Hardening systemów operacyjnych – Kraków 15–16.10.2009r.

Program szkolenia

Dzień 1 (9:00 - 16:00)

8:40-9:00 -- Rejestracja
9:00 - 9:15 -- Powitanie. Przestawienie prelegenta oraz tematyki szkolenia
9:15 - 10:15 -- Linux (część 1)

- Zabezpieczenie systemu w fazie startu
- Usługi (nasłuchujące / nienasłuchujące)
- Uprawnienia – file system
- Pliki zawierające wrażliwe dane
- Pliki SUID/SGID
- Lokalizacja miejsc globalnego zapisu
- Pliki bez właściciela
- Linki
- Urządzenia
- Konta użytkowników oraz konfiguracja środowiska
- Wykorzystanie mechanizmów modelu MAC (AppArmor, SELinux)
- Tuning wybranych parametrów jądra
- Wybrane patche na jądro
- Zarządzanie systemem

10:15 - 10:30 -- Przerwa
10:30 - 11:30-- Linux (część 2)

- Mechanizm chroot
- Mechanizmy związane z wydajnością
- Backup
- Dodatkowe komponenty zwiększające bezpieczeństwo (integralność, rozliczalność)
- Mechanizmy utrudniające atak, po zdobyciu dostępu na poziomie fizycznym
- Mechanizmy aktualizacji systemu, weryfikacja integralności aktualizacji
- Przydatne narzędzia: lsof, ps, netstat, vmstat, find, portmap, nmap & ndiff

11:30 - 11:45 -- Przerwa
12:00-13:15 BSD (na przykładzie FreeBSD)

- Standardowe mechanizmy hardeningu dla systemów klasy *NIX
- Ochrona na poziomie filesystemu
- Parametry jądra
- Kernel securelevel
- Jail vs chroot
- Upgrade systemu

13:15 - 14:45 -- Obiad
15:00 - 16:15 - Windows 2003 Serwer

- Usługi
- Uprawnienia
- Logowanie zdarzeń – uprawnienia / integralność logów
- SAM
- Audit Policy, Account Policy, Security Policy
- Przegląd narzędzi ułatwiających lokalizację rootkitów
- Windows Performance Monitor

Dzień 2 (9:00 – 15:30)

8:15 - 8:45 -- Śniadanie
8:45 - 9:00 -- Poranna kawa
9:00 - 10:00 -- Hardening wybranych usług
- Apache2 + mod_ssl + mod_php
- Modyfikacja parametrów konfiguracji
- Hardening PHP
- Chroot
- Hardening SSL

10:00 - 10:15 -- Przerwa
10:15 - 10:45 -- O czym warto pamiętać konfigurując system klasy (host) firewall?
- Podstawowe klasy firewalli
- Podstawowe informacje o nmap oraz hping2
- Reakcje na nietypowe pakiety
- Problemy z DNS
- Problemy z ICMP

10:45 - 11:00 -- Przerwa
11:00 - 12:30 - Ćwiczenia praktyczne (część 1)
- Każdy uczestnik otrzyma dostęp do dedykowanej dla siebie maszyny wirtualnej z zainstalowanym systemem FreeBSD. Każdy uczestnik po szkoleniu otrzyma recenzję wykonanego przez siebie hardeningu wraz z ewentualnymi komentarzami. Ćwiczenia obejmowały będą:
- Ogólny hardening OS
- Uruchomienie usługi w Jail

12:30 - 13:30 - Obiad
13:45 - 15:00 - Ćwiczenia praktyczne (część 2)
- Zmiany w securelevel
- Hardening usługi działającej w systemie

15:00 - 15:30-- Podsumowanie

Grupa docelowa

Szkolenie przeznaczone jest dla:

- Administratorów systemów
- Pracowników departamentów bezpieczeństwa firm
- Osób odpowiedzialnych za audyt zewnętrzny/wewnętrzny organizacji

Od uczestników wymagana jest wiedza ogólna z zakresu podstawowej znajomości serwerowych systemów operacyjnych: FreeBSD, Linux, Windows 2003 Server.

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 2205 PLN netto / osobę i zawiera:

- Udział w seminarium
- Nocleg w hotelu trzygwiazdkowym (pokoje jednoosobowe)
- Wyżywienie (śniadanie, 2 x obiad, kolacja)
- Książkę (jedna do wyboru): Mastering FreeBSD and OpenBSD Security, Hardening Linux, Professional Windows Desktop and Server Hardening
- Dostępne w trakcie szkolenia: kawa, herbata, woda, soki, ciasteczka - bez limitu
- 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.