

Pakiet szkoleń (online)

1. Administrowanie systemem Windows Server (minimalne wymagania szkolenia)

- Korzystanie z technik i narzędzi administracyjnych w systemie Windows Server,
- Wdrażanie usługi zarządzania tożsamością,
- Zarządzanie usługami infrastruktury sieciowej,
- Konfigurowanie serwerów plików i pamięci masowej,
- Zarządzanie maszynami wirtualnymi z wykorzystaniem wirtualizacji Hyper-V i kontenerów,
- Wdrażanie rozwiązań wysokiej dostępności i odzyskiwania danych po awarii,
- Stosowanie zabezpieczenia w celu ochrony kluczowych zasobów,
- Konfigurowanie usługi zdalnego pulpitu,
- Konfigurowanie wdrożenia infrastruktury pulpitów opartej na maszynach wirtualnych,
- Wdrażanie dostępu zdalnego i usług internetowych,
- Wdrażanie monitorowania usług i wydajności oraz rozwiązywanie problemów,
- Wykonywanie aktualizacji i migracji związanych z AD DS oraz pamięcią masową.
- certyfikat ukończenia szkolenia Microsoft
- czas trwania - co najmniej 40 h

2. Certified Stormshield Network Administrator Server (minimalne wymagania szkolenia)

- sprawnie zarządzał urządzeniami Stormshield i wiedział jak one działają,
- potrafił wdrożyć urządzenie Stormshield w sieci firmowej,
- definiował polityki filtrowania (Firewall i NAT) oraz trasy routingu,
- kontrolował dostęp do stron internetowych (http i https),
- konfigurował polityki bezpieczeństwa dla uwierzytelnionych użytkowników,
- potrafił wdrożyć różne typy wirtualnych sieci prywatnych (VPN) - IPSec VPN i SSL VPN.
- autoryzowany egzamin Certified Stormshield Network Administrator
- dostęp do maszyn wirtualnych Stormshield
- czas trwania - co najmniej 40 h

3. Certified Ethical Hacker v12 Server (minimalne wymagania szkolenia)

- dostęp do platformy szkoleniowej oraz materiałów szkoleniowych,
- dostęp do wirtualnych labów pozwalających na poznanie praktycznej strony hackingu przez co najmniej 6 miesięcy,
- zaświadczenie ukończenia szkolenia oraz voucher na egzamin,\

- czas trwania - co najmniej 40 h
- kurs Certified Ethical Hacker jest częścią ścieżki certyfikacyjnej EC-Council.

4. Techniki hackingu i cyberprzestępczości – Praktyczne wprowadzenie (minimalne wymagania szkolenia) – poziom 1

- praktyczna wiedza z zakresu bezpieczeństwa systemów operacyjnych oraz sieci informatycznych
- poznanie nowoczesnych technik internetowych włamywaczy
- umiejętność dobierania właściwych metod ochrony przed konkretnymi cyberatakami
- czas trwania - co najmniej 21 h
- minimalne zagadnienia szkolenia:
 - Fingerprinting - informacje uzyskiwane z sieci Internet
 - Google Hacking
 - Skanowanie urządzeń w sieci
 - Ataki na systemy operacyjne
 - Ataki na bazy danych
 - Ataki na przeglądarki internetowe
 - Ataki na formaty plików
 - Fałszowanie śladów w zaatakowanym systemie
 - Port knocking
 - Podśluchiwanie transmisji nieszyfrowanych - ruch http
 - Podśluchiwanie transmisji szyfrowanych - ruch HTTPS
 - ARP Spoofing
 - DNS Spoof
 - Budowa serwera TOR
 - Ataki na sieci bezprzewodowe
 - Ataki na WPS
 - Ataki na WEP
 - Ataki na WPA/WPA2
 - Ataki z użyciem tęczy tablic
 - Ataki z użyciem akceleracji graficznej

5. Techniki hackingu i cyberprzestępczości - Ataki na systemy i sieci (minimalne wymagania szkolenia) – poziom 2

- praktyczna wiedza z zakresu bezpieczeństwa systemów operacyjnych oraz sieci informatycznych
- poznanie nowoczesnych technik internetowych włamywaczy
- umiejętność dobierania właściwych metod ochrony przed konkretnymi cyberatakami,
- czas trwania - co najmniej 21 h
- minimalne zagadnienia szkolenia:
 - WHOIS i wyliczanie DNS
 - Wehikuł czasu stron internetowych
 - Budowa własnych pakietów od podstaw

- Zaawansowane skanowanie jednostek w warstwie 2, 3 i 4 z wykorzystaniem szerokiej gamy dostępnych narzędzi
- Identyfikowanie usług sieciowych oraz banerów aplikacji
- Identyfikacja systemów oraz zapór sieciowych
- Skanowanie TCP / UDP / zombie
- Ataki na systemy operacyjne Windows, Linux
- Atakowanie poprzez błędy w oprogramowaniu
- Szybka identyfikacja możliwych ataków na systemy Windows
- Szybka identyfikacja możliwych ataków na systemy Linux
- Automatyzacja ataków
- Ataki słownikowe
- Tworzenie słowników indywidualnych
- Pomijanie haseł w systemach operacyjnych
- Hakowanie kiosków internetowych
- Ataki socjotechniczne
- Hakowanie systemów operacyjnych z wykorzystaniem skryptów PowerShell