Projekt nauka języka

# Koncepcje – rzeczy, które należy po prostu zrozumieć.

Kultura obcego kraju; Sposób mówienia; ich żarty; Akcent; Wymowa; Najlepsze źródła nauki; Sposoby na szukanie rozmów z obcokrajowcami; Etymologia słów; Pochodzenie reguł gramatycznych; Zastosowanie czasów.

# Fakty – rzeczy, które należy zapamiętać.

Słówka; Gramatyka; Czasy.

# Procedury – rzeczy, które należy zastosować.

Umiejętność czytania książek w obcym języku, technicznych, powieści; Sprawne czytanie artykułów z gazet; Rozumienie mowy – audycji radiowych, podcastów, wiadomości; Umiejętność rozmowy z obcokrajowcem.

# Pomysły – rzeczy, które należy zrobić.

Rozmowy z ChatGPT po angielsku; Rozmowy z bliskimi osobami po angielsku, wspólna nauka języka; Czytanie i tłumaczenie artykułów w Internecie; Czytanie darmowych książek technicznych z Interentu; Sporządzanie listy słów i powtarzanie jej; Korzystania z Anki do nauki słówek.

Projekt nauka cyberbezpieczeństwa

# Koncepcje – rzeczy, które należy po prostu zrozumieć.

Trendy w cyberbezpieczeństwie; Metody hakowania; Potrzeby rynku; Co jest bardziej pożądane – studia, czy certyfikaty?; Programowanie w Pythonie; Sieci komputerowe, Systemy Operacyjne.

# Fakty – rzeczy, które należy zapamiętać.

Słowa powiązane z cyberbezpieczeństwem, terminy; Witryny odwołujące się do cyberbezpieczeństwa – ich nazwy; Nazwy programów komputerowych związanych z cyberbezpieczeństwem; Komendy w Bash i Powershell.

# Procedury – rzeczy, które należy zastosować.

Pisanie artykułów blogowych o cyberbezpieczeństwie; Sposoby hakowania systemów; Dokumentowanie efektów pracy.

# Pomysły – rzeczy, które należy zrobić.

Stworzenie strony Internetowej na domowym serwerze z artykułami i oprogramowaniem napisanym na stronie; Tłumaczyć artykuły; Zdobywać certyfikaty z Cisco; Próbować różnych możliwości uzyskania nieautoryzowanego dostępu do systemów.

Projekt nauka języka

# Koncepcje – rzeczy, które należy zrozumieć

* **Dialekty i regionalizmy**: Zrozumienie różnic między standardowym językiem a jego regionalnymi odmianami.
* **Różnice kulturowe**: Jak różnice kulturowe wpływają na komunikację (np. gesty, idiomy).
* **Strategie nauki języka**: Metody takie jak immersja językowa, metoda SRS (spaced repetition system), shadowing.
* **Filozofia języka**: Jak język wpływa na sposób myślenia i postrzegania świata.

# Fakty – rzeczy, które należy zapamiętać

* **Kolokacje**: Często używane frazy (np. „make a decision” zamiast „do a decision” w angielskim).
* **Idiomy i wyrażenia**: Popularne zwroty w danym języku.
* **Lista najczęściej używanych słów**: Słownictwo podzielone na tematyczne kategorie (np. jedzenie, podróże, technologia).

# Procedury – rzeczy, które należy zastosować

* **Tworzenie własnych zdań**: Regularne budowanie zdań z nowo poznanych słów.
* **Prowadzenie dziennika w języku obcym**: Codzienne notowanie myśli lub planów.
* **Oglądanie filmów/seriali z napisami**: Najpierw z napisami w języku ojczystym, potem w języku obcym, aż w końcu bez napisów.

# Pomysły – rzeczy, które należy zrobić

* **Tworzenie podcastów w języku obcym**: Własne nagrania na różne tematy.
* **Grupy językowe online**: Dołączanie do społeczności na Discordzie, Reddit lub Meetup.
* **Oglądanie streamów na żywo**: Angażowanie się w rozmowy na czacie.

Projekt nauka cyberbezpieczeństwa

# Koncepcje – rzeczy, które należy zrozumieć

* **Podstawy kryptografii**: Jak działa szyfrowanie, klucze publiczne/prywatne, protokoły.
* **Zasady bezpieczeństwa danych**: Jak działają firewalle, VPN, IDS/IPS.
* **Analiza ryzyka**: Ocena podatności systemów i ocena wpływu ewentualnych zagrożeń.
* **Model OSI**: Jak dane przepływają przez sieć na różnych warstwach.

# Fakty – rzeczy, które należy zapamiętać

* **Podstawowe luki w zabezpieczeniach**: Typy ataków (SQL Injection, XSS, CSRF, brute force).
* **Narzędzia używane w branży**: Nmap, Wireshark, Burp Suite, Metasploit.
* **Protokoły sieciowe**: TCP/IP, DNS, DHCP, HTTP/HTTPS.
* **Standardy bezpieczeństwa**: NIST, ISO/IEC 27001.

# Procedury – rzeczy, które należy zastosować

* **Symulowanie ataków w bezpiecznym środowisku**: Testowanie luk w lokalnych maszynach wirtualnych.
* **Konfiguracja narzędzi**: Ustawianie środowisk takich jak Kali Linux, Burp Suite czy OpenVAS.
* **Analiza logów**: Monitorowanie i interpretowanie logów z systemów takich jak SIEM.
* **Przygotowanie raportów**: Pisanie sprawozdań z przeprowadzonych testów bezpieczeństwa.

# Pomysły – rzeczy, które należy zrobić

* **Budowa domowego labu**: Symulowanie środowisk sieciowych i systemów do testów penetracyjnych.
* **Certyfikaty branżowe**: Oprócz Cisco, warto zdobyć CompTIA Security+, CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional).
* **Pisanie skryptów w Pythonie**: Automatyzacja powtarzalnych zadań, takich jak skanowanie portów.