Analiza Ruchu Sieciowego

Zakres tematyczny

Dzień 1.

1. Podstawy funkcjonowania sieci (protokoły sieciowe, mechanizmy sieciowe, zasady adresacji)

- Model OSI/ISO i TCP/IP,
- Protokoły warstwy II modelu OSI - ARP
- Protokoły routingu w sieci (RIP, OSPF, BGP, E/IGRP)
- Adresacja IP v4 i IP v6 (klasy adresacji, maski)
- Wykład teoretyczny - 2 godziny
- Ćwiczenia, warsztaty - laboratorium - 2 godziny

2. Konfiguracja urządzeń sieciowych pod kątem monitorowania i analizy ruchu sieciowego

- Konfiguracja karty sieciowej do analizy ruchu w sieci
- Konfiguracja przełącznika do analizy ruchu w sieci
- Omówienie działania aplikacji webowych i ich architektury
- Wykład teoretyczny - 1,5 godziny
- Ćwiczenia, warsztaty - laboratorium - 2,5 godziny

Dzień 2.

3. Bezpieczeństwo w sieci, luki w zabezpieczeniach sieci, ataki na sieć

- Aspekty prawne

Imperium Szkoleniowe
Tel. 22 402 15 04, Fax: 22 258 23 62
biuro@imperiumszkoleniowe.pl

- Ataki na infrastrukturę sieciową i aplikacje webowe: • Wstęp teoretyczny do anatomii ataku – krok po kroku w formie prezentacji • Omówienie teoretyczne podstawowych ataków na aplikacje webowe i systemy operacyjne
- Ataki w praktyce.
- Wykład teoretyczny - 4 godziny
- Ćwiczenia, warsztaty - laboratorium - 4 godziny

Dzień 3.

4. Zagadnienia kontroli ruchu sieciowego, narzędzia w analizie ruchu sieciowego (Linux, Windows)

- Budowa systemu operacyjnego (pod kątem obsługi połączeń sieciowych)
- Narzędzia do analizy ruchu sieciowego

  o Linux

  o Windows

- Wykład teoretyczny - 1 godzina
- Ćwiczenia, warsztaty - laboratorium - 3 godziny

5. Pakiety sieciowe i ich przechwytywanie

- Szczegółowe omówienie ramki IP v.4
- Szczegółowe omówienie ramki TCP i UDP
- Przechwytywanie pakietów http i https, SMB
- Wykład teoretyczny - 2 godziny
- Ćwiczenia, warsztaty - laboratorium - 2 godziny

Dzień 4.

6. Ekstrakcja plików z sieciowych pakietów (pobranie danych z sieci), pliki proxy cache

- Metody ekstrakcji
- Narzędzia do ekstrakcji

- Pliki proxy cache
- Wykład teoretyczny - 1 godzina
- Ćwiczenia, warsztaty - laboratorium - 3 godziny

7. Logi systemowe

- Analiza logów systemowych i logów serwera aplikacyjnego Apache/Nginx z wykorzystanie narzędzia GoAccess, do wyciągnięcia statystyk oraz detalicznych danych.
- Wykład teoretyczny - 1 godzina
- Ćwiczenia, warsztaty - laboratorium - 3 godziny

Dzień 5.

8. Praca z Wireshark.

- Wprowadzenie do działania protokołów sieciowych w formie warsztatów (analiza plików pcap nagranego ruchu na WireShark i tcpdump)
- Preamble: wprowadzenie do narzędzia Wireshark
- Analiza pakietów dla różnych protokołów sieciowych

  o Basic: TCP, UDP, FTP, http, HTTPS, SMB

  o Średniozaawansowane: USB raw, USB with Linux encryption, IPSec.

  o Zaawansowane: Wirusy – slammer, dns remote shell. Crack Traces – teardrop, etc.

- Wykład teoretyczny - 2 godziny
- Ćwiczenia, warsztaty - laboratorium - 6 godzin
- Szkolenie obejmuje 14,5 godzin wykładów teoretycznych oraz 25,5 godzin praktyki (ćwiczenia, warsztaty - laby), łącznie 40 godzin dydaktycznych.

Imperium Szkoleniowe
Tel. 22 402 15 04, Fax: 22 258 23 62
biuro@imperiumszkoleniowe.pl