УДК 004.056

Т. Г. Кирилащук
Д. С. Лавренюк

КОНЦЕПЦІЯ ПІДВИЩЕННЯ ПРИВІЛЕЇВ (PRIVILEGE ESCALATION): ВЕКТОРИ ЗАГРОЗ ТА АРХІТЕКТУРНІ СТРАТЕГІЇ ЗАХИСТУ

Вінницький національний технічний університет

Анотація

Запропоновано концептуальний аналіз проблематики підвищення привілеїв як критичного етапу сучасних кібератак. Проаналізовано основні вектори загроз (вертикальне та горизонтальне підвищення) з урахуванням матриці MITRE ATT&CK. Визначено ключові архітектурні підходи до захисту інформаційних систем, зокрема концепції найменших привілеїв (PoLP), управління привілейованим доступом (PAM) та нульової довіри (Zero Trust).

Ключові слова: кібербезпека, підвищення привілеїв, нульова довіра, MITRE ATT&CK, PAM, принцип найменших привілеїв.

Abstract

A conceptual analysis of the privilege escalation problem as a critical stage of modern cyberattacks is proposed. The main threat vectors (vertical and horizontal escalation) are analyzed considering the MITRE ATT&CK matrix. Key architectural approaches to the protection of information systems, in particular the concepts of least privilege (PoLP), Privileged Access Management (PAM), and Zero Trust, are identified.

Keywords: cybersecurity, privilege escalation, zero trust, MITRE ATT&CK, PAM, principle of least privilege.

Вступ

В умовах стрімкого розвитку інформаційних технологій та ускладнення кібернетичних загроз, забезпечення безпеки корпоративних та державних мереж набуває критичного значення. Сучасні цілеспрямовані атаки (Advanced Persistent Threats, APT) рідко обмежуються простою компрометацією одного вузла. Згідно з методологією аналізу кіберзагроз, зокрема моделлю Cyber Kill Chain, етап підвищення привілеїв (Privilege Escalation) є обов'язковою ланкою для досягнення зловмисниками своїх кінцевих цілей. Отримавши початковий доступ до системи через фішинг або експлуатацію вразливостей периметра, атакуючий зазвичай отримує права звичайного користувача. Для розгортання шкідливого ПЗ, вимкнення засобів захисту або доступу до конфіденційних баз даних необхідні права локального адміністратора (SYSTEM/root) або адміністратора домену, що робить цей етап критичною точкою фокусу як для нападників, так і для систем захисту.

Постановка задачі

Метою є комплексний аналіз механізмів та векторів підвищення привілеїв в сучасних інформаційних системах (на базі Windows та Linux), а також систематизація ефективних архітектурних підходів до протидії цим загрозам.

Результати дослідження

У глобальній базі знань тактик і методів кіберсупротивників MITRE ATT&CK підвищення привілеїв виділено в окрему тактику (TA0004), що налічує десятки специфічних технік експлуатації. Залежно від напрямку руху в ієрархії доступу, вектори атак класифікують на дві основні категорії: вертикальне та горизонтальне підвищення.

Горизонтальне підвищення привілеїв (Account Takeover / Lateral Movement) передбачає отримання доступу до іншого облікового запису з аналогічним рівнем прав. Цей метод активно використовується для розширення поверхні атаки. Зловмисники застосовують техніки викрадення облікових даних з

пам'яті (Credential Dumping), перехоплення хешів паролів (Pass-the-Hash) або маніпуляції з квитками Kerberos (Pass-the-Ticket) у середовищах Active Directory.

Вертикальне підвищення привілеїв (Privilege Elevation) — це процес розширення прав від рівня стандартного користувача до адміністратора. У середовищах Windows найбільш поширеними техніками є експлуатація слабких дозволів на файли та служби, вразливості незакавичених шляхів (Unquoted Service Paths), підміна динамічних бібліотек (DLL Hijacking) та маніпуляції з маркерами доступу (Token Impersonation). У системах на базі Linux зловмисники найчастіше фокусуються на експлуатації вразливостей ядра (Kernel Exploits), неправильно налаштованих правах SUID/SGID для виконуваних файлів, а також на місконфігураціях планувальника завдань Cron та утиліти sudo.

Аналіз інцидентів показує, що понад 70% успішних атак із підвищенням привілеїв базуються не на складних вразливостях нульового дня (Zero-day), а на експлуатації існуючих місконфігурацій системи та недостатньому контролі за життєвим циклом облікових записів.

Для ефективної протидії цим загрозам необхідне впровадження багаторівневих архітектурних рішень:

1. **Принцип найменших привілеїв (PoLP):** Надання користувачам і сервісам лише мінімально необхідного набору прав для виконання їхніх безпосередніх завдань.
2. **Управління привілейованим доступом (PAM):** Впровадження систем контролю за адміністративними сесіями, використання одноразових паролів та концепції доступу "точно вчасно" (Just-In-Time Access), що унеможливлює постійне зберігання високих привілеїв за обліковим записом.
3. **Архітектура нульової довіри (Zero Trust Architecture):** Перехід до мікросегментації мережі та постійної верифікації кожного запиту на доступ до ресурсів, незалежно від того, чи надходить він із внутрішнього периметра.
4. **Проактивний моніторинг:** Застосування рішень класу EDR/XDR (Endpoint/Extended Detection and Response) для виявлення аномальної поведінки процесів, несанкціонованих спроб доступу до системних реєстрів чи критичних файлів конфігурації у реальному часі.

Висновки

Підвищення привілеїв залишається одним із найнебезпечніших та найважливіших етапів будь-якої комплексної кібератаки. Оскільки повністю усунути ризик первинної компрометації неможливо, сучасна стратегія кібербезпеки повинна базуватися на парадигмі "припущення зламу" (Assume Breach). Захист інфраструктури вимагає переходу від реактивних методів блокування до проактивної побудови захищеної архітектури. Впровадження концепцій найменших привілеїв, рішень PAM, моделі Zero Trust та систем глибокого моніторингу кінцевих точок є обов'язковою умовою для мінімізації ризиків переростання локального інциденту у повну компрометацію інформаційної інфраструктури організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Privilege Escalation? CrowdStrike Cybersecurity. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/privilege-escalation/ (дата звернення: 14.02.2026).
2. MITRE ATT&CK. Tactic: Privilege Escalation (TA0004). URL: https://attack.mitre.org/tactics/TA0004/ (дата звернення: 14.02.2026).
3. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020. 53 p.
4. Foster J. C. Privilege Escalation Techniques. Cybersecurity and Infrastructure Security Agency (CISA) Guidelines, 2023. P. 112-118.
5. SANS Institute. Securing the Active Directory: Mitigating Lateral Movement and Privilege Escalation. InfoSec Reading Room, 2024. 34 p.

Дмитро С. Лавренюк – студент Кафедри Захисту Інформації, Вінницький Національний Технічний Університет, Вінниця. dims5688@gmail.com

Науковий керівник: ***Тетяна Г. Кирилащук*** – асистент Кафедри Захисту Інформації, Вінницький Національний Технічний Університет, Вінниця. kgt0998@gmail.com

Dmytro S. Lavreniuk – student of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia. dims5688@gmail.com

Supervisor: ***Tetiana H. Kyrylashchuk*** – assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia. kgt0998@gmail.com