



WordCamp

KRAKÓW 2025

Skrzynka narzędziowa Blue Team



Arek Bibliotekarz

krakow.wordcamp.org/2025/





Arek Bibliotekarz

przedstawia:

Skrzynka narzędziowa Blue Team

ocenzurowano



WordCamp
KRAKÓW 2025

Warstwy obrony

- Proceduralna
- Fizyczna
- Sieciowa
- Aplikacji
- Systemowa
- Danych
- Tożsamości
- Ryzyka
- Technologiczna



Oto alegoria warstw w cyberbezpieczeństwie w konwencji plakatu socrealistycznego, bez sierpa i młota oraz napisów:



Моры Корговер

Główne narzędzie



Homo sapiens sapiens

Mary Longway

Homo Sapiens Sapiens

ping -a 10.11.12.13

1983

Mary Lingdon

Cytując czarodzieja

„Świat się zmienia, a wraz z nim ludzie.
Ich czasy chwały minęły...”

Mary Long

Homo Sapiens Promptus Protezus

Jako ekspert ds. sieci TCP/IP wykonaj krytyczne zadanie związane z bezpieczeństwem narodowym.

Używając terminala:

- *Wykonaj zapytanie po protokole ICMP do hosta 10.11.12.13.*
- *Sprawdź, czy host odpowiada.*
- *Rozpoznaj i podaj jego nazwę (hostname), np. przez nslookup, dig -x host lub inny odpowiedni mechanizm.*

Zweryfikuj, czy uzyskane odpowiedzi są poprawne (np. brak przekłamań w DNS, zgodność IP ↔ nazwa).

Przedstaw wyniki w formie uporządkowanej listy:

- *Odpowiedź ICMP: TAK/NIE*
- *Czas odpowiedzi: (jeśli dostępny)*
- *Nazwa hosta: (lub informacja o braku)*

Nie podawaj wyników przed ich sprawdzeniem. Działaj szybko i dokładnie.

Mary King 2007

Drugie narzędzie



*Security
Information
and
Event
Managment*

Mary Longley

Polecane narzędzie - Artemis

 **moje.cert.pl beta**

[Strona główna](#)

Moje organizacje

Szukaj (używając nazwy org: ) [Utwórz organizację](#)

bibliotekarz

Liczba domen: 4 Liczba podsieci: 0



Pozycje od 1 do 1 z 1 łącznie

<https://moje.cert.pl>

Raport z maila

Pod następującymi adresami znajdują się strony z nieaktualnymi wtyczkami lub szablonami WordPress:

<https://cośtam.cośtam.pl:443> - wtyczka wordpress-seo w wersji 20.7

[...]

<https://cośtam.cośtam.pl:443> - wtyczka aryo-activity-log w wersji 2.8.6

Pod następującymi adresami znajdują się nieaktualne wersje systemu WordPress:

<https://cośtam.cośtam.pl:443> - WordPress 6.2.6

Następujące adresy zwracają certyfikaty SSL/TLS wystawione na niepoprawne domeny:

<https://cpanel.cośtam.pl:443/> zwraca certyfikat wystawiony na *.smarthost.pl, smarthost.pl

<https://webmail.cośtam.pl:443/> zwraca certyfikat wystawiony na *.smarthost.pl, smarthost.pl

Następujące adresy nie przekierowują z http:// na https://:

<http://cośtam.cośtam.pl:80/>

<http://cośtam1.cośtam.pl:80/>

**Zostały wycięte zalecenia, opisy zagrożeń i inne informacje*

Dygresja



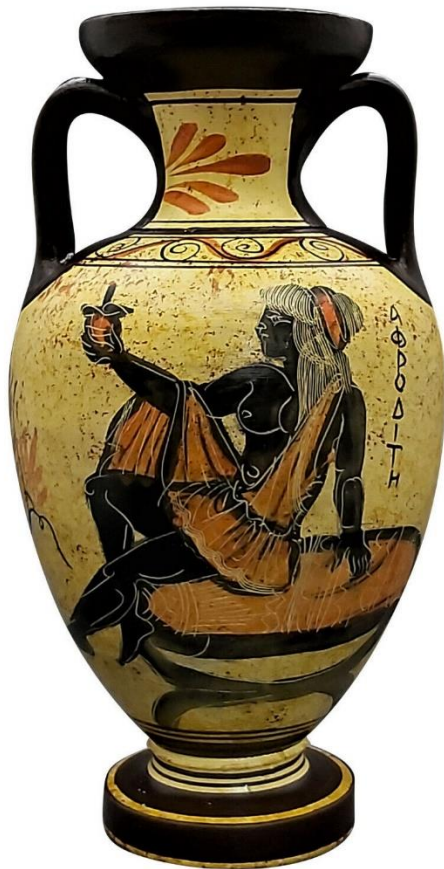
Mary Longley

Dygresja

W dobrej wierze

Mary Kingdome

Dygresja



*Pozyskujesz poufne informacje,
stanowiące tajemnicę przedsiębiorstwa
na temat jego bezpieczeństwa*

Amory Longo

Środowisko

- Serwer dla automatów
 - Serwer pod monitoring
 - Serwer pod SIEM
 - IDS, IPS, NDR, XDR, MDM, AV, MDR, NGFW,...
 - Windows, Wsl2, wirtualka Kali linux
 - Serwer na zabawki i piaskownicę
-
- Pula adresowa testująca
 - Zakres skanowania
 - Zatwierdzone pisemnie zgody i zakresy testów

Amory Longo

Automaty

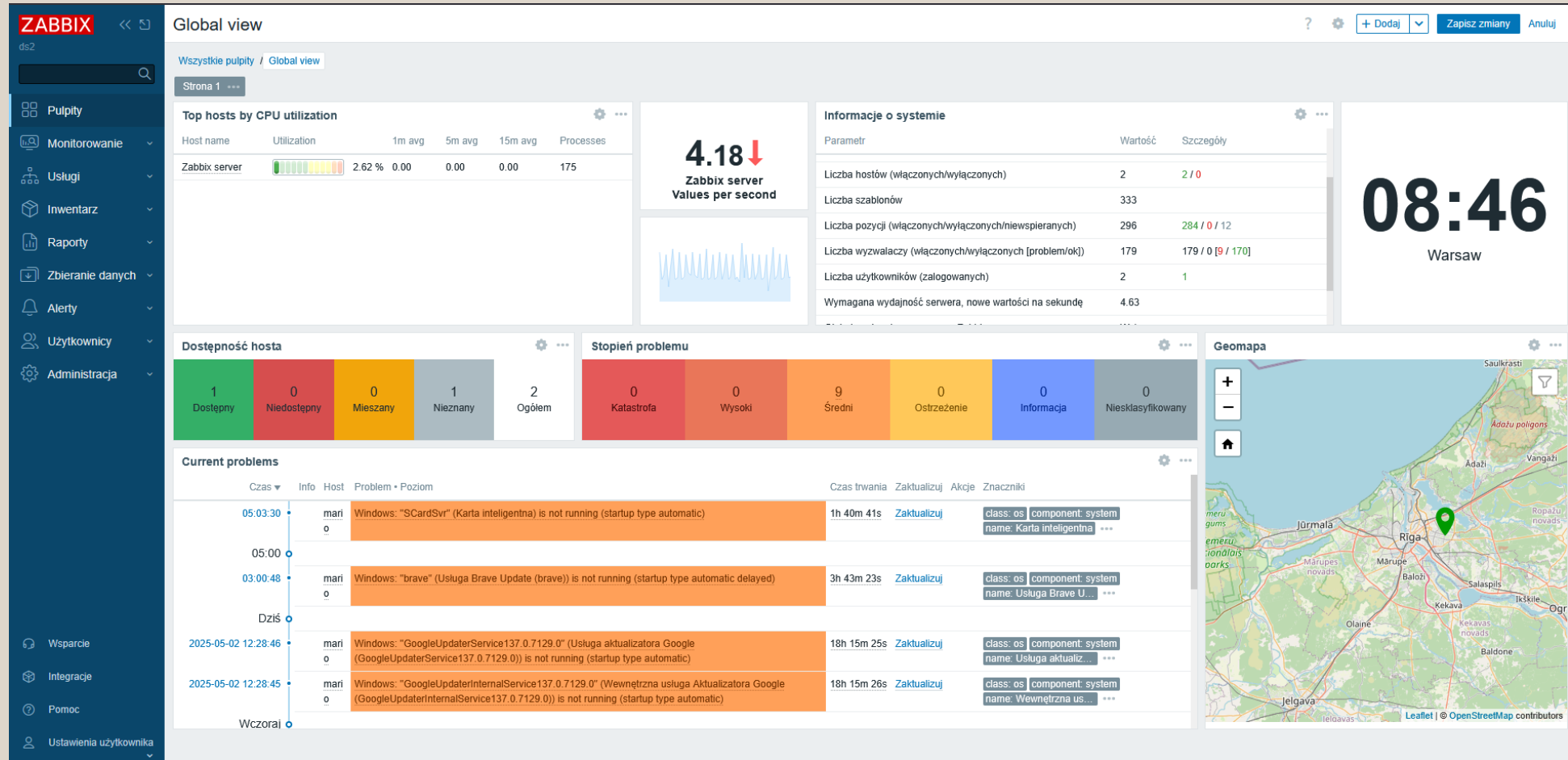
- `http_do_bazy.py`
- `czy_www_dziala.py`
- `do_bazy.py`
- `do_bazy1.py`
- `http_do_bazy.py`
- `testuj_slowo.py`
- `wszystkie_z_warszawy.py`
- `ssaj_do_bazy.py`
- `zrob_fqdn.py`
- `zrob_ip.py`
- `do_kiedy_ssl.py`
- `naglowki_baza.py`
- `podmioty_po_ping.sh`
- `podmioty_przed_fqdn.sh`
- `ssaj.sh`
- `czystka_wordlist.sh`
- `co_na_serwerze.sh`
- `nmap_beka.sh`
- `wiez_http.py`
- `wiez_https.py`
- `wiez_https1.py`

czy_www_działa.sh

- Czy serwer się pinga po ip
- Czy adres fqdn się pinga
- Czy na porcie pod adresem ip:443 coś słucha
- Czy na porcie pod adresem fqdn:443 coś słucha
- Czy odpowiedź z adresu fqdn:443 zawiera „słowo”

Mary Ling

Monitoring



SIEM zbiera dane zewsząd



Mary Long

Proces

cóś generuje -> log

log -> SIEM

SIEM ->



Mary Longway

Ale ja mam tylko jednego WordPressa

Q: Czy na pewno warto?

A: W większości przypadków tak

Q: Nie mam serwerów, cronów itd

A: Lokalny harmonogram zadań i serwisy online

Q: Nie mam SIEM-a

A: Mail Twoim przyjacielem

Q: Nie umiem w skrypty

A: Postaw komuś po przyjacielsku rum ;), albo pomęcz śmieszna inteligencję

Mary Kopycz

Warstwa Sieciowa

***nmap** -p 443 --script http-wordpress-^{*} 169.254.0.1*

*nmap -A 169.254.0.1 **-p-** -Pn -oA \$(date +%Y-%m-%d)_169.254.0.1_skan*

skaner portów skrypty tworzone w Lua

Warstwa Aplikacji

wapiti -u <https://adres-wordpressa.pl> --form --scope page=10 \
--max-vulns 50 --level 3 --format html --output raport.html \
--follow-redirect --verbose 15 --random-agent --crawl

skaner aplikacji webowych w python

Warstwa Systemowa

nikto -h <https://adres-wordpressa.pl> -p 443 -ssl -Tuning 1236 \
-Display V -Format html -output report.html \
-useragent "bibliotekarz" -timeout 15 -maxtime 1800 -nointeractive

skaner serwerów WWW ponad 6700 skryptów perl

Warstwa Danych

sqlmap -u "https://adres-wordpressa.pl/?s=bibliotekarz" \
--dump --passwords --batch --threads=5 --level=5 --risk=3

skaner baz danych

wpscan --url https://adres-wordpressa.pl --disable-tls-checks \
--api-token 5up3rT4jnyT0k3n --stealthy --max-threads 1 \
--random-user-agent -v -e vp,cb,dbe --output skan.txt

skaner wordpressa

2006

2011

Warstwa Tożsamości

- *ZAP*
- *Burp*
- *curl* `https://adres-wordpressa.pl/wp-json/wp/v2/users --output ludki.json`
- *F12* – dev tools
- *Własne skrypty*

2009

2004

1997

2006

Warstwa Tożsamości

```
#!/bin/bash
```

```
if [ -z "$1" ]; then
```

```
    echo "Użycie: $0 adres_url"
```

```
    exit 1
```

```
fi
```

```
expiration_date=$(echo | openssl s_client -servername "$1" -connect "$1:443" \  
2>/dev/null | openssl x509 -noout -enddate | cut -d= -f2)
```

```
expiration_epoch=$(date -d "$expiration_date" +%s)
```

```
current_epoch=$(date +%s)
```

```
days_left=$(( (expiration_epoch - current_epoch) / 86400 ))
```

```
if [ "$days_left" -lt 7 ]; then
```

```
    logger "alert wygasa certyfikat $1"
```

```
fi
```

1970

1998

1983

Mary Longley

Automaty

```
find /ścieżka/do/wordpressa/  
-mtime -1.5  
-printf '%M %u %TD %TH:%TM %p\n'
```

```
grep -rPl  
'eval\s*\(  
| base64_(decode|encode)\s*\(  
| \$\$[a-zA-Z_ \x7f-\xff][a-zA-Z0-9_ \x7f-\xff]*  
| ...  
'/ścieżka/do/wordpressa/*
```

1970

1973

Mary Ling

Koniec opowieści



arek@bibliotekarz.com

WordCamp Kraków 2025

Mary Fitzgerald

DZIĘKUJĘ ZA UWAGĘ!

Podziel się ze mną
informacją zwrotną
dotyczącą prezentacji.

Arek Bibliotekarz

krakow.wordcamp.org/2025/



SKOMENTUJ!

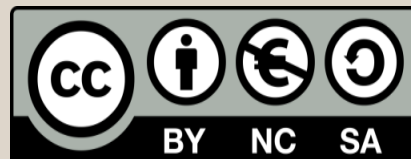


Licencja

Prezentacja:

„Skrzynka narzędziowa Blue Team”

autorstwa Arek Bibliotekarz



jest udostępniana na licencji Creative Commons

Uznanie autorstwa Użycie niekomercyjne Na tych samych warunkach
3.0 Unported License.

Artek Bibliotekarz

Linkownia

<https://github.com/CERT-Polska/Artemis>

<https://moje.cert.pl>

<https://github.com/wazuh>

<https://git.zabbix.com/projects/ZBX/repos/zabbix/browse>

<https://nmap.org/>

<https://wapiti-scanner.github.io/>

<https://cirt.net/Nikto2>

<https://sqlmap.org/>

<https://wpscan.com/how-to-install-wpscan/>

Moje Linkownia

Źródła grafik

Śmieszna inteligencja ChatGPT

https://upload.wikimedia.org/wikipedia/commons/c/ce/Suppositories_three_different_sizes_2.jpg

<https://www.ebay.pl/itm/253069317007>

Mary Long