Автоматизовані тести систем виявлення вторгнень

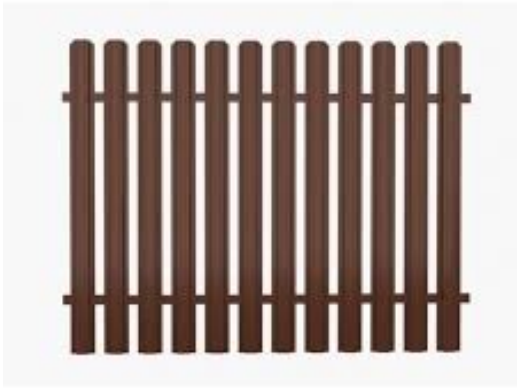
Виконав: студент 4-го року навчання,
Спеціальності: 121 Інженерія програмного забезпечення,
Дейнека Артем Валентинович

Керівник: Глибовець А.М. доктор технічних наук

Система виявлення вторгнень

Система

IDS/IPS



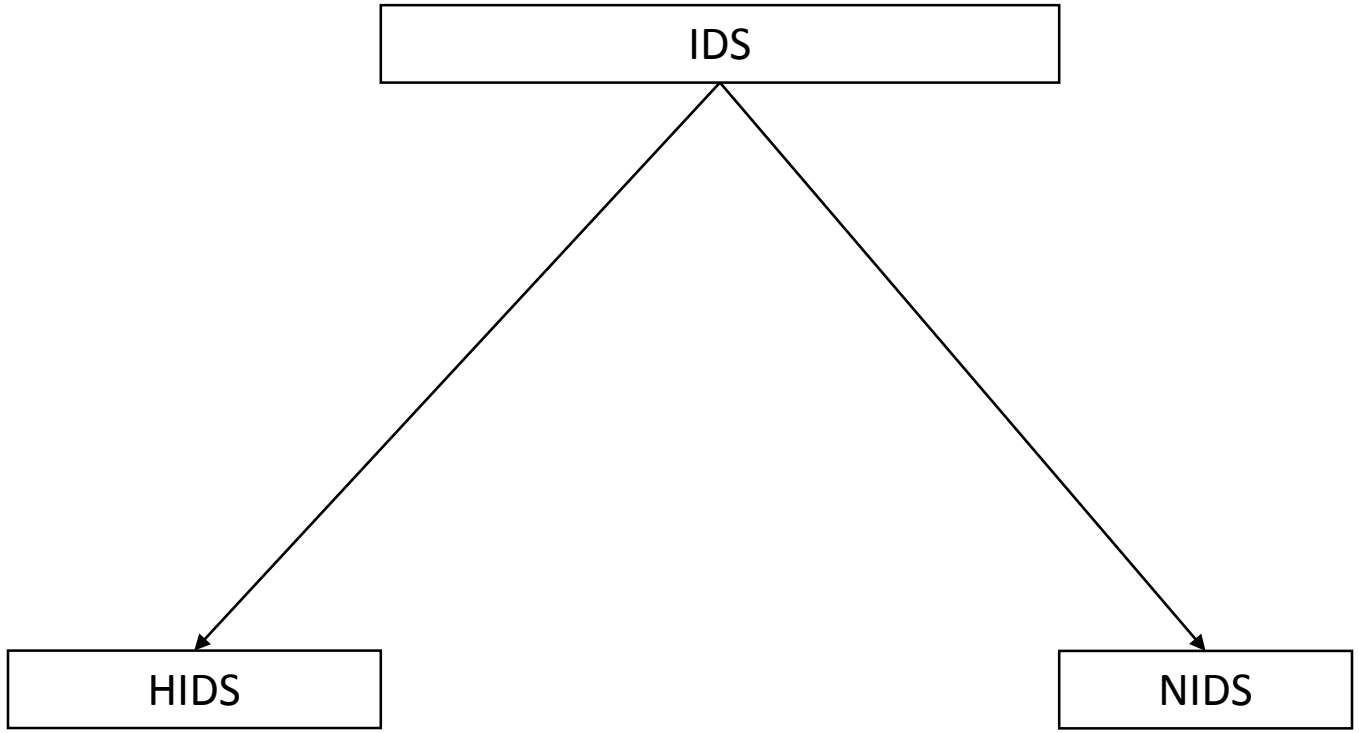
Firewall

Актуальність

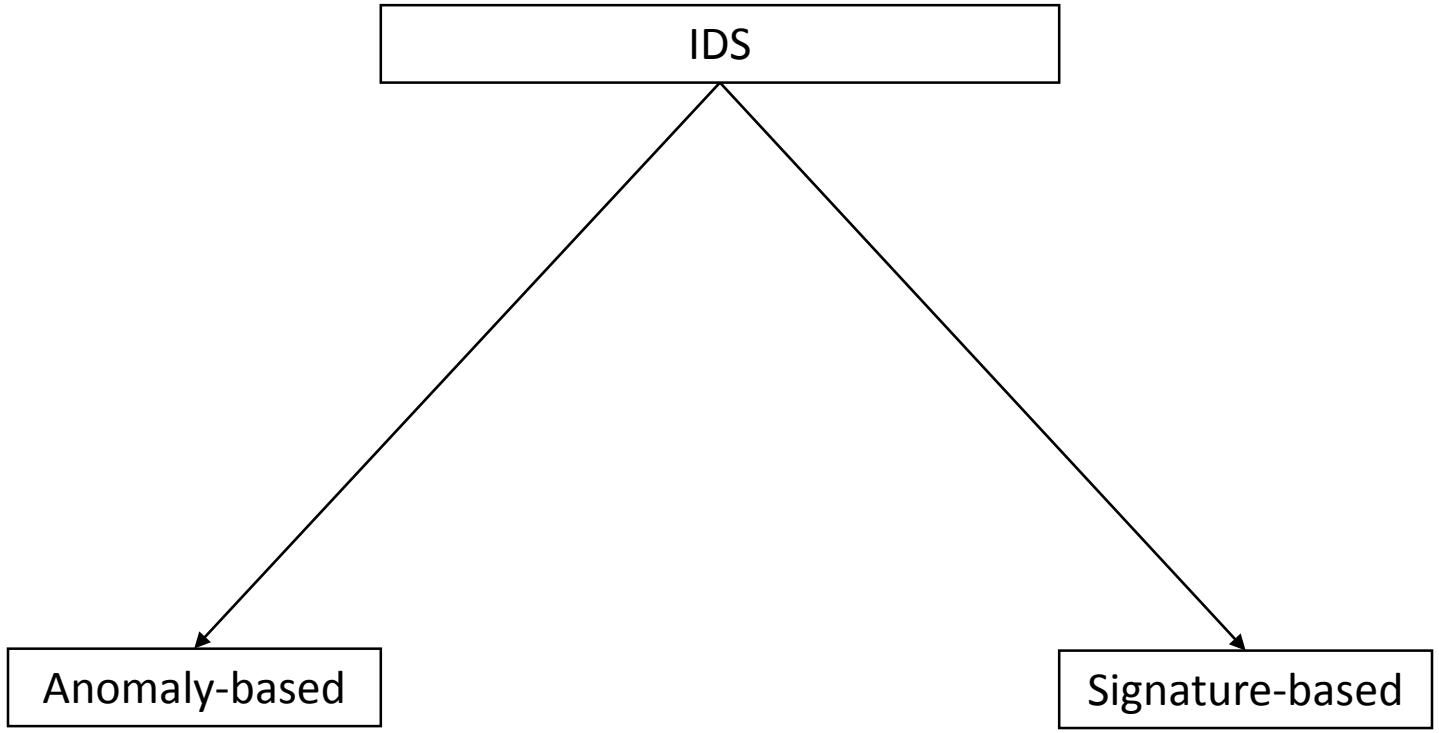
- Перевірка правильності налаштування системи
- Перевірка актуальності системи захисту
- Автоматизація пошуку та усунення вразливостей

Навіщо мене дресирувати? Я і так хороший хлопчик

Види IDS



Види IDS



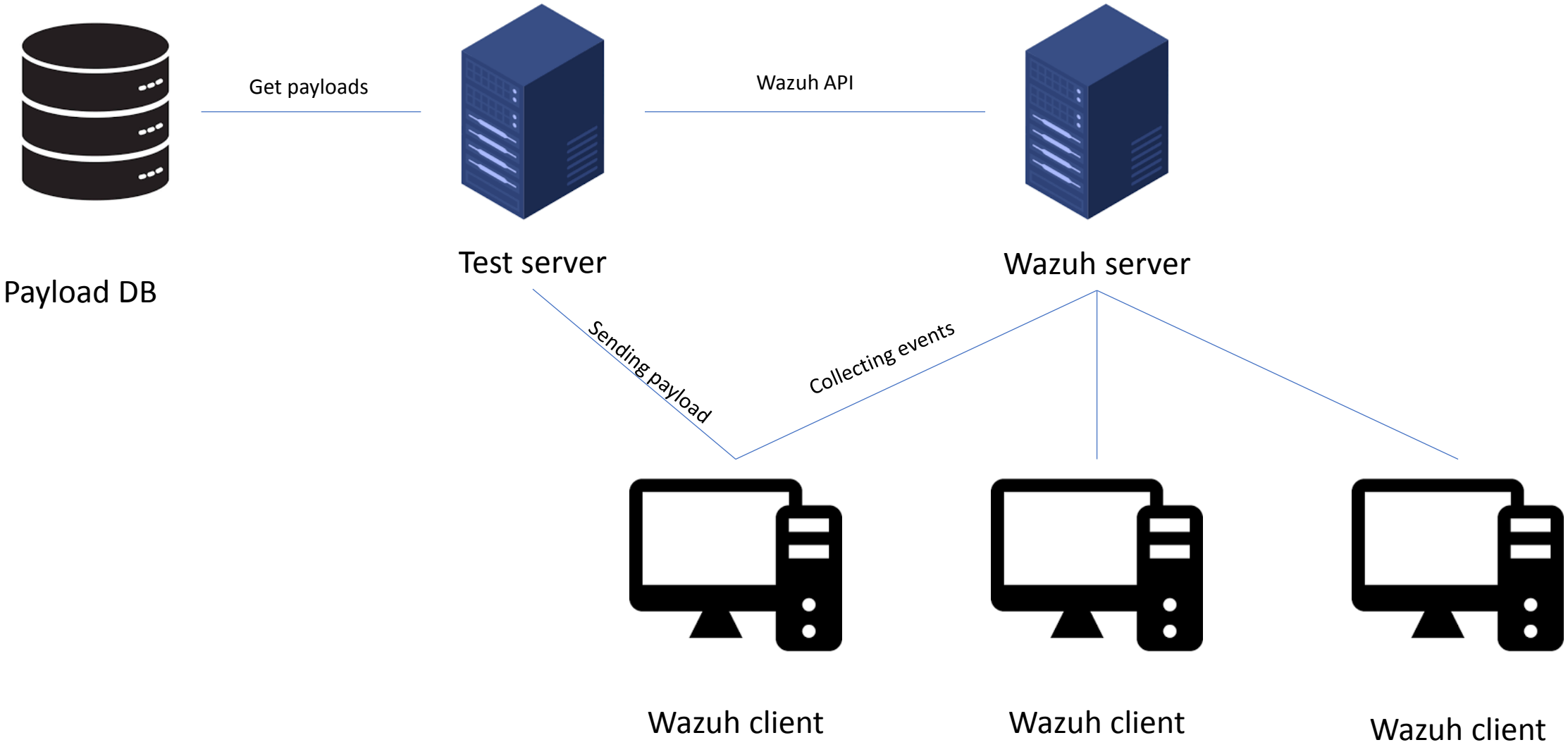
Чому Wazuh?

Вбудоване SIEM рішення

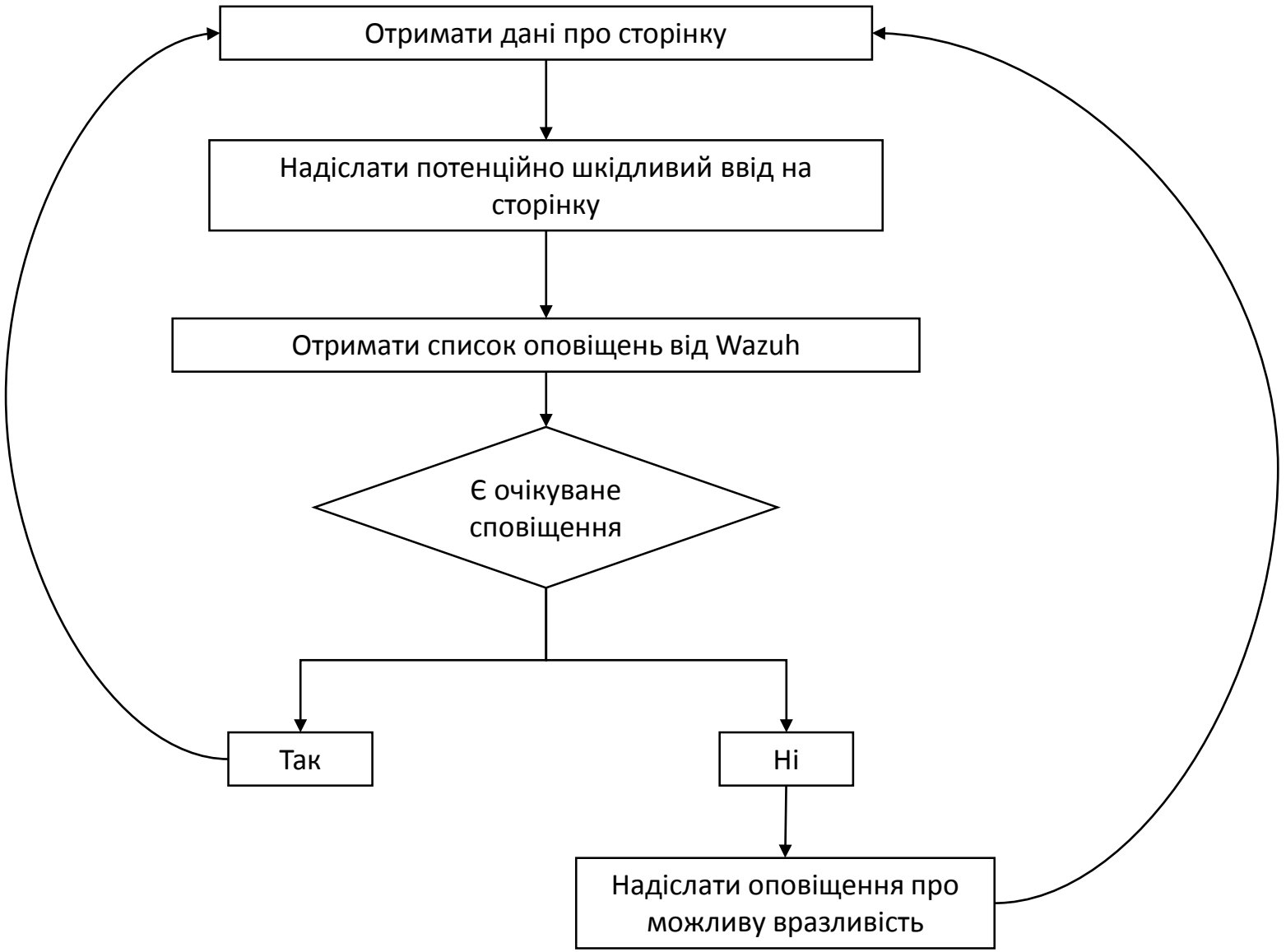
	Time	rule.description
>	Aug 2, 2022 @ 13:34:15.338	Suricata: Alert - GPL ICMP_INFO PING *NIX
>	Aug 2, 2022 @ 13:34:14.339	Suricata: Alert - GPL ICMP_INFO PING *NIX
>	Aug 2, 2022 @ 13:34:13.335	Suricata: Alert - GPL ICMP_INFO PING *NIX
>	Aug 2, 2022 @ 13:34:12.336	Suricata: Alert - GPL ICMP_INFO PING *NIX
>	Aug 2, 2022 @ 13:34:11.334	Suricata: Alert - GPL ICMP_INFO PING *NIX

Можливість інтеграції
інших NIDS

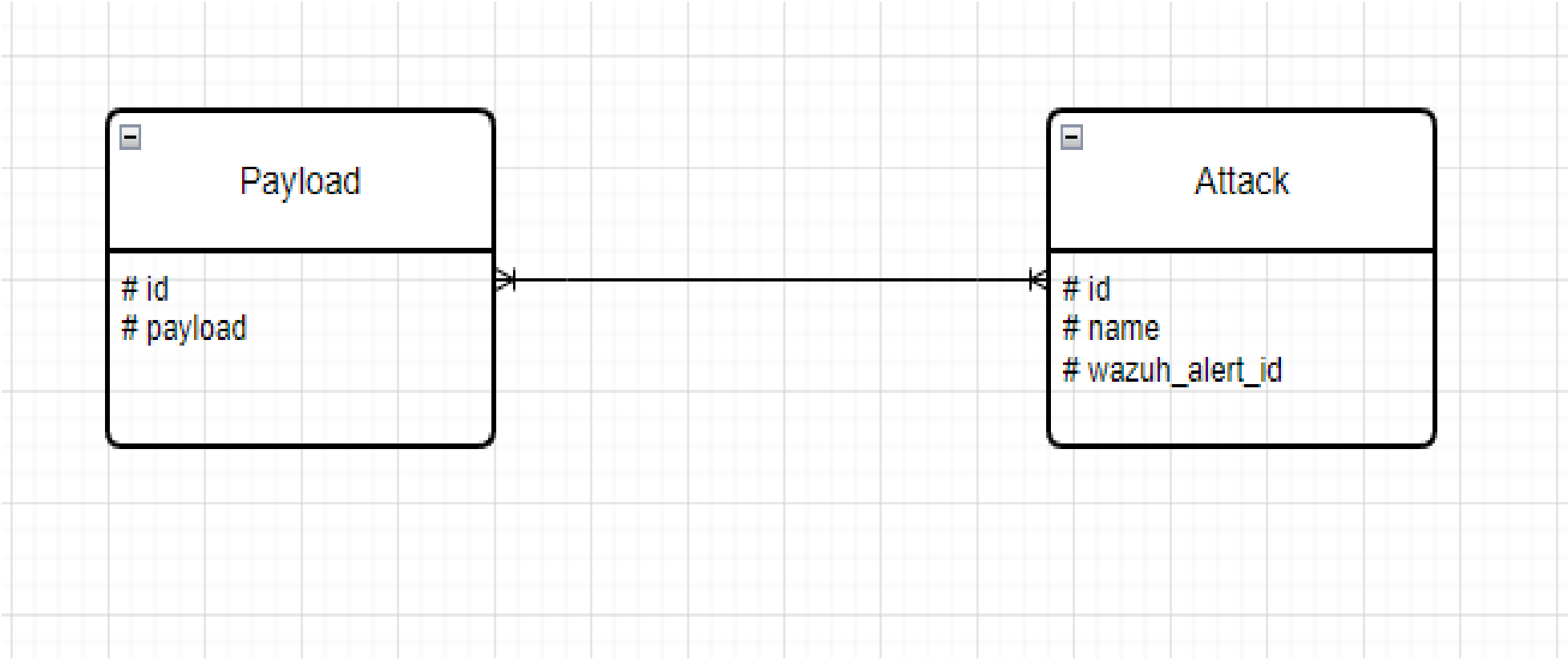
Система тестування



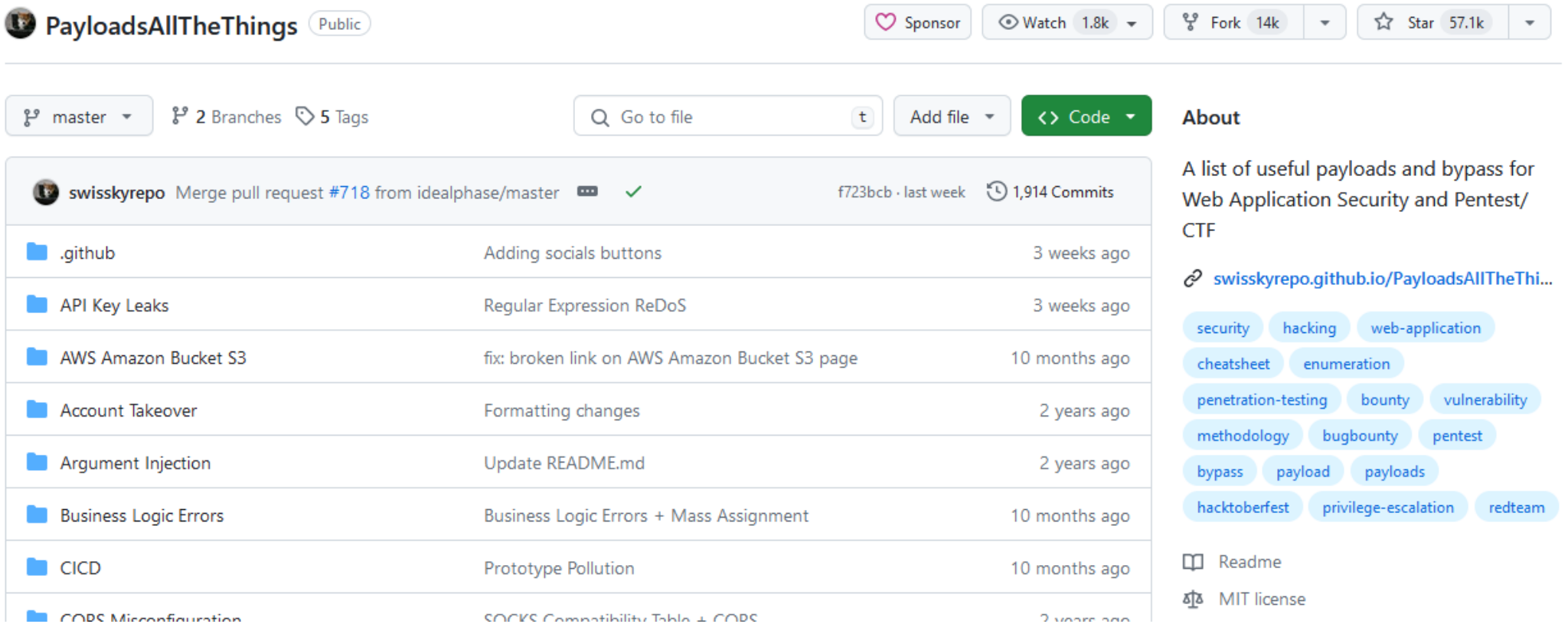
Сервер для тестування



База даних атак

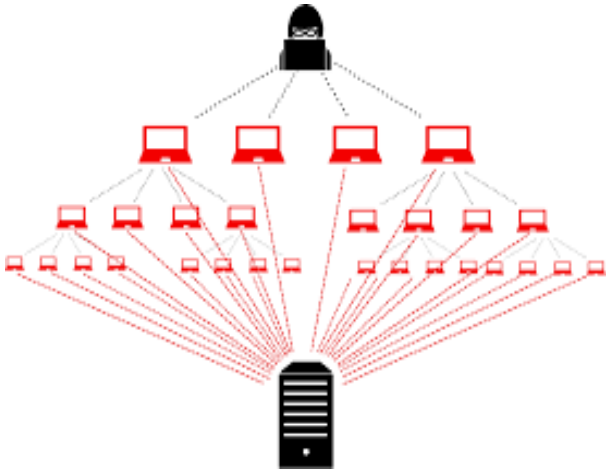


База даних атак

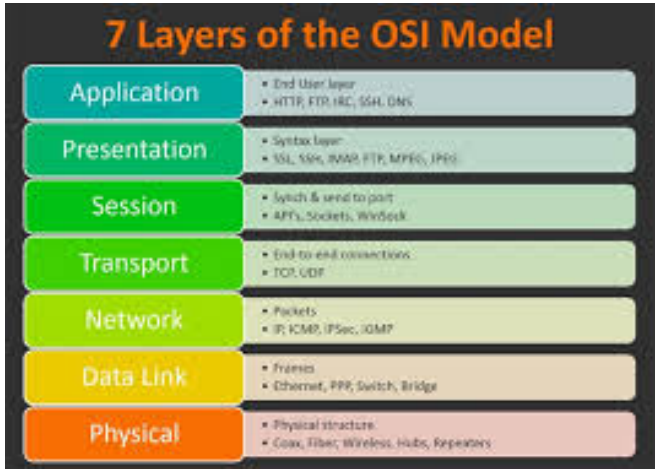


Інформація про цілі

А чи можна краще?



Не всі атаки мають payload у HTTP хедері



Атаки можливі на всіх рівнях

А чи обо’язково оновлювати бд вручну?

Дякую за увагу