# Skanowanie i audyt sieci – Kraków, 01-02.10.2009r.

## Program szkolenia

**Dzień 1 (11:00 - 18:00)**

10:15-10:45 -- Rejestracja
10:45-11:00 -- Powitanie. Przestawienie prelegenta oraz tematyki szkolenia
11:00-11:45 -- Przegląd zasadniczych zagadnień związanych z protokołem IP (TCP/IP)
- Skrótowy przegląd po nagłówkach wybranych typów pakietów
- Nawiązanie połączenia TCP/IP
- Opcje IP, Flagi TCP
- Cechy charakterystyczne UDP - w kontekście skanowania sieci
- Gromadzenie oraz analiza ruchu sieciowego (tcpdump / wireshark)

11:45 - 12:00 -- Przerwa
12:00 - 13:00 -- Nmap - ogólne informacje
- Metody wykrywania aktywnych urządzeń sieciowych oferowane przez nmap
- Najważniejsze typy skanowania portów oferowane przez nmap
- Detekcja usług / oprogramowania systemowego na skanowanej maszynie

13:00 - 14:00 -- Obiad
14:15 - 15:45 -- Elementy zaawansowanej analizy / skanowania usług sieciowych
- Przykłady szczegółowej analizy usług (na przykładzie SSL / IPsec / http load balancer)
- Omijanie systemów klasy firewall / IDS. (m.in. tematyka związana z: SSRR / LSRR / IP ID / fragmentacji IP / TTL / Wabiki / IP Options)

15:45 - 16:00 -- Przerwa
16:00 - 17:15 -- Nmap - pozostałe informacje
- Przykłady skanowania realnych sieci
- Przykłady lokalizacji usług
- Przykłady lokalizacji wewnętrznych warstw sieciowych
- Przykłady lokalizacji wewnętrznej adresacji IP
- Skryptowanie nmap (Nmap Scripting Engine) – omówienie przykładowego skryptu
- Wybrane metody ochrony przed skanowaniem via nmap

17:15-18:00 -- Konsultacje z prelegentem
18:30 -- Kolacja

**Dzień 2 (9:00 - 16:15)**

8:15 - 8:45 -- Śniadanie
8:45 - 9:00 -- Poranna kawa
9:00 - 10:30 -- Nmap - nietypowe użycie mechanizmów klasy "traceroute"
- Opcje IP: record route, time stamp
- Tryb traceroute nmap
- Alternatywa: paris-traceroute
- Alternatywa: hping
- Ndiff
- Zenmap

10:30 - 10:45 -- Przerwa
10:45 - 11:45 -- hping2 - Generowanie typowych / nietypowych pakietów
- Pakiety TCP / UDP / ICMP
- Generowanie dowolnych pakietów IP (przykład: IGMP)

- Generowanie dowolnych pakietów z wykorzystaniem APD

12:00 - 13:00 -- Obiad
13:15 - 14:30 -- Metody zewnętrznego mapowania sieci
- Wykorzystanie pola TTL w różnym typie pakietów (ICMP, TCP, UDP); przykład: selektywna analiza TTL do mapowania mechanizmu przekierowania portów
- Czasowa detekcja systemów firewall
- Nietypowe użycie mechanizmu klasy traceroute
- Selektywne odpytywanie portów
- Skanowanie portów

14:30 - 14:45 -- Przerwa
14:45 - 15:15 -- Alternatywne narzędzia
- Netcat
- Socat
- Wykorzystywanie sieci anonimizacyjnych do ukrywania ruchu
- Wykorzystanie proxifier / analogicznych narzędzi

15:15 - 15:30 -- Zakończenie szkolenia
15:30 - 16:15 -- Konsultacje z prelegentem

## Grupa docelowa

Szkolenie przeznaczone jest dla:

- Pracowników departamentów bezpieczeństwa firm
- Administratorów sieci
- Osób odpowiedzialnych za audyt zewnętrzny/wewnętrzny organizacji
- Osób związanych z branżą informatyki śledczej (computer forensic)
- Pracowników działów IT zainteresowanych tematyką bezpieczeństwa sieci

Od uczestników wymagana jest wiedza z zakresu znajomości protokołu TCP/IP.

## Prowadzący szkolenie

Michał Sajdak jest dyrektorem d/s rozwoju oraz konsultantem w firmie Securitum.

- Absolwent Uniwersytetu Jagiellońskiego (informatyka)
- Posiada wieloletnie doświadczenie w dziedzinach: bezpieczeństwa IT, tworzenia oprogramowania (głównie aplikacje dla instytucji finansowych) oraz administracji systemami
- Posiadacz certyfikatu CISSP (#338973)
- Wykonywał audyty bezpieczeństwa – w tym testy penetracyjne – dla największych organizacji w Polsce

## Cena szkolenia

Cena szkolenia wynosi 2200 PLN netto / osobę i zawiera:

- Udział w seminarium
- Książka "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning"
- Nocleg w hotelu trzygwiazdkowym (pokoje jednoosobowe)
- Dostępne w trakcie szkolenia: kawa, herbata, woda, soki, ciasteczka - bez limitu
- Wyżywienie (śniadanie, 2 x obiad, kolacja)

- Konspekt szkolenia
- Certyfikat ukończenia szkolenia

W przypadku uczestnictwa w szkoleniu dwóch lub większej ilości osób z jednej firmy - dla każdego kolejnego uczestnika udzielamy 20% rabatu.