dr hab. inż. Jerzy Kosiński
Profesor WSPol
Adres e-mail: j.kosinski@wspol.edu.pl
Nr telefonu: 725 99 55 05

Szczytno, dn. 14.05.2017 r.

RECENZJA

książki Adama Ziaji pt.:

Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linux

Szybko zmieniające się technologie teleinformatyczne, w szczególności dynamiczny rozwój Internetu sprawiają, że funkcjonowanie ludzi i organizacji jest praktycznie niemożliwe bez ich wykorzystania. Jednym z podstawowych warunków korzystania z tych zdobyczy technologicznych w gospodarce i życiu obywateli jest ich bezpieczeństwo. Niestety, nie można jego zapewnić w stu procentach i trwale. Należy liczyć się z sytuacją, że to bezpieczeństwo będzie naruszane przez przestępców widzących w wykorzystaniu technologii teleinformatycznych możliwość łatwego i dużego zarobku, przy jednocześnie niewielkim ryzyku ujawnienia. Możliwości są efektem stale odkrywanych nowych podatności i niepełnego usunięcia starych. Niewielkie ryzyko jest wynikiem braku wiedzy i doświadczenia wszystkich, którzy odpowiadają za przeprowadzenie działań zmierzających do ujawnienia, zabezpieczenia i analizy śladów wskazujących na sposób działania i sprawcę.

W powyższym kontekście, książka Pana Adama Ziaji musi być postrzegana bardzo pozytywnie. Autor książki odniósł się w niej bowiem do bardzo istotnego, a jego waga będzie wzrastała, problemu zabezpieczania i analizy śladów wskazujących na cyberwłamanie. Dodatkowo skoncentrował się na rzadziej omawianym w publikacjach środowisku Linux.

Świadczy to dobrze o świadomości Autora potrzeb dotyczących różnych aspektów analizy powłamaniowej, szczególnie pod kątem ataków na strony internetowe, które w dzisiejszych czasach najczęściej padają ofiarą hakerów. Autor uzupełnił to spojrzenie o powłamaniową analizę systemu Linux, w tym botnetów opartych na urządzeniach IoT, analizę zrzutów pamięci RAM, analizę behawioralną złośliwego oprogramowania.

Tytuł recenzowanej publikacji jest adekwatny do jej treści, a problem, którym zajął się autor jest ważny zarówno poznawczo, ale także praktycznie. Układ wzajemnie powiązanych treści tworzy zrozumiały dla czytelnika ciąg przyczynowo-skutkowy i stanowi spójną całość. Język publikacji jest przystępny.

Książka jest bogato ilustrowana przykładami, można wręcz powiedzieć, że to praktyczne działania związane z analizą powłamaniową są komentowane i wyjaśniane.

Zaletą książki jest jej aktualność (co nie jest często spotykane w opisywanym obszarze). Autor opisuje, m.in. SQL Injection (SQLi), Remote Code Execution (RCE), Local File Inclusion (LFI), Remote File Inclusion (RFI), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), Shellshock (CVE-2014-6271), Denial-of-Service (DoS), a także omawia studia przypadków: CMS Joomla, CMS Wordpress, LFI.

Dodatkowym atutem publikacji jest połączenie prezentacji wykorzystywanych narzędzi niekomercyjnych, z wyraźną ich przewagą i narzędzi komercyjnych, ale preferowanie wskazania manualnie przeprowadzonych analiz (włącznie z pisaniem własnych skryptów).

Cyberprzestępcy znajdują i tworzą coraz bardziej zaawansowane sposoby włamań, ukrywają swoje działania i zacierają ślady. Chcąc poprawić cyberbezpieczeństwo i eliminować z Internetu aspołecznych użytkowników trzeba ciągle poszerzać swoją wiedzę i rozwijać umiejętności, także z zakresu analizy włamań. Dzięki takim książkom, każdy zainteresowany tematem użytkownik Internetu jest w stanie samodzielnie wykonać działania, które wydają się nieosiągalne dla niespecjalisty.

Reasumując, recenzowana książka Pana Adama Ziaji jest warta polecenia wszystkim osobom zainteresowanym badaniom kryminalistycznym systemu Linux i aplikacji webowych działających w tym środowisku. Będzie także przydatna wszystkim, których interesują techniczne i prawne (trzeba rozumieć techniczne) aspekty cyberprzestępczości.

Nieliczne uwagi redakcyjne zostały wskazane w załączniku.

Oświadczam, że znam Autora, ale nie występuje konflikt interesów, za który uznaje się:

- bezpośrednie relacje osobiste (pokrewieństwo, związki prawne, konflikt)
- relacje podległości zawodowej
- bezpośrednia współpraca naukowa w ciągu ostatnich dwóch lat