Centrum Edukacji

ul. 1 Maja 12, 41-800 Zabrze

Narzędzia i oprogramowanie

w kształceniu w zawodzie

TECHNIK CYBERBEZPIECZEŃSTWA

Kształcenie w zawodzie Technik Cyberbezpieczeństwa realizowane jest w oparciu o aktualną podstawę programową Ministerstwa Edukacji (kwalifikacje INF.11 i INF.12). Uczeń pracuje na profesjonalnych narzędziach wykorzystywanych w branży IT, obejmujących zarówno systemy obronne, jak i ofensywne testy bezpieczeństwa.

Poniższe zestawienie przedstawia główne kategorie oprogramowania i narzędzi, na których uczeń zdobywa praktyczne umiejętności zawodowe.

Obszar kształcenia	Narzędzia i oprogramowanie
Programowanie	Python (z bibliotekami Pandas, NumPy, Requests, Scapy), Java lub C#, zintegrowane środowiska programistyczne (IDE), system kontroli wersji Git, narzędzia AI wspierające generowanie i weryfikację kodu
Systemy operacyjne	Microsoft Windows oraz dystrybucje Linux — administracja, utwardzanie, konfiguracja zabezpieczeń (AppLocker, SELinux, AppArmor, PAM, Windows Defender Credential Guard), zapory iptables/nftables, PowerShell, Bash
Wirtualizacja i kontenery	Oprogramowanie do wirtualizacji systemów operacyjnych, środowisko Docker do konteneryzacji i izolacji aplikacji
Bazy danych	PostgreSQL (relacyjna baza danych), MongoDB (baza nierelacyjna typu dokumentowego), narzędzia do wersjonowania schematów baz danych, systemy zarządzania sekretami
Sieci komputerowe	Wireshark (analiza ruchu sieciowego), narzędzia diagnostyczne (ping, traceroute, netstat, netcat, ss), oprogramowanie do projektowania i symulacji sieci, OpenVPN, WireGuard, IPsec
Skanowanie podatności i monitoring	nmap, OpenVAS (skanery podatności), systemy IDS/IPS, oprogramowanie SIEM do korelacji i analizy zdarzeń bezpieczeństwa, sprzętowa zapora sieciowa
Kryptografia	Narzędzia do generowania kluczy i certyfikatów (RSA, ECC), oprogramowanie do szyfrowania plików i wolumenów, klucze sprzętowe U2F, aplikacje TOTP (np. Google Authenticator)
Technologie webowe	HTML5, CSS3, JavaScript, jQuery, Fetch API, serwery WWW i reverse proxy z modułem WAF (Web Application Firewall), Swagger do dokumentacji API
Testy penetracyjne	Intercepting proxy do analizy ruchu HTTP/HTTPS, skanery podatności aplikacji webowych, narzędzia statycznej i dynamicznej analizy kodu (SAST/DAST), mitmproxy do symulacji ataków Man-in-the-Middle
Chmura obliczeniowa	Platforma chmurowa (publiczna lub hybrydowa) w modelach IaaS i PaaS — wirtualne sieci prywatne (VPC/VNet), grupy

	bezpieczeństwa, magazyny kluczy, chmurowe systemy logowania zdarzeń
Platformy edukacyjne	Platformy Capture The Flag (CTF), aplikacja treningowa WebGoat z celowo wbudowanymi podatnościami
Narzędzia biurowe i pomocnicze	Pakiet programów biurowych, oprogramowanie do tworzenia diagramów (m.in. ER, sieciowych, architektury bezpieczeństwa), narzędzia AI do raportowania i analizy

Dodatkowe informacje

Zajęcia odbywają się w pracowniach komputerowych wyposażonych w indywidualne stanowiska dla każdego ucznia z dostępem do internetu, sieci lokalnej oraz platformy chmurowej. Uczniowie pracują w środowiskach testowych i izolowanych laboratoriach, co umożliwia bezpieczne ćwiczenie technik ataków i obrony.

Praktyki zawodowe (8 tygodni, 280 godzin) realizowane są w przedsiębiorstwach IT, centrach danych, jednostkach samorządu terytorialnego oraz u operatorów infrastruktury krytycznej.