

Honeypots: Workshop

Beata Zalewa, Not The Hidden Knowledge, 29.04.2025

0 mnie



Security Architect



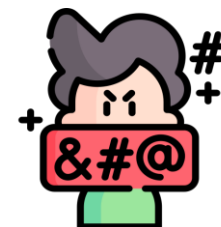
Consultant



Microsoft Certified Trainer



AI & Cybersecurity Practitioner



Developer



Freelancer



Azure @ ❤️



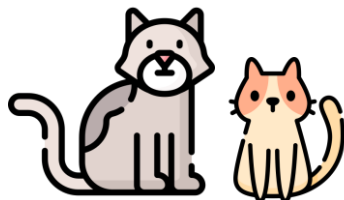
Google Cloud



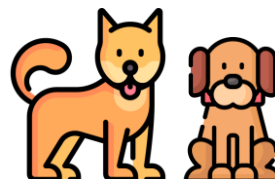
1 Mąż



1 Córka



2 Koty



2 Psy



Kryminały



Fotografia

Agenda

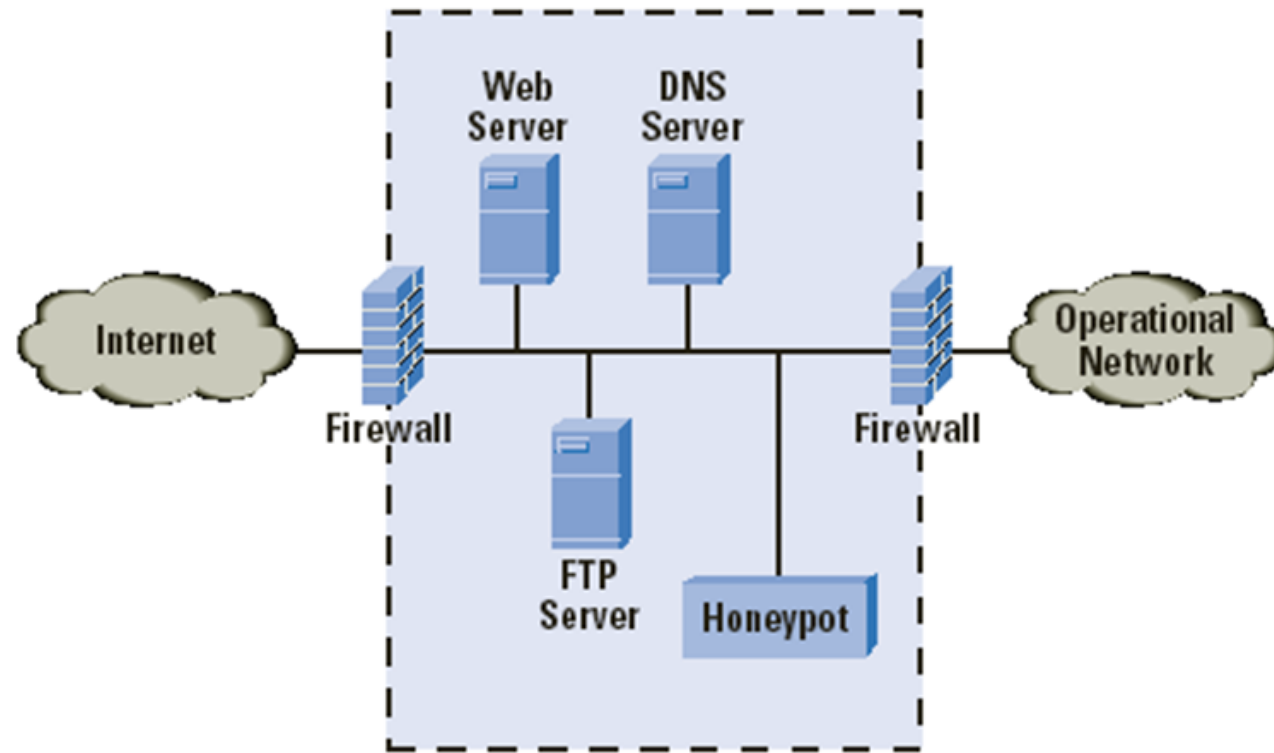
- Podstawy honeypotów
- Dlaczego honeypoty są ważne w cybersecurity?
- Jak zacząć z honeypotami?
- Praktyczne zastosowania honeypotów



PODSTAWY HONEYPOTÓW

CZYM SĄ HONEYPOTY?

A Honey Pot is an intrusion detection technique used to study hackers' movements.



Źródło: internet



CZYM SĄ HONEYPOTY?

Cel honeypotów

Honeypoty są pułapkami zaprojektowanymi w celu przyciągania atakujących i zbierania informacji o ich działaniach.

Badanie technik ataków

Honeypoty służą do analizy technik ataków, co pozwala lepiej zrozumieć zagrożenia w sieci.

Identyfikacja luk w zabezpieczeniach

Honeypoty pomagają w identyfikacji potencjalnych luk w zabezpieczeniach, co jest kluczowe dla ochrony systemów.

RODZAJE HONEYPOTÓW



Honeypoty niskiej interakcji

Honeypoty niskiej interakcji symulują usługi, aby przyciągnąć atakujących i zbierać dane o ich działaniach.

Honeypoty wysokiej interakcji

Honeypoty wysokiej interakcji oferują pełną funkcjonalność systemu, co pozwala na bardziej zaawansowane badania i analizę ataków.

Zastosowania honeypotów

Każdy typ honeypota ma swoje specyficzne zastosowanie w ochronie przed cyberatakami i w badaniach nad bezpieczeństwem sieci.

HISTORIA ZAKŁADANIA PUŁAPEK



An illustration of a wooden trap structure, possibly a pitfall or a snare trap, with several long wooden spears or arrows protruding from it. The trap is made of dark brown wooden planks and is set in a sandy, rocky ground. A pile of arrows with dark fletching and light-colored shafts lies on the ground in front of the trap. The overall style is that of a comic book or a graphic novel.

HISTORIA ZAKŁADANIA PUŁAPEK

HISTORIA ZAKŁADANIA PUŁAPEK

A long-haired brown cat is perched on top of a weathered wooden utility box. The box has a green-painted top edge and is situated in a grassy field with bare trees in the background. The text 'HISTORIA ZAKŁADANIA PUŁAPEK' is overlaid on the left side of the image.

HISTORIA ZAKŁADANIA PUŁAPEK

HISTORIA I ROZWÓJ HONEYPOTÓW

- Honeyputy zaczynały jako proste pułapki na wirusy, pomagające w badaniu zagrożeń w sieci.
 - Honeyputy ewoluowały w odpowiedzi na zmieniające się zagrożenia w sieci, stając się bardziej zaawansowanymi systemami obrony.
 - Dziś honeyputy są kluczowymi elementami strategii bezpieczeństwa, służąc do wykrywania i analizowania zagrożeń.
-



DLACZEGO HONEYPOTY SĄ
WAŻNE W CYBERSECURITY?



WYKRYWANIE I ANALIZA ZAGROŻEŃ

- Honeypoty są używane do zbierania cennych informacji o metodach ataków, co zwiększa bezpieczeństwo systemów.
 - Analiza danych z honeypotów pozwala na identyfikację najnowszych trendów w cyberzagrożeniach, co jest kluczowe dla ochrony.
 - W oparciu o zebrane dane, organizacje mogą tworzyć skuteczne strategie obronne, aby chronić swoje systemy przed zagrożeniami.
-

WZMOCNIENIE SYSTEMÓW OBRONNYCH



Dane z honeypotów

Dane uzyskane z honeypotów pomagają w identyfikacji i zrozumieniu zachowań zagrożeń, co wzmacnia systemy bezpieczeństwa.



Analiza luk w zabezpieczeniach

Analiza działania systemów obronnych pozwala na identyfikację luk, które mogą być wykorzystane przez cyberprzestępców.



Wzmocnienie polityk bezpieczeństwa

Wzmocnienie polityk bezpieczeństwa jest kluczowe dla skutecznej obrony przed nowymi zagrożeniami w cyberprzestrzeni.

JAK ZACZAĆ Z HONEYPOTAMI?



WYBÓR ODPOWIEDNIEGO TYPU HONEYPOTA

- Właściwy wybór honeypota wpływa na skuteczność strategii bezpieczeństwa. Różne typy honeypotów służą różnym celom.
 - Różne typy honeypotów mogą lepiej odpowiadać na specyficzne potrzeby organizacji w zakresie bezpieczeństwa.
 - Zanim podejmiemy decyzję, ważne jest, aby jasno określić cele, które chcemy osiągnąć za pomocą honeypotów.
-

KONFIGURACJA I WDROŻENIE HONEYPOTA

- Dokładna konfiguracja honeypota jest kluczowa dla jego skuteczności w identyfikacji i analizie zagrożeń.
 - Honeypot musi być odpowiednio zabezpieczony, aby nie stał się celem ataków i nie zagrażał sieci.
-



MONITOROWANIE I ANALIZA DANYCH

- Monitorowanie honeypotów jest kluczowe, aby zapewnić ich skuteczność w wykrywaniu ataków i zabezpieczaniu systemów.
 - Regularna analiza danych pozwala na szybkie reagowanie na incydenty oraz na poprawę strategii obronnych.
 - Analiza danych z honeypotów umożliwia zbieranie cennych informacji o metodach ataku, co wzmacnia ochronę systemów.
-



PRAKTYCZNE ZASTOSOWANIA HONEYPOTÓW



PRZYKŁADY UDANYCH WDROŻEŃ

- Honeypoty są skutecznym narzędziem w wykrywaniu zagrożeń i podejrzanej aktywności w sieciach organizacji.
- Honeypoty pomagają w zabezpieczaniu systemów, odwracając uwagę atakujących i zbierając cenne dane o zagrożeniach.

<https://www.controleng.com/throwback-attack-chinese-hackers-fall-for-a-honeypot-trap/>

NAJLEPSZE PRAKTYKI I ZALECENIA

- Honeypoty powinny być starannie integrowane z istniejącą infrastrukturą bezpieczeństwa, aby były efektywne w wykrywaniu zagrożeń.
 - Regularne zarządzanie i monitorowanie honeypotów jest kluczowe dla maksymalizacji ich skuteczności w wykrywaniu ataków.
 - Analiza danych zbieranych przez honeypoty dostarcza cennych informacji o zachowaniach atakujących i pozwala na lepsze zabezpieczenie systemów.
-



ZADANIE PRAKTYCZNE

<https://github.com/paralax/awesome-honeypots>

<https://github.com/beatazalewa/mysite>

<https://github.com/beatazalewa/Workshop-about-honeypots-in-Django>

Stale poszukuję nowych możliwości i ekscytujących wyzwań. Jeśli chcesz się ze mną skontaktować, proszę, skorzystaj z poniższych kanałów:



Email: beata@zalnet.pl

LinkedIn: <https://www.linkedin.com/in/beatazalewa/>

Blog: <https://zalnet.pl/blog/>

X: <https://x.com/beatazalewa>

GitHub: <https://github.com/beatazalewa/Conferences/>

