УДК 004.77
К. Чурбаков
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ МОВИ LUA ДЛЯ РОЗШИРЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ IDS/IPS

UDC 004.77
K. Churbakov

USING LUA LANGUAGE TO EXTEND THE FUNCTIONALITY OF IDS/IPS

Інформаційна безпека є важливим напрямком у сучасних технологіях, а системи виявлення та попередження вторгнень (IDS/IPS) відіграють ключову роль у захисті мереж. Однак стандартні функціональні можливості таких систем можуть бути недостатніми для специфічних потреб, що створює попит на інструменти їхньої адаптації. Використання мови Lua дозволяє створювати гнучкі налаштування та розширювати функціонал IDS/IPS, забезпечуючи адаптивність до нових загроз та підвищення ефективності їх роботи [1].

Впровадження Lua в системи виявлення вторгнень дозволяє ефективно інтегрувати специфічні сценарії аналізу мережевого трафіку, що важливо для виявлення складних і невідомих типів атак. Можливість використання користувацьких скриптів розширює функціональність базових механізмів IDS/IPS, роблячи систему більш гнучкою до змін у кіберзагрозах [2].

Метою дослідження є розробка і тестування інтеграції мови Lua з існуючими IDS/IPS для створення динамічних модулів, здатних забезпечити більш точне виявлення загроз і зменшення кількості хибних спрацьовувань. У роботі застосовувалася мова Lua для створення користувацьких скриптів, які інтегруються із платформою Suricata, що забезпечує обробку мережевого трафіку з дотриманням специфічних правил. Локальне тестування показало підвищення точності і надійності системи виявлення [3].

Особливістю мови Lua є її легкість і висока продуктивність, що робить її ідеальним вибором для інтеграції у реальному часі в умовах великих обсягів мережевого трафіку. Lua дозволяє створювати правила та логіку, які працюють паралельно з основними алгоритмами аналізу без зниження загальної продуктивності системи.

Результати роботи демонструють, що впровадження мови Lua у роботу IDS/IPS може суттєво розширити функціональні можливості цих систем, зокрема шляхом динамічного налаштування правил та адаптації до сучасних викликів у сфері інформаційної безпеки.

Література

1. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. URL: https://www.usenix.org/legacy/events/sec99/full_papers/paxson/paxson.pdf.
2. Roesch M. Snort: Lightweight Intrusion Detection for Networks. URL: https://www.snort.org/downloads/snort/white_paper.pdf.
3. Schlueter K. Lua Programming for Real-World Security. O'Reilly Media, 2020.