Curriculum Vitae

Kamil Frankowicz

E-mail: kamil@frankowicz.me
Web: frankowicz.me

Profil zawodowy

- Bardzo dobra znajomość środowisk klienckich i serwerowych Windows, poparta certyfikatami Microsoft
- Znajomość zagadnień ataków na aplikacje w systemie Windows oraz GNU\Linux
- Znajomość technik analizy podatności oraz złośliwego oprogramowania (zarówno analizy statycznej jak i dynamicznej)
- Wiedza w obszarze ataków na sieci LAN oraz WLAN
- Znajomość środowiska wspomagającego testy penetracyjne - Metasploit Framework
- Umiejętność programowania w języku Python, Ruby, C

Doświadczenie zawodowe

- 4.2016 – obecnie: **Specjalista ds. bezpieczeństwa IT**, NASK \ CERT Polska
  Zakres obowiązków:
  - Analiza złośliwego oprogramowania (głównie na platformę Windows)
  - Analiza podatności w oprogramowaniu oraz exploitów
  - Automatyzacja procesów detekcji i analizy za pomocą skryptów w języku Python
  - Rozwój projektów wewnętrznych
- 8.2014 – obecnie: **Administrator,** DaVinci Medical System Sp. z.o.o.
  Zakres obowiązków:
  - Opracowywanie procedur bezpieczeństwa oraz polityk haseł
  - Konfiguracja i hardening systemów klienckich i serwerowych z rodziny Windows
  - Konfiguracja urządzeń sieciowych oraz rozwiązywanie problemów z ich działaniem
  - Wdrażanie i konfiguracja aplikacji u klientów
  - Rozwiązywanie problemów z działaniem systemów operacyjnych oraz sieci firmowej

Edukacja

- 2012 – 2016: Wojskowa Akademia Techniczna, kierunek: Informatyka, poziom wykształcenia: Inżynier
- 2009 – 2012: I Liceum Ogólnokształcące w Radzyniu Podlaskim, profil: matematyka – fizyka - informatyka

Znajomość języków obcych

- Angielski: dobra znajomość w piśmie, umiejętność czytania dokumentacji technicznej
- Niemiecki: podstawowa znajomość w mowie i piśmie

Referencje

- Paweł Lipowczan - Kierownik projektów informatycznych, DaVinci Medical System Sp. z.o.o, + 48 XXX XXX XXX
- Piotr Tutka – Dyrektor, TUTTI P.i M. Tutka Sc, +48 XXX XXX XXX

Bughunting

Odkryte podatności:

- Szereg podatności podatności oraz tylna furtka w rodzinie routerów LTE: D-Link DWR
- Podatność przepełnienia bufora w routerach Thomson Technicolor TC7200 oraz Thomson TWG870 umożliwiającej zdalny atak na urządzenie (Drugi artykuł na niebezpiecznik.pl)
- Przepełnienie bufora oraz podatność Information Disclosure w urządzeniu Orange LiveBox 2.0
- Podatności XSS, CSRF oraz odmowy usługi w routerze TP-Link TL-WA5210G
- Brak uwierzytelniania w routerze D-Link DSL-2640B umożliwiający zdalny restart urządzenia

Uzyskane certyfikaty

- Microsoft Certified IT Professional: Enterprise Administrator
- Microsoft Certified IT Professional: Server Administrator
- Microsoft Certified Systems Administrator
- Microsoft Specialist: Server Virtualization with Windows Server Hyper-V and System Center
- Microsoft Certified Technology Specialist: Windows Server 2008 R2, Server Virtualization

Inne

Konferencja Security BSides Warsaw 2015

Wystąpienie na konferencji Security BSides Warsaw 2015 (10.10.2015r.) w Warszawie z prezentacją „Analiza podatności routerów SOHO”.

Dodatkowe umiejętności

- Czynne prawo jazdy kategorii B

Zainteresowania

- Bezpieczeństwo teleinformatyczne oraz urządzeń wbudowanych (Internet of Things)
- Psychologia
- Finanse
- Kolarstwo górskie