Imię i nazwisko: _____ Data: _____ Wynik: _____

# Ciemna sieć a głęboka sieć: bezpieczeństwo i Różnice

Indeksowanie przez wyszukiwarki, bazy danych głębokiej sieci, trasowanie cebulowe Tor, anonimowość w sieci i zagrożenia

## PRZEGLĄD NAUKI: DARK WEB A DEEP WEB

**CHRONIONY**
**SZYFROWANIE DANYCH**
Standard AES 256-bitowy

**ZGODNY**
**STANDARDY GLOBALNE**
Ramy prawne RODO (GDPR) i CCPA

**ZERO TRUST**
**POLITYKA DOSTĘPU**
Uwierzytelnianie wieloskładnikowe

**Witaj!** Ten pakiet ćwiczeń przeprowadzi cię przez różnice między głęboką siecią (Deep Web) a ciemną siecią (Dark Web). Poznasz nieindeksowane bazy danych, routing cebulowy w przeglądarce Tor, kryptograficzne domeny .onion i zagrożenia dla anonimowości.

### PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

**Otwórz przewodnik VPN.com po cyberbezpieczeństwie**

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/dark-web-vs-deep-web/

# Twoja ścieżka nauki: strategia dla głębokiej i ciemnej sieci

- Porównaj głęboką sieć (deep web, nieindeksowane bazy danych) z siecią dark web (usługi onion).
- Zrozum, jak routing cebulowy szyfruje i przekazuje ruch sieciowy.
- Oceń ryzyka bezpieczeństwa związane z wchodzeniem na niezweryfikowane strony w sieci Tor.
- Wdrażaj bezpieczną bramę i polityki piaskownicy (sandboxing) na potrzeby crawlowania w ramach analizy zagrożeń.
- Przeanalizuj format adresu kryptograficznego domen usług onion.

## PRZEWODNIK PO GŁĘBOKIEJ I CIEMNEJ SIECI: INSTRUKCJE

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu prywatności w głębokiej i ciemnej sieci. Zakończ zadaniem dodatkowym Myśl szybko.

## BAZY DANYCH GŁĘBOKIEJ SIECI A ROUTING CEBULOWY CIEMNEJ SIECI (WPROWADZENIE)

Deep web składa się z niezindeksowanych stron chronionych hasłami i logowaniem, takich jak prywatna poczta e-mail lub firmowe portale bankowe. Dark web to podzbiór deep webu, który jest celowo ukryty i wymaga wyspecjalizowanych przeglądarek (takich jak Tor) oraz sieci onion, aby uzyskać do niego anonimowy dostęp.

**PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.**

## Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

**1. Czym różni się deep web od surface web?**

- A. Strony deep web nie są indeksowane przez publiczne wyszukiwarki
- B. Ruch w głębokiej sieci jest nielegalny i monitorowany przez organy ścigania
- C. Witryny głębokiej sieci wymagają do dostępu specjalistycznych przeglądarek, takich jak Tor
- D. Strony głębokiej sieci zawsze ładują się szybciej niż strony powierzchniowej sieci

**2. Jak uzyskuje się dostęp do dark webu?**

- A. Przez wyspecjalizowane przeglądarki korzystające z sieci routingu cebulowego
- B. Przez skonfigurowanie niestandardowych ustawień DNS w zwykłych routerach
- C. Przez prywatne konsole wyszukiwania w sieci powierzchniowej dostępne tylko na zaproszenie
- D. Przez zainstalowanie standardowego rozszerzenia przeglądarki blokującego reklamy

**3. Jaka struktura stanowi największą część deep webu?**

- A. Chronione hasłem bazy danych użytkowników i prywatne konta
- B. Nielegalne fora czarnego rynku, na których handluje się nielegalnymi towarami
- C. Niezaszyfrowane protokoły udostępniania plików peer-to-peer
- D. Publiczne bazy danych pamięci podręcznej wyszukiwarek

**4. Co robi routing cebulowy z ruchem sieciowym?**

- A. Szyfruje pakiety i kieruje je przez wiele przekaźników
- B. Zwiększa szybkość pobierania dzięki ominięciu węzłów ISP
- C. Mapuje numery seryjne sprzętu urządzeń na rekordy IP
- D. Usuwa pliki cookie przeglądarki po każdym kliknięciu

**5. Jaki sufiks domeny jest używany wyłącznie w sieciach Tor?**

- A. Kryptograficzne rozszerzenie najwyższego poziomu .onion
- B. Standardowe, starsze komercyjne rozszerzenie .com
- C. Zdecentralizowane rozszerzenie blockchain .eth w Web3
- D. Rozszerzenie technologiczne kodu kraju .ai

## Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

### 6 Pytanie (prawda/fałsz) 6

6. Deep web i dark web oznaczają ten sam segment sieci.

- ○ Prawda
- ○ Fałsz

### 7 Pytanie (prawda/fałsz) 7

7. Portale intranetowe firm są częścią głębokiej sieci (deep web).

- ○ Prawda
- ○ Fałsz

### 8 Pytanie (prawda/fałsz) 8

8. Trasowanie cebulowe całkowicie odszyfrowuje pakiety danych w każdym węźle tranzytowym.

- ○ Prawda
- ○ Fałsz

### 9 Pytanie (prawda/fałsz) 9

9. Dostęp do dark webu naraża urządzenia na wysokie ryzyko złośliwego oprogramowania.

- ○ Prawda
- ○ Fałsz

### 10 Pytanie (prawda/fałsz) 10

10. Standardowe wyszukiwarki internetowe przeszukują i indeksują witryny onion.

- ○ Prawda
- ○ Fałsz

# Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Prywatne portale bankowe znajdują się w nieindeksowanym segmencie, jakim jest _____ .
2. Wyspecjalizowane węzły Tor hostują ukryte usługi w segmencie, jakim jest _____ .
3. Strony Tor używają kryptograficznego rozszerzenia domeny najwyższego poziomu o nazwie _____ .
4. Zaszyfrowane, wielowarstwowe kierowanie ruchu nazywa się _____ .
5. Wyszukiwarki powierzchniowe przeszukują strony, które są publicznie _____ .
6. Sieci cebulowe szyfrują adresy IP klientów, co daje użytkownikom _____ .

**BANK SŁÓW**

.ONION | ANONIMOWOŚĆ | BAZA DANYCH | CIEMNA SIEĆ | GŁĘBOKA SIEĆ | INDEKSOWANE | ROUTING CEBULOWY | WĘZEŁ WEJŚCIOWY

**Wpisz tutaj swoje odpowiedzi:**

1. 
2. 
3. 
4. 
5. 
6. 

# Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

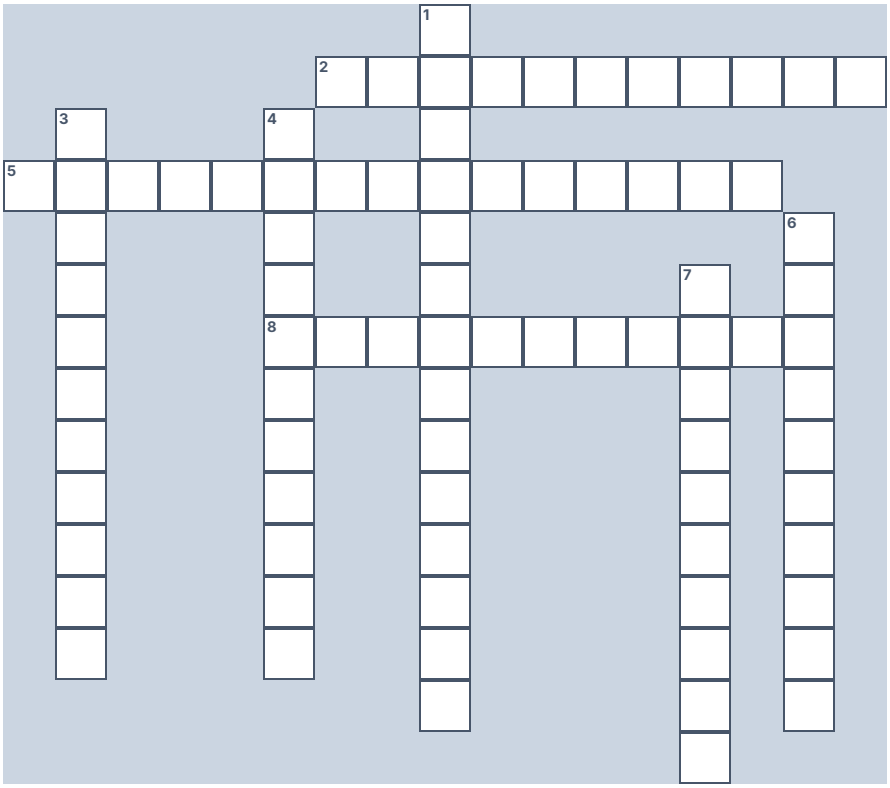
## DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

| | | | |
|---|---|---|---|
| ☐ | 1. Segment głębokiej sieci | A | Zaszyfrowany segment sieci dostępny wyłącznie przez specjalne przeglądarki. |
| ☐ | 2. Portal w dark webie | B | Szyfrowanie danych warstwowo i przekazywanie ich przez trzy węzły. |
| ☐ | 3. Rozszerzenie onion | C | Bezpieczny magazyn zaplecza przechowujący nieindeksowane rekordy systemowe. |
| ☐ | 4. Routing przez Tor | D | Kryptograficzny sufiks domeny najwyższego poziomu używany w sieciach Tor. |
| ☐ | 5. Zaindeksowane strony | E | Węzeł wejściowy służący do uzyskiwania dostępu do sieci Tor. |
| ☐ | 6. Anonimowość użytkownika | F | Treści sieci powierzchniowej skompilowane i dostępne do wyszukiwania w Google. |
| ☐ | 7. Prywatna baza danych | G | Ukrywanie publicznych adresów IP klientów przed serwerami. |
| ☐ | 8. Brama wejściowa | H | Niezindeksowane treści internetowe, takie jak prywatne logowania, wiadomości e-mail i rekordy baz danych. |

## Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.



### POZIOMO

**2. Nieindeksowana zawartość sieci, taka jak prywatne loginy, e-maile i rekordy baz danych (11)**

**5. Szyfrowanie danych warstwami i przekazywanie ich przez trzy węzły (15)**

**8. Zawartość sieci powierzchniowej skompilowana i przeszukiwalna w Google (11)**

### PIONOWO

**1. Węzeł wejścia służący do uzyskania dostępu do sieci Tor (14)**

**3. Kryptograficzny sufiks domeny najwyższego poziomu używany w sieciach Tor (11)**

**4. Ukrywanie publicznych adresów IP klientów przed serwerami (11)**

**6. Zaszyfrowany segment sieci dostępny tylko przez specjalne przeglądarki (10)**

**7. Bezpieczny backend przechowujący nieindeksowane rekordy systemowe (10)**

# Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

## POZIOMO

**2 poziomo: Nieindeksowana zawartość sieci, taka jak prywatne loginy, e-maile i rekordy baz danych (11 liter):**

**5 poziomo: Szyfrowanie danych warstwami i przekazywanie ich przez trzy węzły (15 liter):**

**8 poziomo: Zawartość sieci powierzchniowej skompilowana i przeszukiwalna w Google (11 liter):**

## PIONOWO

**1 pionowo: Węzeł wejścia służący do uzyskania dostępu do sieci Tor (14 liter):**

**3 pionowo: Kryptograficzny sufiks domeny najwyższego poziomu używany w sieciach Tor (11 liter):**

**4 pionowo: Ukrywanie publicznych adresów IP klientów przed serwerami (11 liter):**

**6 pionowo: Zaszyfrowany segment sieci dostępny tylko przez specjalne przeglądarki (10 liter):**

**7 pionowo: Bezpieczny backend przechowujący nieindeksowane rekordy systemowe (10 liter):**

## Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ł | X | J | B | Ź | C | B | R | Ź | O | V | Ż | O | Ż | U |
| T | Ą | H | W | P | Y | C | O | N | M | W | H | Ó | Y | Ź |
| Ć | Ż | Y | H | Ń | I | O | U | S | X | Ę | F | U | V | Ę |
| E | X | H | H | I | Ź | Ń | T | U | G | Z | V | M | K | E |
| I | Ł | A | C | N | N | Ę | I | Ń | L | E | U | N | J | G |
| S | F | N | Y | D | Q | W | N | Ę | S | Ł | S | O | Ć | C |
| A | Ż | O | N | E | Ć | V | G | Q | T | W | J | I | Ż | I |
| K | H | N | A | K | M | Ś | C | E | Ń | E | W | N | C | E |
| O | A | I | D | S | R | U | E | Ą | W | J | N | O | E | M |
| B | O | M | A | O | P | U | B | R | Ź | Ś | P | A | Ć | N |
| Ę | T | O | Z | W | Z | T | U | Z | S | C | S | N | E | A |
| Ł | P | W | A | A | Ć | V | L | J | X | I | Ń | E | K | S |
| G | V | O | B | N | Ń | H | O | C | M | O | B | M | P | I |
| W | W | Ś | B | E | Ś | W | W | R | H | W | Ć | O | E | E |
| B | T | Ć | U | L | Y | E | Y | J | R | Y | Ź | D | Y | Ć |

### LISTA SŁÓW

GŁĘBOKASIEĆ
CIEMNASIEĆ
DOMENAONION
ROUTINGCEBULOWY
INDEKSOWANE
ANONIMOWOŚĆ
BAZADANYCH
WĘZEŁWEJŚCIOWY

# Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

**TERMINY ZE SŁOWNICZKA**

- **A. GŁĘBOKASIEĆ**
- **B. CIEMNASIEĆ**
- **C. DOMENAONION**
- **D. ROUTINGCEBULOWY**
- **E. INDEKSOWANE**
- **F. ANONIMOWOŚĆ**
- **G. BAZADANYCH**
- **H. WĘZEŁWEJŚCIOWY**

**DEFINICJE I POLA DOPASOWANIA**

1. Ukrywanie publicznych adresów IP klientów przed serwerami.
2. Bezpieczny backend przechowujący nieindeksowane rekordy systemowe.
3. Szyfrowanie danych warstwami i przekazywanie ich przez trzy węzły.
4. Nieindeksowana zawartość sieci, taka jak prywatne loginy, e-maile i rekordy baz danych.
5. Zaszyfrowany segment sieci dostępny tylko przez specjalne przeglądarki.
6. Kryptograficzny sufiks domeny najwyższego poziomu używany w sieciach Tor.
7. Węzeł wejścia służący do uzyskania dostępu do sieci Tor.
8. Zawartość sieci powierzchniowej skompilowana i przeszukiwalna w Google.

## Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. OAEŁKSGIĘĆB
2. NNODOAMINOE
3. IOSWDNNEKAE
4. ACDHAYNBAZ
5. IAĆIMSNCEE
6. LGOUNCBWYUROETI
7. WIANOĆOŚOMN
8. EJOWŚCĘYWEZWIŁ

# Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

| | | | | |
|---|---|---|---|---|
| 1 | Powody, dla których warto trzymać się z dala od ciemnej sieci (dark web) | | | |
| 2 | Rzeczy, których wyszukiwarka nie potrafi znaleźć | | | |
| 3 | Urządzenia, które można zhakować | | | |
| 4 | Legalne powody do korzystania z Tora | | | |
| 5 | Powody, dla których warto aktualizować oprogramowanie | | | |
| 6 | Sygnały ostrzegawcze w e-mailu | | | |
| 7 | Rzeczy sprzedawane nielegalnie w ciemnej sieci (dark web) | | | |
| 8 | Osoby, które możesz poprosić o pomoc IT | | | |
| 9 | Bezpieczne nawyki, które możesz zacząć już dziś | | | |
| 10 | Rzeczy do zrobienia po wycieku danych | | | |
| 11 | Rzeczy, które należą do głębokiej sieci (deep web) | | | |
| 12 | Strony, z których korzystasz po zalogowaniu | | | |
| 13 | Słowa związane z anonimowością | | | |
| 14 | Informacje, których nigdy nie powinieneś udostępniać | | | |
| 15 | Rzeczy, które leżą „pod powierzchnią” | | | |

# Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

## STUDIUM PRZYPADKU 1: IDENTYFIKACJA WYCIEKU DANYCH



**Scenariusz:** Firmowy audyt bezpieczeństwa odkrywa, że wrażliwe rekordy bazy danych klientów są sprzedawane na targowisku w sieci onion. Dane nie są indeksowane w Google.

**Pytanie do dyskusji:** Wyjaśnij, których segmentów sieci to dotyczy i jak doszło do tego wycieku.

## STUDIUM PRZYPADKU 2: ANONIMOWOŚĆ A RYZYKO ZŁOŚLIWEGO OPROGRAMOWANIA



**Scenariusz:** Analityk chce sprawdzić źródła informacji o zagrożeniach na stronie w sieci Tor. Pobiera przeglądarkę Tor i wchodzi na stronę.

**Pytanie do dyskusji:** Oceń korzyści w zakresie anonimowości i wskaż kroki ograniczające ryzyko złośliwego oprogramowania.

# Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

**KLUCZ SZYFROWANIA LITERA-LICZBA**

**A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12**

**J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24**

**S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 24 | 20 | 28 | 27 | 12 | 18 | 10 | | 4 | 7 | 3 | 28 | 15 | 20 | 30 | 32 |
| | | | | | | | | | | | | | | | |
| 4 | 11 | 24 | 20 | 18 | 12 | | 1 | 18 | 20 | 18 | 12 | 17 | 20 | 30 | 20 | 26 | 5 |
| | | | | | | | | | | | | | | | | | |
| 28 | 35 | 32 | 27 | 14 | 20 | 30 | 18 | 12 | 14 | 1 | | | | | | | |
| | | | | | | | | | | | | | | | | | |

**Odszyfrowana wiadomość:**

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

### Q1: Czym jest głęboka sieć (deep web)?

Deep web składa się ze wszystkich stron internetowych, których wyszukiwarki nie mogą zindeksować, w tym bankowości internetowej, baz poczty e-mail i czasopism z płatnym dostępem.

### Q2: Czym jest dark web?

Dark web to niewielka część deep webu, celowo ukryta i dostępna tylko przez wyspecjalizowane przeglądarki korzystające z sieci onion.

### Q3: Jak wyszukiwarki indeksują strony?

Wyszukiwarki uruchamiają zautomatyzowane programy (roboty indeksujące), które podążają za publicznymi linkami i indeksują strony niezablokowane dla indeksowania przez dyrektywy robots.

### Q4: Dlaczego bankowość internetowa jest uważana za część deep webu?

Portale bankowe są chronione ekranami logowania i hasłami, co uniemożliwia publicznym wyszukiwarkom indeksowanie stron z wyciągami z konta.

### Q5: Czym jest routing cebulowy (Onion Routing) w przeglądarce Tor?

Trasowanie cebulowe to metoda transmisji, która szyfruje ruch warstwowo i przesyła go przez wiele przekaźników, aby zamaskować adresy IP użytkowników.

# Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

### Q6: Czy korzystanie z dark webu jest nielegalne?

Nie. Dostęp do dark webu jest w większości krajów legalny, choć angażowanie się w nielegalne rynki lub działania cyberprzestępcze jest zabronione.

### Q7: Dlaczego strony w dark webie ładują się wolno?

Ruch jest kierowany i odszyfrowywany przez co najmniej trzy globalne przekaźniki (wejściowy, środkowy, wyjściowy), co zwiększa opóźnienie transmisji.

### Q8: Co oznacza przyrostek domeny .onion?

To wyspecjalizowany przyrostek domeny najwyższego poziomu używany w sieciach Tor, wskazujący na kryptograficznie generowane adresy zamiast standardowych serwerów DNS.

### Q9: Jakie ryzyko wiąże się z linkami w dark webie?

Witryny nie mają żadnej kontroli bezpieczeństwa, co naraża użytkowników na wysokie ryzyko infekcji złośliwym oprogramowaniem, skrypty phishingowe i oszustwa transakcyjne.

### Q10: Kto stworzył protokół routingu sieci Tor?

Technologia została pierwotnie opracowana przez Laboratorium Badawcze Marynarki Wojennej USA w latach 1990. w celu ochrony łączności rządowej.

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

### Q1: Jak węzły pośrednie chronią anonimowość w Torze?

Każdy węzeł odszyfrowuje tylko jedną warstwę danych routingu, znając wyłącznie poprzedni i następny przeskok, ale nigdy jednocześnie źródło i cel.

### Q2: Jaka jest rola węzła wyjściowego?

Węzeł wyjściowy odszyfrowuje ostatnią warstwę szyfrowania i wysyła ruch do publicznego serwera docelowego lub serwera onion.

### Q3: Czym jest brama mostków Tor (Tor bridges)?

Mosty (bridges) to niewymienione publicznie przekaźniki wejściowe Tora, używane do omijania blokad ISP i cenzury w regionach ograniczających dostęp do przeglądarki Tor.

### Q4: Jak podmioty z dark webu wykorzystują kryptowaluty?

Przestępcy używają anonimowych kryptowalut do przeprowadzania transakcji finansowych na czarnych rynkach, omijając standardowe kontrole transakcji bankowych.

### Q5: Dlaczego standardowe wyszukiwarki nie potrafią przeszukiwać głębokich baz danych?

Roboty indeksujące nie mogą wprowadzać poświadczeń logowania, rozwiązywać zabezpieczeń CAPTCHA ani uruchamiać skryptów zapytań SQL na zapleczu, które są wymagane do dostępu do głębokich baz danych.

# Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

### Q6: Czym jest serwer katalogowy w sieciach Tor?

To zaufany serwer przechowujący listę aktywnych przekaźników wejściowych, pośrednich i wyjściowych, których klienci używają do budowania ścieżek routingu.

### Q7: Jak złośliwi aktorzy podsłuchują ruch na węzłach wyjściowych (exit node sniffing)?

Nieuczciwi operatorzy węzłów wyjściowych mogą przechwytywać niezaszyfrowany ruch HTTP opuszczający sieć Tor, kradnąc nazwy użytkowników i pliki cookie.

### Q8: Czym różni się Tor od I2P?

Tor używa scentralizowanego katalogu przekaźników i węzłów wyjściowych do publicznego dostępu do sieci, a I2P używa zdecentralizowanej struktury peer-to-peer do hostowania wewnętrznego.

### Q9: Jak organy ścigania śledzą rynki dark webu?

Agencje używają analizy blockchain, lokalizują fizyczne konfiguracje hostingu serwerów i prowadzą operacje z wykorzystaniem przynęt, aby zidentyfikować operatorów.

### Q10: Jak wyciek DNS zagraża anonimowości klienta?

Wycieki DNS występują, gdy zapytania DNS przeglądarki są wysyłane bezpośrednio przez lokalnego dostawcę internetu, zamiast być kierowane przez szyfrowaną sieć Tor.

## Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

**1. WGLĄD W BEZPIECZEŃSTWO**

Deep web jest znacznie większy niż przeszukiwalny surface web, ponieważ większość treści znajduje się za logowaniem i w bazach danych.

**2. WGLĄD W BEZPIECZEŃSTWO**

Dark web to niewielka, celowo ukryta część deep webu, do której dociera się za pomocą narzędzi takich jak Tor.

**3. WGLĄD W BEZPIECZEŃSTWO**

Routing Tor szyfruje pakiety danych trzykrotnie, zdejmując warstwy szyfrowania jak warstwy cebuli w każdym przekaźniku.

**4. WGLĄD W BEZPIECZEŃSTWO**

Tor wyrósł z projektu routingu cebulowego prowadzonego przez Laboratorium Badawcze Marynarki Wojennej USA, a jego kod został udostępniony jako wolne oprogramowanie. [1]

**5. WGLĄD W BEZPIECZEŃSTWO**

Adresy onion to 56-znakowe ciągi alfanumeryczne generowane kryptograficznie z par kluczy publicznych.

**6. WGLĄD W BEZPIECZEŃSTWO**

Węzły wyjściowe mogą odczytywać ruch w postaci jawnej, co oznacza, że w sieci Tor nadal wymagane jest TLS/HTTPS, aby zabezpieczyć dane sesji.

**7. WGLĄD W BEZPIECZEŃSTWO**

Strony intranetowe, dyski w chmurze i prywatne bazy danych stanowią największe segmenty przechowywania danych w deep webie.

**8. WGLĄD W BEZPIECZEŃSTWO**

Wyspecjalizowane wyszukiwarki, takie jak DuckDuckGo, prowadzą portale onion, aby umożliwić anonimowe wyszukiwanie w sieciach Tor.

**9. WGLĄD W BEZPIECZEŃSTWO**

Ponad 2 miliony użytkowników codziennie łączy się z siecią Tor, aby omijać cenzurę i zachować prywatność komunikacji.

**10. WGLĄD W BEZPIECZEŃSTWO**

Globalne operacje organów ścigania (takie jak Operation Bayonet) zamykają duże ciemne rynki, przejmując sprzęt hostingowy.

# Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych.

## PUBLIKACJE NAUKOWE I BRANŻOWE

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

## Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

**1** **Indeksowanie w wyszukiwarce** GŁĘBOKA SIEĆ — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Strony głębokiej sieci znajdują się za ekranami logowania i w bazach danych, co uniemożliwia robotom wyszukiwarek ich indeksowanie. Źródło: IETF RFC 3986.

**2** **Dostęp do Tora** DARK WEB — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Dark web składa się z ukrytych usług onion dostępnych tylko przez przeglądarki takie jak Tor. Źródło: IETF RFC 3986.

**3** **Głębokie bazy danych** BAZY DANYCH — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Konta chronione hasłem i dokumenty firmowe stanowią największą część głębokiej sieci. Źródło: NIST Digital Identity.

**4** **Trasowanie cebulowe** SIEĆ TOR — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Trasowanie cebulowe szyfruje pakiety danych warstwowo i przekazuje je przez wiele węzłów, aby zapewnić anonimowość. Źródło: IETF RFC 3986.

**5** **Domena Onion** SUFIKS — **Poprawna odpowiedź: A**

### UWAGA DLA NAUCZYCIELA

Kryptograficzny sufiks domeny.onion kieruje ruch wewnątrz sieci Tor bez publicznego DNS. Źródło: IETF RFC 3986.

## Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

**6** **Segmenty sieciowe** STRUKTURA

**Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Deep web obejmuje wszystkie niezindeksowane strony, a dark web to niewielki, szyfrowany podsegment onion. Źródło: IETF RFC 3986.

**7** **Intranety korporacyjne** GŁĘBOKA SIEĆ

**Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Strony intranetowe znajdują się za portalami z hasłem i nie są indeksowane, co oznacza, że należą do deep webu. Źródło: NIST Digital Identity.

**8** **Szyfrowanie warstwowe** PRZEKAŹNIKI

**Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Przekaźniki onion odszyfrowują tylko jedną warstwę trasowania, aby chronić anonimowość użytkownika, a nigdy cały pakiet. Źródło: IETF RFC 3986.

**9** **Narażenie na złośliwe oprogramowanie** ZAGROŻENIA

**Poprawna odpowiedź: Prawda**

### UWAGA DLA NAUCZYCIELA

Rynki w ciemnej sieci nie mają żadnego filtrowania bezpieczeństwa, co wiąże się z ogromnym ryzykiem zainfekowania złośliwym oprogramowaniem. Źródło: Center for Internet Security (CIS).

**10** **Pytanie 10**

**Poprawna odpowiedź: Fałsz**

### UWAGA DLA NAUCZYCIELA

Zwykłe roboty wyszukiwarek nie korzystają z Tora, więc nie mogą dotrzeć do witryn .onion ani ich indeksować.

# Klucze słownictwa i kryteria oceny

**Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).**

## PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

| | | | |
|---|---|---|---|
| H 1. Segment głębokiej sieci | A 2. Portal w dark webie | D 3. Rozszerzenie onion | B 4. Routing przez Tor |
| F 5. Zaindeksowane strony | G 6. Anonimowość użytkownika | C 7. Prywatna baza danych | E 8. Brama wejściowa |

## PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

| | | | |
|---|---|---|---|
| 1 GŁĘBOKA SIEĆ | 2 CIEMNA SIEĆ | 3 .ONION | 4 ROUTING CEBULOWY |
| 5 INDEKSOWANE | 6 ANONIMOWOŚĆ | | |

## PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

| | | | |
|---|---|---|---|
| 1 F – ANONIMOWOŚĆ | 2 G – BAZADANYCH | 3 D – ROUTINGCEBULOWY | 4 A – GŁĘBOKASIEĆ |
| 5 B – CIEMNASIEĆ | 6 C – DOMENAONION | 7 H – WĘZEŁWEJŚCIOWY | 8 E – INDEKSOWANE |

## UWAGI DO DYSKUSJI DLA NAUCZYCIELI

**Kluczowe pojęcia:**
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Segment głębokiej sieci, Portal w dark webie i Rozszerzenie onion oraz podać przykład każdego z nich.

**Studia przypadków:**
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

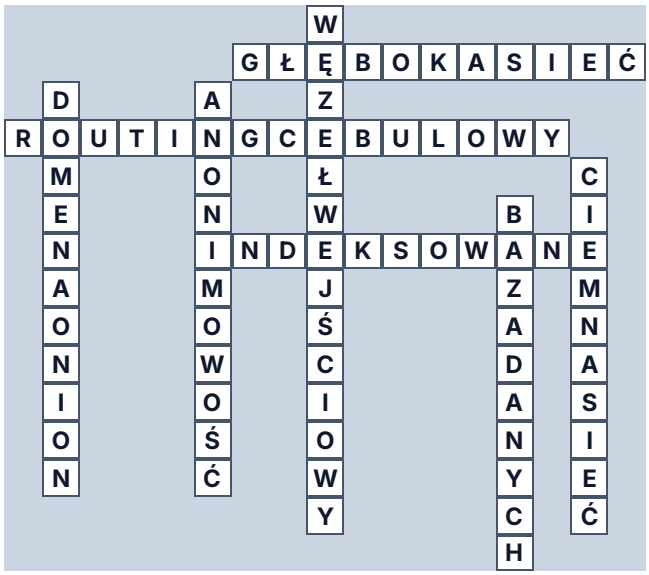
**Ocena źródeł:**
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

# Klucze do łamigłówek i uwagi dla nauczyciela

## ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ł | X | J | B | Ź | C | B | R | Ź | O | V | Ż | O | Ż | U |
| T | Ą | H | W | P | Y | C | O | N | M | W | H | Ó | Y | Ź |
| Ć | Ż | Y | H | Ń | I | O | U | S | X | Ę | F | U | V | Ę |
| E | X | H | H | I | Ź | Ń | T | U | G | Z | V | M | K | E |
| I | Ł | A | C | N | N | Ę | I | Ń | L | E | U | N | J | G |
| S | F | N | Y | D | Q | W | N | Ę | S | Ł | S | O | Ć | C |
| A | Ż | O | N | E | Ć | V | G | Q | T | W | J | I | Ż | I |
| K | H | N | A | K | M | Ś | C | E | Ń | E | W | N | C | E |
| O | A | I | D | S | R | U | E | Ą | W | J | N | O | E | M |
| B | O | M | A | O | P | U | B | R | Ź | Ś | P | A | Ć | N |
| Ę | T | O | Z | W | Z | T | U | Z | S | C | S | N | E | A |
| Ł | P | W | A | A | Ć | V | L | J | X | I | Ń | E | K | S |
| G | V | O | B | N | Ń | H | O | C | M | O | B | M | P | I |
| W | W | Ś | B | E | Ś | W | W | R | H | W | Ć | O | E | E |
| B | T | Ć | U | L | Y | E | Y | J | R | Y | Ź | D | Y | Ć |

## ROZWIĄZANIE KRZYŻÓWKI




## PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

### POZIOMO

**2 poziomo: GŁĘBOKASIEĆ** Nieindeksowana zawartość sieci, taka jak prywatne loginy, e-maile i rekordy baz danych (11 liter)

**5 poziomo: ROUTINGCEBULOWY** Szyfrowanie danych warstwami i przekazywanie ich przez trzy węzły (15 liter)

**8 poziomo: INDEKSOWANE** Zawartość sieci powierzchniowej skompilowana i przeszukiwalna w Google (11 liter)

### PIONOWO

**1 pionowo: WĘZEŁWEJŚCIOWY** Węzeł wejścia służący do uzyskania dostępu do sieci Tor (14 liter)

**3 pionowo: DOMENAONION** Kryptograficzny sufiks domeny najwyższego poziomu używany w sieciach Tor (11 liter)

**4 pionowo: ANONIMOWOŚĆ** Ukrywanie publicznych adresów IP klientów przed serwerami (11 liter)

**6 pionowo: CIEMNASIEĆ** Zaszyfrowany segment sieci dostępny tylko przez specjalne przeglądarki (10 liter)

**7 pionowo: BAZADANYCH** Bezpieczny backend przechowujący nieindeksowane rekordy systemowe (10 liter)

# Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

## KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. OAEŁKSGIĘĆB — **GŁĘBOKASIEĆ**
2. NNODOAMINOE — **DOMENAONION**
3. IOSWDNNEKAE — **INDEKSOWANE**
4. ACDHAYNBAZ — **BAZADANYCH**
5. IAĆIMSNCEE — **CIEMNASIEĆ**
6. LGOUNCBWYUROETI — **ROUTINGCEBULOWY**
7. WIANOĆOŚOMN — **ANONIMOWOŚĆ**
8. EJOWŚCĘYWEZWIŁ — **WĘZEŁWEJŚCIOWY**

## KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

**"ROUTING CEBULOWY CHRONI ANONIMOWOŚĆ UŻYTKOWNIKA"**

# Klucz odpowiedzi do studiów przypadków

## A Studium przypadku 1: Identyfikacja wycieku danych

Rozwiązanie dla nauczyciela

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Analiza scenariusza: Firmowy audyt bezpieczeństwa wykrywa, że wrażliwe rekordy bazy danych klientów są sprzedawane na rynku w sieci onion. Dane nie są zindeksowane w Google.
- Zalecana strategia i rozwiązanie: Zaangażowane segmenty: Prywatna baza danych należy do głębokiej sieci (deep web – nieindeksowana, ale bezpieczna). Rynek, na którym handluje się skradzionymi danymi, znajduje się w ciemnej sieci (sieć onion, dark web). Jak do tego doszło: Hakerzy ominęli zabezpieczenia serwera, wykradli bazę danych z głębokiej sieci i anonimowo wystawili ją w ciemnej sieci, aby uniknąć namierzenia przez organy ścigania.

## B Studium przypadku 2: Anonimowość a ryzyko złośliwego oprogramowania

Rozwiązanie dla nauczyciela

### WYTYCZNE OCENIANIA

**Odpowiedzi uczniów powinny obejmować następujące punkty:**

- Analiza scenariusza: Analityk chce sprawdzić kanały informacji o zagrożeniach w witrynie Tor. Pobiera przeglądarkę Tor i wchodzi na stronę.
- Zalecana strategia i rozwiązanie: Korzyści: Tor kieruje ruch przez trzy węzły, maskując korporacyjny adres IP analityka. Ryzyko i jego ograniczanie: linki w dark webie nie podlegają żadnej weryfikacji reputacji. Analitycy muszą uruchamiać Tor w izolowanych maszynach wirtualnych (VM), wyłączyć JavaScript w ustawieniach Tor i unikać pobierania jakichkolwiek plików, aby chronić sieć korporacyjną.