

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

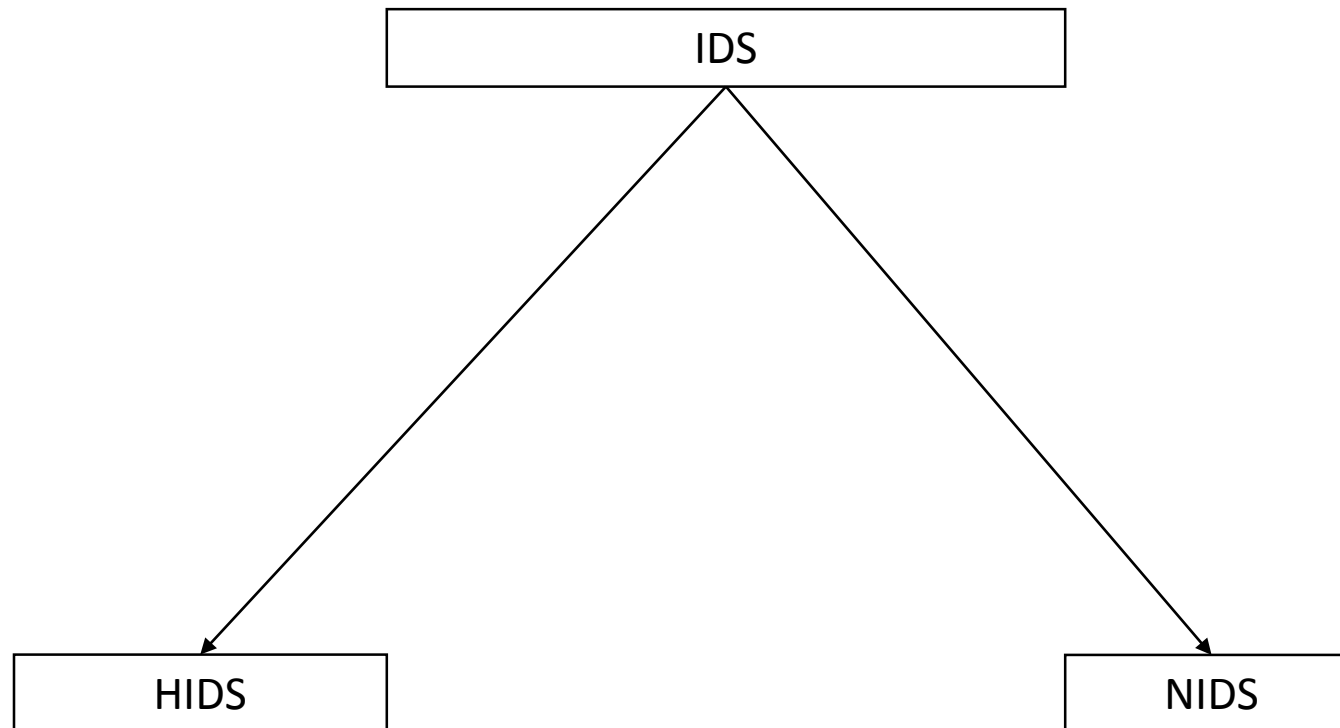
- Перевірка правильності налаштування системи
- Перевірка актуальності системи захисту
- Автоматизація пошуку та усунення вразливостей



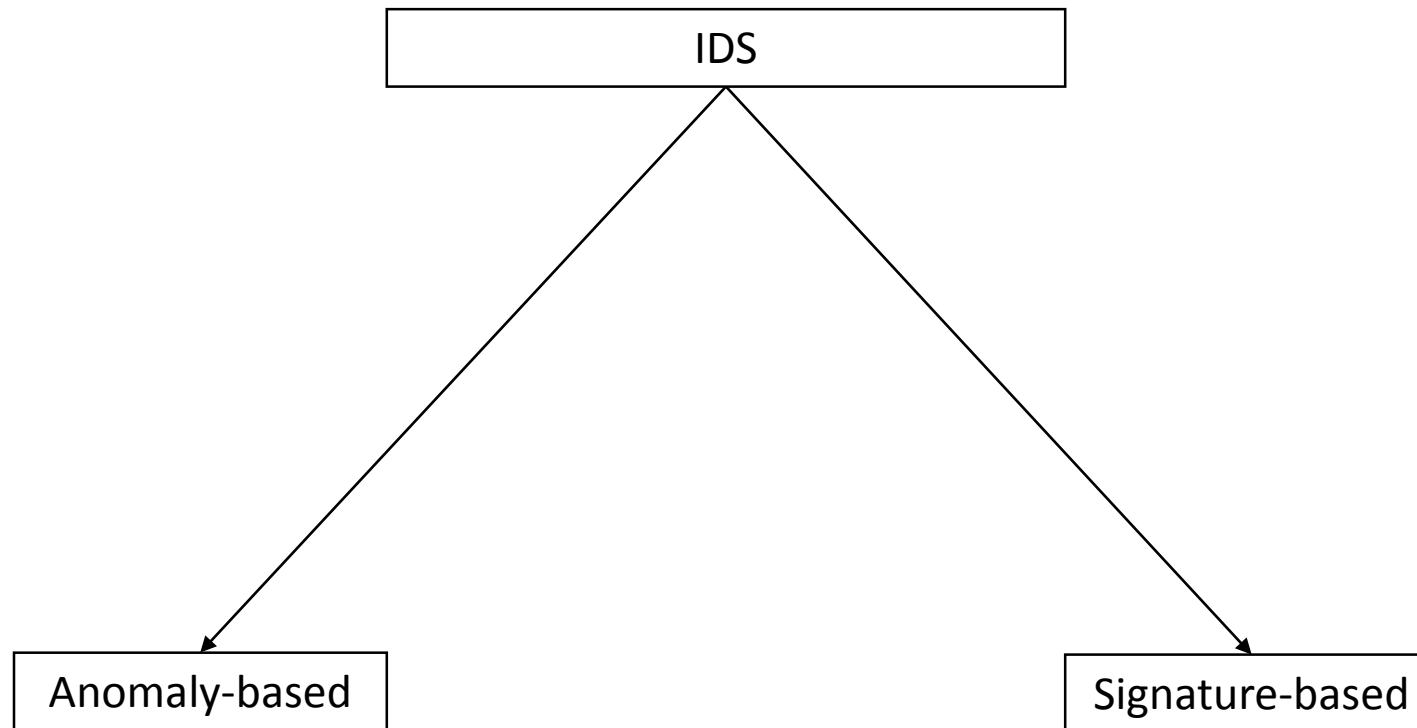
Навіщо мене
дресировати?

Я і так
хороший
хлопчик

Види IDS



Види IDS



Чому Wazuh?

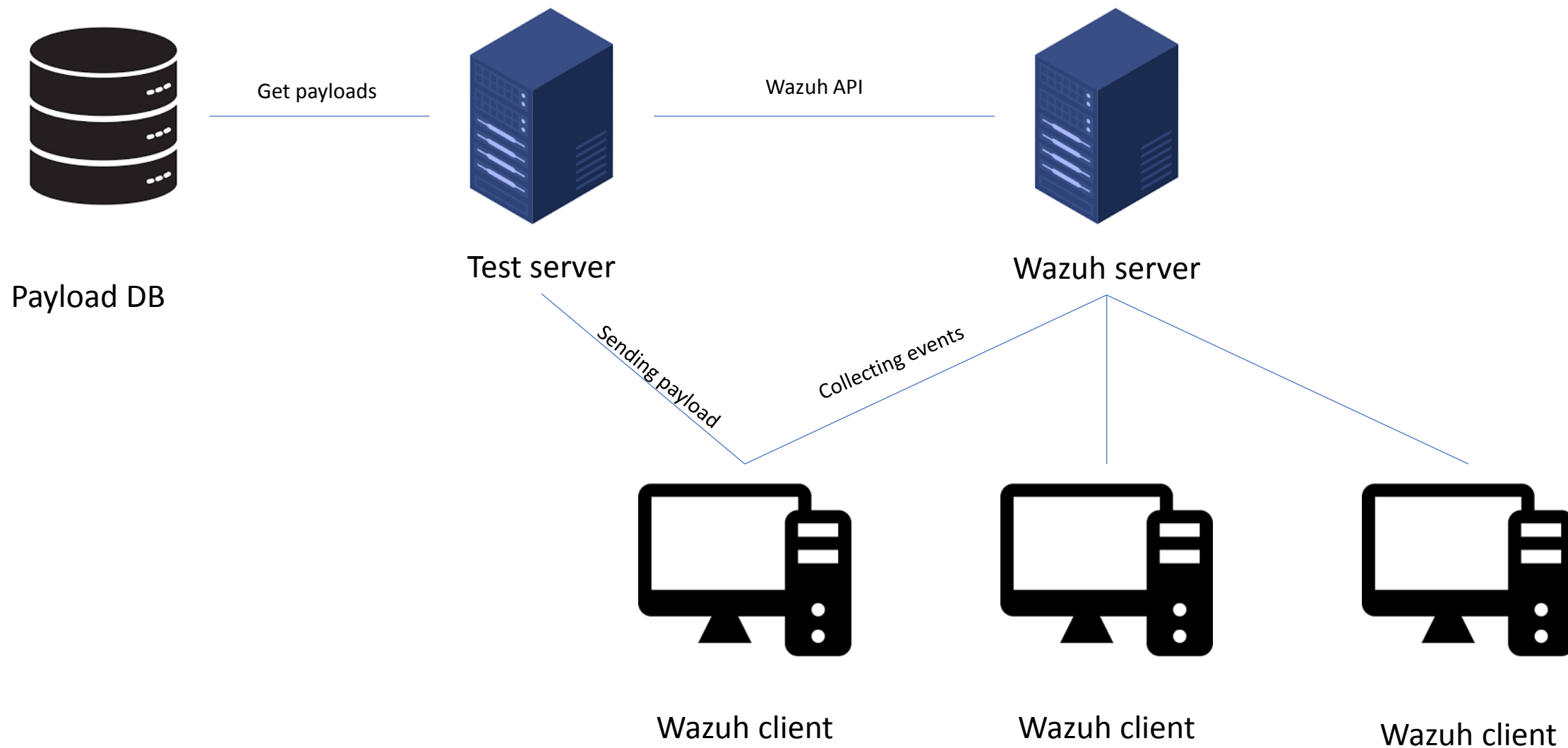


Вбудоване SIEM рішення

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

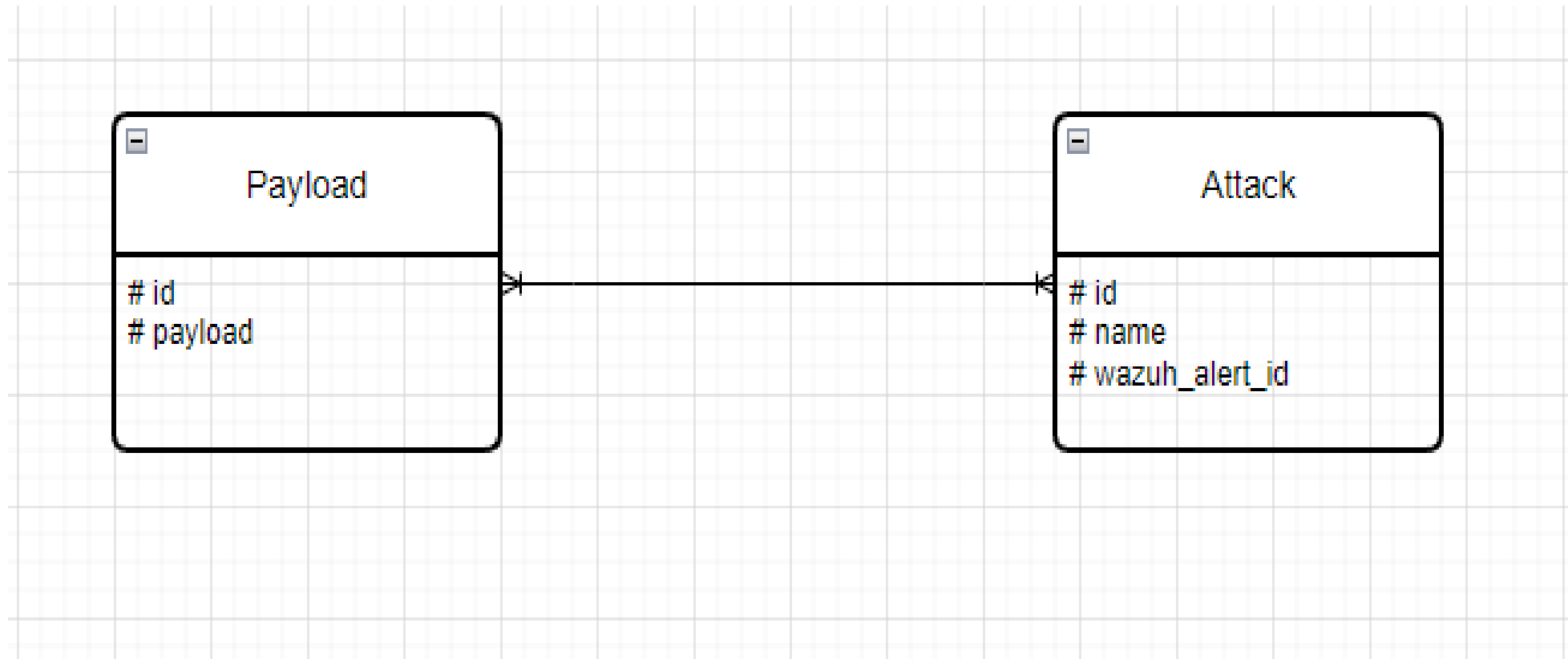
Система тестування



Сервер для тестування



База даних атак



База даних атак

 **PayloadsAllTheThings** Public

[Sponsor](#) [Watch 1.8k](#) [Fork 14k](#) [Star 57.1k](#)

[master](#) [2 Branches](#) [5 Tags](#) [Add file](#) [Code](#)

 **swisskyrepo** Merge pull request #718 from idealphase/master f723bcb · last week 1,914 Commits

 .github	Adding socials buttons	3 weeks ago
 API Key Leaks	Regular Expression ReDoS	3 weeks ago
 AWS Amazon Bucket S3	fix: broken link on AWS Amazon Bucket S3 page	10 months ago
 Account Takeover	Formatting changes	2 years ago
 Argument Injection	Update README.md	2 years ago
 Business Logic Errors	Business Logic Errors + Mass Assignment	10 months ago
 CICD	Prototype Pollution	10 months ago
 COPS Misconfiguration	SOCKS Compatibility Table + COPS	2 years ago

About

A list of useful payloads and bypass for Web Application Security and Pentest/CTF

swisskyrepo.github.io/PayloadsAllTheThings/

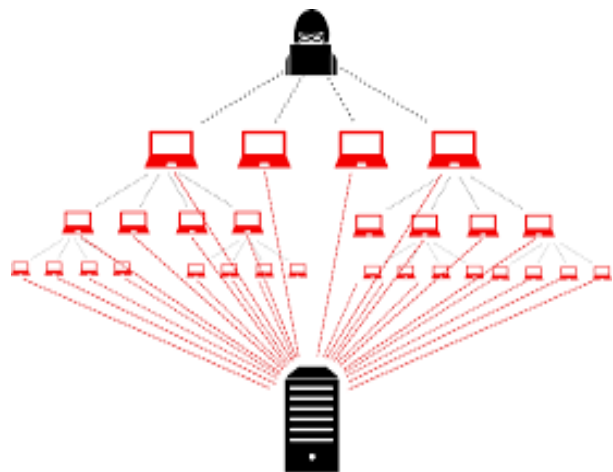
security hacking web-application cheatsheet enumeration penetration-testing bounty vulnerability methodology bugbounty pentest bypass payload payloads hacktoberfest privilege-escalation redteam

[Readme](#) [MIT license](#)

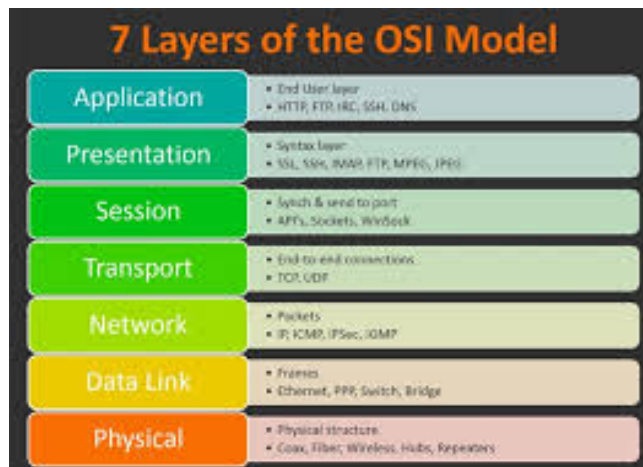
Інформація про цілі



А чи можна краще?



Не всі атаки мають
payload у HTTP хедері



Атаки можливі на всіх рівнях



А чи обов'язково оновлювати бд
вручну?

Дякую за увагу