СЕКЦІЯ XVII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРАТАК НА МЕРЕЖЕВІ РЕСУРСИ

Михайленко Дмитро Денисович
студент факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Науковий керівник: Мелкозьорова Ольга Михайлівна
ORCID ID: 0000-0002-1134-2925
канд. техн. наук, доцент кафедри безпеки інформаційних систем і технологій
Харківський національний університет імені В.Н. Каразіна, Україна

Забезпечення потрібного рівня кібербезпеки при експлуатації інформаційно-телекомунікаційних систем є критично важливим напрямом діяльності в сучасному, технологічно залежному світі. Загроза кібератак стала постійною проблемою, як для окремих Інтернет користувачів, так і для корпоративних інформаційних ресурсів підприємств і державних структур. Сучасні кіберзловмисники постійно вдосконалюють тактику і методики нападу для крадіжки конфіденційної інформації, компрометації цільових систем і максимальної нанесення шкоди виробничим та бізнес процесам жертви.

Оскільки залежність сучасного інформаційного суспільства від технологій продовжує лише зростати, то вкрай важливо своєчасно робити відповідні кроки, стосовно розуміння сутності і способів реалізації відомих кібератак [1-3], щоб прогнозувати можливі дії в напряму нейтралізації потенційних загроз безпеки, на послідуючої ітерації їх розвитку. Така робота охоплює ретельний аналіз загальних властивостей різних типів атак та постійне вдосконалення існуючих технологій і методик їх використання для своєчасного реагування на інциденти інформаційної безпеки (ІБ) різної природи, масштабів і наслідків [4-5].

В межах даного матеріалу проведено стислий розгляд найбільш часто використовуваних різновидів кібератак на мережеві корпоративні ресурси (далі Web-ресурси), та огляд відповідних заходів для їх протидії.

За даними *FireEye Labs* [6] найчастіше, хакерські атаки зачіпають такі галузі як: - фінансові установи, телекомунікації, виробництво і страхування. А відповідний звіт від *Positive Techonologies* [7], декілька доповнює даний перелік, додатково поширюючи його на такі галузі, як: - державні установи, освіта та медицина, відзначаючи, при цьому, що біля 67% відомих атак, мали яскраво виражений цілеспрямований характер. Атаки можуть бути націлені на широке коло потенційних жертв, від окремих користувачів до інформаційних систем підприємств та/або урядів.

При цьому під час атак на корпоративні ресурси метою атакуючих, зазвичай, є блокування штатних умов і режимів роботи інформаційних систем жертви, доступ до чутливих (конфіденційних) інформаційних ресурсів компанії, таких як інтелектуальна власність, дані клієнтів та дані платежів тощо. Серед найчастіше використовуваних кіберзловмисниками різновидів атак, особливе місце посідають наступні:

1. *Відмова в обслуговуванні* (або *DoS*) - набір дій, що призводить до підвищення навантаження на Web-ресурс, що досягається за рахунок надсилання великої кількості запитів на сервер-жертву. Метою такої атаки є свідоме перевантаження сервера, що або тимчасово виводить ресурс з ладу, або ускладнює виявлення подальших дій атакуючої сторони. Для нарощування атаки може використовуватися відповідні кластерні структури наперед підготовлених мережевих вузлів (ботів), які посилають запити на джерело (*DDoS*). Захист від подібного роду атак [5,8] реалізується за рахунок:

- активації наявних апаратних резервів і канальних ресурсів використовуваної IT- інфраструктури, втому числі за рахунок впровадження режимів віртуалізації функцій ІБ (*VR пули та VR блейди*);
- оперативної зміни поточних параметрів роботи серверу;
- корегування мережевих інтерфейсів;
- зміни діючих режимів брандмауерів;
- фільтрація трафіку на основі максимальної пропускної здатності сервера та аналізу пакетів (*зміна режимів корпоративних proxi*);
- використання можливостей технології [9].

2. *Спуфінг* - спрямована на спотворення цільової інформації на атакованому ресурсі жертви. Має декілька різновидів, наприклад:

- створення неіснуючих (фальшивих) веб-сторінок для збору особистих даних жертв (*Web spoofing*). В цьому випадку, перевірка справжності сайтів (*хоча б доменного імені*) дає змогу уникнути негативних наслідків;
- перехоплення трафіку жертви, атака *Man In The Middle (MITM)*. *MITM* атака має наступні модифікації: *IP*, *ARP* та *DNS spoofing*.

Стратегія захисту від *spoofing* атак:

- використання технологій *VPN* або *VPS* і передача даних за технологією *HTTPS* [5], внаслідок чого атакуючий не має доступу до вмісту пакетів, що істотно обмежує його наступні дії;
- впровадження більш складних механізмів (*порядку*) автентифікації суб'єктів мережі та алгоритмічних запобіжників зміни архітектури. Так як під час проведення *MITM*-атаки, хакер «представляється» іншим легітимним пристроєм цільового ресурсу, маючи намір змінити такі параметри, як *MAC*, *IP*, та *DNS-Table*, то впровадження додаткових алгоритмічних заходів, встановлює додаткові перевірки автентичності подібних дій [10].

3. *Ін'єкції коду* – реалізує впровадження шкідливого коду в легітимне програмне забезпечення (ПЗ), яка виконується на апаратній та/або програмній платформі жертви атаки. Експлуатує такі вразливості, як: – відсутність перевірки введення; – використання застарілого ПЗ; – некоректна/хибна конфігурація системи; – використання «вразливих» (*скомпрометованих*) зовнішніх ресурсів та/або мережевого устаткування. Основними різновидами видами є: – *XSS*; – *SQL, Shell* та *Object injection*. Оскільки всі різновиди ін'єкції коду використовують помилки або вразливості діючого програмного коду, захист від них - використання методик *secure coding* [11].

4. *Повний перебір* (*Brute Force*) – ця атака є найпростішою у реалізації, проте потребує значного часу для знаходження діючих комбінацій параметрів безпеки цільового ресурсу та/або процесу. Зазвичай головною метою цієї атаки є підбір поточних параметрів автентифікації користувачів (логіна і пароля) та аналіз оточення цільової системи (атака *Path traversal* [12]). Використовуючи різні стратегії і методи реалізації *Brute Force* [13], атакуюча сторона намагається скоротити час пошуку дійсних комбінацій автентифікації. Ефективними методиками для протидії *Brute Force* є [14]: - блокування підозрілих акаунтів; - використання технології CAPTCHA; - впровадження алгоритмічних засобів санкціонування повноважень [10]; - впровадження біометричних складових [15] в загальний алгоритм (механізм) автентифікації користувачів. Для запобігання атаки *Path Traversal* [16] ефективною мірою є обмеження користувачів у доступі до файлів сервера.

Більшість мережевих атак можуть бути використані окремо. Так згідно з [17], найчастіше використовують такі атаки *SQL Injection*, *Path Traversal* та *XSS*, проте їх більша частина все ж є комбінованою. Це дає змогу підвищити шанс проведення «успішної» атаки. Наприклад, використання *ARP spoofing*, як частини загальній *DOS* атаки. Отримавши доступ до цільової мережі, зловмисник може підмінити *ARP cache* так, щоб перенаправити вісь трафік мережі до одного (цільового) вузла та/або, навпаки, спотворити *ARP cache* вузлу так, щоб порушити його мережеву взаємодію з іншими вузлами.

Висновки.

1. Залежність сучасного суспільства від інформаційних технологій продовжує стрімко зростати, тому розуміння сутності і способів реалізації відомих кібератак забезпечує можливість прогнозування потенційних дій, стосовно парирування загроз ІБ, на послідуючих ітераціях їх розвитку.

2. Найпоширенішими з атак на *WEB*-ресурси є, *SQL Injection*, *Path Traversal* та *XSS*, при цьому, їх комбінування значно підвищує можливі наслідки відповідних інтегрованих атак.

3. Найбільший інтерес хакерів – це сфери державних установ, фінансів, послуг та медицини.

Список використаних джерел:

1. Яремчук, К., Воскобойников, Д., & Мелкозьорова, О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. Комп'ютерні науки та кібербезпека, (2), 28-34. https://periodicals.karazin.ua/cscs/article/view/21038.
2. Лахтін, І., Михайленко, Д., & Нарєжній, О. (2022). Порівняння комерційних сканерів вразливостей веб-додатків та сканерів з відкритим кодом. Комп'ютерні науки та кібербезпека, (2), 41-49. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/21040.
3. Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. Комп'ютерні науки та кібербезпека, (2), 35-40. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/21039.
4. Гайкова, В., & Малахов, С. (2021). Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. Комп'ютерні науки та кібербезпека, (1), 50-59. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/17435.
5. Безопасная сеть вашей компании / Джон Маллери, Джейсон Занн и др.; пер. с англ. Е. Линдеманн. – М.: НТ Пресс, 2007. – 640 с.
6. FireEye Cyber Threat Map (2018) DOI: https://www.fireeye.com/cyber-map/threat-map.html (дата звернення: 9.02.2023).
7. Актуальные киберугрозы: III квартал 2022 года (2022) DOI: https://www.ptsecurity.com/

ru-ru/research/analytics/cybersecurity-threatscape-2022-q3/ (дата зверненя: 9.02.2023).
8. Что такое DDoS-атаки, и как защитить от них свой сайт? (2023) DOI: https://aws.amazon.com/ru/shield/ddos-attack-protection/ (дата зверненя: 9.02.2023).
9. Рузудженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/15751.
10. Мелкозьорова, О., Лєсная, Ю., & Малахов, С. (2022). Особливості інтеграції систем захисту від несанкціонованих дій в сучасних інформаційних системах. Комп'ютерні науки та кібербезпека, (1), 39-44. Вилучено з: https://periodicals.karazin.ua/cscs/article/view/20912.
11. Keith Turpin, Jon Gadsden. (2022). OWASP Secure Coding Practices-Quick Reference Guide | OWASP Foundation DOI: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/(дата зверненя: 9.02.2023).
12. Ways to Directory Bruteforcing on Web Server - Hacking Articles DOI: https://www.hackingarticles.in/5-ways-directory-bruteforcing-web-server/ (дата зверненя: 9.02.2023).
13. Brute force attack: A definition + 6 types to know | Norton (2021) DOI: https://us.norton.com/blog/emerging-threats/brute-force-attack (дата зверненя: 9.02.2023).
14. Blocking Brute Force Attacks | OWASP Foundation DOI: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks (дата зверненя: 9.02.2023).
15. Олешко И. В. Сравнительный анализ методов аутентификации по отпечатку пальца / И. В. Олешко // материалы 4-го междунар. радиоэлектрон. форума (МРФ'2011) 18-21 окт. 2011 г.: сб. науч. тр. Т.2: междунар. конф. "Телекоммуникационные системы и технологии" (МКТСТ'2011) / АНПРЭ, ХНУРЭ. – Х.: АНПРЭ, ХНУРЭ, 2011. – С. 335–338. Вилучено з: http://surl.li/ewsye.
16. Path Traversal | OWASP Foundation DOI: https://owasp.org/www-community/attacks/Path_Traversal (дата зверненя: 9.02.2023).
17. Атаки на веб-приложения: итоги 2018 года (2019) DOI: https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2019/ (дата зверненя: 9.02.2023).