https://doi.org/10.15407/intechsys.2025.02.055
УДК 004.7

О.Б. ГОДЛЕВСЬКИЙ, канд. фіз.-мат. наук, старш. наук. співроб.,
Інститут кібернетики імені В.М. Глушкова НАН України,
просп. Акад. Глушкова, 40, м. Київ, 03187, Україна
https://orcid.org/0009-0005-8067-077X
a.godl49@gmail.com

М.К. МОРОХОВЕЦЬ, канд. фіз.-мат. наук, старш. наук. співроб.,
Інститут кібернетики імені В.М. Глушкова НАН України,
просп. Акад. Глушкова, 40, м. Київ, 03187, Україна
https://orcid.org/0009-0008-2191-8677
marina.morokhovets@gmail.com

Н.М. ЩОГОЛЕВА, науковий співроб.,
Інститут кібернетики імені В.М. Глушкова НАН України,
просп. Акад. Глушкова, 40, м. Київ, 03187, Україна
https://orcid.org/0009-0004-4700-7426
natashch2904@gmail.com

АНАЛІЗ ПОШИРЕНИХ ТИПІВ МЕРЕЖЕВИХ АТАК ТА ЧИННИКИ, ЩО УМОЖЛИВЛЮЮТЬ ЇХ УСПІШНЕ ЗДІЙСНЕННЯ

Подано огляд поширених типів мережевих атак. Для кожного типу атак описано джерела та об'єкти атаки, мету та результати атаки, дії, що виконуються для досягнення мети атаки. Для кожного типу атак зазначено, що уможливлює здійснення атак. На базі знайдених відомостей зібрано та класифіковано чинники, що уможливлюють успішне здійснення атак. Окреслено напрями посилення стійкості до мережевих атак.

Ключові слова: *комп'ютерна мережа, кібератака, інформаційна безпека, протоколи інтернету.*

Вступ

Об'єкти мережевого середовища кіберпростору — дані, що передаються в мережі та зберігаються у сховищах, під'єднаних до мережі, прикладні програми, сервери та інші пристрої — загрожені через

Cite: Годлевський О.Б., Мороховець М.К., Щоголева Н.М. Аналіз поширених типів мережевих атак та чинники, що уможливлюють їх успішне здійснення. *Information Technologies and Systems*, Київ, 2025, Том 2 (2), 55–80. https://doi.org/10.15407/intechsys.2025.02.055

зловмисні дії нападників (атаки), які націлені на викрадення й спотворення даних у мережевому просторі, внесення шкідливого вмісту у інформаційні ресурси, що доступні користувачам мережі, та перешкоджання нормальній роботі мережі.

У даній роботі подано огляд поширених типів мережевих атак. Мета роботи — виявити чинники та їх комбінації, що уможливлюють успішне здійснення атак зловмисниками на їх цільові об'єкти. Розробникам та користувачам програм та сховищ даних, що під'єднані до комп'ютерної мережі, знати ці чинники важливо, щоб мати змогу посилювати стійкість до мережевих атак та враховувати те, з чого користаються нападники. Для того, щоб виявити чинники, на базі загальнодоступних джерел проаналізовано ці типи мережевих атак. З урахуванням результатів аналізу окреслено напрями посилення стійкості до мережевих атак.

1. Основні та допоміжні терміни

Визначення атаки на інформаційну систему, кібератаки. Було запропоновано такі визначення атаки на інформаційну систему:

— «напад на систему безпеки, що походить від інтелектуальної загрози, тобто розумової дії, яка є умисною спробою (особливо у сенсі методу або способу) обійти служби безпеки та порушити безпеку системи» [1] (2000 р., Інженерна робоча група Інтернету *(Internet Engineering Task Force)*);

— «будь-яка зловмисна діяльність у намаганнях збирати, порушувати, не давати використовувати, псувати або руйнувати ресурси інформаційної системи чи саму інформацію» [2] (2010 р., Комітет з систем національної безпеки (США) *(Committee on National Security Systems)*).

Було також запропоновано термін «кібератака»:

«атака через кіберпростір, спрямована ініціатором на використання кіберпростору задля порушення, виведення з ладу чи зловмисного контролювання комп'ютерного середовища/інфраструктури або руйнування цілісності даних чи викрадення контрольованої інформації» [2] (2010 р., Комітет з систем національної безпеки (США) *(Committee on National Security Systems)*).

Інформаційна безпека. Основні якості інформаційної безпеки — це так звана КЦД-тріада (*CIA: confidentiality, integrity, availability*) [3]:

К — конфіденційність (щоб *читати* дані та переписку (тобто те, що передається каналами зв'язку), потрібен дозвіл);

Ц — цілісність (щоб *діяти* з даними та каналами зв'язку, потрібен дозвіл));

Д — доступність (користувач *має* доступ до даних та каналів зв'язку).

Мережева атака. У даній роботі йдеться про мережеві атаки. Мережевою атакою називаємо кібератаку, що здійснюється через комп'ютерну мережу.

Під семантикою мережевої атаки розуміємо опис перебігу та результатів атаки. Складниками опису є відомості про: джерело атаки, об'єкт (цільову жертву) атаки, мету атаки, дії, що виконуються для досягнення мети й допоміжні засоби здійснення атаки та її носії, результат атаки.

За наслідками мережева атака призводить до порушення однієї чи кількох складників КЦД-тріади.

Метою нападників, що здійснюють мережеві атаки, є:

— контроль роботи мережі або її складників, а також комп'ютерних служб, під'єднаних до мережі;

— порушення дієздатності мережі або її складників, а також комп'ютерних служб, під'єднаних до мережі.

Допоміжні терміни. Адреса протоколу інтернету, або ІП-адреса (*IP address*, скорочення від *Internet Protocol address*) — числова позначка пристрою, приєднаного до такої комп'ютерної мережі, що використовує для зв'язку набір мережевих протоколів, відомий під назвою *TCP/IP*. Адреса контролю доступу до середовища, або КДС-адреса (*MAC address*, скорочення від *medium access control address*) — унікальний ідентифікатор, приписаний контролеру мережевого інтерфейсу (*NIC*), використовується як мережева адреса для зв'язку в межах сегмента мережі. Сегмент мережі — це ділянка комп'ютерної мережі. Тип та обсяг сегмента залежать від типу мережі та пристрою чи пристроїв, що застосовано для з'єднання кінцевих вузлів. Гост (*host*) — вузол інтернету, який має ІП-адресу.

2. Атака «відмова в обслуговуванні»

Атака «відмова в обслуговуванні» (ВвО, *denial-of-service attack, DoS attack*) [4, 5] — поширений тип мережевих атак, порушує доступність та конфіденційність.

Семантика атаки «відмова в обслуговуванні»

Джерелом атаки є зловмисна особа, яка провадить атаку власноруч за допомогою обчислювальної машини чи іншого технічного пристрою з певною адресою в інтернеті (ІП-адресою) або за допомогою засобів, що уможливлюють проведення атаки автоматизовано.

Об'єктом атаки є або обчислювальна машина чи мережевий ресурс, зокрема, сервер чи вебсторінка, під'єднані до мережі, (атака рівня мережі), або процес (атака рівня застосування).

Метою атаки є порушення чи руйнування дієздатності певної служби, що під'єднана до мережі.

*Дії, що виконуються для досягнення мети атаки***.** Різновиди дій нападника такі:

• захаращення ресурсів жертви:

— нападник надсилає цільовій жертві багато запитів, що потребують відповіді, завантажуючи жертву своїми завданнями до такої міри, що обслуговування нею інших користувачів уповільнюється або блокується;

— нападник надсилає цільовій жертві великі обсяги даних або такі запити, відповіді на які потребують пересилання великих обсягів даних від жертви, через що перевантажується пропускна здатність каналу зв'язку жертви, а це спричиняє уповільнення обслуговування або нездатність обслуговувати інших користувачів;

— нападник ініціює багато з'єднань з цільовою жертвою та підтримує їх напіввідкритими, через що вичерпуються резерви з'єднань з жертвою й вона не може обслуговувати правомірних користувачів;

• сповільнення руху даних:

— нападник надсилає цільовій жертві правомірний запит на пересилання (нападнику) даних великого обсягу, але здійснює читання відповіді вкрай повільно, через що надовго зменшується можливість жертви обслуговувати інших користувачів;

— нападник надсилає цільовій жертві правомірний запит на пересилання (жертві) даних великого обсягу, але пересилає дані вкрай повільно (в обох цих випадках затягування часу руху даних надовго зменшується можливість жертви обслуговувати інших користувачів);

• нападник віддалено адмініструє обладнання цільової жертви (маршрутизатори, принтери, інше обладнання), пошкоджуючи систему жертви до такої міри, що її треба замінити або переустановити обладнання.

Результат атаки:

• для жертви:

— збитки та втрати різного типу (матеріальні, репутаційні тощо) через порушення у роботі служби, що зазнала нападу, або її руйнування;

— отримання стимулів до виявлення джерела нападу та виявлення причин успіху нападу, а також до удосконалення організації служби, що зазнала атаки, та безпекових заходів;

• для нападника:

— роботу певної служби, що під'єднана до мережі, порушено або припинено;

— нападник може далі використати результат атаки як можливість шантажувати жертву, вимагаючи викуп за усунення наслідків нападу.

Перша в історії атака ВвО сталася 6 вересня 1996 р. [6].

Різновидами атаки ВвО є розподілена атака ВвО (distributed denial-of-service attack, *DDoS attack*) та розширена постійна атака ВвО (an advanced persistent *DoS attack*).

2.1. Розподілена атака «відмова в обслуговуванні». Якщо атака ВвО здійснюється одночасно з кількох джерел, то така атака називається розподіленою атакою ВвО [5]. Напад може здійснюватися на кілька об'єктів одночасно. Атака ВвО вважається розподіленою атакою ВвО, коли у ній задіяно більше, ніж 3–5 вузлів різних мереж [7].

Розподілені атаки ВвО здійснюються, зокрема, на хмарні сервіси [8].

Розподілена атака ВвО є більш небезпечною, ніж атака ВвО, позаяк захиститися від неї важче. Масштаби розподілених атак ВвО останнім часом збільшилися й перевищили обсяг 2.3 Тб/сек [9, 10], а також досягли показника 71 млн. запитів на секунду [11].

Розподілені атаки ВвО бувають рівня мережі та рівня застосування (рівня прикладних програм (ПП), доступ до яких забезпечується через мережу). Атаки рівня мережі потужні, але частота їх зменшується [12]. Атаки рівня ПП не мають тенденції до зменшення [12]. Вони потребують менше ресурсів, ніж атаки рівня мережі, але часто супроводжують їх.

Семантика розподіленої атаки ВвО

Об'єкти атаки. Розподілена атака ВвО може мати один чи кілька об'єктів нападу.

Джерелом атаки є зловмисна особа, що провадить атаку за допомогою засобів, що уможливлюють здійснення атаки автоматизовано, або група зловмисників, що здійснюють атаку власноруч чи використовують спеціальне програмне забезпечення (ПЗ).

Способи формування множини джерел атаки:

— формується група людей, учасники якої за домовленістю одночасно починають напад (атаку ВвО) з різних джерел на певну цільову жертву або на сукупність цільових жертв;

— формується група людей, що надають зловмиснику згоду використовувати їхнє обладнання для здійснення атаки;

— формується мережа ботів, тобто група пристроїв, під'єднаних до інтернету, на кожному з яких працює один або кілька ботів (веброботів, тобто прикладних програм, які у великих масштабах запускають автоматизовані завдання через інтернет).

Мета атаки. Мета розподіленої атаки ВвО рівня мережі та сама, що й мета атаки ВвО. Розподілені атаки ВвО рівня ПП здійснюються здебільшого з метою розривання транзакцій та отримання доступу до баз даних. Також метою розподілених атак ВвО може бути спричинення додаткових витрат на боці оператора ПП, який використовує ресурси на основі хмарних обчислень; це робиться, щоб завдати фінансових втрат власнику ПП або зробити його менш конкурентоздатним [8, 13, 14].

*Дії, що виконуються для досягнення мети атаки***.** Це дії, що лежать в основі атак ВвО.

Результат атаки. Розподілені атаки ВвО рівня мережі спричиняють такі самі наслідки для цільових жертв, як й атаки ВвО, але у більших масштабах.

Атаки рівня ПП можуть порушити роботу служб повернення інформації (за запитом замовника) або функції пошуку на вебсайті.

2.2. Розширена постійна атака «відмова в обслуговуванні». Атака цього різновиду (розширена постійна атака ВвО) [15] становить розширену постійну загрозу протягом тривалого періоду. Найдовша відома атака цього типу тривала 38 днів [16].

Семантика розширеної постійної атаки ВвО

Об'єкти атаки. Кілька цільових жертв: одна справжня, основна, решта — другорядні, ними користаються, аби відвернути увагу від нападу на основну.

Джерело атаки. Таке саме, як у розподіленій атаці ВвО.

Мета атаки. Така сама, як й атаки ВвО, розподіленої атаки ВвО.

*Дії, що виконуються для досягнення мети атаки***.**

Розширене зондування (збирання та аналізування перед атакою даних, віднайдених у відкритих джерелах; посилене сканування задля уведення в оману, аби протягом тривалих періодів уникати виявлення).

Здійснення нападу на основну та другорядні жертви, тактичне перемикання між кількома цілями, аби відвернути увагу й ухилитися від захисних заходів.

Здійснення одночасних багатопотокових атак з використанням складних інструментів, що працюють на рівнях 3–7 моделі взаємозв'язку відкритих систем (*Open Systems Interconnection, OSI*) [5], тобто на рівнях від перенесення пакетів даних у мережевому середовищі до контактування з користувачем.

Узгоджене використання засобів протягом усього періоду нападу.

Результат атаки. Ураження основної жертви, порушення у роботі другорядних жертв.

Зазначимо, що відмова в обслуговуванні може виникнути не лише у результаті зловмисних спланованих дій, як-от атаки ВвО чи розподілені атаки ВвО рівня мережі, а також через те, що занадто багато звичайних незалежних один від одного правомірних користувачів починають майже одночасно звертатися до певної служби, перевантажуючи її ресурси.

2.3. Способи здійснення атак ВвО

Атаки ВвО здійснюються:

— навальним нападом, тобто швидко завалюючи об'єкт атаки запитами на обслуговування (діючи «грубою силою»);

— з використанням знань про роботу ПП жертви та мережевих протоколів, аби скласти завдання для жертви, яке буде схоже на правомірне, але виснажуватиме ресурси жертви;

— з використанням шкідливого ПЗ та завдяки користанню з недоліків та вразливостей на боці жертви.

Аби уникнути виявлення системами безпеки з боку жертви нападники вдаються до підроблення адрес відправників у інтернеті (IP-адрес).

Здійснення атаки ВвО грубою силою

Нападник спрямовує на цільову жертву великий за обсягом потік пакетів, захаращуючи ресурси жертви, через що перенасичується пропускна здатність або вичерпуються інші ресурси системи жертви. Напад з багатьох джерел підсилює здатність перенавантажити смугу пропускання. Для атак використовують пакети даних, що перено-

сяться у мережі за допомогою різноманітних протоколів інтернету (*TCP, UDP, ICMP* тощо [5]).

Здійснення атаки ВвО на основі знань про роботу атакованих об'єктів (використання нападником функціональних здатностей жертви чи мережевого обладнання, яким користується жертва)

Користання з автомасштабування

Аби забезпечити гнучкість обслуговування та належну його якість, деякі служби, ПП, що працюють у хмарному середовищі, використовують автомасштабування, тобто механізм збільшення або зменшення застосування (платних) ресурсів залежно від обсягу вхідного потоку даних. Нападник спрямовує на жертву потік даних, поки жертва не збільшить свої ресурси, аби впоратися з цим потоком, після цього нападник призупиняє атаку, а жертва залишається з надмірним ресурсом (який мусить оплачувати). Жертва зменшує ресурс, а нападник відновлює атаку. Хвилі атаки можуть повторюватися. Атакою такого різновиду є атака йо-йо (*уо-уо*) [8, 13, 14]. Жертва потерпає від погіршення якості обслуговування правомірних користувачів у періоди масштабування, а також від фінансових витрат на надлишкові ресурси.

Користання зі способів роботи протоколів інтернету й можливості встановлювати значення параметрів протоколів

Для виснаження ресурсів жертви нападник використовує спосіб роботи протоколу керування передачею (*Transmission Control Protocol*, *TCP* [5]), а саме попередній обмін повідомленнями («рукостискання») у три етапи. Нападник не вимагає завершення процесу рукостискання й намагається виснажити чергу запитів на з'єднання (чергу *SYN*) у пункті призначення або переповнити смугу пропускання сервера. Приклад такої атаки — захаращення *SYN* (*SYN-flooding*) [5]. Нападник створює напіввідкриті з'єднання й таким чином вичерпує доступні з'єднання жертви. Здійснюється атака таким чином. Гост надсилає серверу велику кількість пакетів, часто з підробленою адресою відправника. Кожен з пакетів сервер обробляє як запит на з'єднання, для чого породжує напіввідкрите з'єднання, потім надсилає пакет-відповідь та чекає на відповідь з адреси відправника. Якщо адреса відправника підроблена, відповідь не надходить, а з'єднання залишається відкритим. Зрештою доступні з'єднання сервера вичерпуються, й він не може обслуговувати правомірних користувачів [5].

Щоб вичерпати ресурси жертви, нападник використовує можливість задавати параметри *TCP*. Він надсилає правомірні запити рівня застосування (тобто прикладних програм), але здійснює читання відповідей вельми повільно, через що з'єднання довго залишаються відкритими й резерв з'єднань жертви вичерпується. Щоб затягувати час руху даних, нападник встановлює дуже малий розмір вікна прийому *TCP* й повільно спустошує буфер прийому *TCP*. [17]

Нападник використовує спосіб оброблення запиту *POST* за допомогою мережевого протоколу передавання гіпертекстів *HTTP*. За

запитом *POST* вебсервер має прийняти дані, вміщені у тіло запиту, згідно з обсягом даних, що надано у заголовку запиту. Нападник надсилає правомірний заголовок *HTTP* із запитом *POST*, а далі надсилає тіло повідомлення із вкрай малою швидкістю. Цільовий сервер намагається прийняти повідомлення відповідно до значення параметру «Довжина вмісту» (*Content Length*) у заголовку, що може тривати довго. Нападник ініціює сотні-тисячі таких з'єднань доти, доки усі ресурси для вхідних з'єднань на боці жертви не вичерпаються, через що інші з'єднання унеможливлюються, доки не будуть надіслані усі дані, що почали надсилатися. [18]

Нападник користається з можливості задати тривалість часу існування датаграми (значення поля *TTL* (*time to live*) у заголовку інтернет-пакета). Він надсилає пакети з малим значенням *TTL*. Якщо час *TTL* спливає, пакет відкидається, а ЦП маршрутизатора має сформувати та надіслати відповідь про перевищення часу згідно з мережевим протоколом керування повідомленнями (*Internet Control Message Protocol, ICMP* [5]). Породження великої кількості відповідей може призвести до перевантаження ЦП маршрутизатора [19].

Один з різновидів захаращування та виснажування ресурсів жертви атаки ВвО — це перевищення пропускної здатності каналу зв'язку жертви. Виявилося, що є багато служб (та відповідних протоколів), якими можна скористатися як віддзеркалювачами (тобто засобами, що надсилають відповідь відправнику, навіть тоді, коли він її не потребує) для підсилення атаки на виснаження смуги пропускання. Для низки протоколів обчислено коефіцієнт підсилення (це є спеціальна міра обсягу інформації, що надсилається у відповідь відправнику) [20]. Так, наприклад, у відповіді на запит до сервера *NTP* (*NTP — Network Time Protocol*) з використанням команди *monlist* відправнику надсилаються відомості про сотні гостів, що останнім часом запитували час у сервера *NTP*.

Застосування знань про роботу ПП на боці жертви

Стандартні запити *HTTP* надсилаються цільовому вебсерверу часто, при цьому для оброблення даних запиту потрібні складні процедури, що потребують багато часу, або операції з базами даних, які можуть вичерпати ресурси цільового вебсервера. Прикладом атаки такого типу є атака *CC* [21–23].

Застосування засобів інтернетної телефонії

Засоби інтернетної телефонії (тобто телефонного зв'язку за допомогою протоколу інтернету) дають змогу породжувати (навіть автоматизовано) велику кількість телефонних викликів й використовувати це для атаки ВвО [24, 25].

Здійснення атак ВвО за допомогою шкідливого ПЗ та користання з вразливостей на боці жертви та вразливостей мережевих протоколів

Шкідливе ПЗ у атаках ВвО

Нападник вбудовує засоби здійснення атаки ВвО у шкідливе ПЗ (як-от хробаки, трояни), яке потрапляє у певну систему, а далі атака розпочинається без відома власника цієї системи. Прикладами такого ПЗ є хробак *MyDoom* [26], що запускає атаку у визначений день та час.

Прикладом шкідливого ПЗ, що запускає атаку ВвО, є *Stacheldraht* [27]. Для здійснення атаки ВвО за допомогою *Stacheldraht* зловмисник спочатку уражає шкідливим ПЗ низку систем, що здійснюють оброблення даних, далі використовує клієнтську програму, аби зв'язатися з цими системами, а вони дають команди зомбі-агентам просувати атаку ВвО. У атаці за допомогою *Stacheldraht* нападник користається з вразливостей програм, що обслуговують віддалені з'єднання й працюють на віддалених гостах, що є цільовими жертвами.

Напади рівня ПП (рівня застосування) користаються з дефектів у програмах, що чекають на зв'язок з віддаленими гостами, й використовують програми-пролази (тип шкідливого ПЗ, *exploits*), що можуть змусити ПП, які виконуються на сервері, заповнити дисковий простір чи вичерпати усю доступну пам'ять або час ЦП. Прикладом вірусу, що вичерпує наявні ресурси системи, є *fork-bomb* [28, 29]. Вірус *fork-bomb* містить нескінченний цикл. При роботі вірусу повторно запускається один й той самий процес, що поглинає час ЦП, а також завантажує таблицю процесів операційної системи.

Нападник вдається до автоматизації атакувальних дій. Так, відомий інструмент атаки ВвО *Slowloris* [30, 31]. Атака починається з того, що відкривається з'єднання з цільовою жертвою — вебсервером — та підтримується відкритим якомога довше. Засобом для підтримування відкритого з'єднання є надсилання часткового запиту. *Slowloris* періодично надсилає низки заголовків *HTTP*, не завершуючи запиту. Уражені сервери підтримуватимуть з'єднання відкритими, використовуючи максимально резерв одночасних підключень, через що відмовлятимуть у підключеннях іншим клієнтам.

Заражені шкідливим ПЗ комп'ютери використовуються як пульсуючі зомбі, спрямовані на здійснення періодичних нетривалих захаращень вебсайтів жертви з метою уповільнення їх роботи. Атаки, спрямовані не так на припинення роботи мережевих служб, як на уповільнення роботи мережі або мережевих служб (атаки погіршення обслуговування), важко виявити, вони можуть гальмувати доступ до мережевих служб тривалий час й зрештою значно зашкодити [32].

Атаці з використанням шкідливого ПЗ передує підготовча робота. Спочатку за допомогою шкідливого ПЗ (хробака) нападник інфікує сотні-тисячі пристроїв інтернету речей. Хробак поширюється через мережі та системи, перебираючи контроль над погано захищеними пристроями інтернету речей (як-от термостати, годинники з підтримкою *Wi-Fi*, пральні машини). Власник чи користувач зазвичай не дізнається відразу, що сталося зараження пристрою. Далі заражений пристрій стає складником атаки: коли набирається достатня кількість заражених пристроїв, вони отримують команду

зв'язатися з надавачем послуг інтернету. Тобто спочатку формується мережа ботів (ботнет), а потім цей ботнет атакує жертву. Приклад — шкідливе ПЗ *Mirai* [33], призначене для формування мережі зомбі (ботнету).

Користання з недоліків у проєктуванні систем з метою спричинити самозахаращення жертви

Нападник, аби ініціювати з'єднання, надсилає на відкритий порт цільової жертви пакет *TCP* (пакет, що транспортується за допомогою *TCP*, протоколу керування передачею), що потребує відповіді джерелу, але дані про джерело (ІП-адреса) підроблено таким чином, що вони збігаються з даними пункту призначення, через що цільова жертва (гост) постійно відповідає самій собі. Прикладом такого нападу є атака *LAND* [34, 35]. Здійсненню самозахаращення сприяють недоліки у проєктуванні систем: пристрій має можливість приймати запит на проводові з'єднання, що надходить від цього самого пристрою.

Користання з прорахунків у налаштуванні мережевих пристроїв

Неналежне налаштування мережевих пристроїв використовується у атаці *smurf* [36, 37]: надсилання даних з адресою типу «розсіяна адреса» *(broadcast address)* уможливлює надсилання пакетів усім машинам-гостам певної мережі, а не якійсь конкретній машині. Нападник надсилає багато інтернет-пакетів з підробленою адресою джерела, прописаною як адреса жертви. Більшість пристроїв у мережі за замовчанням відповідатимуть, надсилаючи відповідь на ІП-адресу джерела, через що машина жертви захаращується потоком даних.

Користання з хиб захисних засобів

Нападник користається з недоліків у захисних засобах жертви, через які можливе віддалене адміністрування обладнання жертви (маршрутизаторів, принтерів чи іншого мережевого обладнання). Нападник користається з цих вразливостей, аби змінити прошивку пристрою або пошкодити її. В результаті пристрій стає недієздатним, його потрібно ремонтувати або замінити [38]. Цей прийом застосовується у атаці ВвО. Прикладом ПЗ такого типу є *BrickerBot* [39]; це шкідливе ПЗ спричиняє постійну ВвО пристроїв інтернету речей.

Користання з різноманітних вразливостей на боці жертви та вад мережевих протоколів

За допомогою протоколу користувацьких датаграм (*User Datagram Protocol, UDP*), який не вимагає з'єднання з сервером (це означає, що ІП-адреса джерела не перевіряється, коли запит приймається сервером), нападник може надсилати жертві запити з підроблених ІП-адрес, відповіді на які є значних обсягів. (Про підроблення ІП-адрес див. у розділі 3.)

Для розподіленої атаки ВвО використовувались дефекти у засобах обслуговування однорангових серверів. Зокрема, нападники користались з *DC++* (клієнта однорангового обміну файлами, якого можна застосувати для під'єднання до мережі «Прямого зв'язку»

(Direct Connect) чи до розширеного протоколу прямого з'єднання *(ADC protocol)*), даючи команду клієнтам великих центрів однорангового обміну файлами від'єднатися від їхньої однорангової мережі й натомість приєднатися до вебсайту жертви [40–42].

Користаючись з вразливостей на боці жертви, нападник може спричинити цілочисельне переповнення, маніпулюючи максимальним розміром сегмента (*maximum segment size*) та вибірковим підтвердженням (*selective acknowledgment*) [43, 44].

Користаючись з вади у механізмі короткої перерви під час повторного передавання даних за допомогою протоколу *TCP*, нападник надсилає короткі синхронізовані хвилі потоку даних, аби розірвати *TCP*-з'єднання у каналі зв'язку, яким передаються ці дані [45]. Напад такого зразка названо атакою землерийки *(shrew attack)* [46, 47]: коли клієнт надсилає запити на сервер, зловмисник одночасно надсилає низку запитів на маршрутизатор, змушуючи маршрутизатор призупинити передавання даних; пакети відкидаються під час короткої перерви у передаванні даних *(retransmission timeout, RTO)* (мінімільний рекомендований час перерви 1 сек.); після перерви клієнт повторно передає втрачені пакети, значно сповільнюючи передавання *TCP*. Аби втрутитися у передавання даних клієнта й спровокувати його призупинення, нападник має відслідковувати процес передавання даних клієнта на сервер, тобто діяти як шкідливий посередник (про «шкідливого посередника» див. у розділі 4).

Через помилку у коді збирання фрагментів пакетів *TCP/IP* низки операційних систем сервер неспроможний зібрати фрагментований пакет, якщо нападник надсилає спотворені фрагменти пакету цільовій жертві. Це використано у атаці *teardrop* [48]: нападник надсилає цільовій жертві (серверу) спотворені фрагменти пакету: з перекриттям, з перевищенням корисного навантаження, сервер неспроможний зібрати фрагментований пакет, тому виникає ВвО.

Щоб виснажувати мережі та сервери, нападники використовують вразливості протоколів *UPnP* (*Universal Plug and Play*, сукупність мережевих протоколів, що дають змогу різноманітним пристроям безпосередньо виявляти наявність один одного у мережі та підтримувати мережеве обслуговування [49]). До вразливостей протоколів *UPnP* належать: неправильні стандартні налаштування (налаштування за замовчанням), через які пристрої залишаються відкритими для віддаленого доступу, брак механізму перевірки справжності, вразливості віддаленого виконання коду [50].

Те, що деякі маршрутизатори мають вразливості ПЗ *UPnP*, дає змогу нападнику спрямувати відповіді з порту 1900, через який працює протокол *UPnP*, у напрямку за власним вибором [50–52].

Вразливість протоколу визначення адреси (*Address Resolution Protocol, ARP*) дає можливість нападнику зв'язати свою КДС-адресу з ІП-адресою іншого комп'ютера або пристрою, тобто обманути цей протокол (див. розділ 3).

В результаті призначений справжньому адресату потік даних переспрямовується на адресу зловмисника, через що виникає відмова в обслуговуванні дійсного адресата. У цьому разі відмова в обслуговуванні полягає в тому, що потік даних не доходить до адресата, якому він призначався.

Зазначимо, що інструменти здійснення розподілених атак ВвО виявлено в товарообігу [53].

3. Атаки обману протоколів

Є низка різновидів таких атак, зокрема, обман протоколу визначення адреси (*ARP* spoofing), або «отруєння кешу» *ARP* [54].

Ці атаки порушують конфіденційність.

Протокол виявлення адреси, або ПВА (*Address Resolution Protocol* [55]) призначений для того, щоб дізнатися адресу рівня каналу зв'язку (як-от КДС-адресу), що пов'язана з даною ІП-адресою рівня мережі. Отже, ПВА реалізує відображення множини ІП-адрес у множину КДС-адрес.

Семантика атаки обману ПВА

Джерелом атаки є зловмисна особа, яка провадить атаку в межах деякої локальної мережі, використовуючи або власну обчислювальну машину, або підготовлений до атаки гост з цієї локальної мережі, або за допомогою програмних засобів, що уможливлюють автоматизоване здійснення атаки.

Об'єктами атаки є гости у зоні локальної мережі, зокрема, їхні кеші, де зберігаються повідомлення ПВА, а отже, служби та користувачі, передавання даних між якими здійснюється за підробленими у результаті атаки адресами.

Метою атаки є зв'язування КДС-адреси нападника з ІП-адресою іншого госта, як-от шлюзу, що використовується за умовчанням, аби надалі будь-який потік даних, призначений для цієї ІП-адреси, надсилався нападнику.

Дії, що виконуються для досягнення мети атаки. Нападник надсилає підроблені ПВА-повідомлення в зону локальної мережі.

Результат атаки:

• для жертв:

— витік даних;

• для нападника:

— отримання доступу до потоку даних, що передається каналом зв'язку;

— можливість розпочати атаку «шкідливого посередника», атаку ВвО.

Що уможливлює здійснення атаки обману ПВА.

Атаку можна здійснити лише у мережах, що використовують ПВА, до того у нападника має бути прямий доступ до локального сегменту мережі, на який спрямовано атаку.

Атаці сприяють певні особливості роботи ПВА (вважаються вразливостями ПВА). ПВА застосовується для перетворення адрес шару

мережі (інтернет) на адреси рівня каналу зв'язку. Коли IP-датаграма пересилається від одного госта до іншого у межах локальної мережі, за IP-адресою пункту призначення має бути виявлено КДС-адресу, щоби здійснити передавання даних каналом зв'язку. Коли відома IP-адреса іншого госта й потрібна його КДС-адреса, у локальну мережу у режимі поширення надсилається пакет (*broadcast packet*), так званий ПВА-запит. Машина призначення, IP-адреса якої вказана у цьому ПВА-запиті, відповідає, надсилаючи ПВА-відповідь, що містить КДС-адресу тієї IP-адреси. ПВА є протоколом без збереження стану. Гости у мережі автоматично зберігатимуть у кеші будь-які відповіді ПВА, які вони отримують, незалежно від того, чи були надіслані відповідні запити від цих гостів. Навіть записи ПВА, термін дії яких не вичерпався, будуть затерті, коли надійде новий пакет ПВА-відповіді. У ПВА немає способу, за допомогою якого гост може перевірити справжність однорангового вузла, від якого походить пакет. Отже, обмеженість можливостей ПВА спричиняє вразливість, що уможливлює обманювання ПВА [5, 54, 56].

Нападник може надсилати ПВА-відповідь з IP-адресою деякого пристрою у локальній мережі та підробленою КДС-адресою (як КДС-адресу, відповідну IP-адресі, нападник вказує КДС-адресу свого (контрольованого ним) пристрою), й ця ПВА-відповідь автоматично зберігатиметься у кешах гостів мережі без перевірки справжності відправника.

Зазначимо, що існує низка знарядь, що можуть бути використані для провадження атаки обманювання ПВА (наприклад [57–59]).

4. Атака «шкідливий посередник»

Атаки типу «шкідливий посередник» (атаки ШП, *MITM*, *man-in-the-middle attacks*) [5, 60] порушують конфіденційність та цілісність.

Семантика атаки ШП

Джерелом атаки є зловмисна особа, яка провадить атаку за допомогою обчислювальної машини.

Об'єктами атаки є канал зв'язку (протокол передачі даних), за допомогою якого здійснюється обмін повідомленнями між кореспондентами, а також кореспонденти, що користуються цим каналом для передачі повідомлень.

Метою атаки є несанкціонований доступ до повідомлень, що передаються каналом зв'язку, та перехоплення цих повідомлень.

Дії, що виконуються для досягнення мети атаки [5]**.** Нападник має знати структуру та властивості методу передавання даних, що використовується, а також знати про те, що передавання повідомлення планується. У нападника має бути можливість встановити з'єднання з жертвами. Нападник встановлює з'єднання з кореспондентами (K1, K2), що мають на меті обмінюватися повідомленнями, причому з K1 він з'єднується під виглядом K2, а з K2 — під виглядом K1. Кореспон-

дент К1 надсилає своє повідомлення, вважаючи, що адресатом є кореспондент К2, але насправді повідомлення отримує нападник й чинить з цим повідомленням на свій розсуд: ознайомлюється зі змістом повідомлення, копіює його, вносить зміни у повідомлення. Далі нападник надсилає повідомлення (можливо, модифіковане) кореспонденту К2, який вважає, що відправником є К1.

Результат атаки:

• для жертв:

— витік даних;

— спотворення змісту повідомлень, що їх передають каналом зв'язку;

• для нападника:

– отримання доступу до змісту повідомлень, що передаються каналом зв'язку;

– підміна передаваних повідомлень;

– видалення інформації, що передається каналом зв'язку;

– перенаправлення повідомлення, що передається каналом зв'язку, до пункту, який не передбачався відправником повідомлення;

– зміна параметрів з'єднання між сервером та клієнтом при встановленні між ними з'єднання.

Що уможливлює здійснення атаки ШП.

Наявність можливості контролю інформаційних потоків у системі передавання даних (соціальна мережа, публічний сервіс електронної пошти, система миттєвого обміну повідомленнями належать до публічних засобів комунікації без захисту; власник ресурсу, який забезпечує комунікацію, має контроль над інформацією, якою обмінюються кореспонденти, отже, має потенційну можливість посередництва).

Знаходження нападника у зоні прийому *Wi-Fi* (нападник може втрутитися як ШП у зоні прийому незашифрованої точки доступу безпроводової мережі *Wi-Fi*).

Використання проміжних серверів під час передавання даних (нападник може розбити оригінальне *TCP*-з'єднання на два нових (між собою та клієнтом та між собою та сервером), позаяк не завжди між клієнтом та сервером існує безпосередній зв'язок, у багатьох випадках вони пов'язані через низку проміжних серверів, а деякі з них можуть бути використані зловмисником).

Здійснення атаки ШП на менш безпечні протоколи, наприклад, *SSH*, *IPsec*, *PPTP*.

Обманні дії нападника (нападник намагається уникнути перевіряння справжності кореспондентів, що обмінюються даними (автентифікації); для цього він або користається з недоліків наявних процедур перевіряння справжності, або використовує сертифікат (підтвердження справжності), отриманий шахрайським способом, зокрема, це можливо тоді, коли сам центр сертифікації став жертвою атаки ШП).

Нехтування вимогами інформаційної безпеки з боку користувачів.

Зв'язок між атакою ШП та іншими атаками. Атака ШП уможливлює інші атаки, як-от «впорскування *SQL*» (див. розділ 5), «запуск сценарію, що передається через сайт» (див. розділ 7).

5. Атака «впорскування *SQL*»

Атаки «впорскування *SQL*» (*SQL injection attacks*) [61] порушують конфіденційність, цілісність та доступність.

Перші громадські обговорення «впорскування *SQL*» почалися близько 1998 р. [62].

Семантика атаки «впорскування *SQL*»

Джерелом атаки є зловмисна особа, яка провадить атаку за допомогою обчислювальної машини або за допомогою засобів, що уможливлюють автоматизоване здійснення атаки.

Об'єктом атаки є прикладні програми (застосунки), що керуються даними *(data-driven applications)*, як-от вебсайти, бази даних *SQL* будь-якого типу.

Метою атаки є розкриття даних атакованої системи, псування чи руйнування даних атакованої системи.

*Дії, що виконуються для досягнення мети атаки***.** Загальний план дій нападника: у вхідне поле команд при побудові запиту *SQL* вміщуються шкідливі оператори *SQL (malicious SQL statements)*. Більш детально: оператори *SQL* складаються з даних, що використовуються оператором *SQL*, а також команд, що контролюють те, як виконується оператор *SQL*; нападник так заповнює поля запиту, що після формування запиту з вмісту цих полів у запиті зрештою утворюється шкідлива команда; для цього під час підготовки вхідних даних для запиту у поле даних нападник уводить рядок, що не є даними відповідно до призначення цього поля, а натомість містить команду та/або інструкцію, що зрештою спотворює запит, що мав би будуватися за вхідною формою, тобто нападник використовує поля запиту не за призначенням.

Результат атаки:

- для жертви:
  - витік даних;
  - втрата, спотворення, руйнування даних;
- для нападника:
  - отримання несанкціонованого доступу до даних;
  - здійснення витоку даних;
  - підроблення даних;
  - руйнування даних.

Що уможливлює успіх атаки «впорскування *SQL*». «Впорскування *SQL*» мусить користатися з безпекової вразливості прикладного ПЗ. Приклади такої вразливості:

— вхід користувача ПЗ неправильно фільтрується щодо рядків символів керувальних послідовностей, вставлених у в оператори *SQL*;

— вхід користувача ПЗ не є строго типізованим та виконується несподіваним чином.

Крім описаного «впорскування *SQL*» виявлено також «сліпе впорскування *SQL*» [63].

6. Атака віддзеркалення

Атака віддзеркалення *(reflection attack)* [5] — спосіб нападу на систему «виклик-відгук» підтвердження справжності, яка використовує той самий протокол у обох напрямках, тобто кожна сторона застосовує для підтвердження справжності той самий протокол, що й інша сторона. Ця атака порушує конфіденційність та цілісність.

Семантика атаки віддзеркалення

Джерелом атаки є зловмисна особа, яка провадить атаку власноруч за допомогою обчислювальної машини.

Об'єктами атаки є система підтвердження справжності «виклик-відгук», яка використовує той самий протокол в обох напрямках (тобто кожна сторона застосовує для підтвердження справжності той самий протокол, що й інша сторона), а також сторона (далі — *цільова жертва*, *жертва*), що користується цією системою.

Мета атаки — обманом змусити цільову жертву дати відповідь на виклик самої жертви.

*Дії, що виконуються для досягнення мети атаки***.**

Нападник ініціює з'єднання з цільовою жертвою.

Цільова жертва надсилає виклик ініціатору з'єднання (у випадку атаки віддзеркалення — нападнику), аби перевірити справжність ініціатора з'єднання.

Нападник відкриває інше з'єднання з жертвою й надсилає жертві від себе її виклик.

Жертва відповідає на виклик.

Нападник надсилає жертві відповідь самої жертви через початкове з'єднання (а інше, допоміжне з'єднання, скасовує).

Результат атаки:

• для жертви:

— вступає у контакт з об'єктом, справжність якого насправді не перевірена й не підтверджена;

• для нападника:

— має повністю автентифіковане підключення до каналу.

Що уможливлює здійснення атаки.

Нападник підроблюється під цільову жертву, а на стороні цільової жертви немає засобу виявлення підробки.

7. Атака «Запуск сценарію, що передається через сайт»

Атака «запуск сценарію, що передається через сайт» (*cross-site scripting attack,* атака СПчС, *XSS attack*) [64] є випадком впорскування коду. Порушує конфіденційність та цілісність.

Короткі пояснення термінів

Запуск сценарію, що передається через сайт (СПчС, *cross-site scripting, XSS*) — це тип безпекової вразливості (хиба СПчС), що трапляється у деяких прикладних програмах вебу (вебзастосунках). Термін уведено у 2000 р. [65, 66].

Про вразливості СПчС повідомляли й користалися з них з 1990-х років. Вразливість СПчС дає можливість нападнику вмонтовувати клієнтські сценарії у вебсторінки, які бачать інші користувачі [67].

Більшість фахівців виділяють принаймні два різновиди хиб СПчС: непостійні та стійки [68].

Нестійка (або віддзеркалена) вразливість до СПчС: вебклієнт подає дані (зазвичай у параметрах запиту *HTTP*), на боці сервера здійснюється негайне оброблення даних (граматичний аналіз), результати виводяться на сторінку цього клієнта. Носієм атаки може бути вебадреса *URL* у електронній пошті, вебадреса сайту, якому довіряють, атака можлива через сайт, що має вразливість СПчС.

Стійка (збережена) вразливість СПчС: сервер зберігає дані, які постачає нападник, а потім ці дані відображуються на «нормальних» сторінках, що повертаються користувачам під час звичайного переглядання (вмісту сайту), й при цьому не здійснюється належний захист від можливого шкідливого вмісту *HTML*-тексту (екранування *HTML*).

Семантика атаки СПчС

Джерелом атаки є зловмисна особа, яка провадить атаку власноруч за допомогою обчислювальної машини.

Об'єктами атаки є вебсайт, його користувачі та їхні локальні середовища.

Метою атаки є користання з результатів виконання створеного нападником шкідливого сценарію, впорснутого у носій атаки.

Дії, що виконуються для досягнення мети атаки.

Нападник створює шкідливий сценарій (ШС) та добирає носій атаки. Залежно від того, на яку саме вразливість застосунків розраховує нападник, він добиратиме той чи інший носій атаки.

Нападник впорскує ШС у вираз, що є на позір безпечним й може оброблятися вразливими ПП на боці сервера чи клієнта.

Нападник організовує розміщення шкідливого виразу таким чином, щоб його бачили інші користувачі.

Нападник може застосувати засоби соціальної інженерії, аби спонукати користувача (як цільову жертву) активувати носій атаки (наприклад, натиснути на посилання, що містить шкідливий код).

Результат атаки:

• для жертв:

— користувач — активізує носій атаки;

— вебсервер — містить носій атаки;

— локальне середовище користувача (та користувач) — потерпає від наслідків виконання шкідливого сценарію (ШС) (наприклад, відбувається витік даних користувача, зокрема, секретних);

• для нападника:

— у вебсайт впорснуто шкідливий сценарій (у сторінку вебсайту, яку бачать інші користувачі);

— здобуто доступ до секретних даних користувача (або багатьох користувачів) вебу.

7.1. Що уможливлює здійснення атаки СПчС

Атаки СПчС користаються з відомих вразливостей у ПП вебу (прикладних програмах, доступ до яких здійснюється за допомогою пошуковика вебу), їхніх серверах або системах, що підключаються до цих ПП.

Використовуючи одну з таких вразливостей, нападник вкладає шкідливий вміст у дані, що передаються з підданого небезпеці (через наявну вразливість) сайту. Коли такий комбінований вміст надходить у програму-переглядач на боці клієнта, він є доставленим з надійного джерела і тому працює згідно із дозволами, наданими системі на тому сайті.

Знаходячи способи впорскування шкідливих сценаріїв у вебсторінки, нападник може здобути привілеї доступу до секретного вмісту сторінки, файлів *Cookie* сеансу та іншої інформації, яку програма-переглядач зберігає для користувача.

Коли користаються зі стійкої вразливості СПчС шкідливий сценарій передається автоматично; жертву спеціально не обирають, жертвою виявляється кожен користувач, до якого потрапляє заражена сторінка, а також сайт, через який поширюється сценарій (вразливий сайт).

Носієм впорскування можуть стати будь-які дані, що їх може контролювати нападник, й які надійшли до ПП вебу електронною поштою, від електронних журналів тощо.

7.2. Способи здійснення атак СПчС

Атаки СПчС здійснюються:

— з використанням нестійкої вразливості СПчС;

— з використанням стійкої вразливості СПчС.

Здійснення атаки як віддзеркалення з використанням нестійкої вразливості СПчС

Носієм атаки такого типу є зазвичай електронна пошта або нейтральний вебсайт.

Загальний опис перебігу атаки з віддзеркаленням:

— нападник готує приманку у вигляді вебадреси, яка містить носій СПчС;

— нападник забезпечує розміщення приманки там, де її може побачити цільова жертва (користувач), наприклад, на нейтральному вебсайті, або надсиляє приманку жертві електронною поштою;

— жертва бачить безневинну на вигляд вебадресу *URL*, що вказує на надійний сайт (але ця адреса містить носій СПчС, про що жертва не знає);

— якщо цей (що вважається надійним) сайт має вразливість до носія СПчС, то натискання на посилання може призвести до того, що програма-переглядач жертви виконає впорснутий сценарій.

Приклад перебігу атаки з використанням нестійкої вразливості СПчС [69].

Учасники подій:

— вебсайт (ВС);

— користувач (К), що відвідує ВС;

— нападник (Н), який дізнається, про те, що ВС має нестійку вразливість СПчС (віддзеркалення).

К має змогу зареєструватися на ВС, вказавши своє ім'я та пароль. К може зберігати на ВС свої секретні дані, як-от відомості про рахунки. Коли якийсь користувач реєструється на ВС, програма-переглядач зберігає файли *Cookie* авторизації, а обидві машини (клієнт та сервер) мають запис про те, що цей користувач зареєстрований.

Дії Н та їх наслідки.

1) Н відвідує сторінку «Пошук», тобто сторінку сайту ВС для здійснення пошуку, уводить у відповідне поле пошуковий запит й натискає клавішу, аби подати запит.

Якщо результат не знайдено, на сторінці (що повертається користувачу) буде показано введений пошуковий запит, після якого написано фразу «не знайдено», також з'явиться вебадреса *URL* сайту ВС з відомостями про пошуковий запит.

Якщо запит, наприклад, має вигляд «квіти», то на сторінці з'являється такий текст: «квіти не знайдено», а вебадреса *URL* має вигляд: «*http://BC.org/search?q*=квіти».

Якщо запит має вигляд: «<*script*>*alert*('СПчС');</*script*>», то:

а) з'являється віконце тривоги з написом «СПчС»,

б) на сторінці з'являється фраза «не знайдено», а також повідомляється про помилку з текстом 'СПчС',

в) *URL* має вигляд: «*http://BC.org/search?q*=<*script*>*alert*('СПчС');</*script*>», що свідчить про поведінку ПП сервера, якою може скористатись зловмисник.

2) Н конструює такий *URL*, аби скористатися з виявленої вразливості:

http://BC.org/search?q=квіти<*script%20scr="http://H.com/*ВНС.*js*"></*script*>.

Н може закодувати символи <, >, /, ", щоб можливий читач не зміг негайно розібратися, що ця вебадреса шкідлива.

3) Н надсилає електронний лист якомусь користувачу сайту ВС із закликом «Гляньте-но, які гарні квіти!» та підготовленим посиланням.

4) Цей електронний лист отримує користувач К, який любить квіти і переходить за посиланням. В результаті звернення до ВС у відповідь з'являється фраза «квіти не знайдено», а також діє ярлик сценарію (<*script*>) (на екрані цього не видно) й завантажується та працює шкідлива програма (ВНС.*js*, ВНС — «вельми небезпечний сценарій») нападника Н, запускаючи атаку. К забуває про це (про лист та спробу пошуку цікавинки за посиланням).

5) Програма ВНС.*js* діє у програмі-переглядачеві користувача К так, наче її джерелом є сайт ВС. Вона захоплює копію файлу *Cookie* авторизації К й надсилає її на сервер нападника Н, де Н може її переглядати.

6) Н вміщує файл *Cookie* авторизації К у свою програму-переглядач як свій власний, заходить на ВС й вже зареєстрований як К.

7) Н заходить у розділ рахунків сайту ВС, переглядає номер кредитної картки користувача К та захоплює копію. Далі Н змінює пароль, відтоді К не може зареєструватися.

Кінець прикладу.

Здійснення атаки СПчС з використанням стійкої вразливості СПчС

Загальний опис перебігу атаки з використанням стійкої вразливості СПчС:

— нападник приєднується до сайту С, де користувачі можуть виставляти (розміщувати) повідомлення у форматі *HTML*, аби інші користувачі могли їх прочитати; нападник має свій профіль (короткий біографічний начерк) на цьому сайті;

— нападник пише сценарій, призначений для запуску з програм-переглядачів інших користувачів, коли вони відвідують його профіль на сайті С; сценарій призначено для викрадення персональних даних користувачів, що зберігаються на сервері сайту С.

— коли нападник отримує запит від деякого користувача сайту С, він дає на нього принагідну відповідь, але у кінці своєї відповіді вміщує свій шкідливий сценарій; якщо цей сценарій вміщено у структурний елемент <*script*>, він не з'являтиметься на екрані.

— коли якийсь користувач К, зареєстрований на сайті С, переглядає профіль нападника, у якому міститься відповідь зі шкідливим сценарієм, цей сценарій виконується автоматично програмою-переглядачем користувача К й викрадає копію персональних даних К безпосередньо з машини К й надсилає швидке повідомлення на сервер нападника, що збирає ці дані.

Приклад перебігу атаки з використанням стійкої вразливості СПчС [69].

Учасники подій: нападник (Н), вебсайт (ВС), користувач (К).

1) Н отримує для себе обліковий запис на сайті ВС.

2) Н завважує, що ВС має стійку вразливість СПчС: якщо хтось заходить у розділ новин й розміщує коментар, ВС покаже усе, що введено. Якщо текст коментаря містить ярлики *HTML*, вони будуть додані до того, що було на вебсторінці спочатку, зокрема, будь-які ярлики сценарію запрацюють, коли сторінка завантажується (коли її хтось переглядає).

3) Н читає статтю у розділі новин і вводить такий, наприклад, коментар:

«Мені у цій оповіді сподобалися півники. Вони такі кумедні! <*script scr="http://H.com/*ВНС.*js*">».

4) Коли К (або хтось інший) завантажує сторінку з коментарем, працює ярлик сценарію нападника Н та викрадає файл *Cookie* авторизації К й надсилає його на сайт нападника Н.

5) Н тепер може відібрати у К сеанс та видавати себе за К.

Кінець прикладу.

Різновидами СПчС є видозмінений СПчС [70] та запуск сценарію на основі Об'єктної моделі документа (ОМД, *Document Object Model, DOM*) [71].

Запуски сценаріїв, що передаються через сайт, виконані на вебсайтах, становили приблизно 84 % усіх безпекових вразливостей, засвідчених *Symantec* до 2007 р. [72].

Підсумки та висновки

За допомогою аналізу поширених типів мережевих атак виявлено, що для здійснення цих атак нападники користаються з:

1) навального нападу (атаки ВвО);

2) функційних можливостей ПП жертви чи мережевого обладнання (атаки ВвО);

3) недоліків у проєктуванні мережевого ПЗ та ПП, що працюють на боці клієнта чи сервера, зокрема, з браку перевірок даних, що надходять на вхід ПП (атаки: ВвО, обману ПВА, ШП, впорскування *SQL*, СПчС, віддзеркалення);

4) прорахунків у налаштуванні мережевих пристроїв (атаки ВвО);

5) хиб або браку захисних засобів (атаки: ВвО, ШП);

6) вразливостей мережевих програм, зокрема, помилок у коді (атаки: ВвО, СПчС);

7) наявності проміжних засобів з'єднання (атаки ШП);

8) шкідливого ПЗ (атаки ВвО);

9) нехтування вимогами інформаційної безпеки з боку користувачів (атаки ШП);

10) соціальної інженерії (атаки СПчС).

Отже, в арсеналі нападників є: навальний напад , шкідливе ПЗ, знання про різноманітні вразливості та прорахунки на боці жертви, засоби соціальної інженерії, докладне знання про те, як функціонує мережеве обладнання та ПЗ жертви. Найбільша кількість виявлених чинників пов'язана з атаками типу ВвО, а чинник 3 пов'язаний з усіма розглянутими типами атак. Зазначимо, що завдяки обізнаності про роботу мережевого обладнання та ПП, що під'єднані до мережі, нападники мають можливість здійснювати атаки, поводячись при цьому стосовно протоколів мережі та стосовно атакованих служб як правомірні користувачі й навіть не шукаючи хиб захисних засобів чи вразливостей ПЗ на боці жертви.

У відповідь на напад суб'єкт на боці жертви атаки може здійснити: пошук джерел нападу, виявлення причин успіху нападу, вдосконалення організації служби, що зазнала атаки, та посилення безпекових заходів.

Зазначимо, що попри безпосереднє реагування на кожен конкретний випадок атаки того чи іншого типу розробникам ПЗ, що призначено для роботи в мережі, доцільно уживати перспективних заходів, що сприяли б стійкості до мережевих атак, враховуючи те, з чого користаються нападники.

З огляду на те, що чинник 3 (користання з недоліків у проєктуванні мережевого ПЗ та ПП, під'єднаних до мережі) пов'язаний з усіма розглянутими типами атак, виходить, що винятково важливим напрямом посилення стійкості до мережевих атак, розглянутих в цій роботі, є удосконалення розроблення проєктів ПЗ мереж та ПП, що працюють у мережі, аби запобігти появі вразливостей, якими можуть скористатися зловмисники. Зокрема, на наш погляд, проєктувальнику слід забезпечувати повноту побудувань, як-от:

— визначати ознаки «правильних» та «неправильних» даних, що надходять на вхід програмних складників мережі або є результатом їхньої роботи;

— визначати ознаки нормальних та аварійних ситуацій перебігу процесів у мережі;

— розробляти засоби контролю даних та мережевих процесів;

— розробляти засоби оброблення аварійних ситуацій.

З огляду на роль людського фактору у здійсненні атак важливою для протистояння мережевим атакам є обізнаність користувачів мережі щодо вимог інформаційної безпеки та щодо загроз з боку засобів соціальної інженерії.

Важливий напрям убезпечення від мережевих атак — удосконалення наявних та розроблення новітніх систем забезпечення комп'ютерної безпеки. Зокрема, є потреба у тому, щоб вміти відрізнити розподілену атаку ВвО на службу, під'єднану до мережі, від раптового сплеску звернень правомірних користувачів до цієї служби. Тобто йдеться про те, щоб розпізнати атаку на службу у разі, коли кількість звернень до неї раптово й незвичайно збільшується.

ЛІТЕРАТУРА / REFERENCES

1. Shirey, R. Internet Security Glossary. URL: https://www.rfc-editor.org/info/rfc2828 [Accessed May. 2000]
2. Information Security. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
3. NIST Special Publication 1800-26A. URL: https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html
4. Understanding Denial-of-Service Attacks. URL: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks
5. Computer networks / Andrew S. Tanenbaum, David J. Wetherall. — 5th ed.. URL: https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf
6. Distributed Denial of Service Attacks. *The Internet Protocol Journal,* Vol. 7 (4). URL: https://web.archive.org/web/20190826143507/https:/www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

7. DDoS Mitigation using Cumulus Linux. URL: https://www.hyperscalers.com/how-to-implement-DDoS-mitigation-cumulus-linux-bare-metal-switches-BMS-100G-networking
8. Mor Sides, Anat Bremler-Barr, Elisha Rosensweig. Yo-yo attack: vulnerability in auto-scaling mechanism. *SIGCOMM – 15: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 103–104. https://doi.org/10.1145/2785956.2790017
9. Amazon 'thwarts largest ever DDoS cyber-attack' 18 June 2020. *BBC Newsб, Jun 18, 2020. URL:* https://www.bbc.com/news/technology-53093611
10. AWS Security Blog. AWS Shield Threat Landscape report is now available. By Mário Pinho, 29 May. 2020. URL: https://aws.amazon.com/blogs/security/aws-shield-threat-landscape-report-now-available
11. The Cloudflare Blog. Cloudflare mitigates record-breaking 71 million request-per-second DDoS attack 2023-02-13. By Omer Yoachimik, Julien Desgats, Alex Forster. URL: https://blog.cloudflare.com/cloudflare-mitigates-record-breaking-71-million-request-per-second-ddos-attack
12. The Cloudflare Blog. The New DDoS Landscape 2017-11-23 By Junade Ali. URL: https://blog.cloudflare.com/the-new-ddos-landscape
13. Kubernetes Autoscaling: YoYo Attack Vulnerability and Mitigation. Ronen Ben David, Anat Bremler Barr. URL: https://arxiv.org/abs/2105.00542
14. Xiaoqiong Xu, Jin Li, Hongfang Yu, Long Luo, Xuetao Wei, Gang Sun. Digital Towards Yo-Yo attack mitigation in cloud auto-scaling mechanism. Communications andNetworks,2020,Vol. 6 (3),369–376.https://doi.org/10.1016/j.dcan.2019.07.002
15. Video games company hit by 38-day DDoS attack. *Gold, Steve (21 August 2014).SC Magazine UK. URL:* https://web.archive.org/web/20170201181833/https:/www.scmagazineuk.com/video-games-company-hit-by-38-day-ddos-attack/article/541275
16. 38-Day Long DDoS Siege Amounts to Over 50 Petabits in Bad Traffic. URL: https://news.softpedia.com/news/38-Day-Long-DDoS-Siege-Amounts-to-Over-50-Petabits-in-Bad-Traffic-455722.shtml
17. Slow Read DDoS Attacks. URL: https://www.netscout.com/what-is-ddos/slow-read-attacks
18. Slow Post Attacks. URL: https://www.netscout.com/what-is-ddos/slow-post-attacks
19. TTL Expiry Attack Identification and Mitigation. URL: https://sec.cloudapps.cisco.com/security/center/resources/ttl_expiry_attack.html
20. UDP-Based Amplification Attacks. URL: https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks
21. What Is a CC Attack? URL: https://support.huaweicloud.com/en-us/antiddos_faq/antiddos_01_0020.html
22. The method of defence CC attack, Apparatus and system. URL: https://patents.google.com/patent/CN106161451A/en
23. CC (Challenge Collapsar) attack protection method and device. URL: https://patents.google.com/patent/CN106330911A/en
24. Voice over IP. URL: https://www.cse.wustl.edu/~jain/cis788-99/h_8voip.htm
25. Voice over IP: Protocols and Standards, Rakesh Arora. URL: https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols
26. [Review] MyDoom Virus: The Most Destructive & Fastest Email Worm. URL: https://www.minitool.com/backup-tips/mydoom-virus.html?amp
27. Geoffrey Cheng. Analysis on DDOS tool Stacheldraht v1.666. URL: https://www.giac.org/paper/gcih/229/analysis-ddos-tool-stacheldraht-v1666/102150
28. Fork bomb. URL: http://catb.org/~esr/jargon/html/F/fork-bomb.html
29. The Jargon File, Version 4.2.2, 20 Aug 2000. **Editor**: Eric S. Raymond, Guy L. Steele. URL: https://www.gutenberg.org/cache/epub/3008/pg3008-images.html
30. Slowloris DDoS attack. URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris

31. Slowloris attack. URL: https://www.invicti.com/learn/slowloris-attack
32. Degradation of Service Attack. By Editorial Staff. URL: https://www.devx.com/terms/degradation-of-service-attack/#:~:text=A%20Degradation%20of%20Service%20Attack%20is%20a%20type%20of%20cyber,to%20access%20for%20legitimate%20users
33. Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, Jeffrey Voas. DDoS in the IoT: Mirai and Other Botnets. Computer, 2017, Vol. 50 (7), 80–84. https://doi.org/10.1109/MC.2017.201
34. LAND Attacks. URL: https://www.imperva.com/learn/ddos/land-attacks/#:~:text=A%20LAND%20Attack%20is%20a,processed%20by%20the%20TCP%20stack
35. Understanding LAND Attacks: Risks and Mitigation. URL: https://www.indusface.com/learning/land-attacks
36. Tfreak. URL: https://hackepedia.org/?title=Tfreak
37. What is a Smurf DDoS attack? By Martin Pramatarov. URL: https://www.cloudns.net/blog/what-is-smurf-ddos-attack
38. Permanent Denial-of-Service Attack Sabotages Hardware. By Kelly Jackson Higgins. URL: https://web.archive.org/web/20081208002732/http:/www.darkreading.com/security/management/showArticle.jhtml?articleID=211201088
39. "BrickerBot" Results In Permanent Denial-of-Service. URL: https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service
40. Prolexic Distributed Denial of Service Attack Alert. URL: https://web.archive.org/web/20070803175513/http:/www.prolexic.com/news/20070514-alert.php
41. Peer-to-peer networks co-opted for DOS attacks. *Robert Lemos. URL:* https://www.theregister.com/2007/05/30/p2p_dos_attacks
42. Denying distributed attacks. *Fredrik Ullner. URL:* https://dcpp.wordpress.com/2007/05/22/denying-distributed-attacks
43. SACK Panic and Other TCP Denial of Service Issues. URL: https://web.archive.org/web/20190619100453/https:/wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SACKPanic
44. CVE-2019-11479. URL: https://web.archive.org/web/20190621224631/https:/cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11479
45. Yu Chen, Kai Hwang and Yu-Kwong Kwok, «Filtering of shrew DDoS attacks in frequency domain,» *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)l*, Sydney, NSW, Australia, 2005, 8–793. https://doi.org/10.1109/LCN.2005.70
46. Vinicius de Miranda Rios, Pedro R M Inacio, Damien Magoni, Mario M Freire. Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey. *IEEE Access*, 2022, Vol. 10, 76648–76668. https://doi.org/10.1109/ACCESS.2022.3191430
47. Kuzmanovic, Aleksandar, Knightly, Edward W. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. *ACM. Conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM'03*, August 25–29, 2003, Karlsruhe, Germany, *75–86*. https://doi.org/10.1145/863955.863966
48. CERT Advisory CA-1997-28 IP Denial-of-Service Attacks. URL: https://vuls.cert.org/confluence/display/historical/CERT+Advisory+CA-1997-28+IP+Denial-of-Service+Attacks
49. UPnP Forum. UPnP Specifications Named International Standard for Device Interoperability for IP-based Network Devices. URL: https://web.archive.org/web/20140401035712/http://upnp.org/news/documents/UPnPForum_02052009.pdf
50. New DDoS Attack Method Demands a Fresh Approach to Amplification Assault Mitigation by Avishay Zawoznik, Johnathan Azaria, Igal Zeifman. URL: https://www.imperva.com/blog/archive/new-ddos-attack-method-demands-a-fresh-approach-to-amplification-assault-mitigation

51. Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS. By Marek Majkowski. URL: https://blog.cloudflare.com/ssdp-100gbps
52. How does a SSDP Attack work? URL: https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack
53. Stress-Testing the Booter Services, Financially. URL: https://krebsonsecurity.com/2015/08/stress-testing-the-booter-services-financially/
54. ARP Cache Poisoning (Gibson Research Corporation). URL: https://www.grc.com/nat/arp.htm
55. David C. Plummer. An Ethernet Address Resolution Protocol — or — Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. URL: https://datatracker.ietf.org/doc/html/rfc826
56. ARP Vulnerabilities: The Complete Documentation. URL: https://web.archive.org/web/20110305160956/http:/www.l0t3k.org/security/tools/arp/
57. APE — The ARP Poisoning Engine. URL: https://web.archive.org/web/20120709235815/http:/www.megapanzer.com/2012/04/11/ape-the-arp-poisoning-engine/
58. Windows 10 ARP Spoofing with Ettercap and Wireshark. URL: https://cybr.com/cybersecurity-fundamentals-archives/windows-10-arp-spoofing-with-ettercap-and-wireshark/
59. Richard Dezso. How to Perform an ARP Poisoning Attack. May 13, 2024. URL: https://www.stationx.net/how-to-perform-an-arp-poisoning-attack/
60. Fact Sheet: Machine-in-the-Middle Attacks . URL: https://www.internetsociety.org/resources/doc/2020/fact-sheet-machine-in-the-middle-attacks/
61. SQL Injection. URL: https://learn.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms161953(v=sql.105)?redirectedfrom=MSDN
62. *Michael Kerner*. How Was SQL Injection Discovered? *URL:* https://www.esecurityplanet.com/networks/how-was-sql-injection-discovered/
63. OWASP. *Blind SQL Injection*. URL: https://owasp.org/www-community/attacks/Blind_SQL_Injection
64. Kirsten S. OWASP. Cross Site Scripting (XSS). URL: https://owasp.org/www-community/attacks/xss/
65. Happy 10th birthday Cross-Site Scripting! URL: https://learn.microsoft.com/en-ca/archive/blogs/dross/happy-10th-birthday-cross-site-scripting
66. 2000 CERT Advisories. URL: https://insights.sei.cmu.edu/documents/507/2000_019_001_496188.pdf
67. *Leyden John*. Facebook poked by XSS flaw. *URL:* https://www.theregister.com/2008/05/23/facebook_xss_flaw/
68. Cross Site Scripting. URL: http://projects.webappsec.org/w/page/13246920/Cross%*20Site*%20Scripting
69. XSS Attack Examples (Cross-Site Scripting Attacks) by Lakshmanan Ganapathy on February 16, 2012. URL: https://www.thegeekstuff.com/2012/02/xss-attack-examples/
70. What is Mutation XSS (mXSS)? URL: https://kpmg.co.il/technologyconsulting/blog/what-is-mutation-xss-mxss
71. Types of XSS. URL: https://owasp.org/www-community/Types_of_Cross-Site_Scripting
72. Symantec Internet Security Threat Report Trends for July–December 06 Vol. 11, 2007. URL: https://docs.broadcom.com/doc/istr-07-march-en

Отримано / Received: 19.12.2024

A.B. Godlevsky, PhD (Phys.-Math.), Senior Researcher,
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0005-8067-077X
a.godl49@gmail.com

M.K. Morokhovets, PhD (Phys.-Math.), Senior Researcher,
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0008-2191-8677
marina.morokhovets@gmail.com

N.M. Shchogoleva, Researcher,
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0004-4700-7426
natashch2904@gmail.com

ANALYSIS OF COMMON TYPES OF NETWORK ATTACKS,
AND FACTORS ENABLING THEIR SUCCESSFUL IMPLEMENTATION

Introduction. A survey of common types of network attacks, i.e. cyberattacks carried out through a computer network, is presented. The purpose of the work is to expose factors enabling attacks to be fulfilled successfully.

Methods. To expose the factors, common types of network attacks were analysed on the basis of sources open to general use.

Results. As a summary, it was found out that attackers have in their arsenal: brute force, malicious software, knowledge on various vulnerabilities and flaws on a victim's side, social engineering tools, and detailed knowledge on how both network equipment and victim's software function. It is significantly that due to their knowledge on how network equipment and applications connected to a network function attackers can realize their malicious intentions while behaving themselves as legitimate users regarding the network protocols and regarding the attacked services and without even looking for flaws in the protective resources or software vulnerabilities on the victim's side. It turned out, that such factor as flaws in network software designing relates every type of attack considered.

Conclusions. Taking into account the results of the analysis, the directions of intensifying the resilience to network attacks are outlined: improving the working out of projects of network software and applications that operates in a network in order to prevent arising vulnerabilities which attackers can exploit; improving the existing computer security systems and developing novel ones; network users' conversance with information security requirements and the threats of social engineering means.

Keywords: *computer network, cyberattack, information security, Internet protocols.*