



Prima aprilisowe rozmowy kwalifikacyjne

Beata Zalewa, Michał Błaszczak, Krystian Kaczmarek
Not The Hidden Knowledge, NTHW, 01.04.2025

Pytanie 1

Jakie są podstawowe zasady bezpieczeństwa cybernetycznego i czy można je porównać do zasad trzymania się z dala od ciastek w biurze?

Odpowiedź 1

Perplexity

Zasady Bezpieczeństwa Cybernetycznego vs. Ciasteczka w Biurze

1. **Unikaj ciasteczek, jak unikasz phishingu:** Podobnie jak nie dajesz się skusić na ciasteczka, tak samo nie dajesz się skusić na podejrzaną linki w mailach.
2. **Chroń swoje dane, jak chroń swoje ciasteczka:** Nikomu nie dajesz swoich ciasteczek, tak samo nikomu nie dajesz swoich haseł.
3. **Aktualizuj systemy, jak odświeżasz ciasteczka:** Stare ciasteczka stają się nieświeże, tak samo stare systemy stają się niebezpieczne.
4. **Używaj MFA, jak używasz zamka na szafce z ciasteczkami:** Dodatkowa warstwa zabezpieczeń, aby nikt nie dostał się do Twoich ciasteczek... czy danych.
5. **Twórz kopie zapasowe, jak przechowujesz ciasteczka w bezpiecznym miejscu:** Na wypadek, gdyby Twoje ciasteczka (dane) zniknęły, masz ich kopię zapasową.

W ten sposób, zarówno unikanie ciastek, jak i przestrzeganie zasad cyberbezpieczeństwa, wymaga dyscypliny i świadomości, aby uniknąć "zagrożeń" zarówno w sieci, jak i w kuchni biurowej.

Pytanie 2

Co to jest malware i czy można go porównać do nieproszonego gościa na imprezie, który kradnie twoje przekąski?

Malware to złośliwe oprogramowanie zaprojektowane do wyrządzenia szkody lub uzyskania nieautoryzowanego dostępu do systemów komputerowych, sieci lub urządzeń ¹ ² ³ . Może ono przybierać różne formy, takie jak wirusy, trojany, ransomware, spyware i adware ¹ ⁴ .

Porównanie malware do nieproszonego gościa na imprezie, który kradnie przekąski, jest interesujące. Oto kilka punktów porównania:

1. **Niezaproszony Gość:** Malware jest jak nieproszony gość, który pojawia się bez zaproszenia i zaczyna działać wbrew Twoim oczekiwaniom. Podobnie jak nieproszony gość może zacząć jeść Twoje przekąski bez pozwolenia, malware infekuje Twoje urządzenie bez Twojej wiedzy.
2. **Kradzież Przekąsek:** Malware może "ukraść" Twoje dane osobiste lub finansowe, tak jak nieproszony gość kradnie przekąski. W obu przypadkach dochodzi do utraty czegoś cennego bez Twojej zgody.
3. **Zakłócenie Imprezy:** Podobnie jak nieproszony gość może zakłócić atmosferę na imprezie, malware może zakłócić działanie Twojego systemu, powodując problemy techniczne i frustrację.
4. **Trudność w Usunięciu:** Czasem trudno jest usunąć malware z systemu, tak jak może być trudno pozbyć się nieproszonego gościa z imprezy. W obu przypadkach wymaga to pewnych działań, aby przywrócić porządek.

Porównanie to ilustruje, jak malware może być postrzegane jako niepożądany element, który zakłóca normalne funkcjonowanie systemu, tak jak nieproszony gość zakłóca spokój na imprezie.

Odpowiedź
2
Perplexity

Pytanie 3

Co to jest atak MITM?

Odpowiedź 3

MITM lub Man-in-the-Middle to rodzaj ataku, w którym osoba atakująca przechwytuje komunikację między dwiema osobami. Główną intencją MITM jest dostęp do informacji poufnych.

Pytanie 20.

Ponad 100 najważniejszych pytań i odpowiedzi podczas rozmów kwalifikacyjnych dotyczących bezpieczeństwa cybernetycznego

<https://www.guru99.com/pl/cyber-security-interview-questions.html>

Pytanie 4

Czym różni się kod błędu 503 od 404 i 301?

Odpowiedź 4

Czym różni się kod błędu 503 od 404 i 301?

- 503 – usługa niedostępna
- 404 – strona nie istnieje (nie znaleziono)
- 301 – trwale przeniesiony

Kody błędów to istotna informacja. Wiesz, że informacje diagnostyczne mogą być przydatne. Rozumiesz, jak działają narzędzia w stylu `dirbuster`.

Pytania rekrutacyjne na juniora

<https://blog.szurek.tv/post/pytania-rekrutacyjne-na-juniora/>

Pytanie 5

Jakie są dobre praktyki przy tworzeniu silnych haseł i czy można je zapamiętać bez zapisywania na karteczce przyklejonej do monitora?

Odpowiedź 5

Perplexity

Tworzenie Silnych Haseł: Jak Zapamiętać Bez Karteczki

1. **Zrób z hasła piosenkę:** Napisz krótką piosenkę, w której hasło jest refrenem. W ten sposób będziesz je mógł łatwo zapamiętać, a przy okazji będziesz mógł zaśpiewać swoje hasło na imprezie.
2. **Stwórz historię:** Wykorzystaj pierwsze litery słów w Twojej ulubionej historii, aby utworzyć hasło. Na przykład: "Kot Jedzie Na Wakacje" staje się "KJNW".
3. **Celowe błędy ortograficzne:** Dodaj błędy ortograficzne do Twojego hasła, aby było bardziej złożone. Zamiast "Kot", użyj "K0t".
4. **Menedżer Haseł:** Używaj menedżera haseł, który przechowuje Twoje hasła w bezpieczny sposób. To jak skrzynka na ciasteczka, tylko zamiast ciasteczek są hasła.

W ten sposób, możesz mieć silne hasła bez konieczności zapisywania ich na karteczce przyklejonej do monitora. A jeśli zapomnisz hasło, zawsze możesz zaśpiewać swoją piosenkę, aby je sobie przypomnieć!

Pytanie 6

Co to jest DDoS?

Odpowiedź 6

Co to jest DDoS?

Jest odmianą ataków DoS, z tym że atak jest rozproszony i pochodzi z wielu źródeł równolegle.

100 pytań na junióra w sieciach

<https://innasiec.pl/100-pytan-na-juniora-w-sieciach/>

Pytanie 7

What is Phishing? Provide an example.

Odpowiedź 7

4. What is Phishing? Provide an example.

- **Phishing:** A cyberattack in which malicious actors employ deceptive emails or messages to deceive individuals into disclosing sensitive information.
- Example: An email claiming to be from a bank, requesting the recipient to provide their login credentials by clicking a link that leads to a fake website.

Top Cybersecurity Interview Questions and Answers for 2025

<https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-interview-questions>

Pytanie 8

What is a VPN?

Odpowiedź 8

12. Q: What is a VPN?

Your interviewer may ask about VPNs to see if you're familiar with the basics of network processes. To take this answer a step further, provide the definition along with an example of how a VPN works.

A: A VPN is a virtual private network. It can be applied to both small-scale networks and to large informational data systems.

41+ Cybersecurity Interview Questions and Answers to Help You Ace Your Next Interview

<https://cybertalents.com/blog/41-questions-to-help-you-prepare-for-a-cybersecurity-interview>

Pytanie 9

Czym jest test penetracyjny i czy to jak próba włamania się do własnego domu, aby sprawdzić, czy drzwi są bezpieczne?

Odpowiedź 9

Perplexity

Test Penetracyjny: Jak Próba Włamania Się do Własnego Domu

1. **Kontrolowany Atak:** Podobnie jak próbujesz włamać się do własnego domu, aby sprawdzić drzwi, test penetracyjny to kontrolowany atak na system, aby ocenić jego bezpieczeństwo. Tylko że zamiast drzwi, sprawdzamy zabezpieczenia systemów informatycznych.
2. **Wykrywanie Słabości:** Zarówno w domu, jak i w systemie komputerowym, celem jest wykrycie słabości, które mogą być wykorzystane przez niepowołane osoby. W domu to może być otwarte okno, a w systemie – luka w oprogramowaniu.
3. **Poprawa Bezpieczeństwa:** Po zidentyfikowaniu słabości, zarówno w domu, jak i w systemie, można wprowadzić poprawki, aby zwiększyć bezpieczeństwo. W domu zamkniesz okno, a w systemie – zaktualizujesz oprogramowanie.
4. **Zgoda Właściciela:** Podstawową różnicą między testem penetracyjnym a włamaniem jest zgoda właściciela systemu na przeprowadzenie testu. W domu nie potrzebujesz pozwolenia, ale w systemie – tak.

W ten sposób, test penetracyjny jest jak próba włamania się do własnego domu, ale zamiast drzwi, sprawdzamy zabezpieczenia systemów informatycznych, a wszystko odbywa się z pełną zgodą "właściciela domu" – czyli systemu.

Pytanie 10

What made you interested in working in cyber security?

Odpowiedź 10

1What made you interested in working in cyber security?

With this question, the interviewer seeks to understand your motivations for pursuing a career in cyber security and establish whether you're suited to the demands of the role. In answering, you could mention your general interest in IT and any situations you've encountered that drew your attention to the importance of cyber security. You may also want to describe any personal qualities, such as [key skills](#) or personality traits, that make you suited to the role.

Example answer: *'I've always had an interest in computer systems, and I used to build and fix computers for friends and family in my spare time as a teenager. I helped my grandparents when they experienced a phishing attack that led to someone stealing their credit card details. I realised the importance of cyber security and created a more secure computer system for them. This led me to studying cyber security at university and pursuing it as a career. My personality suits this role because I'm analytical, inquisitive and have a strong eye for detail.'*

35 cyber security interview questions, with sample answers

<https://uk.indeed.com/career-advice/interviewing/cyber-security-interview-questions>

Pytanie 11

Co to są honeypoty i jak można je wykorzystać – czy to jak postawienie ciastka na środku stołu, aby złapać mysz?

Honeypoty: Jak Ciastko na Środku Stołu

1. **Pułapka na Hakerów:** Podobnie jak ciastko na środku stołu jest pułapką dla myszy, honeypot jest pułapką dla hakerów. Zamiast ciastka, honeypot oferuje atrakcyjne dane lub symuluje słabo zabezpieczony system, aby przyciągnąć uwagę atakujących.
2. **Monitorowanie Zachowań:** Gdy mysz przyjdzie po ciastko, możesz ją obserwować i dowiedzieć się, jak się zachowuje. Podobnie, honeypot pozwala monitorować zachowania hakerów, aby zrozumieć ich techniki i metody.
3. **Bezpieczne Środowisko:** Ciastko na stole nie zagraża Twoim meblom, a honeypot działa w odizolowanym środowisku, aby nie narazić Twoich prawdziwych danych na niebezpieczeństwo.
4. **Zwiększenie Bezpieczeństwa:** Po złapaniu myszy (lub zrozumieniu zachowań hakerów), możesz wzmocnić zabezpieczenia swojego domu (lub systemu). Honeypot pomaga w identyfikacji słabości i dostosowaniu strategii obronnych.

W ten sposób, honeypot jest jak ciastko na środku stołu – obie są pułapkami, które pomagają wykryć i zrozumieć zachowania "nieproszonych gości", czy to myszy, czy hakerów! 🍰💖

Wykorzystanie Honeypotów:

- **Wykrywanie Zagrożeń:** Honeypoty pomagają wykryć nowe typy ataków i techniki, które mogą nie być jeszcze znane systemom bezpieczeństwa.
- **Analiza Zachowań:** Pozwalają na monitorowanie i analizę działań atakujących, co ułatwia doskonalenie strategii obronnych.
- **Ochrona Systemów:** Mogą odciążyć systemy obronne, przekierowując ataki na siebie, dzięki czemu chronią prawdziwe dane i systemy.

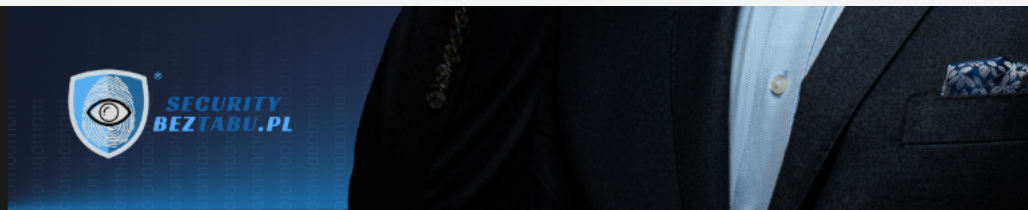
Przykład z Praktyki: Chińscy hakerzy zostali "nabrani" przez honeypoty, które symulowały przemysłowe systemy SCADA. Atakujący próbowali przejąć kontrolę nad tymi systemami, nie wiedząc, że są to pułapki ¹.

Odpowiedź
11
Perplexity

Pytanie 12

Czym jest autoryzacja dwuskładnikowa (2FA) i jakie są jej korzyści?

Odpowiedź 12



To tylko **hipotetyczne** pytania i potraktuj je jako **trening**. Mogą one paść podczas rozmowy kwalifikacyjnej – **ale nie muszą**. To bardziej informacja dla Ciebie gdzie warto się podszkolić. Poniżej lista 100 pytań:

1. Jakie są podstawowe zasady bezpieczeństwa cybernetycznego?
2. Czym jest phishing i jak można się przed nim chronić?
3. Co to jest malware? Podaj przykłady różnych typów malware.
4. Jakie są dobre praktyki przy tworzeniu silnych haseł?
5. Czym jest autoryzacja dwuskładnikowa (2FA) i jakie są jej korzyści?

Pytanie 13

Jakie są zalety i wady korzystania z oprogramowania typu open source w kontekście bezpieczeństwa – czy to jak dzielenie się przepisem na ciasto, ale z ryzykiem, że ktoś doda za dużo soli?

Odpowiedź 13

Perplexity

"Korzystanie z oprogramowania open source to jak przygotowanie ciasta z przepisem, który jest dostępny dla wszystkich. Z jednej strony, każdy może dodać swoją szczyptę soli i poprawić smak, ale z drugiej strony, istnieje ryzyko, że ktoś doda za dużo soli i całe ciasto będzie niezdatne do spożycia. W przypadku open source, 'sól' to potencjalne luki bezpieczeństwa, które mogą być wykorzystane przez hakerów. Jednak dzięki otwartości kodu, społeczność może szybko zareagować i 'odsolone' ciasto naprawić, zanim będzie za późno."

Pytanie 14

Czym jest inżynieria społeczna i jak można się przed nią bronić – czy to jak nie dawać się przekonać nieznajomemu, że jest twoim długo zaginionym kuzynem?

Odpowiedź 14

Perplexity

"Inżynieria społeczna to jak próba przekonania cię, że twój długo zaginiony kuzyn jest w stanie cię odwiedzić, choć ostatni raz widziałeś go na weselu twoich dziadków. Właściwie to jest to jak próba sprzedaży ci lodów w środku zimy, mówiąc, że są one 'idealne na każdą porę roku'. Ale nie daj się nabrać! Zawsze weryfikuj tożsamość i nie ufaj nikomu, kto dzwoni i mówi, że jest z 'firmy SuperTelco' – chyba że masz ochotę na dodatkowe godziny rozmów z 'technikiem', który naprawi twoje łącze internetowe... albo twoje życie."

Pytanie 15

Jak działa protokół HTTPS i dlaczego jest bezpieczniejszy niż HTTP – czy to jak wysyłanie listów w zaklejonej kopercie zamiast na otwartej pocztówce?

Odpowiedź 15

Perplexity

"HTTPS to jak wysyłanie listów w zaklejonej kopercie, ale zamiast pieczęci używa się superzaawansowanego kodu, który uniemożliwia otwarcie koperty bez zostawienia śladu. To jak próba otwarcia puszki zupy bez otwieracza – nie wiesz, co jest w środku, a nawet gdybyś próbował, to i tak byś nic nie zobaczył, bo wszystko jest zakodowane. Z kolei HTTP to jak wysyłanie pocztówki, na której każdy może napisać 'Kocham cię!' i podpisać się jako twój sekretarny kochanek. Więc, jeśli chcesz, aby twoje sekrety pozostały sekretami, używaj HTTPS – to jak mieć super tajną skrzynkę pocztową, do której tylko ty masz klucz! A jeśli ktoś próbuje włamać się do twojej koperty, to jest jak próba otwarcia zamka z wytrychem – nie ma szans, bo kod jest za silny!"

Pytanie 16

Jak długo należy się uczyć, aby znaleźć pierwszą pracę w cybersecurity?

Odpowiedź 16

← All Roadmaps

🔖 Schedule Learning Time

📄 Download

🔗 Share

Cyber Security Expert

Step by step guide to becoming a Cyber Security Expert in 2025

📅 Roadmap

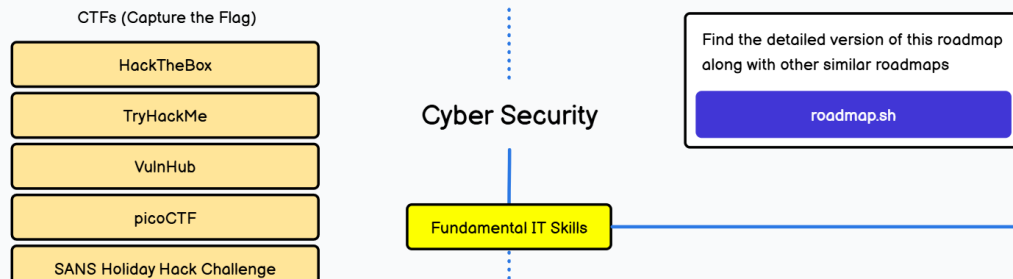
📁 Projects

soon

🗨 Suggest Changes

0% DONE 0 of 301 Done

📊 Track Progress



Cyber Security Expert roadmap

<https://roadmap.sh/cyber-security>

The background of the slide features a close-up, vertical view of several green leaves, likely from a plant like a banana or a similar broad-leafed species. The leaves are vibrant green and show prominent veins. They are arranged in a way that creates a sense of depth and texture, with some leaves in sharp focus and others slightly blurred in the background.

Ask The Experts by Albercik