# Szerokie bezpieczeństwo IT – Kraków, 08-09.10.2009r.

## Program szkolenia

**Dzień 1 (11:00 – 18:00)**

10:15-10:45 -- Rejestracja
10:45-11:00 -- Powitanie. Przestawienie prelegenta oraz tematyki szkolenia
11:00-12:30 -- Network

- Czy w środowisku switchowanym można podsłuchiwać? (ARP poisoning i inne ataki w L2)
- Atak MITM na https w środowisku switchowanym (pokaz)
- Co można zrobić nmap-em? (pokaz mniej znanych typów skanowania)
- ICMP tunelling w 5 minut (pokaz zestawienia tunelu)
- DNS tunelling
- Omijanie firewalli (szybki przegląd po firewallach)
- IP jumping ? Jak zlokalizować wrażliwe usługi?
- ethernet tap – do czego może być przydatny?
- Czy istnieje coś poza Ethernet ? ;-)
- VPN – czy samo posiadanie VPN czyni nas bezpieczniejszym (a może mniej bezpiecznym?)
- SSH + Proxifier = VPN? (pokaz utworzenia szyfrowanego tunelu)
- Jak uzyskać (prawie) dowolne IP w Internecie?
- Całkowicie odcięcie komunikacji sieciowej pomiędzy DMZ i corenetem, przy jednoczesnym zapewnieniu dwustronnej komunikacji on-line dla tego typu sieci (rozwiązania klasy Message Queue)

12:30-12:45 - Przerwa
12:45- 13:30 - WLAN

- WPA-PSK to nie wszystko - 802.1X jako przydatny mechanizm w Enterprise WiFi.
- Gdzie tak naprawdę tkwi problem w WEP? Wnioski przy projektowaniu/wdrażaniu własnych rozwiązań powiązanych z kryptografią
- RADIUS - czy tylko wykorzystywany w neostradzie ?
- Anteny kierunkowe – z jakiej odległości można złapać sygnał WiFi?
- Blokady MAC, Brak rozgłaszania SSID – czy skuteczne zabezpieczenia?

13:30 - 14:30 -- Obiad
14:45-15:45 - Application

- Na co tak naprawdę podatne są aplikacje desktopowe?
- XSS – niedoceniane zagrożenie
- SQLi – ataki czasowe blind (pokaz pobrania informacji z bazy danych)
- Infrastruktura i biblioteki – jedno z najpoważniejszych aktualnie zagrożeń
- Google hacking – kopalnia podatności w portalach dostępna dla każdego
- Fierwalle aplikacyjne – czym różnią się od firewalli sieciowych?

15:45-16:00 - Przerwa
16:00-17:00 - OS

- Best practises – czy to wszystko?
- Komercyjne dokumentacje hardeningowe
- Jak zautomatyzować hardening?
- Instalacja aktualizacji (z niespodzianką)
- Rozliczalność – często zapominany element bezpieczeństwa (do czasu)
- Jak monitorować? Ciekawe, darmowe alternatywy do NAGIOS
- Bezbolesny chrooting usług
- Wydajność  OS to nie tylko CPU…

17:15-18:00 - Konsultacje z prelegentem

18:30 -- Kolacja

**Dzień 2 (9:00 – 15:00)**

8:15 - 8:45 -- Śniadanie
8:45 - 9:00 -- Poranna kawa
9:00 -- 10:00 -- Crypto

- Szyfry blokowe – kiedy niepoprawny wybór trybu może skończyć się tragedią?
- Uwierzytelnianie CBC-MAC i szyfrowanie MAC = nieszczęśliwe połączenie
- SSL AD 2009 – jaką jakość szyfrowania zapewnia…?
- Ataki replay na szyfrowane protokoły – przykłady zastosowań
- Kiedy szyfrowanie nie zapewnia integralności i z czym może się to wiązać?
- OpenSSL a testowanie wydajności terminacji SSL
- Problemy z CA (i całą infrastrukturą PKI)
- Co tak naprawdę znajduje się w certyfikacie X.509?
- Funkcje hash – czy powinny coś zapewniać poza niemożliwością odwracalności?
- Podpis cyfrowy – czym tak naprawdę jest?

10:00-10:15 -- Przerwa
10:15-10:45 -- Security

- Bezpieczeństwo fizyczne (okablowanie, wejścia do serwerowni, wytrychowanie zamków)
- Kilka słów o formalnych modelach bezpieczeństwa i certyfikacjach systemów (TCSEC, Common Criteria)
- BCP/DRP – kto się zabezpiecza i z czym to się je?
- Kontrola dostępu DAC (Discretionary Access Control) to nie wszystko ?
- Zagrożenia – czy ataki hackerskie to najpoważniejszy problem?
- „Hackers lie. Skillful hackers lie well. And well-rounded hackers can lie both to people and to machines."

10:45 - 11:15 -- Machines

- Skąd wziąć tani sprzęt do testów i jak uczyć się assemblera (architektura inna niż x86)
- Jak buduje się urządzenia sieciowe i jaki to ma wpływ na bezpieczeństwo?
- Fizyczny dostęp do urządzeń

11:15 - 11:30 -- Przerwa
11:30 - 12:45 -- Tools

- Wireshark / tcpdump –jakie strony są najczęściej odwiedzane przez pracowników?
- Jak vendorzy naciągają funkcjonalności i zalety swoich narzędzi?
- Wireshark – inne narzędzia w suicie
- Snort – kilka ciekawostek
- mod_security – kolejny network IDS?
- Antywirus na wszystko pomoże…?
- Crackowanie haseł
- Audyt rozwiązania X na wszystko pomoże...? Kilka słów o testach penetracyjnych
- Firewall psychologiczny – kilka środków odstraszających
- Rootkit/spyware detector – uzupełnienie dla antywirusów

12:45 - 13:45 - Obiad
14:00 - 14:30 - Books & resources

- Ciekawe książki o bezpieczeństwie IT (anglojęzyczne)
- Certyfikacje – IT security – przegląd
- Wybrane ciekawe źródła informacji o bezpieczeństwie IT (blogi security, cheat sheets, ...)
- Przegląd po projektach OWASP

14:30 - 15:00 - Konsultacje z prelegentem

## Grupa docelowa

Szkolenie przeznaczone jest dla:

- Pracowników departamentów bezpieczeństwa firm
- Pracowników działów IT
- Osób odpowiedzialnych za wdrażanie zabezpieczeń w organizacjach
- Osób pragnących usystematyzować / poszerzyć swoją ogólną wiedzę z zakresu bezpieczeństwa IT

## 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 1755 PLN netto / osobę i zawiera:

- Udział w seminarium
- 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.