SECURITUM

SZKOLENIE

Bezpieczeństwo sieci / Testy penetracyjne

Grupa docelowa

programiści | administratorzy | pentesterzy

Poziom zaawansowania

★ ★ ★

O SZKOLENIU

- Trzydniowe szkolenie warsztatowe
- Praktyczna prezentacja metod ochrony sieci przed zagrożeniami
- Techniki prowadzenia testów penetracyjnych infrastruktury
- Przegląd narzędzi ułatwiających przeprowadzenie testów bezpieczeństwa
- Praca na realnych systemach w LAB (routery / switche / serwery / aplikacje) z podatnościami
- Wybrane zagadnienia z zakresu monitoringu bezpieczeństwa sieci

DODATKOWE INFORMACJE

FORMULARZ ZGŁOSZENIOWY

UCZESTNICY O SZKOLENIU

Bardzo profesjonalne, z bardzo dużą ilością praktyki. Pozwoliło też zmienić mój sposób myślenia o bezpieczeństwie.

Bardzo dobra organizacja (miejsce, laboratorium, agenda).

Bardzo ciekawe szkolenie poszerzające tematy ważne dla bezpieczeństwa danych. Jedyne, jakie znalazłem, poruszające tego typu tematy.

Intensywne i rozwijające. Jestem pod wrażeniem i polecam!

Praktyka! Pierwsze szkolenie, gdzie można coś faktycznie przećwiczyć. Ciekawe źródła wiedzy i narzędzi. Sporo informacji „best practice".

Przegląd narzędzi do hackowania i ochrony oraz omówienie niektórych z nich. Możliwość wykonania ćwiczeń utrwalających zdobytą wiedzę.

RAMOWY PROGRAM SZKOLENIA

Wstęp – elementy bezpieczeństwa informacji

- Elementy wchodzące tradycyjnie w zakres bezpieczeństwa informacji
- Biznesowe podejście do kwestii związanych z bezpieczeństwem IT (wstęp do analizy ryzyka)

Testy penetracyjne jako metoda testowania bezpieczeństwa sieci

Modyfikacja komunikacji sieciowej

- Przechwytywanie dowolnych pakietów, ich modyfikacja oraz retransmisja (oprogramowanie scalpy)
- Proste tworzenie dowolnych pakietów (oprogramowanie scalpy)
- Utworzenie komunikacji ARP w celu zatrucia tablicy ARP na wybranej stacji roboczej

Bezpieczeństwo sieci – Ethernet

- Podsłuchiwanie rozmów VoIP – LAB z telefonami IP
- Podsłuch transmisji w środowisku switchowanym – atak klasy MAC flooding (port stealing)
- Podsłuch transmisji w środowisku switchowanym – atak klasy ARP Poison Routing
- Atak man-in-the-middle w środowisku switchowanym – na serwis chroniony protokołem HTTPS
- Ustawienie wrogiego serwera DHCP oraz wykonanie ataku klasy man-in-the middle na serwis WWW chroniony protokołem HTTPS

Bezpieczeństwo warstwy 3 modelu OSI

- Skanowanie portów TCP/UDP na wybranym serwerze
  - techniki proste
  - techniki zaawansowane
- Określenie oprogramowania działającego na docelowym serwerze (oprogramowanie usługowe oraz wersja systemu operacyjnego)

Bezpieczeństwo IPsec

- Skanowanie VPN (na podstawie IPsec)
- Brute force hasła dostępowego dla IPsec

Bezpieczeństwo sieci Wi-Fi

- Ataki na WEP/WPA/WPA2
- Topologia WPA2 Enterprise
- Lab na realnych access pointach
- WPS

Systemy klasy IPS (Intrusion Prevention System) oraz firewalle aplikacyjne

- Wprowadzenie do tematyki
- Oferowane metody ochrony
- Tworzenie własnych reguł w systemie IPS (na przykładzie snort)
- Metody testowania bezpieczeństwa systemu IDS
- Omijanie systemów IPS / Application Firewall (na przykładzie infrastruktury web)

Podatności klasy buffer overflow

Realizacja przykładowego testu penetracyjnego w LAB

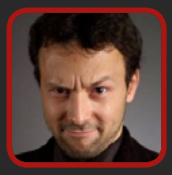
- Rozpoznanie celu
- Wykorzystanie kilku podatności
- Objęcie testem aplikacji / elementów sieciowych
- Finalnie uzyskanie uprawnień administratora na docelowym systemie

SZKOLENIE POLECAJĄ

ROSWALTO · ZAUFANA TRZECIA STRONA.PL · sekurak.pl · programista

TRENER

Michał Sajdak



- Założyciel serwisu sekurak.pl
- Posiada certyfikaty: CEH, CISSP, CTT+
- Zgłasza istotne błędy bezpieczeństwa w urządzeniach sieciowych (m.in. Cisco, HP, TP-Link)
- Bierze udział w kilkudziesięciu testach penetracyjnych rocznie
- Szkoli aktywnie od ponad 5 lat
- Prelegent na konferencjach (m.in.): Confidence (2009, 2011, 2013, 2015), Secure (2013, 2014, 2015), SEMAFOR (2010, 2012, 2015), Securitybsides (2012), Seconference (2009), SecCon (2011), OWASP@Krakow (2011), AIESEC (2012)

PUBLIKACJE

- *Podatność CSRF*
- *Luki w urządzeniach TP*
- *Podatność SQL injection*

WIDEO ZE SZKOLEŃ

- *Prezentacja Secure 2014*
- *Fragment ze szkolenia*
- *Embedded Devices Hacking*

ZAPISZ SIĘ

FORMULARZ ZGŁOSZENIOWY

DODATKOWE INFORMACJE

< SZKOLENIA@SECURITUM.PL >