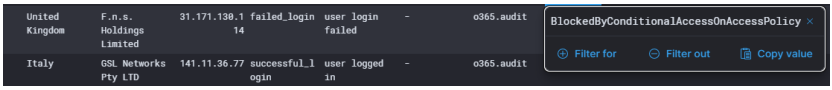

Рис. 1. Фіксація невдалого входу користувача

Проаналізувавши активність за допомогою IP2Proxy та AbuseIPDB було помічено, що насправді IP адреса є VPN, яка насправді походить з Німеччини, та має сумнівну репутацію (рис. 2).

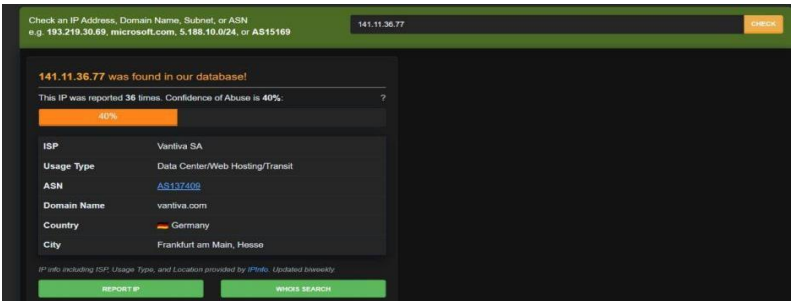

Рис. 2. Виявлена підозріла IP адреса

В результаті подальших перевірок було визначено, що користувач в результаті переходу за фішинговим посиланням ввів свої дані. Після виконання розриву сесій, зміни пароля та подальших перевірок атаку вдалось припинити.

Підбиваючи підсумки, навіть для такого простого процесу як авторизація можна використати десятки різних технік та атак, які дозволять обійти навіть найбільш досконалі системи захисту. Проте, якщо вчасно отримати повідомлення про підозрілі дії, можна виконати розрив сесії до виконання шкідливих дій. Тому актуальність використання моніторигових систем для аналізу стану безпеки зростатиме і надалі.

Розгортання системи моніторингу безпеки VPN-з'єднання на базі WireGuard

УДК 004.056

Каріна Крушельницька[1], Марина Деркач[2], Віталій Тимощук[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]karina.kryshel@gmail.com, [2]m_derkach@tntu.edu.ua, [3]Tymoshchuk@tntu.edu.ua

У сучасних мережевих інфраструктурах VPN-з'єднання забезпечують створення захищених каналів передачі даних через Інтернет. У свою чергу, системи моніторингу дозволяють контролювати віддалений доступ до ресурсів, поєднуючи у єдину безпечну мережу територіально віддалені офіси, а також відстежувати підозрілу активність та своєчасно виявляти загрози.

Для реалізації такого підходу при розгортанні системи моніторингу безпеки використано систему виявлення вторгнень на основі мережі Suricata, яка демонструє широкі аналітичні можливості для моніторингу мережевого

середовища, зокрема здатна перевіряти не лише структуровані дані пакетів, а й додаткові атрибути трафіку, такі як сертифікати TLS, HTTP-запити, DNS-транзакції, що дозволяє виявляти складні атаки на різних рівнях мережевої взаємодії [1]. Інструмент функціонує на прикладному рівні моделі OSI, забезпечуючи глибоку видимість і аналіз кількох пакетів одночасно, незважаючи на роботу на програмному рівні, Suricata зберігає повний доступ до інформації заголовків пакетів, що дозволяє детально аналізувати протоколи транспортного, мережевого та навіть прикладного рівнів, включно з можливістю оцінки шифрованих даних. Для VPN-з'єднання обрано протокол WireGuard, що характеризується гнучкістю та високою продуктивністю, забезпечуючи як конфіденційність, так і цілісність даних [2]. На відміну від інших протоколів WireGuard заплутує метадані пакетів, включаючи довжину передачі та IP-адреси відправників і одержувачів, тому ключі для кожного пакету узгоджуються в приватному порядку без участі третіх сторін, що робить його набагато швидше, а також є більш безпечним, оскільки немає потенційних витоків при обміні ключами з центральним сервером.

У розгорнутій системі реалізовано механізм регулярного моніторингу параметрів з'єднання, що включає IP- та MAC-адреси, ендпоінти та часові характеристики рукостискання. Аналіз даних дозволяє виявляти аномалії, зокрема несанкціоновані MAC-адреси, їх зміну або появу нових пристроїв. Також система виконує перевірку геолокації на основі IP-адреси з визначенням країни, міста та організації. Виявлені відхилення від попередніх значень інтерпретуються як потенційні загрози, а отримані дані кешуються для оптимізації API-запитів. Додатково реалізовано аналіз стабільності з'єднання із урахуванням часу відповіді та значень TTL. Аномальні зміни TTL можуть вказувати на зміну маршрутизації або перенаправлення трафіку. Результати моніторингу зберігаються у логах з'єднань та аномалій.

У ході тестування розгорнутої системи моніторингу безпеки VPN-з'єднання проведено пасивну та активну мережеві розвідки. Під час пасивного спостереження здійснено перехоплення трафіку, що дозволило перевірити коректність налаштувань системи. Результати показали валідність правил виявлення ICMP (ping)-пакетів. Додатково виконано аналіз журналів Security, System та Application з метою виявлення спроб несанкціонованого доступу, мережевих помилок і подій, що можуть свідчити про наслідки атак. Отримані дані підтвердили коректне виявлення ICMP-трафіку. Для фільтрації та візуального аналізу HTTP/POST-запитів, а також ідентифікації потенційно чутливої інформації використано інструмент Wireshark. У межах активної мережевої розвідки змодельовано атаку шляхом виконання ARP-сканування. Надалі імітовано роботу шкідливого програмного забезпечення, яке здійснює аналіз активних пристроїв у мережевому сегменті з метою подальшої компрометації. Такий тип загроз характеризується надсиланням великої кількості ARP-повідомлень, що призводить до перевантаження мережі та зниження якості доступу до Інтернету для користувачів. Ба більше, така активність може бути підготовчим етапом до складніших атак, зокрема поширення шкідливого ПЗ, сканування портів і вразливостей, а також реалізації DDoS і MiTM атак. Результати експерименту (рис. 1) демонструють, що

розгорнута система моніторингу успішно зафіксувала спробу атаки, а також коректно визначила час її виникнення.

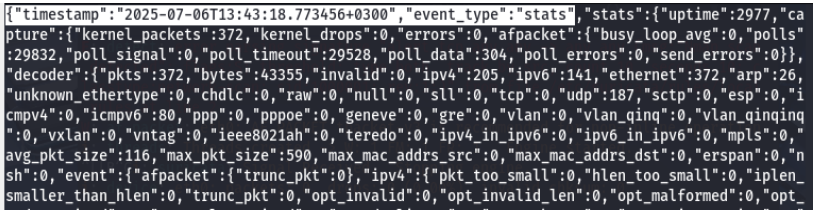
{"timestamp":"2025-07-06T13:43:18.773456+0300","event_type":"stats","stats":{"uptime":2977,"capture":{"kernel_packets":372,"kernel_drops":0,"errors":0,"afpacket":{"busy_loop_avg":0,"polls":29832,"poll_signal":0,"poll_timeout":29528,"poll_data":304,"poll_errors":0,"send_errors":0}},"decoder":{"pkts":372,"bytes":43355,"invalid":0,"ipv4":205,"ipv6":141,"ethernet":372,"arp":26,"unknown_ethertype":0,"chdlc":0,"raw":0,"null":0,"sll":0,"tcp":0,"udp":187,"sctp":0,"esp":0,"icmpv4":0,"icmpv6":80,"ppp":0,"pppoe":0,"geneve":0,"gre":0,"vlan":0,"vlan_qinq":0,"vlan_qinqinq":0,"vxlan":0,"vntag":0,"ieee8021ah":0,"teredo":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":116,"max_pkt_size":590,"max_mac_addrs_src":0,"max_mac_addrs_dst":0,"erspan":0,"nsh":0,"event":{"afpacket":{"trunc_pkt":0},"ipv4":{"pkt_too_small":0,"hlen_too_small":0,"iplen_smaller_than_hlen":0,"trunc_pkt":0,"opt_invalid":0,"opt_invalid_len":0,"opt_malformed":0,"opt_

Рис.1. Результати тестування системи моніторингу

В межах роботи написано скрипт для аналізу лог-файлів системи. Захист журналів включає контроль цілісності, резервне копіювання та виявлення несанкціонованих змін, оскільки вони є критичним джерелом інформації про інциденти безпеки. Водночас ефективність такого захисту забезпечується поєднанням автоматизованих засобів, контролю доступу та моніторингу.

У результаті розроблено гнучку та ефективну систему моніторингу безпеки VPN-з'єднання на базі WireGuard, придатну як для забезпечення віддаленого доступу до корпоративних ресурсів, так і для освітніх і дослідницьких цілей у сфері мережевої безпеки. Результати тестування підтверджують здатність системи збирати інформацію про VPN-клієнтів, автоматично виявляти підозрілу активність і своєчасно ідентифікувати потенційні загрози.

1. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T. (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, 1-11.
2. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

Ідентифікація STRIDE загроз та пріоритизація засобів захисту SSDF для CI/CD процесів

УДК 004.056+ 004.415

Тарас Лобур[1], Руслан Козак[2]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]taras.lobur@tntu.edu.ua, [2]ruslank@tntu.edu.ua

Галузь IT широко використовує практики DevOps (Development and Operations) і CI/CD (Continuous Integration / Continuous Delivery), які забезпечують безперервну інтеграцію коду, автоматизоване тестування та швидке розгортання продуктів. Однак із ростом рівня автоматизації наслідки потенційних кіберзагроз стають масштабними [1]. Попри значну кількість досліджень, присвячених DevSecOps, CI/CD та інтеграції безпеки в життєвий цикл розробки [2, 3, 4], аналіз вказує на відсутність праць, у яких здійснювалася