EITC/IS/ACNS

Zaawansowane bezpieczeństwo sieci informatycznych

Szczegółowa zawartość programowa kursu (15 godz.):

- Podstawowe problemy bezpieczeństwa sieci komputerowych
    - Warstwa sieciowa
    - Warstwa transportowa
    - Warstwa aplikacyjna
    - Typowe ataki na infrastrukturę sieciową
    - Ataki Denial of Service (DoS)
        - Przegląd ataków DoS
        - Metody obrony przed atakami DoS/DDoS
    - Mechanizmy bezpieczeństwa zdalnego dostępu
    - Narzędzia bezpieczeństwa
- Tunele wirtualne VPN
    - Konfiguracje sieci VPN
    - Protokół IPsec
        - Tryby pracy protokołów IPsec
        - Protokół AH (Authentication Header)
        - Protokół ESP (Encapsulating Security Payload)
        - Asocjacja bezpieczeństwa (Security Association)
        - Zarządzanie kluczami
        - Ograniczenia
        - IPsec w Windows
        - Bezpieczeństwo w IPv6
    - Propagowanie połączeń aplikacyjnych (port forwarding)
    - Tunele SSL
- Zapory sieciowe i translacja adresów
    - Podstawowe funkcje systemów firewall
    - Podstawowe komponenty systemów firewall
        - Router filtrujący
        - Komputer Twierdza
        - Strefa Zdemilitaryzowana
    - Translacja adresów – Network Address Translation (NAT)
    - Dodatkowa funkcjonalność zapór sieciowych
    - Problemy realizacji zapór sieciowych
- Metody atakowania aplikacji WWW i mechanizmy ich ochrony
    - Kradzież kodu źródłowego
    - Pola ukryte HTML
    - Zmienne Cookies
    - Path Traversal
    - SQL Injection
    - Przejęcie sesji
    - Denial of Service (DoS)
    - Podsumowanie
- Systemy programowych zapór sieciowych i systemy wykrywania włamań IDS
    - Programowe zapory sieciowe
    - Zapora sieciowa netfilter/iptables
        - Konfiguracja iptables
        - Translacja adresów
        - Moduły rozszerzające IPTABLES
        - Krótkie opisy celów (TARGETs)

        - Informacje dodatkowe
        - Przykłady
    - Wbudowana zapora osobista w systemach Windows
    - Systemy wykrywania włamań
    - System Snort
- Bezpieczna konfiguracja serwera HTTP na przykładzie Apache
    - Serwer Apache
    - Dziennik serwera Apache
    - Ścieżki logiczne i fizyczne
    - Dyrektywy blokowe
    - Ochrona dostępu wg adresów
    - Ochrona dostępu poprzez uwierzytelnianie użytkowników
    - Połączenia HTTPS
    - Podsumowanie
- Tworzenie sieci VPN w środowisku Linux i Windows
    - Zastosowania technologii VPN
    - Oprogramowanie OpenVPN
        - Podstawy działania
        - Połączenie VPN Linux - Linux z wykorzystaniem mechanizmu współdzielonego klucza
        - Połączenie VPN Linux - Linux z wykorzystaniem mechanizmu certyfikatów cyfrowych
        - Połączenie VPN Linux - Windows z wykorzystaniem mechanizmu współdzielonego klucza
        - Podsumowanie możliwości programu OpenVPN
    - Oprogramowanie Openswan
        - Protokół IPsec
        - Budowanie sieci VPN z użyciem oprogramowania Openswan
- Spoofing
    - Rodzaje spoofingu
        - IP spoofing (Internet Protocol spoofing)
        - Web spoofing
        - E-mail spoofing
        - DNS spoofing
        - Caller ID spoofing
        - SMS spoofing
    - IP spoofing – podstawy teoretyczne