Imię i nazwisko: _____ **Data:** _____ **Wynik:** _____

Bezpieczeństwo i szyfrowanie w publicznych sieciach Wi-Fi

Ataki typu man-in-the-middle, fałszywe punkty dostępowe, podsłuchiwanie pakietów, tunele VPN i szyfrowanie HTTPS.

PRZEGLĄD NAUKI: BEZPIECZEŃSTWO PUBLICZNYCH SIECI WI-FI

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 bezpieczeństwo publicznych sieci Wi-Fi. Poznasz nieszyfrowane sieci, ataki typu man-in-the-middle (MitM), nieautoryzowane punkty dostępu, podsłuchiwanie pakietów, tunele VPN i bezpieczeństwo transmisji HTTPS.

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/bezpieczenstwo-publicznego-wifi/

Twoja ścieżka nauki: bezpieczeństwo publicznych sieci Wi-Fi

- Rozpoznaj typowe zagrożenia w publicznych sieciach Wi-Fi, w tym podsłuchiwanie pakietów i fałszywe punkty dostępu.
- Wdróż szyfrowane tunele VPN, aby zabezpieczyć dane w tranzycie.
- Wymuszaj HTTPS i bezpieczne ustawienia przeglądarki dla pracowników zdalnych.

INSTRUKCJE DO PRZEWODNIKA O BEZPIECZEŃSTWIE PUBLICZNYCH SIECI WI-FI

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 bezpieczeństwa zdalnego dostępu. Zakończ zadaniem dodatkowym Myśl szybko.

BEZPIECZEŃSTWO PUBLICZNYCH SIECI WI-FI I OCHRONA TRANSMISJI (WPROWADZENIE)

Niezaszyfrowane publiczne hotspoty Wi-Fi narażają ruch sieciowy na podsłuchiwanie pakietów i podszywanie się typu Evil Twin. Kierowanie ruchu przez bezpieczne szyfrowane tunele VPN i egzekwowanie reguł HSTS tylko dla HTTPS chroni sesje przed przechwyceniem w sieci lokalnej.

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

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Czym jest atak typu Man-in-the-Middle (MitM)?

- A. Przechwytywanie i zmienianie komunikacji między dwiema stronami we wspólnej sieci
- B. Technika wydobywania danych z bazy, wymierzona w rekordy użytkowników
- C. Przeciążanie serwerów WWW żądaniami ruchu sieciowego
- D. Wymazywanie woluminów lokalnego dysku twardego

2. Czym jest nieautoryzowany punkt dostępu (Evil Twin)?

- A. Złośliwy hotspot Wi-Fi skonfigurowany z tym samym SSID co legalna sieć
- B. Narzędzie administracyjne służące do monitorowania kopii zapasowych baz danych
- C. Konfiguracja bezpiecznej bramy VPN
- D. Rekord DNS mapujący autoryzowane serwery pocztowe

3. W jaki sposób VPN chroni ruch w publicznych sieciach Wi-Fi?

- A. Opakowuje wszystkie pakiety sieciowe w zaszyfrowany tunel, przez co są nieczytelne dla snifferów
- B. Automatycznie blokuje wszystkie przychodzące żądania połączeń
- C. Zmienia adres MAC fizycznej karty sieciowej
- D. Usuwa zapisane pliki cookie w przeglądarce

4. Czym jest podsłuchiwanie pakietów (packet sniffing)?

- A. Używanie narzędzi sprzętowych lub programowych do przechwytywania i rejestrowania pakietów sieciowych
- B. Skanowanie lokalnych katalogów w poszukiwaniu zduplikowanych plików
- C. Ograniczanie uprawnień odczytu bazy danych na podstawie ról użytkowników
- D. Szyfrowanie dysków pamięci masowej za pomocą kluczy AES-256

5. Jaką rolę pełni HTTPS?

- A. Szyfrowanie ruchu sesji między przeglądarką a serwerem WWW
- B. Filtrowanie przychodzących wiadomości e-mail na bramie
- C. Kompresowanie obrazów w celu szybszego ładowania stron
- D. Zarządzanie strukturami plików w pamięci masowej podłączonej do sieci

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Połączeni użytkownicy mogą łatwo przechwytywać dane w postaci zwykłego tekstu w otwartych publicznych sieciach Wi-Fi.

- ◯ Prawda
- ◯ Fałsz

7 Pytanie 7

7. Nieautoryzowane punkty dostępu (Evil Twin) są zawsze autoryzowane przez administratorów sieci.

- ◯ Prawda
- ◯ Fałsz

8 Pytanie 8

8. VPN jest nieskuteczny w ochronie ruchu przed podsłuchiwaniem pakietów w sieciach publicznych.

- ◯ Prawda
- ◯ Fałsz

9 Pytanie 9

9. HTTPS szyfruje wyłącznie ścieżkę URL, pozostawiając ładunek pakietu w postaci jawnego tekstu.

- ◯ Prawda
- ◯ Fałsz

10 Pytanie 10

10. Hotspoty Wi-Fi z zabezpieczeniem WPA3 oferują silniejszą ochronę niż otwarte sieci bez hasła.

- ◯ Prawda
- ◯ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

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

1. Wykradanie prywatnych haseł w publicznych sieciach Wi-Fi to _____ komunikacji.
2. Analizowanie surowych pakietów w sieci lokalnej wykorzystuje _____ pakietów.
3. Fałszywy hotspot udający hotelową sieć Wi-Fi to tzw. _____ .
4. Zabezpieczenie przesyłanego ruchu WWW wymaga szyfrowania za pomocą _____ .
5. Szyfrowanie wszystkich danych wychodzących z sieci wykorzystuje klienta _____ .
6. Zaszyfrowana ścieżka komunikacji przez sieci publiczne to _____ .

BANK SŁÓW

HTTPS | PODSŁUCHIWANIE PAKIETÓW | PRZECHWYTYWANIE | TUNEL | VPN | WPA TRZY | ZAPORA SIECIOWA | ZŁY BLIŹNIAK

Wpisz tutaj swoje odpowiedzi:

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

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

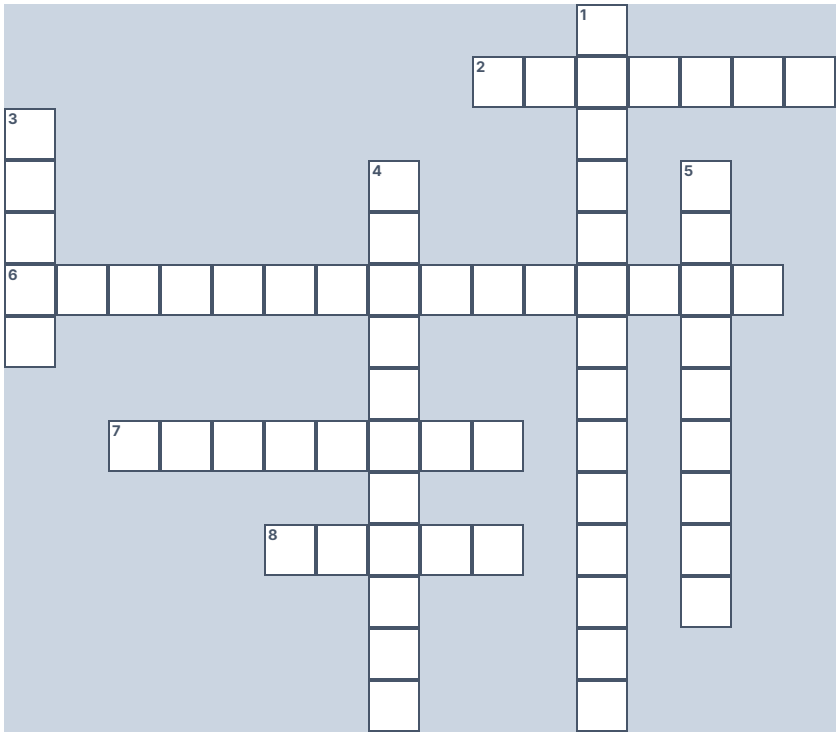
DOPASOWYWANIE DEFINICJI

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

☐	1. PRZECHWYTYWANIE	A	Nowoczesny standard zabezpieczeń Wi-Fi.
☐	2. PODSŁUCHIWANIE PAKIETÓW	B	Bezpieczna ścieżka danych podczas transmisji.
☐	3. EVIL TWIN	C	Filtrowanie ruchu przychodzącego.
☐	4. HTTPS	D	Fałszywy hotspot podszywający się pod Wi-Fi.
☐	5. VPN	E	Odczytywanie ruchu w tranzycie.
☐	6. TUNEL	F	Przechwytywanie pakietów danych sieciowych.
☐	7. WPA3	G	Zaszyfrowana wirtualna sieć prywatna.
☐	8. ZAPORA SIECIOWA	H	Bezpieczna transmisja internetowa.

Punkt kontrolny 5: Krzyżówka

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



POZIOMO

2. Nowoczesny standard bezpieczeństwa Wi-Fi. (7)

6. Odczytywanie ruchu w trakcie przesyłania. (15)

7. Przechwytywanie pakietów danych sieciowych. (8)

8. Bezpieczna ścieżka danych w tranzycie. (5)

PIONOWO

1. Filtrowanie ruchu przychodzącego. (14)

3. Bezpieczna transmisja WWW. (5)

4. Fałszywy hotspot udający sieć Wi-Fi. (11)

5. Szyfrowana wirtualna sieć prywatna. (9)

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: Nowoczesny standard bezpieczeństwa Wi-Fi. (7 liter):

6 poziomo: Odczytywanie ruchu w trakcie przesyłania. (15 liter):

7 poziomo: Przechwytywanie pakietów danych sieciowych. (8 liter):

8 poziomo: Bezpieczna ścieżka danych w tranzycie. (5 liter):

PIONOWO

1 pionowo: Filtrowanie ruchu przychodzącego. (14 liter):

3 pionowo: Bezpieczna transmisja WWW. (5 liter):

4 pionowo: Fałszywy hotspot udający sieć Wi-Fi. (11 liter):

5 pionowo: Szyfrowana wirtualna sieć prywatna. (9 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

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

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

LISTA SŁÓW

PRZECHWYTYWANIE SNIFFING ZŁYBLIŹNIAK HTTPS KLIENTVPN TUNEL WPATRZY ZAPORASIECIOWA

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. PRZECHWYTYWANIE**
- **B. SNIFFING**
- **C. ZŁYBLIŹNIAK**
- **D. HTTPS**
- **E. KLIENTVPN**
- **F. TUNEL**
- **G. WPATRZY**
- **H. ZAPORASIECIOWA**

DEFINICJE I POLA DOPASOWANIA

1. Nowoczesny standard bezpieczeństwa Wi-Fi. ____
2. Fałszywy hotspot udający sieć Wi-Fi. ____
3. Przechwytywanie pakietów danych sieciowych. ____
4. Bezpieczna ścieżka danych w tranzycie. ____
5. Filtrowanie ruchu przychodzącego. ____
6. Odczytywanie ruchu w trakcie przesyłania. ____
7. Szyfrowana wirtualna sieć prywatna. ____
8. Bezpieczna transmisja WWW. ____

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

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

1. HWYTWRYZA NPIEEC
2. LKŁZAIYINŹB
3. KTNLVNEPI
4. YPRTZWA
5. FINGFSNI
6. PHTST
7. ELTNU
8. OIOAECAAZS PWIR

Zadanie dodatkowe: Myśl szybko

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

1	Powody, dla których warto aktualizować oprogramowanie			
2	Urządzenia, które łączą się z Wi-Fi automatycznie			
3	Informacje, których nigdy nie powinieneś udostępniać			
4	Bezpieczne nawyki, które możesz zacząć już dziś			
5	Sposoby na bezpieczne korzystanie z internetu w kawiarni			
6	Urządzenia, które można zhakować			
7	Rzeczy, które haker może zobaczyć w otwartej sieci Wi-Fi			
8	Oznaki fałszywej sieci Wi-Fi			
9	Alternatywy dla publicznego Wi-Fi			
10	Sygnały ostrzegawcze w e-mailu			
11	Rzeczy, których nie robisz w publicznym Wi-Fi			
12	Miejsca z bezpłatnym Wi-Fi			
13	Sposoby na ochronę twoich kont			
14	Oznaki, że komputer jest zainfekowany			
15	Nazwy Wi-Fi, które wydają się podejrzane			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

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

STUDIUM PRZYPADKU 1: OGRANICZANIE PODSŁUCHU PAKIETÓW W PUBLICZNEJ SIECI WI-FI



Scenariusz: Zdalny przedstawiciel handlowy połączony z publiczną siecią Wi-Fi na lotnisku zauważa, że kilka wrażliwych e-maili biznesowych wyciekło wkrótce po wysłaniu ich w postaci jawnego tekstu.

Pytanie do dyskusji: Przeanalizuj ryzyka sieci publicznych i opisz rozwiązanie szyfrujące ruch.

STUDIUM PRZYPADKU 2: OBRONA PRZED FAŁSZYWYM HOTSPOTEM EVIL TWIN



Scenariusz: Atakujący uruchamiają nieuczciwy bezprzewodowy punkt dostępu o nazwie „CoffeeShop_Guest”, naśladujący prawdziwy hotspot kawiarni i przechwytujący ruch sieciowy od nieświadomych gości.

Pytanie do dyskusji: Opisz szczegółowo kroki weryfikacji służące do wykrywania i blokowania nieuczciwych punktów dostępu.

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

25	33	32	9	24	28	13		24	28	4	11													
22	28	3	15	12	4	33	18	7	13		25	12	7	4	12		30	12	9	12				
						33	1		22	20	17	20	4	2		29	22	18						

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: Dlaczego publiczne Wi-Fi jest niebezpieczne?

Otwarte publiczne Wi-Fi nie szyfruje ruchu w powietrzu, więc osoby w pobliżu mogą przechwycić wszelkie niezabezpieczone dane. [2]

Q2: Czym jest podsłuchiwanie pakietów (packet sniffing)?

Sniffer pakietów przechwytuje surowe dane przepływające przez interfejs sieciowy, ujawniając hasła w postaci zwykłego tekstu i szczegóły ruchu.

Q3: Czym jest Evil Twin?

Fałszywy punkt dostępu stworzony przez hakerów, który naśladuje nazwę i ustawienia zaufanego lokalnego hotspotu Wi-Fi.

Q4: Jak VPN mnie chroni?

Kieruje Twój ruch przez zaszyfrowany tunel, ukrywając Twoją aktywność przeglądania przed lokalnymi podsłuchiwaczami sieci.

Q5: Czy HTTPS chroni mnie w publicznych sieciach Wi-Fi?

Tak, szyfruje dane wymieniane między Twoją przeglądarką a stroną, a VPN dodaje kolejną warstwę ochrony.

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

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Czym jest WPA3?

Nowoczesny standard Wi-Fi Protected Access, oferujący silniejsze szyfrowanie i ochronę przed atakami słownikowymi offline. [1]

Q7: Czy publiczne Wi-Fi może dostarczać złośliwe oprogramowanie?

Tak, atakujący mogą przechwytywać ruch i wstrzykiwać do sesji przeglądarki złośliwe monity o pobranie plików (drive-by downloads).

Q8: Jakie ryzyko wiąże się z udostępnianiem plików?

Jeśli udostępnianie plików jest włączone, inni użytkownicy w sieci publicznej mogą odczytywać lub modyfikować Twój lokalny katalog folderów.

Q9: Czym jest portal przechwytujący (captive portal)?

Strona logowania, której sieci w hotelach lub kawiarniach używają do udzielania dostępu do internetu, a która czasem może zostać sfałszowana przez atakujących.

Q10: Czy powinienem wyłączać Wi-Fi, gdy z niego nie korzystam?

Tak, wyłączenie Wi-Fi uniemożliwia urządzeniu automatyczne łączenie się z niezaufanymi sieciami.

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 atak typu man-in-the-middle wykorzystuje DNS?

Przez użycie fałszowania DNS (DNS spoofing) na nieuczciwym routerze, aby kierować przeglądarki ofiar na łudząco podobne strony docelowe phishingu zamiast na docelowe domeny.

Q2: Czym jest przechwycenie sesji (session hijacking)?

Atakujący przechwytujący nieszyfrowany plik cookie sesji w publicznej sieci Wi-Fi i importujący go w celu ominięcia logowania poświadczeniami.

Q3: Czym jest SSL stripping?

Atak typu MitM, w którym atakujący obniża bezpieczne żądanie HTTPS użytkownika do niezaszyfrowanego HTTP i przechwytuje dane logowania w postaci zwykłego tekstu.

Q4: Jak HSTS chroni przed SSL stripping?

HTTP Strict Transport Security zmusza przeglądarki do łączenia się wyłącznie przez HTTPS i odmawia powrotu do nieszyfrowanego HTTP. [3]

Q5: Czym jest VPN z tunelowaniem dzielonym?

Konfiguracja kierująca przez VPN tylko ruch firmowy, a dane z publicznego internetu wysyłająca bezpośrednio, co może powodować ryzyko ujawnienia ścieżki wycieku.

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: Dlaczego WPA2 jest podatny na atak KRACK?

Atak Key Reinstallation wykorzystuje czteroetapowy uzgadniacz (handshake) WPA2 do odszyfrowywania pakietów bez hasła do Wi-Fi.

Q7: Czym jest izolacja klientów (client isolation)?

Ustawienie bezpieczeństwa routera uniemożliwiające połączonym urządzeniom Wi-Fi bezpośrednią komunikację ze sobą, co blokuje lokalne podsłuchiwanie.

Q8: Jak atakujący wykorzystują fałszywe serwery DNS?

Konfigurują fałszywe routery, które przypisują klientom fałszywe serwery DNS, co pozwala im przechwytywać i przepisywać wszystkie wyszukiwania w sieci.

Q9: Czy VPN może ukryć mój lokalny adres MAC?

Nie. Adresy MAC to lokalne identyfikatory warstwy 2; zamiast tego użyj wbudowanego w urządzeniu ustawienia randomizacji MAC (adres prywatny).

Q10: Czym jest atak podszywania się pod portal przechwytujący?

Atakujący hostujący fałszywy portal uwierzytelniania na fałszywym hotspocie, aby ukraść dane logowania pod pretekstem darmowego dostępu do Wi-Fi.

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

Pracownicy zdalni często korzystają z Wi-Fi w kawiarniach, hotelach i na lotniskach, gdzie nie mają kontroli nad bezpieczeństwem sieci.

2. WGLĄD W BEZPIECZEŃSTWO

Fałszywy hotspot typu Evil Twin może skopiować dokładną nazwę i adres MAC zaufanej sieci, wprowadzając urządzenia w błąd.

3. WGLĄD W BEZPIECZEŃSTWO

Oprogramowanie do podsłuchiwania pakietów, takie jak Wireshark, jest bezpłatne i może wyświetlać nieszyfrowane hasła HTTP jawnym tekstem.

4. WGLĄD W BEZPIECZEŃSTWO

Zabezpieczenia WPA3 wykorzystują równoczesne uwierzytelnianie równych sobie (SAE), aby chronić przed lokalnymi atakami typu brute force.

5. WGLĄD W BEZPIECZEŃSTWO

Ataki SSL stripping omijają podstawowe zabezpieczenia HTTPS, przechwytując początkowe przekierowania HTTP na bramie.

6. WGLĄD W BEZPIECZEŃSTWO

Nagłówki odpowiedzi HTTP Strict Transport Security (HSTS) powstrzymują przeglądarki przed powrotem do nieszyfrowanych połączeń HTTP. [3]

7. WGLĄD W BEZPIECZEŃSTWO

Wyłączenie opcji „Auto-Connect" zapobiega łączeniu się smartfonów z podobnie wyglądającymi fałszywymi sieciami w przestrzeniach publicznych.

8. WGLĄD W BEZPIECZEŃSTWO

Firmowe konfiguracje VPN typu „always-on" wymuszają kierowanie całego ruchu sieciowego pracowników zdalnych przez firmowe zapory sieciowe.

9. WGLĄD W BEZPIECZEŃSTWO

Nieautoryzowane punkty dostępu mogą podawać sfałszowane odpowiedzi DNS, przekierowując docelowe domeny na serwery phishingowe.

10. WGLĄD W BEZPIECZEŃSTWO

Bez VPN inni użytkownicy otwartego hotspotu mogą zobaczyć, z jakimi witrynami i serwerami łączy się twoje urządzenie.

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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest atak typu Man-in-the-Middle (MitM)? → Przechwytywanie i zmienianie komunikacji między dwiema stronami we wspólnej sieci

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest nieautoryzowany punkt dostępu (Evil Twin)? → Złośliwy hotspot Wi-Fi skonfigurowany z tym samym SSID co legalna sieć

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

W jaki sposób VPN chroni ruch w publicznych sieciach Wi-Fi? → Opakowuje wszystkie pakiety sieciowe w zaszyfrowany tunel, przez co są nieczytelne dla snifferów

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest podsłuchiwanie pakietów (packet sniffing)? → Używanie narzędzi sprzętowych lub programowych do przechwytywania i rejestrowania pakietów sieciowych

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaką rolę pełni HTTPS? → Szyfrowanie ruchu sesji między przeglądarką a serwerem WWW

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 Pytanie 6

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Połączeni użytkownicy mogą łatwo przechwytywać dane w postaci zwykłego tekstu w otwartych publicznych sieciach Wi-Fi.

7 Pytanie 7

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: Evil Twin to nieautoryzowany hotspot utworzony przez atakującego, aby naśladować prawdziwy.

8 Pytanie 8

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: VPN szyfruje ruch w tunelu, więc lokalne sniffery nie mogą go odczytać.

9 Pytanie 9

Poprawna odpowiedź: Fałsz

UWAGA DLA NAUCZYCIELA

Fałsz: HTTPS szyfruje całą wymianę HTTP, w tym ścieżkę adresu URL i treść strony.

10 Pytanie 10

Poprawna odpowiedź: Prawda

UWAGA DLA NAUCZYCIELA

Hotspoty Wi-Fi z zabezpieczeniem WPA3 oferują silniejszą ochronę niż otwarte sieci bez hasła.

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

E 1. PRZECHWYTYWANIE	F 2. PODSŁUCHIWANIE PAKIETÓW	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNEL	A 7. WPA3	C 8. ZAPORA SIECIOWA

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 PRZECHWYTYWANIE	2 PODSŁUCHIWANIE PAKIETÓW	3 ZŁY BLIŹNIAK	4 HTTPS
5 VPN	6 TUNEL		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 G – WPATRZY	2 C – ZŁYBLIŹNIAK	3 B – SNIFFING	4 F – TUNEL
5 H – ZAPORASIECIOWA	6 A – PRZECHWYTYWANIE	7 E – KLIENTVPN	8 D – HTTPS

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia PRZECHWYTYWANIE, PODSŁUCHIWANIE PAKIETÓW i EVIL TWIN oraz podać przykład każdego z nich.

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

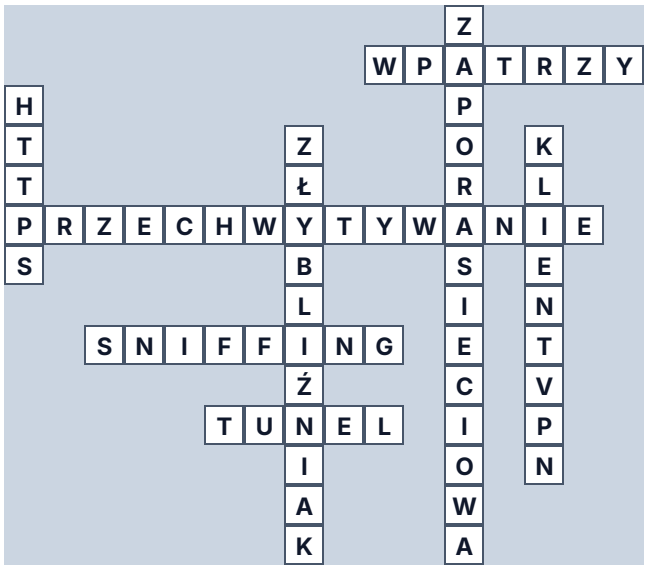
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

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

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: WPATRZY Nowoczesny standard bezpieczeństwa Wi-Fi. (7 liter)

6 poziomo: PRZECHWYTYWANIE Odczytywanie ruchu w trakcie przesyłania. (15 liter)

7 poziomo: SNIFFING Przechwytywanie pakietów danych sieciowych. (8 liter)

8 poziomo: TUNEL Bezpieczna ścieżka danych w tranzycie. (5 liter)

PIONOWO

1 pionowo: ZAPORASIECIOWA Filtrowanie ruchu przychodzącego. (14 liter)

3 pionowo: HTTPS Bezpieczna transmisja WWW. (5 liter)

4 pionowo: ZŁYBLIŹNIAK Fałszywy hotspot udający sieć Wi-Fi. (11 liter)

5 pionowo: KLIENTVPN Szyfrowana wirtualna sieć prywatna. (9 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

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

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. HWYTWRYZANPIEEC **PRZECHWYTYWANIE**
2. LKŁZAIYINŹB **ZŁYBLIŹNIAK**
3. KTNLVNEPI **KLIENTVPN**
4. YPRTZWA **WPATRZY**
5. FINGFSNI **SNIFFING**
6. PHTST **HTTPS**
7. ELTNU **TUNEL**
8. OIOAECAAZSPWIR **ZAPORASIECIOWA**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"SZYFRUJ RUCH PUBLICZNEJ SIECI WIFI ZA POMOCĄ VPN"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Ograniczanie podsłuchu pakietów w publicznej sieci Wi-Fi

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Zdalny dyrektor sprzedaży połączony z publiczną siecią Wi-Fi na lotnisku zauważa, że kilka wrażliwych e-maili biznesowych wyciekło wkrótce po wysłaniu ich jawnym tekstem.
- Zalecana strategia i rozwiązanie: Nakaż używanie firmowego klienta VPN na wszystkich zdalnych stacjach roboczych. Wymuś rozszerzenia przeglądarki działające wyłącznie przez HTTPS i blokuj niezaszyfrowane protokoły (takie jak HTTP i FTP) na zaporze sieciowej klienta.

B Studium przypadku 2: Obrona przed fałszywym hotspotem Evil Twin

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Atakujący uruchamiają fałszywy punkt dostępu bezprzewodowego o nazwie „CoffeeShop_Guest", naśladujący prawdziwy hotspot kawiarni, i przechwytują ruch sieciowy nieświadomych gości.
- Zalecana strategia i rozwiązanie: Przeprowadź audyt adresów MAC BSSID punktów dostępowych, aby zweryfikować autentyczność sieci. Wymuś walidację stanu klienta, aby blokować połączenia z otwartymi sieciami, i nakaż używanie hotspotów komórkowych do pracy z danymi wrażliwymi.