International Science Journal of Engineering & Agriculture
2023; 2(6): 31-38
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20230206.04
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Механізми здійснення кібератак та їх аналітичного виявлення

Анастасія Ігорівна Вавіленкова
Кафедра кібербезпеки / Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України, Київ, Україна
ORCID 0000-0002-9630-4951

Олексій Іванович Скіцько
Центр кібербезпеки / Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України, Київ, Україна
ORCID 0000-0003-4122-0889

Артем Андрійович Півень
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України, Київ, Україна

Для цитування цієї статті:
Вавіленкова Анастасія Ігорівна, Скіцько Олексій Іванович, Півень Артем Андрійович. Механізми здійснення кібератак та їх аналітичного виявлення. International Science Journal of Engineering & Agriculture. Vol. 2, No. 6, 2023, pp. 31-38. doi: 10.46299/j.isjea.20230206.04
Надійшла до редакції: 30 жовтня 2023 р.; **Схвалено:** 30 листопада 2023 р.;
Опубліковано: 01 грудня 2023 р.

Анотація: У матеріалах статті піднімається проблема організації інформаційної та кібербезпеки з метою захисту від кіберзлочинців. Авторами проаналізовано два основні способи здійснення DDos-атак: логічний, що полягає у використанні уразливостей програмного забезпечення та дає змогу кіберзлочинцю викликати критичну помилку, яка призведе до порушення працездатності системи, та спосіб надсилання великої кількості пакетів інформації на комп'ютер, що атакується. Автори проводять дослідження для реалізації однієї з найпоширеніших видів атаки SYN flood за допомогою утиліти Kali Linux – Hping3, який обробляє фрагментацію, довільний розмір пакетів, і може бути використана для передачі файлів, інкапсульованих до протоколів, що підтримуються. Для виявлення атаки SYN flood пропонується використати програмне забезпечення Wireshark. Експериментальні дослідження показали доцільність використання аналізатора з подальшим налаштуванням фільтрів для виявлення атак певного виду. Окреслено ключову мету кіберзахисту як не лише запобігання початковій атаці, але й її раннє розпізнавання серед низки інших подій. Окреслено заходи для запобігання кіберзлочинам зокрема, створення комплексних баз даних відомих системних вразливостей і сигнатур атак, встановлення сенсорів раннього попередження та мереж сповіщення, обмін інформацією в кіберрозвідці, створення стандартів керування інформаційною безпекою, а також прийняття нових законів про запобігання кібератакам. Тому чим більша кількість експериментів з виявлення кібератак буде проведена, тим більше напрацювань буде у базі заходів протидії кіберзагрозам.

Ключові слова: кібератаки, кіберзловмисники, Wireshark, утиліта, DDos-атака, експлойт.

1. Вступ

Одним із актуальних на сьогодні завдань продовжує залишатися захист конфіденційних даних, отримання яких є основною задачею кіберзловмисників. До конфіденційної інформації, яка потребує захисту, відносять комерційні таємниці, дані про здоров'я, персональну інформацію, такі дані приватних досліджень, як результати екпериментів, формули, процеси, конфігурації систем та обладнання, програмне забезпечення, продукти авторського права [1]. При цьому процес отримання конфіденційних даних кіберзлочинцями складається із декількох етапів, кожен з яких є підготовчим для наступного, наприклад, початковий доступ можна отримати через фішингові електронні листи, далі отримати доступ до адміністративних документів та облікових записів, застосувати інсталяційні сервери та ін. Тобто для здійснення кібератаки зловмисник повинен зробити масу кроків, виконати цілий алгоритм, що повинен починатися з розвідки для виявлення потенційних цілей за допомогою ексфільтрації чи видалення, високочутливих даних установи. Саме тому для розробки інструментів захисту від кібератак необхідно досконало розуміти механізми здійснення кібератак, а також можливі способи їх відстеження, чому і присвячено матеріали цієї статті.

2. Об'єкт і предмет дослідження

Об'єктом дослідження є процес здійснення DDos-атак. Предметом дослідження є програмні сервіси для реалізації та моделювання атак.

3. Мета та задачі дослідження

Мета даної статті полягає у аналізі роботи основних механізмів здійснення кібератак з використанням утиліт Kali Linux для виявлення їх особливостей та напрацювання заходів захисту.

4. Аналіз літератури

Національний інститут стандартів і технологій США визначає загрозу, як будь-яку подію чи обставину з впливом на діяльність від потенційного до незворотного. До них можна віднести і стихійні лиха, пожежі, несправність обладнання, але найбільше загроз саме у сфері інформаційних технологій спричиняють кібератаки [1].

Також потрібно розрізняти не лише типи даних, що зберігаються на підприємстві, але й розумітися на специфіці їх зберігання. Тому необхідно проводити інвентаризацію даних, систем, де ця інформація зберігається, і засобів безпеки, які є у цих системах. Це перший крок до визначення вразливостей, якими можуть бути помилки в програмному забезпеченні, ненадійна конфігурація пристроїв, політики або процедури, де не розглянуто загрозу належним чином.

Проблеми організації безпеки та різноманітні способи боротьби з кіберзлочинцями стали предметом багатьох міжнародних науково-технічних конференцій [2-4]. У законі України «Про основні засади забезпечення кібербезпеки України» [5] надано визначення основних термінів, що використовуються у сфері кібербезпеки, та основні принципи застосування закону, що дає змогу ідентифікувати ті чи інші дії в області кіберпростору. Основні аспекти захисту інформації також розглядаються такими авторами, як Когут Ю.І., Бурячок В.Л., Аносов В.В. [6-8], що досліджують питання кібервійни та безпеки об'єктів критичної інфраструктури, кіберпростір та основні аспекти кіберзахисту.

Активний кіберзахист також забезпечується Національним інститутом стандартів та технологій (NIST), який провадить діяльність щодо активізації навчання та розвитку персоналу у галуз кібербезпеки [9-10]. Національна освітня ініціатива у сфері кібербезпеки (NICE) під егідою NIST створює програми, сприяє змінам та інноваціям з метою розвитку

персоналу в сфері кіберпростору та подальшого захисту ним держави від існуючих та виникаючих проблем. Проте у час, коли інформаційний простір переобтяжений надлишково інформацією, все важчим стає відокремити потенційно небезпечні дії та симптоми від звичайної поведінки систем та незловмисного програмного забезпечення, адже з появою різноманітних сервісів, створених на основі генеративних моделей штучного інтелекту, потреба у захисті даних експоненційно зросла, адже перевагами використання алгоритмів штучного інтелекту можуть користуватися не лише розробники систем, але й кіберзлочинці. Саме тому дуже важливо вміти розрізняти види можливих атак та знати засоби боротьби з ними.

5. Методи досліджень

Поняття «постійна загроза» означає, що багато організацій здійснюють кібератаки для того, щоб існувати. Ці організації виконують свою роботу і, якщо компанія чи підприємсто є у цілях для атаки, то кіберзлочинців не зупинить антивірус, підбір логіна чи пароля, і вони будуть діяти різними методами для досягнення свої мети. І від того, наскільки швидко та ефективно буде визначено вид акаки, що здійснюється зловмисником, залежить те, нааскільки швидко можна буде їм запобігти та прийняти правильні решення проти конкретної онлайн-атаки. Також під час виявлення кібератак звертають увагу на так звані індикатори кіберзагроз – це конкретні технічні засоби, якими можна користуватися для виявлення можливої зловмисної діяльності. Тобто необхідно моніторити середовище підприємства, певної комп'ютерної мережі, шукаючи будь-який індикатор злому, який вкаже на те, що атака здійснена.

Більшість кібератак виконують за моделлю, подібною до тієї, коли система встановлена, і тоді зловмисники намагаються розуміти, як краще атакувати систему.

Розрізняють два основні способи здійснення DDos-атак.

1. *Логічний спосіб*, що полягає у використанні уразливостей програмного забезпечення, що встановлене на комп'ютері, який атакується, і дає змогу кіберзлочинцю викликати критичну помилку, яка призведе до порушення працездатності системи.

Однією з найнебезпечніших атак, що використовує такий спосіб здійснення DDos-атак, є атака нульового дня – коли розробник дізнається про здайснену атаку лише після того, як вона уже була здійснена через вразливості програмного забезпечення, зад опомогою яких зловмисник зміг створити експлойт нульового дня та застосувати його у зловмисних цілях. Таким чином, атака буде тривати доти, поки розробник не усуне уразливості та не зробить оновлення.

Прикладом такого виду атак є атака у 2017 році на Microsoft Word, коли експлойт нульового дня зламав банківські рахунки [11], атака 2020 року на платформу Zoom, під час якої кіберзловмисники отримали віддалений доступ до ПК через вразливість старішої версії Windows [12] та ін.

Захистом від атак нульового дня є використання інструментів безпеки, вбудованих в операційну систему, використання антивірусів, зменшення поверхні атак, своєчасне встановлення оновлень та чіткий план дій на кожному підприємстві у випадку реалізації загрози атаки нульового дня. Також у контексті можливості у будь-який час застосовувати кіберзлочинцями атаки нульового дня, розрізняють також поняття мережі з нульовим рівнем довіри, яка орієнтується на те, що будь-який пристрій або обліковий запис можуть зламати, тому жодному ресурсу неможна беззастережно довіряти, а тому при будь-якій спробі доступу повинен надаватися дозвіл.

Мережа з нульовим рівнем довіри є одним із засобів, що використовує різноманітні інструменти для здійснення автентифікації особи, що працює з системою. Ще одна проблема для комп'ютерних мереж – це не лише зловживання обліковими записами, коли хтось видає себе за іншого, але й коли пристрій, який є частиною мережі, зламав зловмисник. Покроковий

контроль доступу – це основа моделі системи з нульовою довірою, що обмежує будь-які неочікувані з'єднання.

2. *Спосіб надсилання великої кількості пакетів інформації на комп'ютер, що атакується, або flood*. Такі атаки викликають перевантаження мережі та направлені або на блокування каналів зв'язку та маршрутизаторів (оскільки обсяг даних перевищує об'єм ресурсів для їх обробки, стає неможливим отримання даних від інших користувачів і система відмовляє їм в обслуговуванні), або спрямовані на переповнення ресурсів операційної системи та додатків (змушують систему використовувати обчислювальні потужності не за призначенням).

Так, наприклад, в основі атаки *Ping-of-Death* лежить уразливість протоколу TCP/IP – фрагментація пакетів даних. На комп'ютер жертви надсилається сильно фрагментований ICMP-пакет, розмір якого перевищує допустимий у протоколі, тому під час відновлення пакету, операційна система повністю зависає.

Атака *SYN-flood* – також використовує уразливість протоколу TCP/IP, зокрема, механізм «потрійного рукостискання». Кіберзловмисник надсилає жертві велику кількість пакетів TCP SYN, змушуючи тим самим відкрити TCP-з'єднання та реагувати на них, у свою чергу потім не завершуючи процес встановлення з'єднання, тобто порушуючи таким чином механізм «потрійного рукостискання». В результаті жертва перевантажена та не в змозі встановити з'язок у відповідь на реальні SYN-запити.

6. Результати досліджень

Для реалізації атаки *SYN flood* можна, наприклад, використати сервіс *Hping3* – утиліту *Kali Linux*, яка може надсилати користувацькі TCP/IP-пакети та відображати цілі, як це робить програма *Ping* з відповідями ICMP. *Hping3* обробляє фрагментацію, довільний розмір пакетів, і може бути використана для передачі файлів, інкапсульованих до протоколів, що підтримуються. Для того, щоб почати спрямовувати атаку *TCP SYN Flood* на хост із встановленою операційною системою *Windows 10* (IP-192.168.1.***), потрібно використати таку команду (рис.1):

hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.*

де:

-c – кількість пакетів;

-S – флаг SYN;

-d – розмір байт;

-w – розмір TCP-вікна;

-p – порт;

--flood – флаг для максимально швидкого надсилання;

--rand-source – флаг, який використовується для генерування фейкових IP-адрес, щоб замаскувати реальний IP.

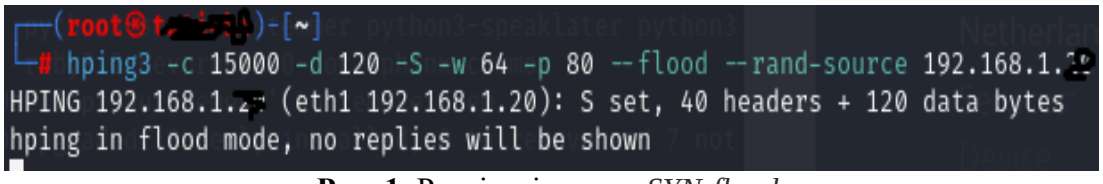

Рис. 1. Реалізація атаки *SYN-flood.*

Для того, щоб виявити атаку *TCP SYN Flood*, потрібно запустити програмне забезпечення **Wireshark**, яке розміщене на базі операційної системи Kali Linux та за допомогою команди «*Start*» виконати захоплення пакетів, які пересилаються у локальній мережі. Далі виявити атаку *TCP SYN Flood* доволі легко, тому що потік TCP-трафіка зростає

різко і в дуже великій кількості. Очевидно, що при SYN-атаці пакети будуть з прапорцем [**SYN**], які отримує атакуючий обчислювальний засіб (рис. 2):

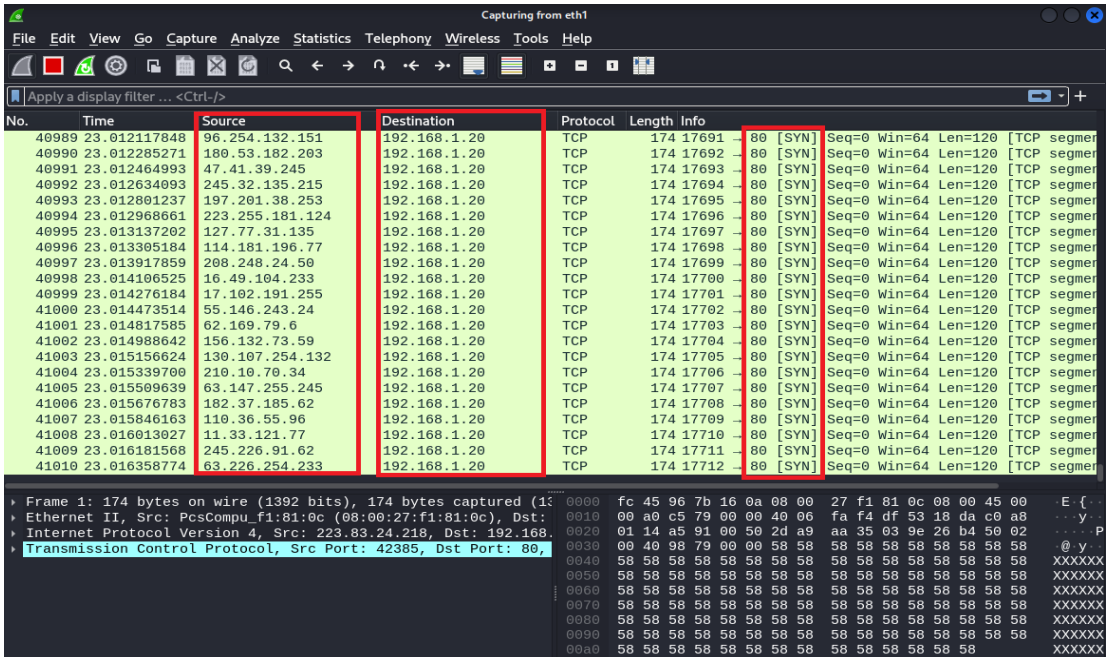

Рис. 2. Виявлення атаки TCP SYN Flood за допомогою утиліти Wireshark.

Для виявлення атаки також можна скористатись окремим фільтром трафіка, який відображає отримання пакетів *SYN* без підтвердження (*ACK*) (рис. 3):

tcp.flags.syn == 1 and tcp.flags.ack == 0

Отримавши інформацію про велику кількість TCP-пакетів з флагами *SYN* без наступного підтвердження на запити від сервера, можна помітити, що усі вони мають різні IP-адреси, але надсилаються на один і той самий порт (в нашому випадку port: 80).

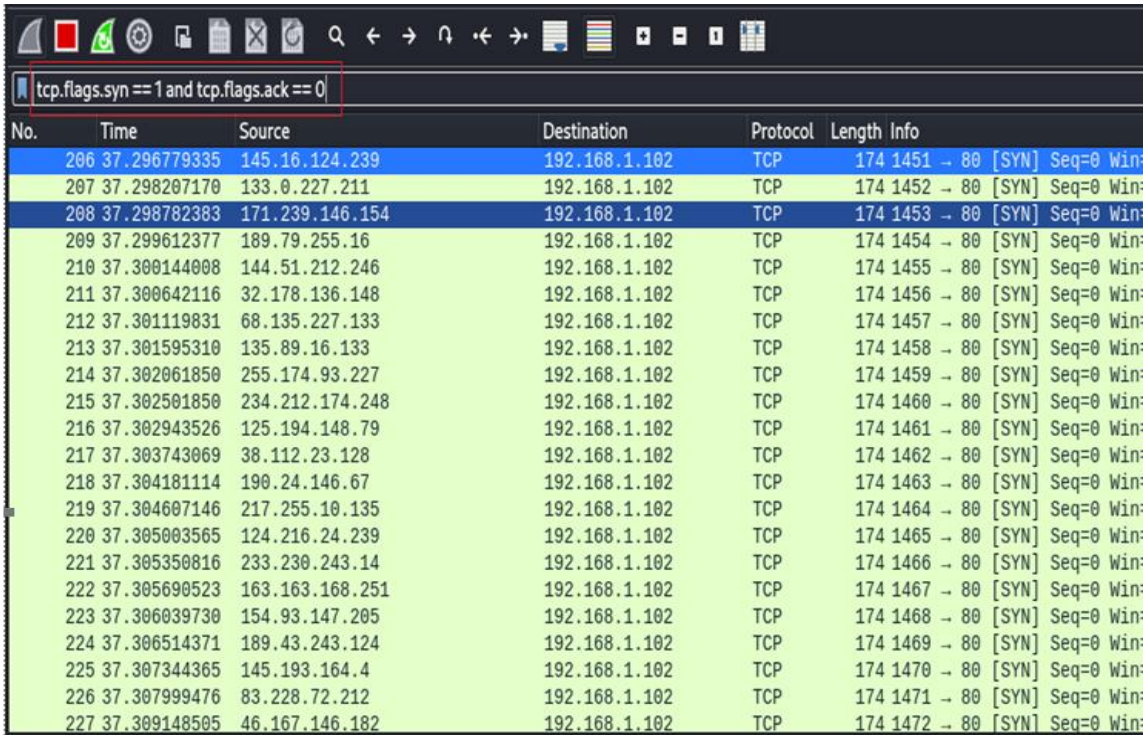

Рис. 3. Виявлення атаки *SYN-flood.*

Наступний фільтр допоможе знайти кількість отриманих пар пакетів від клієнтів (з встановленими прапорцями *SYN*, а після – з прапорцем *ACK*). Це є точною ознакою атаки *TCP SYN Flood* на систему:

tcp.flags.syn == 1 and tcp.flags.ack == 1

Для захисту від атаки типу *SYN flood* можна використовувати брандмауер, який блокує вхідні пакети *SYN.* Ще один варіант – збільшити розмір черги з'єднань та зменшити значення часу очікування з'єднання.

7. Перспективи подальшого розвитку досліджень

Враховуючи специфіку описаних вище способів здійснення DDos-атак, виникає потреба в активному кіберзахисті. Ключовою метою кіберзахисту є не лише запобігання початковій атаці, але й її раннє розпізнавання серед низки інших подій. Є випадки, коли індикатори з'явилися за два роки до виявлення атаки, що призвело до скачування службової інформації, доки вона не була виявлена.

Тому одним із механізмів аналітичного виявлення кіберзагроз є отримання та опрацювання інформації щодо суб'єктів загрози, шкідливих інструментів, технік зловмисних дій та інших деталей, яка допомагає зрозуміти загрози і ризики для підприємства.

Розвідка кіберзагроз – це найкращий спосіб розуміти, які типи загроз можуть бути використані: це опрацьована інформація про суб'єктів загрози, шкідливі інструменти й техніки, що допоможе краще захистити свою мережу, бути озброєним знаннями щодо того, як найімовірніше буде здійснена атака.

Для упередження кібератак створюють спеціальні мережі з нульовим рівнем довіри – це означає, що ставиться припущення про те, що будь-який пристрій або мережа вже можуть бути зламагі, а внутрішня мережа не вважається зоною довіри, жодному ресурсу не можна довіряти, а мережеві підключення не є надійними. Проте для отримання регулярної інформації щодо стану мережі навіть з нульовим рівнем довіри необхідно використовувати спеціальне програмне забезпечення для моніторингу поведінки трафіку у мережі. Таким програмним забезпеченням може служити утиліта Kali Linux – WireShark.

8. Висновки

Для захисту даних також можуть використовуватися апаратні технології: апаратний брандмауер (блокує) блокує небажаний трафік на основі правил, які визначають вхідний і вихідний трафік, дозволений у мережі; спеціалізовані системи виявлення вторгнень (IDS), які виявляють ознаки атак або незвичного трафіку в мережі та надсилають сповіщення; системи запобігання вторгненням (IPS), які виявляють ознаки атак або незвичного трафіку в мережі, генерують попередження і вживають коригувальних дій, а також служби фільтрування контенту, що контролюють доступ і передачу небажаного або образливого вмісту [13-15].

Отже, запобігання кіберзлочинам є складним завданням, яке потребує застосування скоординованих дій, зокрема, створення комплексних баз даних відомих системних вразливостей і сигнатур атак, встановлення сенсорів раннього попередження та мереж сповіщення, обмін інформацією в кіберрозвідці, створення стандартів керування інформаційною безпекою, а також прийняття нових законів про запобігання кібератакам. Тому чим більша кількість експериментів з виявлення кібератак буде проведена, тим більше напрацювань буде у базі заходів протидії кіберзагрозам.

Список літератури:

1) Богуш В. М., Бровко В. Д., Настрадін В. П. (2020). Кіберпростір: основи кібербезпеки та кіберзахисту. Київ: Нац. акад. СБУ, 272 с.

2) Marco Roscini (2023) Cyber Targeting

3) Cyberspace as a Domain of Operations (2023), Tallinn, Estonia

4) Вавіленкова А.І., Душкевич В.С., Лозниця Р.А. (2023). Види налаштувань безпеки комп'ютера: Proceedings of the V International Scientific and Practical Conference «Formation of perceptions of the structure of scientific methodology», 30-31 січня, 2023, Відень, Австрія: InterSci,2023.,С. 47–50.

5) Gpo основні засади забезпечення кібербезпеки України (2017). Закон України від 5 жовтня 2017 року № 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6) Бурячок В.Л., Аносов А. О., Семко В. В., Соколов В. Ю., Складанний П. М. (2019). Технології забезпечення безпеки мережевої інфраструктури. [Підручник] . Київ: КУБГ, 218 с.

7) Когут Ю. І. (2021). Кібервійна та безпека об'єктів критичної інфраструктури: Практ. посібник . Київ: Консалтингова компанія "СІДКОН", 332с.

8) Левченко О. (2021). Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : Монографія / О. Левченко. Житомир : Євро-Волинь, 172с.

9) Вільям Ньюхаус, Стефані Кіт, Бенджамін Скрібнер, Грег Вітте (2017). Національна освітня ініціатива у сфері кібербезпеки (NICE) Загальні принципи управління персоналом у сфері кібербезпеки. Available at: https://qc.csi.cip.gov.ua/storage/files/st/1_NIST.SP.800-181ua_edited%20!!!!.pdf https://doi.org/10.6028/NIST.SP.800-181

10) Гуцалюк М. В., Марущак А. І., Мельник Д. С. (2023) Організаційно-правові основи забезпечення кібербезпеки : Підручник / [та ін.]; За заг. ред. Присяжнюка М.М.Київ: Наук.-вид. відділ НА СБ України, 320с.

11) Курс Cisco Курс мережевої академії Cisco Networking Academy «IT Essentials: PC Hardware and Software». [Електронне джерело]. URL: https://www.netacad.com

12) Юхименко П. (2021). Глобалізація та політика національної безпеки. Підручник, 402 с.

13) Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. (2020). Захист інформації в комп'ютерних системах: підручник. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 236с.

14) Жилін А. В., Шаповал О. М. , Успенський О. А. (2021). Технології захисту інформації в інформаційно- телекомунікаційних системах: навч. посіб. Київ, ІСЗЗІ КПІ ім. Ігоря Сікорського. Вид-во «Політехніка», 213 с.

15) Лісовська Ю.П. (2019). Кібербезпека: ризики та заходи. Кондор, 272 с.

Cyberattack execution mechanisms and their analytical identification

Anastasiia Vavilenkova
Department of Cyber security / Educational and Scientific Institute for Information Security and Strategic Communications, National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID 0000-0002-9630-4951

Oleksii Skitsko
Centre of Cyber security / Educational and Scientific Institute for Information Security and Strategic Communications, National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID 0000-0002-9630-4951

Artem Piven
Educational and Scientific Institute for Information Security and Strategic Communications, National Academy of the Security Service of Ukraine, Kyiv, Ukraine

Abstract: This article addresses the imperative of organizing information and cyber security to counter cyber threats. The authors scrutinize two primary techniques employed in Distributed Denial of Service (DDoS) attacks: the logical approach, utilizing software vulnerabilities to induce critical errors leading to system malfunction, and the inundation of the targeted computer with a substantial volume of information packets. The study focuses on implementing a prevalent form of DDoS attack known as SYN flood using the Kali Linux utility Hping3. This utility accommodates fragmentation, arbitrary packet size, and facilitates the transmission of files encapsulated in supported protocols. For the detection of SYN flood attacks, the authors propose the utilization of Wireshark software. Experimental investigations demonstrate the efficacy of employing the analyzer with subsequent filter configuration for the identification of specific attack types. The primary objective of cyber defense is emphasized as not only thwarting the initial attack but also promptly detecting it amidst a multitude of events. Proactive measures to prevent cybercrimes include the establishment of comprehensive databases containing known system vulnerabilities and attack signatures, the deployment of early warning sensors and notification networks, the fostering of information exchange in cyber intelligence, the formulation of information security management standards, and the enactment of new legislation addressing the prevention of cyberattacks. Consequently, conducting a greater number of experiments focused on cyberattack detection contributes to the development of an extensive repository of countermeasures against cyber threats.

Keywords: cyber-attacks, cybercriminals, Wireshark, utility, DDoS attack, exploit.