SECURITUM

SZKOLENIE

Wprowadzenie do bezpieczeństwa IT

Grupa docelowa

Managerowie IT | ABI | Audytorzy
Programiści | Administratorzy

Poziom zaawansowania

★ ★ ★

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
- Prelegent na konferencjach (m.in.): Confidence (2009-2016), Secure (2013-2016), SEMAFOR (2010-2016), Securitybsides (2012), Seconference (2009), AIESEC (2012), Testingcup (2016), Sekurak Hacking Party (2015, 2016)
- Autor najlepszych prezentacji (wg ankiet uczestników) na konferencjach: Secure, Semafor, Testingcup

PUBLIKACJE

- *Podatność CSRF*
- *Luki w urządzeniach TP-Link*
- *Podatność SQL injection*
- *Analiza ryzyka IT*

WIDEO ZE SZKOLEŃ

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

ZAPISZ SIĘ

FORMULARZ ZGŁOSZENIOWY

! DODATKOWE INFORMACJE

< SZKOLENIA@SECURITUM.PL >

O SZKOLENIU

- ✔ kurs dla osób nieposiadających doświadczenia w bezpieczeństwie IT
- ✔ szkolenie z praktyczną prezentacją przekazywanej wiedzy (pokazy „na żywo")
- ✔ solidne i konkretne uporządkowanie wiedzy z bezpieczeństwa IT
- ✔ przegląd praktyczny najważniejszych pojęć i mechanizmów bezpieczeństwa IT
- ✔ ataki na systemy IT / metody ochrony (głośne włamania z ostatnich lat)
- ✔ pakiet dokumentacji do bezpłatnego wykorzystania w firmie
- ✔ po szkoleniu będziesz mógł rozpocząć samodzielną analizę bezpieczeństwa systemów w firmie

! DODATKOWE INFORMACJE

FORMULARZ ZGŁOSZENIOWY

UCZESTNICY O SZKOLENIU

> *Profesjonalne, przerosło oczekiwania, podejście indywidualne, możliwość własnych pytań w przerwach.*
>
> *Dobre, merytoryczne, zrozumiałe tłumaczenie.*
>
> *Techniczne przykłady, duża widza prowadzącego.*
>
> *Jeśli to było wprowadzenie, to bardzo obszerne.*
>
> *Jasny i precyzyjny język przekazywanych informacji.*
>
> *Duża baza wiedzy przekazana w bardzo jasny i profesjonalny sposób, dla użytkowników, którzy zaczynają pracę w systemach IT.*

RAMOWY PROGRAM SZKOLENIA

Elementy bezpieczeństwa informacji

- Poufność, integralność, dostępność, rozliczalność oraz przykłady naruszeń
- Zarządzanie ryzykiem – czyli sposób na racjonalne wydawanie środków na bezpieczeństwo

Częste problemy bezpieczeństwa w systemach IT

- Świadomość bezpieczeństwa w systemach IT
- DoS / DDoS
- Wybrane problemy na urządzeniach sieciowych i aplikacjach
- Socjotechnika
- Pokazy praktyczne: podsłuch telefonów VoIP, atak na urządzenie sieciowe, aplikację webową i VPN

Wybrane zagadnienia bezpieczeństwa warstwy sieciowej

- Firewalle
- Systemy IDS jako jeden z elementów monitoringu bezpieczeństwa sieci
- Bezpieczeństwo sieci Wi-Fi:
  - Ochrona Access Point / ochrona klienta
  - Tryby ochrony sieci: Open / WEP, WPA, WPA2
  - Czym jest sieć klasy WPA2-Enterprise
  - Jak zbudować bezpieczną sieć Wi-Fi

Jak ochronić swoją sieć – elementy monitoringu bezpieczeństwa

- W jaki sposób zorganizować monitoring bezpieczeństwa sieci, do czego jest przydatny?
- Systemy klasy IDS/WAF

Bezpieczeństwo aplikacji WWW

- Praktyczne omówienie kilku częstych błędów bezpieczeństwa w aplikacjach webowych
- W jaki sposób zabezpieczyć własną aplikację?
- Czego wymagać od dostawców aplikacji?

Bezpieczeństwo infrastruktury mobilnej

- Zagrożenia dla infrastruktury mobilnej
- Jak budować bezpieczną architekturę mobilną?
- W jaki sposób zwiększyć bezpieczeństwo smartfonów?
- Gdzie szukać szczegółowych dokumentacji?

Bezpieczeństwo IoT

- Przykłady ataków z ostatnich lat
- Metody zabezpieczenia różnych urządzeń
- Narzędzia sprawdzające bezpieczeństwo urządzeń

Bezpłatna dokumentacja i narzędzia dostępne w Internecie

SZKOLENIE POLECAJĄ

ROSWALTO sekurak.pl programista