiewicz, s10061  
Maciej Kowal, s10057

Laboratoria prowadzone przez: dr inż. Leszek Wolaniuk

Akademia Wojsk Lądowych

imienia Generała Tadeusza Kościuszki

we Wrocławiu

Wrocław 12 czerwca 2024r.

Spis treści

[1. Wstęp. 3](#_Toc161922536)

[1.1. Cel Laboratorium. 3](#_Toc161922537)

[1.2. Założenia wykonywanych zadań. 3](#_Toc161922538)

[1.3. Elementy składowe wykonanych zadań. 3](#_Toc161922539)

[2. Opis wykonanych zadań. 4](#_Toc161922540)

[2.1. Zadanie nr. 1 4](#_Toc161922541)

[2.2. Zadanie nr. 2 4](#_Toc161922542)

[2.3. Zadanie nr. 3 4](#_Toc161922543)

[3. Podsumowanie 5](#_Toc161922544)

[3.1. Wnioski 5](#_Toc161922545)

[Załączniki 6](#_Toc161922546)

**1. Wstęp**

OSINT (Open Source Intelligence) to technika zbierania informacji z publicznie dostępnych źródeł. Celem projektu jest stworzenie zestawu skryptów wsadowych, które umożliwią przeprowadzenie rozpoznania OSINT na wybranym obiekcie, firmie lub organizacji.

**2. Cel projektu**

Głównym celem jest zautomatyzowanie procesu zbierania informacji z różnych źródeł internetowych, aby uzyskać jak najwięcej danych o wybranym obiekcie, uporządkować i przedstawić.  
  
**Skrypty mają za zadanie:**

- Zidentyfikować i zebrać dane kontaktowe.

- Uzyskać informacje o domenach i powiązanych adresach IP.

- Wyszukać informacje w bazach danych rejestrów (np. WHOIS).

- Przeszukać publicznie dostępne raporty, artykuły i dokumenty.

**3. Technologie i narzędzia**

Wykorzystane zostaną następujące technologie i narzędzia:

Narzędzia OSINT: theHarvester, , Amass, Censys, Maltego, Sublist3r.

API: różne API dostępne online, np. Google Custom Search API.

**4. Struktura projektu**

Projekt będzie oparty na użyciu plików wsadowych, gdzie każdy z plików implementuje poszczególne narzędzie typu theHarvester, Maltego, Amass, Censys, Sublist3r. Każdy z tych plików będzie możliwy do uruchomienia z konsoli, np. za pomocą polecenia sudo ./NazwaNarzędzia.sh nazwa\_organizacji\_domeny. Dane zbierane przez poszczególne narzędzia będą zapisywane do osobnych plików tekstowych, aby zachować klarowność i uporządkowanie.  
  
**5. Plan realizacji projektu**

**Faza 1: Analiza wymagań i projektowanie architektury:** W tej fazie przeprowadzimy szczegółową analizę potrzeb użytkowników oraz zaprojektujemy strukturę projektu, uwzględniając wykorzystanie plików wsadowych do implementacji poszczególnych narzędzi OSINT.

**Faza 2: Implementacja poszczególnych modułów:** Przystąpimy do implementacji każdego modułu poprzez stworzenie plików wsadowych dla każdego narzędzia. Każdy plik będzie odpowiedzialny za uruchomienie danego narzędzia i zapisanie danych do odpowiedniego pliku tekstowego.

**Faza 3: Testowanie i optymalizacja:** Po zaimplementowaniu modułów przeprowadzimy dokładne testy, aby upewnić się, że każdy plik wsadowy działa poprawnie i zbiera odpowiednie dane. Następnie dokonamy wszelkich niezbędnych optymalizacji w celu poprawy wydajności i jakości kodu.

**Faza 4: Wdrożenie i szkolenie użytkowników:** Wdrożymy projekt w środowisku produkcyjnym oraz przeprowadzimy szkolenie użytkowników, aby mogli skutecznie korzystać z plików wsadowych i zbieranych danych.

**6. Implementacja programu**

**Stworzenie środowiska programistycznego:** Na początku stworzymy odpowiednie środowisko programistyczne, w którym będziemy pracować nad projektowaniem i implementacją plików wsadowych.

**Implementacja poszczególnych plików wsadowych:** Następnie przystąpimy do implementacji każdego pliku wsadowego zgodnie z wcześniej ustalonym planem. Będziemy regularnie testować każdy skrypt, aby upewnić się, że działa on poprawnie i zapisuje dane zgodnie z naszymi oczekiwaniami.

**Testowanie funkcjonalności i poprawa błędów:** Po zaimplementowaniu każdego pliku wsadowego przeprowadzimy szczegółowe testy funkcjonalne, aby upewnić się, że wszystkie narzędzia działają poprawnie. W przypadku wykrycia błędów dokonamy ich poprawy.

**Dokumentacja implementacji i instrukcja użytkowania:** Na koniec sporządzimy dokumentację techniczną, która opisze proces implementacji oraz instrukcję użytkowania dla osób, które będą korzystać z naszego programu.

7. Wyniki zbierania danych:

a) Plik wsadowy sublist3r.sh zbiera informacje o subdomenach dla podanej organizacji

* Pokazuje liczbę unikalnych subdomen znalezionych
* Wypisuje listę subdomen znalezionych dla danej organizacji

b) Plik wsadowy Maltego.sh zbiera informacje podane informacje:

* Nazwa domeny: np. wp.pl
* Typ abonenta: np. organizacja
* Serwery nazw (nameservers): np.
* - ns1.task.gda.pl [153.19.250.101]
* - ns1.wp.pl [212.77.106.200]
* - ns2.wp.pl [153.19.88.162]
* Data utworzenia: np. 28 kwietnia 1998 roku, 13:00:00
* Data ostatniej modyfikacji: np. 5 kwietnia 2024 roku, 16:21:04
* Data odnowienia: np. 27 kwietnia 2025 roku, 14:00:00
* Informacje dodatkowe:
  + - Opcja utworzenia: np. 10 lutego 2020 roku, 10:51:12
  + - Data wygaśnięcia opcji: np. 10 lutego 2026 roku, 10:51:12

Dodatkowo, Maltego wyświetla informacje dotyczące rejestratora domeny, w tym:

* Nazwa rejestratora:
* Adres rejestratora:
* Numer telefonu rejestratora:
* Adres e-mail rejestratora:

Maltego korzysta z odpowiedzi WHOIS, aby uzyskać te informacje i prezentuje je w formie graficznej, ułatwiając analizę związków między nimi.

c) Plik wsadowy Cynsys.sh zbiera informacje podane informacje:

Informacje o serwerach i usługach:

* Adresy IP
* Nazwy hostów
* Otwartych portów
* Banerów serwisowych (informacje przekazywane przez serwery podczas nawiązywania połączenia, np. typ i wersja serwera HTTP)
* Protokół komunikacyjny (np. HTTP, HTTPS, FTP)

Certyfikaty SSL/TLS:

* Dane z certyfikatów X.509 używanych do szyfrowania ruchu HTTPS
* Certyfikaty SSL, w tym certyfikaty pośrednie i korzeń
* Informacje o podpisujących jednostkach certyfikujących (CA)

Informacje DNS:

* Zapisy DNS, w tym rekordy A, AAAA, MX, TXT, CNAME, NS
* Historie zapytań DNS

Informacje o systemach operacyjnych i aplikacjach:

* Identyfikacja systemów operacyjnych działających na urządzeniach
* Wersje aplikacji i oprogramowania działającego na serwerach

Geolokalizacja:

* Informacje o lokalizacji fizycznej adresów IP, często na poziomie kraju, regionu i miasta

Informacje o organizacjach:

* Dane o organizacjach, które są właścicielami adresów IP
* Informacje o autonomicznych systemach (AS), do których należą adresy IP

d) Plik wsadowy Amass.sh zbiera informacje podane informacje:

Domeny i subdomeny: Zidentyfikowane pełne nazwy domen i subdomen związane z wp.pl (np. beta.tech.wp.pl, api.ac.wp.pl).

Rekordy adresów: Powiązania nazw domen z ich odpowiednimi adresami IP (np. wp.pl jest związane z 212.77.98.9).

Rekordy CNAME: Powiązania nazw domen z innymi nazwami domen (np. portal.twojaksiegowosc.wp.pl z a3c82b07599b8491a99012d13433ed1f-fc1f3484ce774853.elb.eu-central-1.amazonaws.com).

Rekordy NS: Serwery nazw dla domen (np. ns1.wp.pl, ns2.wp.pl).

Bloki adresów IP: Zakresy adresów IP, które zawierają określone adresy (np. 212.77.96.0/21 zawiera 212.77.98.9).

ASN: Numery systemów autonomicznych i organizacje nimi zarządzające (np. 12827 jest zarządzane przez WIRTUALNAPOLSKA GDANSK).