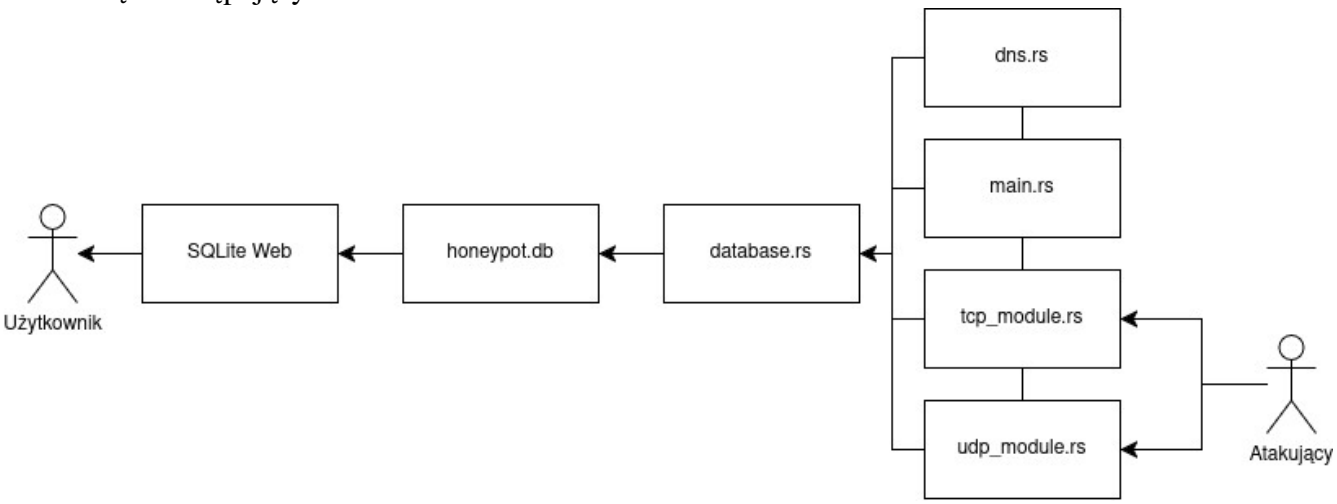
DNS Honeypot

1. Architektura systemu:

DNS honeypot został napisany w języku Rust. Zapewnił on wysoką wydajność całego systemu. System składa się z następujących modułów:



- **udp_module.rs/tcp_module.rs:** Warstwy transportowe, pozwalające na odebranie danych od atakującego. Moduł UDP jest dla podstawowych klas zapytań a moduł TCP jest dla większych zapytań takich jak np. ANY.
- **main.rs:** Główny punkt wejściowy aplikacji, odpowiedzialny za inicjację modułów i koordynację przepływu danych.
- **dns.rs:** Odpowiada za przetwarzanie protokołu DNS. Parsuje zapytania i wyciąga kluczowe pola.
- **database.rs:** Odpowiada za komunikację z bazą danych. Obsługuje logowanie wydarzeń w czasie rzeczywistym i wysyłanie raportów dziennych.
- **SQLite web:** Pozwala na przeglądanie zebranych danych.

2. Reguły klasyfikacji ataków:

Reguła	**Logika**	**Cel**
Flood Attack	Ponad 60 zapytań z jednego adresu IP w krótkim odstępie czasu.	Przeciążenie serwisu.
Zone Transfer	Zapytania typu AXFR, IXFR lub SOA.	Próba pobrania całej zawartości strefy.
DNS Tunneling	Zapytania o długości nazwy domeny przekraczającej 60 znaków.	Ukryte wyprowadzanie danych lub omijanie zabezpieczeń sieciowych.
Amplification Attempt	Zapytania o rekordy typu ANY lub TXT.	Wykorzystanie serwera do ataków DDoS o dużym wolumenie.
Forbidden Domain	Zapytania o domeny znajdujące się na czarnej liście.	Próba kontaktu ze złośliwym oprogramowaniem lub serwerem atakującego.

3. Wyniki testów:

W celu przetestowania serwera użyłem skryptu, który przez dwa dni wysyłał losowe zapytania. Poniżej możemy zobaczyć tabelę zbiorczą ataków, który DNS honeypot wykrył:

day	total_events	by_class	first_seen	last_seen
2026-01-25	60	Flood Attack	2026-01-25 23:40:30.349	2026-01-25 23:51:02.178
2026-01-26	60	Flood Attack	2026-01-26 15:18:14.190	2026-01-26 15:28:46.134
2026-01-25	213	Zone Transfer	2026-01-25 11:32:54.832	2026-01-25 23:50:51.022
2026-01-26	267	Zone Transfer	2026-01-26 00:01:03.070	2026-01-26 15:28:35.714
2026-01-25	71	DNS Tunneling	2026-01-25 11:33:25.021	2026-01-25 23:51:01.095
2026-01-26	89	DNS Tunneling	2026-01-26 00:01:33.202	2026-01-26 15:28:45.789
2026-01-25	71	Amplification Attempt	2026-01-25 11:33:25.090	2026-01-25 23:51:01.153
2026-01-26	89	Amplification Attempt	2026-01-26 00:01:33.262	2026-01-26 15:28:45.846
2026-01-25	71	Forbidden Domain	2026-01-25 11:33:25.124	2026-01-25 23:51:01.185
2026-01-26	89	Forbidden Domain	2026-01-26 00:01:33.290	2026-01-26 15:28:45.874

4. Przykładowe zdarzenia:

- Przykładowe dwa ataki typu **Flood Attack:**

ID	timestamp	day	question	question_lenght	response	server_ip	server_port	client_ip	client_port	q_type
10	2026-01-25 11:33:25.160	2026-01-25	flood-fkvkf17u.com.	59	127.189.2.84	0.0.0.0	53	172.19.0.1	46638	A
11	2026-01-25 11:33:25.192	2026-01-25	flood-kcc61dv1.com.	59	28.229.131.3	0.0.0.0	53	172.19.0.1	59035	A

+58 wierszy.

ip	timestamp	day	question	question_lenght	response	server_ip	server_port	client_ip	client_port	q_type
78	2026-01-25 11:43:57.636	2026-01-25	flood-zbblhpso.com.	59	76.202.115.163	0.0.0.0	53	172.19.0.1	40650	A

79	2026-01-25 11:43:57.666	2026-01-25	flood-2a2haawm.com.	59	122.26.30.229	0.0.0.0	53	172.19.0.1	33849	A

+58 wierszy.

- Przykładowe dwa ataki **Zone Transfer:**

ID	timestamp	day	question	question_lenght	response	server_ip	server_port	client_ip	client_port	q_type
71	2026-01-25 11:43:37.388	2026-01-25	example.com.	52	ns1.example.com. admin.example.com. 2023101001 360 ...	0.0.0.0	53	172.19.0.1	55438	SOA
72	2026-01-25 11:43:47.420	2026-01-25	example.com.	52	ns1.example.com. admin.example.com. 2023101001 360 ...	0.0.0.0	53	172.19.0.1	33824	SOA

- Przykładowe dwa ataki typu **DNS Tunneling:**

ID	timestamp	day	question	question_lenght	response	server_ip	server_port	client_ip	client_port	q_type
74	2026-01-25 11:43:57.498	2026-01-25	v1-1769337837.a5b6c7d8e9f0.g1h2i3j4k5l6.m7n8o9p0q1r2.s3t4u5v6w7x8.example.com.	118	220.26.244.161	0.0.0.0	53	172.19.0.1	42512	A
142	2026-01-25 11:54:29.798	2026-01-25	v1-1769338469.a5b6c7d8e9f0.g1h2i3j4k5l6.m7n8o9p0q1	118	33.164.133.5	0.0.0.0	53	172.19.0.1	59186	A

- Przykładowe dwa ataki typu **Amplification Attempt:**

ID	timestamp	day	question	question_lenght	response	server_ip	server_port	client_ip	client_port	q_type
143	2026-01-25 11:54:29.827	2026-01-25	google.com.	51	Windows Intel Core i5-14600KF	0.0.0.0	53	172.19.0.1	36328	HINFO
211	2026-01-25 12:05:02.123	2026-01-25	google.com.	51	Windows Intel Core i5-14600KF	0.0.0.0	53	172.19.0.1	35272	HINFO

- Przykładowe dwa ataki typu **Forbidden Domain:**

ID	timestamp	day	question	question_lenght	response	server_ip	server_port	client_ip	client_port	q_type
213	2026-01-25 12:05:02.184	2026-01-25	zakazanadomena.com.	59	110.222.53.166	0.0.0.0	53	172.19.0.1	51535	A
281	2026-01-25 12:15:34.350	2026-01-25	zakazanadomena.com.	59	110.222.53.166	0.0.0.0	53	172.19.0.1	33333	A