ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Бойко Віктор Дмитрович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент

ПРОБЛЕМИ ШВИДКОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ У ВЕБ-СЕРВЕРАХ СЕРЕДНЬОГО ТА НИЗЬКОГО РІВНЯ

Основою сучасного глобального Інтернету є веб-сервери або системи доставки веб-контенту. Як правило, це робочі станції під керуванням операційної системи Linux або інших операційних систем, сумісних з POSIX, на яких розгортається інфраструктура веб-сервера – або класична версія LAMP, або більш вдосконалені MEAN або MEARN системи [1], або з використанням тих же системах, але запущені в контейнерах, або за допомогою хмарної платформи.

Завдяки широкому розподілу хмарних технологій для сучасних систем доставки веб-контенту є характерною наявність багатьох систем низького та середнього рівня. Найчастіше такі системи не мають власного SIEM, крім того, навіть основні інструменти IPS/IDS не завжди налаштовані правильно. Це призводить до того, що кіберінциденти часто виникають, вони погано знаходяться і часто оператор перебуває у важкій ситуації, змушені реагувати на інцидент «вручну» без спеціалізованих засобів. У таких випадках оператор змушений вирішувати проблеми на кількох рівнях одночасно: визначити, що проблема пов'язана з кіберінцидентом, визначити джерело проблеми, ізолювати розповсюдження проблеми далі, зберегти дані для більш детального аналізу інциденту, щоб зрозуміти та повністю відновити killchain вторгнення, вжити заходів для запобігання подібних інцидентів у майбутньому.

Його завдання ускладнюється об'єктивними факторами, пов'язаними з тим, як працює сучасна система доставки веб-контенту. Основні проблеми було перераховано вище: відсутність централізованого SIEM, неграмотна конфігурація (або загалом) інструменти IPS/IDS. До цього варто додати велику кількість даних, пов'язаних з роботою веб-сервера, та складністю віддаленого доступу до нього, що найбільш забезпечується ssh, а також широке розповсюдження систем оркестрування та контейнеризації процесів.

У той же час, швидкість відповіді є критичною – особливо у випадку, коли проблема продовжує розповсюджуватись. На думку деяких експертів, "вікно можливостей" може становити лише 20 хвилин[2]. Крім того, з усіма недоліками існуючих систем, рішення, як правило, "необхідне вчора" – оператору доводиться мати справу з існуючою системою та всіма недоліками її конфігурації, оскільки альтернативи у вигляді перевстановлення або зміни та реформування системи зазвичай дорого і пов'язана з втратою даних та ресурсами.

Однією з проблем прискорення реакції на кіберінциденти є низька кваліфікація оператора. Перш за все, це незнання специфіки: операційної системи – систем управління процесами SystemD, SysV тощо. Відсутність навичок та вміння ефективно працювати за допомогою ssh-з'єднання. Тенденція покладатися на автоматизовані системи реагування. І не менш важливе – деградація навичок через ши-

роке використання LLM. Наразі ця деградація досягла такого ступеню [3], що за аналогією з "смертю від GPS" [4] ми вже можемо говорити про "смерть від LLM".

Рішення полягає у формуванні та консолідації практичних навичок та знань оператора, що дозволить йому швидко реагувати на кіберзагрози. Ці навички можуть бути представлені у вигляді піраміди. Основою піраміди будуть базові навички та знання: знання специфіки операційної системи та прикладного програмного забезпечення, навички дистанційної роботи. Майже вся віддалена робота в даний час включає не лише можливість використання SSH, але і використання мультиплексорів командного рядка (tmux, screen), а також вдосконалених засобів організації сеансу на відстані (mosh).

На наступному рівні піраміди розташовуються навички оперативної реакції "близького горизонту" – це включає навички оперативного аналізу стану операційної системи та компоненти стека програмного забезпечення по гарячих слідах інциденту. Компоненти аналізу можна розділити на чотири великі категорії:

- стан системних журналів
- стан файлової системи
- стан пам'яті, та процесів
- мережевий трафік

Ці категорії є універсальними для кожного з наступних рівнів організації навичок, але особливо важливі на цьому рівні.

На наступному рівні оператор повинен мати навички ізоляції та зберігання даних для подальшого аналізу – ці навички включають до себе можливість підтримувати стан системи для вищезазначених категорій, а крім того – здатність працювати з додатковими форматами даних – наприклад, pcap, pcapng для аналізу "знімків" мережевого трафіку, отриманого за допомогою wireshark / tcppdump та інших утиліт.

Не зайве нагадати про таку стару утиліту, як tape archiver (tar), що дозволяє створювати архівні томи файлів, зберігаючи всі метадані, включаючи часові позначки, що визначають час доступу та зміну файлів, а крім того, дає можливість організувати процедуру інкрементального резервування. І нарешті, рівень детального аналізу "довгого горизонту", на якому аналізуються збережені дані, використовуючи додаткові інструменти, включаючи залучення штучного інтелекту та інструментів машинного навчання, для виявлення глибоких тенденцій, аналізу складних випадків тощо. Оператор повинен використовувати всі ці навички послідовно. Часто виявляється, що для оперативного виявлення та ізоляції загрози достатньо дуже невеликої кількості знань та навичок.

Розглянемо один із випадків: веб-сайт організації почав проявляти ознаки вторгнення зловмисного програмного забезпечення – сторінки деяких розділів не відкривались, або перенаправляли браузер користувача на сторінку за межами сайту. Швидкий аналіз виявив, що файли в корені основного каталогу сайту мають різні часові позначки редагування. Це виявилося за допомогою звичайної утиліти ls з ключами "-tr" – "сортувати аз часом" та "-al" – "печатати деталі про знайдені файли". Нижче наведено анонімізований приклад отриманого дампу:

```
# ls -tr -al
...
-rw-r----- 1 www-data www-data 742 dec 10 2024 config.php
drwxr-xr-x 21 www-data www-data 4,0K dec 11 2024 report
-rw-r--r-- 1 www-data www-data 1,1M feb 15 11:05 list.txt
-rw-r--r-- 1 www-data www-data 53 feb 15 11:09
google90f4110c1a683f29.html
-rw-r--r-- 1 www-data www-data 452K feb 15 11:21 index.php
```

Такий дамп дозволив не тільки встановити та виявити змінені файли (list. txt google90f4110c1a683f29.html index.php), але й момент вторгнення до системи ("11:05 15 лютого") – що, в свою чергу, дозволило знайти момент вторгнення у логах веб-серверу та в системному журналі операційної системи. Крім того, пошук вздовж файлової системи змінених файлів до цієї дати з діапазоном на день, дозволив виявляти та встановити факти вторгнення у інших пов'язаних з цим веб-хостів. Для цього було досить просто використати утиліта find з параметрами пошуку файлів за датою редагування файлу.

Зрештою, сліди призвели до взлому системи з використанням вразливості [5] на одному з сусідніх сайтів. Вразливість була закрита, проблема була вирішена. Цей випадок свідчить про те, як дуже невеликий набір навичок та знань дозволяє оператору виявляти та усунути факти вторгнення. Конкретні рекомендації будуть наведені в одному з наступних звітів.

Список використаних джерел:

1. Neeraj K. Differences Between LAMP vs MEAN vs MERN 2025. URL: https://orionesolutions.com/lamp-vs-mean-vs-mern/
1. Catalin C. You have around 20 minutes to contain a Russian APT attack. URL: https://www.zdnet.com/article/you-have-around-20-minutes-to-contain-a-russian-apt-attack/.
2. Lee H. P. H. et al. The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects from a Survey of Knowledge Workers. 2025. URL: https://arxiv.org/pdf/2108.04974
3. Lin A. Y. et al. Understanding" death by gps" a systematic study of catastrophic incidents associated with personal navigation technologies. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2017. P. 1154-1166.
4. CVE-2022-35914. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35914

Ключові слова: SIEM, руткіти, виявлення зловмисного програмного забезпечення, зловмисне програмне забезпечення, кібератака, журнал, перевірка, хеш, IDS, IPS, мережева інфраструктура, цифрова форензіка, веб-сервери, LAMP, MEAN, MERN, kill chain, вторгнення.

Keywords: SIEM, rootkits, malware detection, malware, cyberattack, log, blackout, verification, hash, IDS, IPS, network infrastructure, digital forensic, LAMP, MEAN, MERN, kill chain.