УДК 621.031.2
DOI: 10.31673/2409-7292.2021.011925

Веселков Н.Л., Марченко В.В.

МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ OPEN-SOURCE ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ВТОРГНЕНЬ В СФЕРАХ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ УКРАЇНИ

Розглянуто використання методів виявлення вторгнень, таких як IDS та Honeypot для захисту мережевих інфраструктур малого і середнього бізнесу України.

Ключові слова: IDS, Honeypot, кібератака, вторгнення, захист бізнесу, кіберзагроза, інформаційна безпека

Вступ

Малий і середній бізнес в Україні забезпечує 60% ВВП країни і є основою економіки нашої країни. На сьогодні Україна швидко диджаталізується, вже можливо оформити ФОПа онлайн через застосунок Дія, що дозволяє українцям відкрити малий бізнес не виходячи з квартири. В свою чергу диджиталізація бізнесу також зростає з кожним роком і наразі важко уявити підприємця без власного сайту, інтернет магазину чи сторінках в соціальних мережах. Важливо зазначити, що конфіденційна інформація яка циркулює в малому і середньому бізнесах ніяк не відрізняється від конфіденційної інформації в великому бізнесі, але як показує практика, питання захисту інформації в сферах малого та середнього не турбує підприємців так сильно як у сфері великого бізнесу. Це можна пов'язати з наступними факторами:

необізнаність власників бізнесу в сфері кібербезпеки;

нестача фінансового та людського ресурсу для забезпечення гарного рівня захисту;

складна процедура сертифікування і ліцензіювання систем захисту інформації;

неправильна оцінка ризиків компаніями.

За останні п'ять років кількість кіберзлочинів в Україні зросла вдвічі, а глобальне дослідження компанії Check Point Software Technologies показало, що кількість кібератак на бізнес у світі зросла на 58% у 2020 році відносно 2019 року. Перехід на дистанційні формати праці і все більша диджіталізація створюють умови для зростання числа таких злочинів, а управління кіберризиками стало інструментом виживання бізнесу. І хоч багато українських компаній роблять певні зусилля для захисту своїх даних і систем часто вони просто не готові до кібератак. У деяких випадках стратегія з кібербезпеки зводиться до закупівлі великої кількості програмного й апаратного забезпечення. Але зазвичай ці продукти лише забирають фінанси компанії, не маючи при цьому гарні показники ефективності. Це зазвичай пов'язано з тим, що компанії не має гарний компетентний штат фахівців і захист організації закінчується на закупівлі вже зазначених продуктів, а будь-який більш комплексний підхід до безпеки відсутній.

Також існують і випадки коли компанія не має фінансових ресурсів для закупівлі великої кількості програмного та апаратного забезпечення, але має штат гарних фахівців і стратегію захисту. В таких випадках компанії можуть використовувати безкоштовні рішення з відкритим кодом. Це можуть бути продукти розроблені як великими компаніями так і звичайними користувачами-ентузіастами. Основні переваги open-source рішень це можливість дуже широкого налаштування систем, наявність великої кількості відкритих доповнень до систем та звичайно їх безкоштовність.

В сучасних реаліях можна дуже легко побудувати систему захисту яка буде складатися виключно з технологій з відкритим кодом, але в цій статі ми розглянемо лише ті рішення які допомагають своєчасно виявити вторгнення зловмисника в мережу. Метою даної публікації є розгляд open-source технологій виявлення вторгнень з метою їх розгортання на підприємствах які відносяться до малого та середнього бізнесу в Україні.

Open-source IDS/IPS

IDS (Intrusion Detection System) — це компонент мережевої безпеки, основною задачею якого є виявлення аномальних дій в мережі та сповіщення про них. IDS системи відносять до бінарних класифікаторів, тобто системі на основі прописаних правил треба віднести подію до однієї з двух категорій, у IDS системи це або нормальна поведінка системи або аномалія, а потім на основі зробленого вибору виконати певний алгоритм дій. Система запобігання вторгнень (IPS) була розроблена для доповнення роботи мережевого екрану. IPS системи створені на базі IDS, однак, при виявленні ознак вторгнення, дана система сама приймає комплекс дій для його запобігання, на відміну від IDS яка тільки інформує адміністратора, який вже сам приймає рішення щодо дій.

1. Suricata

Suricata напевно одна з найпопулярніших open-source IDPS на даний момент. У Suricata основні функції виконують окремі модулі, а саме модулі захоплення, збору, декодування, виявлення і виведення. За замовчуванням трафік який аналізує система йде напряму до модуля декодування одним потоком, хоча так використовується більше ресурсів системи. При необхідності потоки можна розділити в налаштуваннях і розподілити по процесорам. Для перехоплення трафіку можуть використовуватися різні інтерфейси, основні з яких IPFW, IPFRing, AF_PACKET, PF_RING, LibPcap, NFQueue, крім того, модульна архітектура Suricata спрощує підключення нових елементів для захоплення, декодування, аналізу і обробки мережевих пакетів.

Suricata не потребує великої кількості фізичних ресурсів, а для розгортання і налаштування системи не треба мати дуже поглиблені знання. В режимі IDS базовий набір правил допомагає виявляти більшість кібератак вже після розгортання системи (після встановлення в системі вже приблизно 30000 правил), а для режиму IPS треба лише налаштувати взаємодію з іншими службами (зазвичай з iptables в мережевому екрані).

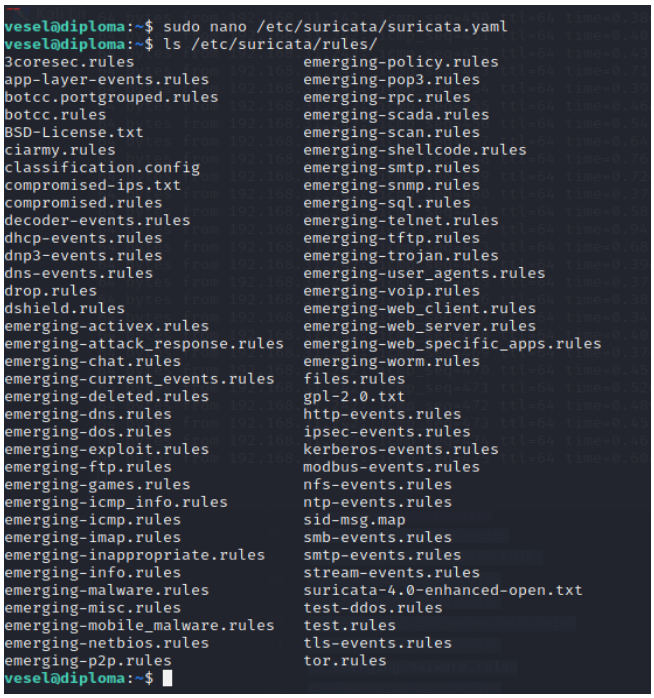

Рис. 1. Список всіх базових бібліотек правил Suricata

Окрему увагу треба зосередити, що так як Suricata є мережевою IDS (NIDS), то максимальна ефективність системи досягається при аналізі трафіку який вже пройшов мережевий екран. Для цього зазвичай систему розгортають поза мережевим екраном, екрануючи на неї копію трафіку (SPAN). Також можливий варіант розгортання при використані VPN.

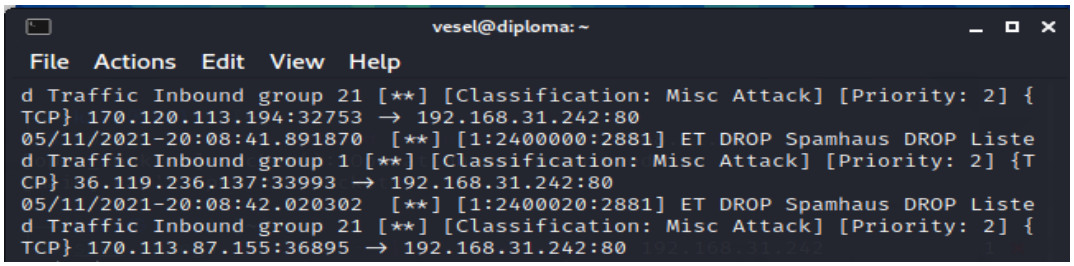

Рис. 2. Виявлення спам атак в Suricata

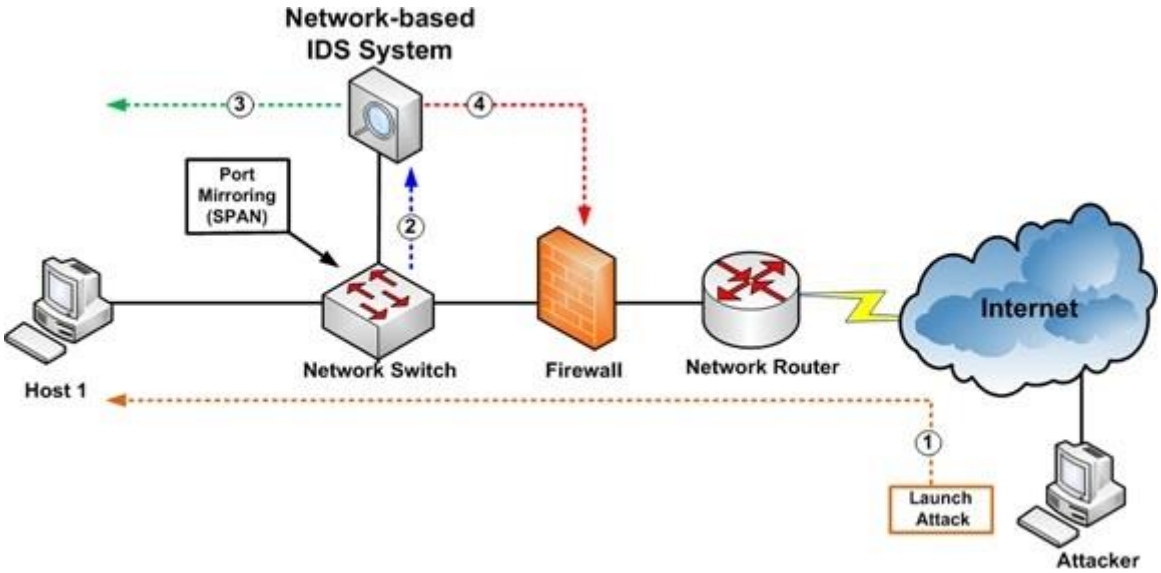

Рис. 1.3. Приклад розгортання Suricata в мережі

Для зручності моніторингу роботи IDS рекомендуємо встановити веб-інтерфейс, наприклад Kibana або SELKS. Розгортання цих веб-інтерфейсів нескладне, вони також є open-source продуктами, а в офіційні документації Suricata є рекомендації щодо їх налаштування.

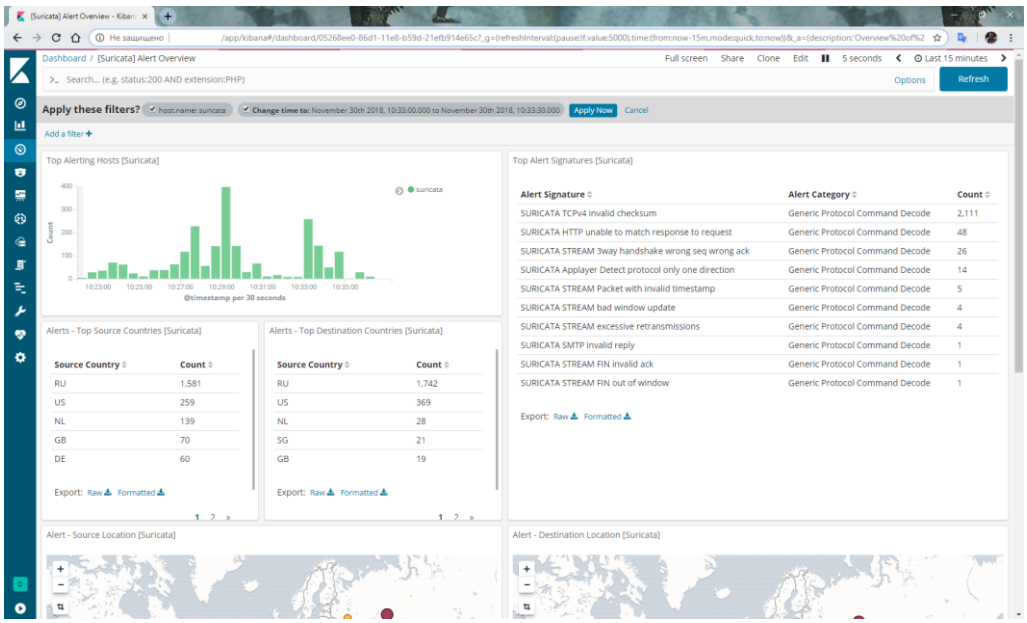

Рис. 1.4. Веб-інтерфейс Kibana для Suricata

2. OSSEC

OSSEC (Open Source Security Correlator) — це open-source HIDS, розроблена фондом OSSEC. Ця система характеризується своєю масштабованістю та мультиплатформою, оскільки працює як на Windows так і на різних дистрибутивах Linux та MacOS. Як HIDS, ця система здатна аналізувати журнали, перевіряти цілісність файлів, моніторити стан системи.

OSSEC може виявити DDOS, брутфорс, експлойти, витік даних і інших зовнішніх атаках. Система проводить моніторинг мережі користувача в режимі реального часу і взаємодіє з системою, після того як користувач вносить до неї якісь зміни. OSSEC використовує агент-серверну модель, виділений сервер забезпечує агрегування та аналіз для кожного хоста.

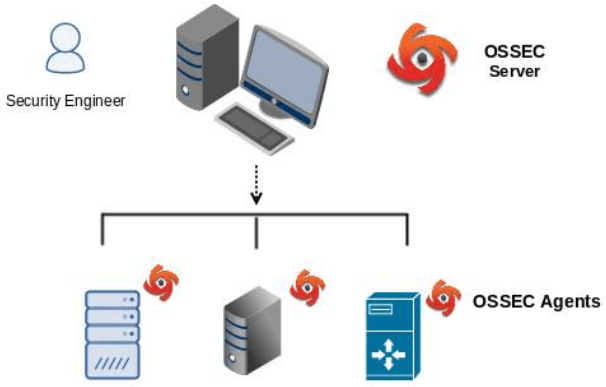

Рис. 2.1. Інфраструктура OSSEC

Розгортання OSSEC так само як і Suricata не потребує великої кількості ресурсів й знань. Однак, так як система хостова то розгортання її на всіх пристроях в мережі може зайняти доволі великий ресурс часу. Тому рекомендуємо встановлювати систему лише на критично важливі пристрої, наприклад на веб-сервери чи комп'ютери які обробляють важливу корпоративну інформацію. В OSSEC є офіційний веб-інтерфейс, який теж доволі легко інсталюється.

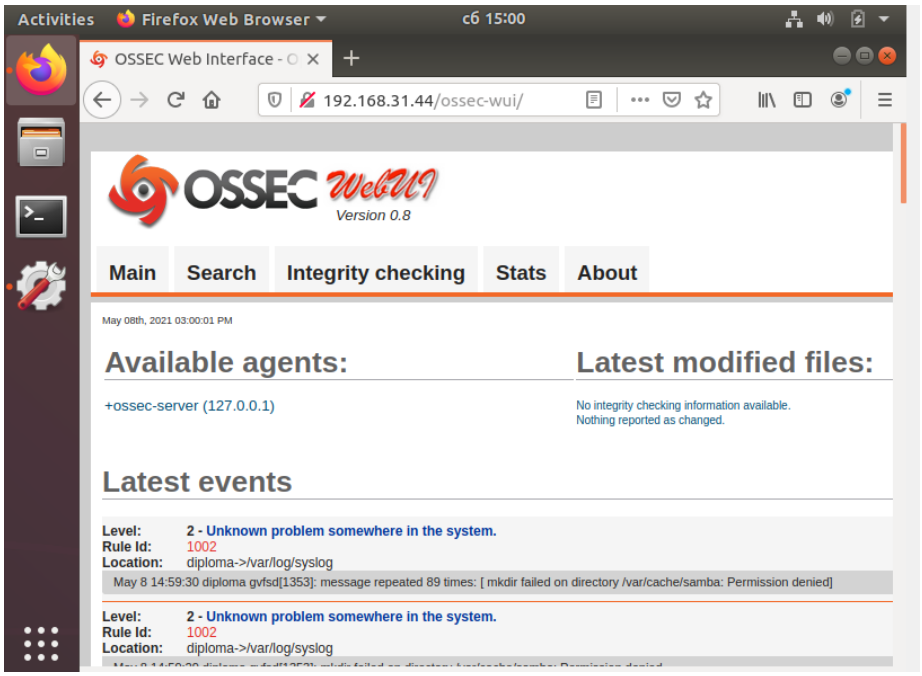

Рис. 2.2. Веб-інтерфейс OSSEC

Open-source Honeypot

Honeypot – це технологія яка виступає приманкою для зловмисника. Такою приманкою в системі може виступати принтер, маршрутизатор, веб-сервер або інший мережевий ресурс, який не взаємодіє з іншими ресурсами мережі. Відсутність взаємодії потрібна для того, щоб будь яка активність цього ресурса виступала як індикатор його компрометації. Honeypot обдурює зловмисника, він вважає, що це частина корпоративної мережі, атакує цю систему, а адміністратор безпеки збирає всю інформацію про цю атаку. Такою інформацію може бути інформація як про зловмисника, наприклад його IP-адреса чи інформація про атаку та методи які були використані при її реалізації.

За метою розгортання Honeypot розділяють на дослідницькі та практичні (виробничі) пастки. Роль дослідницьких пасток в тому, щоб зібрати як можна більше інформації про зловмисника, його поведінку та методи. Практичні Honeypot в своє чергу націлені на виявлення вторгнення, так як їх розгортають в межах реальної корпоративної мережі.

Зазвичай у мережі розгортається декілька пасток в різни сегментах, що збільшує ефективність технології та збільшує вірогідність попадання зловмисника в таку пастку.

3. Cowrie

Cowrie – це SSH/Telnet Honeypot який може виявляти bruteforce та shell атаки. Це рішення допомагає виявляти атаки на сервере обладнання організації, так як симулює реальний сервер, але його компрометація не загрожує організації. Для роботи Cowrie треба завантажити сам продукт та налаштувати SSH підключення. Зазвичай порт SSH з базового 22 заміняють на 22222, а підключення до 22 порту привласнюють 2222 порту Cowrie.

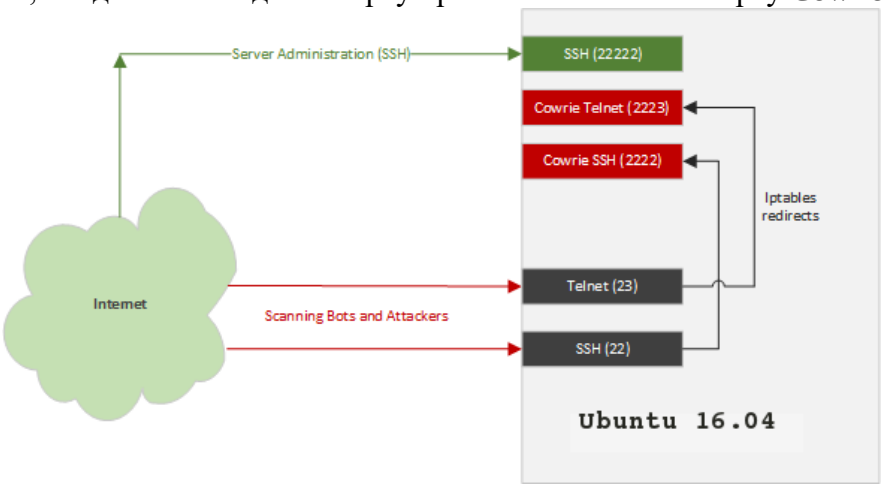

Рис. 3.1. Модель роботи Cowrie

```
# ====================================================================
=
# SSH Specific Options
# ====================================================================
=


# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any IPv4 address
#listen_addr = 0.0.0.0
# (use :: for listen to all IPv6 and IPv4 addresses)
#listen_addr = ::


# Port to listen for incoming SSH connections.
#
# (default: 2222)
listen_port = 22


# SSH Version String
#
# Use these to disguise your honeypot from a simple SSH version scan
# Examples:
```

Рис. 3.2. Налаштування SSH

Cowrie дозволяє своєчасно виявляти вдалі та невдалі спроби підключення зловмисника до мережевого та серверного обладнання, що дає змогу відділу безпеки своєчасно реагувати на інциденти кібербезпеки. Розгортання системи нескладне, однак потребує пильності фахівця який її розгортає.

4. HoneyDrive

HoneyDrive - дистрибутив Linux honeypot, віртуальний модуль (OVA) з встановленою версією Xubuntu Desktop 12.04.4 LTS, що містить більше 10-ти встановлених і попередньо налаштований honeypot'ів, таких як Kippo SSH honeypot, Dionaea і Amun honeypots, Honeyd shell, Glastopf web honeypot і Wordpot, Conpot SCADA / ICS honeypot, PhoneyC і інші. Крім того, він містить багато корисних встановлених скриптів і утиліт для аналізу, візуалізації та обробки даних, які він може захопити, як Kippo-Graph, Honeyd-Viz, DionaeaFR, стек ELK. Також в даній системі є більш ніж 90 відомих інструментів аналізу шкідливих програм, форензік і моніторингу мережі.

Розгортання HoneyDrive дуже просте, так як це віртуальний образ. Також важливо зазначити, що більшість встановлених продуктів система налаштовує автоматично.

Рис. 4.1. Робочий стіл HoneyDrive

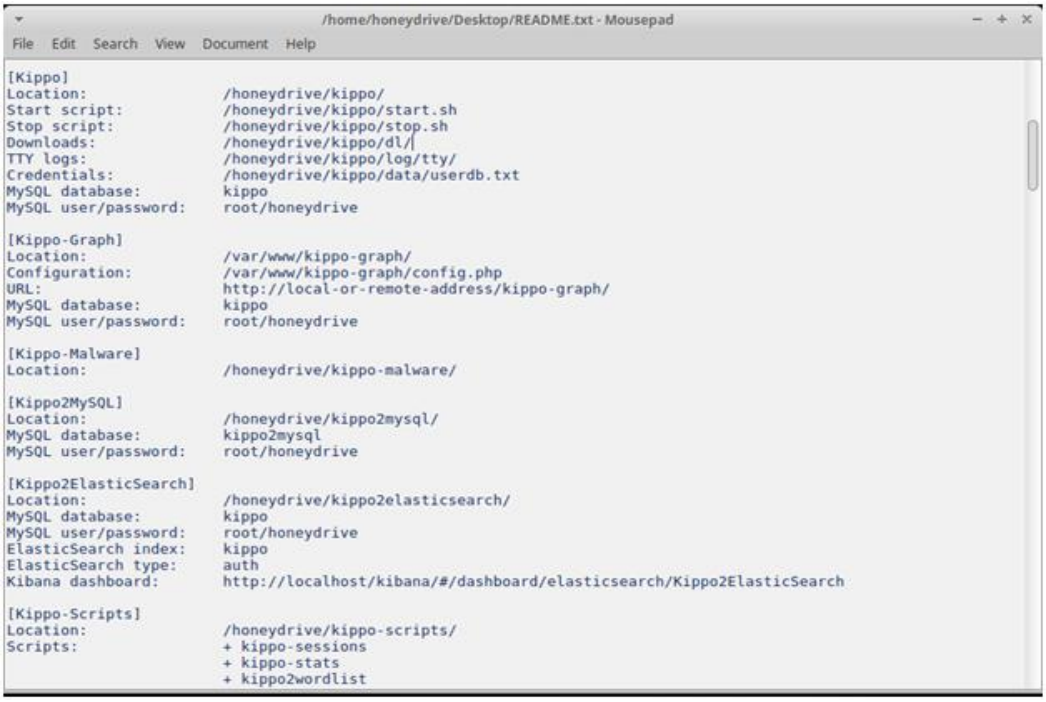

Рис. 4.2. Файл з основною інформацією про продукти в HoneyDrive

Висновки

1. Малий і середній бізнес України є основою економіки і тому є дуже важливим ресурсом нашої країни. Захист інформації в цій сфері є важливою проблемою, вирішення якої повинно турбувати як власників бізнесу так і державу.

2. Кількість кібератак з кожним роком збільшується, що створює нові ризики для бізнесу.

3. В перспективі використання методів виявлення вторгнень з відкритим кодом дозволяє зекономити фізичні та фінансові ресурси організацій.

4. Використання одночасно і мережевих і хостових IDS зменшує ризики реалізації кіберзагроз в мережах організацій.

Технологія Honeypot є гарним доповненням до інших ресурсів комплексних системи захисту інформації.

Перелік посилань

1. 1. Як бізнесу захистити себе від кібератак [Електронний ресурс] – Режим доступу: https://home.kpmg/ua/uk/home/media/press-releases/2020/12/yak-biznesu-zakhystyty-sebe-vid-kiberatak.html.
2. Suricata Documentation [Електронний ресурс] – Режим доступу: https://suricata.readthedocs.io/en/suricata-6.0.0/install.html.
3. Lhotsky B. Instant OSSEC Host-based Intrusion Detection System / Brad Lhotsky., 2013. – 62 с.
4. Cowrie SSH/Telnet Honeypot [Електронний ресурс] – Режим доступу: https://github.com/cowrie/cowrie.
5. Nathalie Weiler. Honeypots for Distributed Denial of Service Attacks // Computer Engineering and Networks Laboratory (TIK), Swiss Federal Institute of Technology ETH Z ¨urich, Switzerland 2002.

Надійшла: 26.01.2021 Рецензент: д.т.н., професор Гайдур Г.І.