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.
