Wzmocnij swój OPS w DevOPS

Niskopoziomowe profilowanie aplikacji PHP

/ 02.10.2021

/ Łukasz Biegaj

Agenda

1/ Wprowadzenie

2/ Profilowanie aplikacji

3/ Aplikacja demonstracyjna

4/ Analiza ruchu sieciowego

5/ Analiza syscalli

6/ GNU Debugger

7/ Podsumowanie

> Wprowadzenie

- Programista

Image by Innova Labs from Pixabay

> Wprowadzenie

- Programista
- Administrator

Nerd on computer from knowyourmeme.com

> Wprowadzenie

- Programista
- Administrator
- DevOps

Image by Dr StClaire from Pixabay

Profilowanie aplikacji

Znane i lubiane narzędzia

Aplikacja demonstracyjna

> Budowa aplikacji demonstracyjnej

Hands-on

> Analiza ruchu sieciowego

```
tcpdump -i any -n
tcpdump -i any -n <wyrażenie PCAP>
tcpdump -i any -n port 53
tcpdump -i any -n -A -s 0
```

`-i any` – dowolny interfejs sieciowy
`-i eth0` – konkretny interfejs sieciowy
`-n` – nie resolvuj nazw DNS i serwisów
`port 53` – przykładowe wyrażenie PCAP
`-A` – pokazuj zawartość pakietów w postaci ASCII
`-s 0` – pokazuj całe pakiety danych

https://danielmiessler.com/study/tcpdump/ - a tcpdump tutorial with examples, 50 ways to isolate Traffic

> Analiza syscalli

`lsof -n -p <PID>` – pokaż pliki otwarte przez proces

`strace -p <PID>` – śledź syscalle procesu

`strace -f -p <PID>` – śledź syscalle procesu oraz jego dzieci

`strace -s 1024 -p <PID>` – capturowanie stringów do 1kB

`strace -tt -p <PID>` – dodaj timestampy przy outpucie

> Profilowanie strace spowalnia aplikację

> GNU Debugger - podstawy

`gdb -p <PID>` - podpięcie się pod proces

`bt` - aktualny backtrace

`step` - przejdźdo następnej instrukcji

`continue` - kontynuuj do końca/do kolejnego breakpointa

`info os files` - pokaż aktualnie otwarte pliki

`call syscall(...)` - wywołaj konkretny syscall

> GNU Debugger - receptury

`info os files` - sprawdź otwarte pliki/połączenia

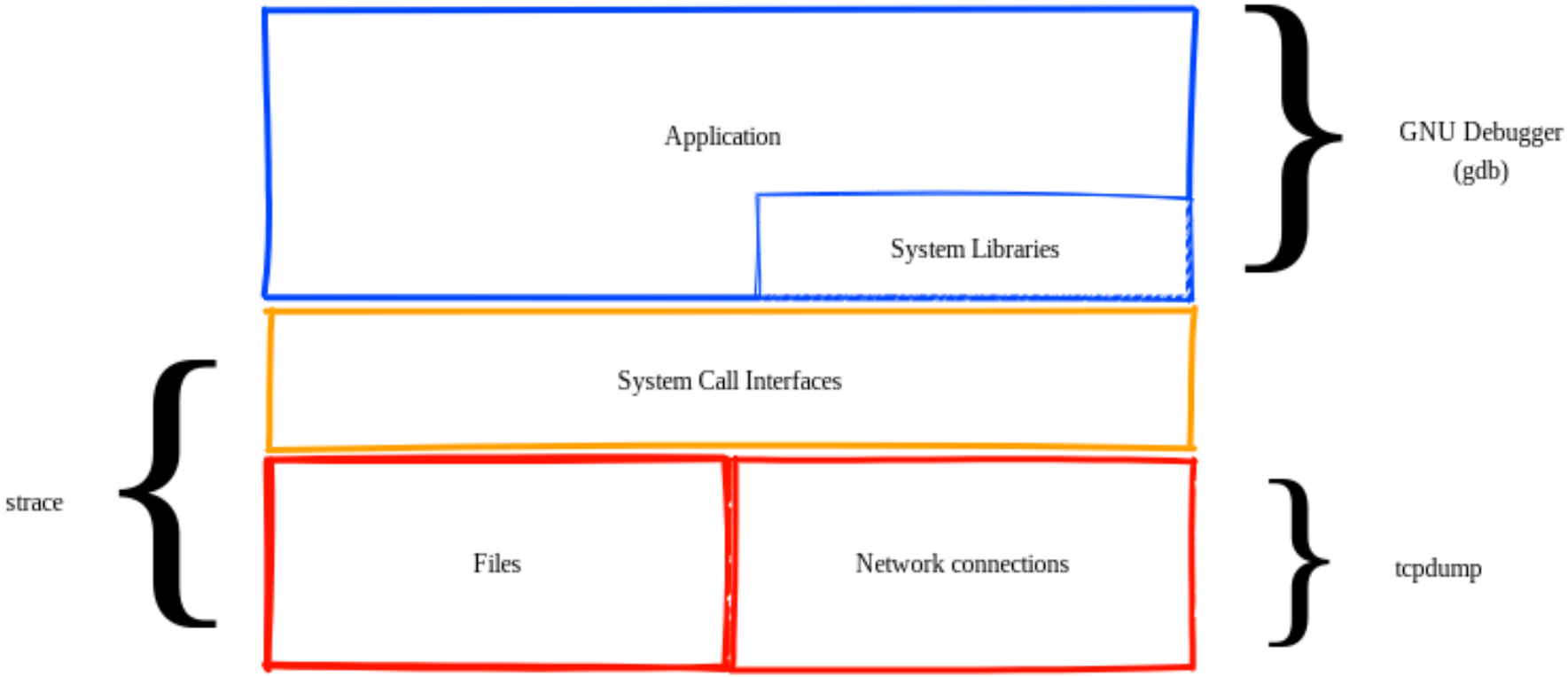
`call (int)close(3)` - zamknij file deskryptor numer 3

`call (int)open("/data/log3.txt", 66, 0666)` - otwórz nowy plik

`call (int)dup3(5,2)` - nadpisz filedeskryptor 2 filedeskryptorem 5

Podsumowanie

> Wykorzystane narzędzia



Koniec

https://github.com/lpiob/phpsummit-2021