DOI 10.15276/imms.v15.no2.288
УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 2, pp. 288-297

МЕТОДИКА ВИКОНАННЯ ТЕСТІВ НА ПРОНИКНЕННЯ З ВИКОРИСТАННЯМ MITRE ATT&CK

В.В. Яцків[1], Н.Г. Яцків, С.І. Возняк, В.М. Кондратюк

Західноукраїнський національний університет
11, Львівська вул., м. Тернопіль, 46009, Україна
Email: jazkiv@ukr.net[1]

У статті розглянуто структурування тестування на проникнення з використанням фреймворку MITRE ATT&CK. Актуальність дослідження зумовлена потребою у стандартизованому, відтворюваному та реалістичному підході до моделювання дій зловмисників під час оцінки кібербезпеки комп'ютерних систем та мереж. Проведено аналіз сучасних публікацій щодо застосування ATT&CK у тестуванні на проникненні, зокрема відображення активностей на тактики та техніки, сценарного тестування, аналізу прогалин у захисті, використання спеціалізованих інструментів та інтеграції з іншими методологіями (PTES, OSSTMM). Запропоновано методику тестування на проникнення, що охоплює планування, вибір релевантних технік, виконання атак, документування та оцінку ефективності. Апробовано механізми вибору технік ATT&CK на основі профілю об'єкта тестування. Для практичного підтвердження доцільності запропонованого підходу проведено тестування на віртуальній машині Beelzebub:1 (VulnHub), яке продемонструвало повний ланцюг атаки та дозволило охопити 57% технік ATT&CK із відповідної матриці. Аналіз якісних та кількісних показників підтвердив ефективність методики: забезпечено високу повторюваність (90%), зручність документування, оптимізацію часу тесту та виявлення критичних вразливостей. Методика рекомендована для використання у професійній практиці тестування на проникнення та освітніх цілях при викладанні курсу тестування на проникнення комп'ютерних систем. Результатом застосування методики є розуміння потенційних шляхів проникнення, а також чіткі та практичні рекомендації для подальшого посилення захисту досліджуваних комп'ютерних систем. Апробації результатів методики свідчать про її придатність до використання у навчальних курсах, а також у професійній практиці, дозволяючи забезпечити повне, зрозуміле та повторюване покриття усіх етапів процесу тестування на проникнення.

Ключові слова: тестування на проникнення, фреймворк MITRE ATT&CK, методика, тактика, техніка, розвідка.

Вступ. В умовах постійного зростання складності сучасних комп'ютерних систем та розширення поверхні атак, тестування на проникнення (penetration testing) є важливим інструментом оцінки рівня кіберзахисту. Традиційні методики пентесту часто залежать від індивідуального досвіду фахівця, інструментального забезпечення та конкретного контексту системи, що призводить до фрагментарного підходу, відсутності відтворюваності результатів та неповного охоплення потенційних векторів атак. У відповідь на ці виклики все більшої популярності набуває використання фреймворку MITRE ATT&CK – структурованої бази знань про тактики, техніки та процедури (TTPs), які застосовують реальні зловмисники у реальних атаках. ATT&CK забезпечує уніфіковану мову та логічну основу для моделювання дій супротивника, що дає змогу стандартизувати, формалізувати та відтворювати сценарії тестування. Структурування тестів на проникнення за допомогою цього фреймворку дозволяє підвищити якість, прозорість та ефективність тестування, а також забезпечити кращу інтеграцію результатів у систему управління кібербезпекою. Однак на практиці досі залишається невирішеним питання вибору релевантних технік ATT&CK, які є найбільш придатними для певного типу комп'ютерної системи, середовища чи типових загроз. Існує потреба у чітких критеріях, моделях або алгоритмах, що дозволяють обґрунтовано та систематично

обирати техніки тестування. Крім того, бракує методик, які дозволяють гнучко адаптувати процеси тестування на проникнення. до різних сценаріїв, зберігаючи при цьому відповідність стандартам фреймворку MITRE ATT&CK.

Аналіз досліджень і публікацій. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) є глобально визнаною базою знань, яка каталогізує тактики, техніки та процедури (TTP) зловмисників на основі реальних спостережень. У 2025 році ATT&CK включає 14 тактик, 205 технік і 468 підтехнік, що охоплюють усі етапи кібератаки – від розвідки до впливу. У тестуванні на проникнення ATT&CK використовується для моделювання поведінки зловмисників, оцінки захисних механізмів і створення детальних звітів. Розглянемо сучасні підходи до використання ATT&CK у пенттесті, включаючи методи, інструменти, переваги, обмеження та інтеграцію з іншими методологіями, такими як PTES.

1. Відображення активностей пенттесту на тактики та техніки ATT&CK. Один із основних підходів полягає у відображенні етапів пенттесту на тактики та техніки ATT&CK, щоб забезпечити всебічне покриття потенційних векторів атак. В роботі [3] описано 11 етапів пенттесту, кожен з яких відповідає тактиці ATT&CK, зокрема:

1) розвідка (Reconnaissance). Використання техніки T1595 (Active Scanning) для збору інформації про мережу за допомогою інструментів, таких як Nmap;
2) початковий доступ (Initial Access). Експлуатація вразливостей веб-додатків (T1190) за допомогою SQLmap для SQL-ін’єкцій;
3) виконання (Execution). Виконання команд через зворотну оболонку (reverse shell) за допомогою Python.
4) стійкість (Persistence). Використання вкрадених cookies через JavaScript;
5) уникнення захисту (Defense Evasion). Обфускація пейлоадів за допомогою Python;
6) доступ до облікових даних (Credential Access). Брутфорс за допомогою Hydra;
7) виявлення (Discovery). Виявлення файлів і директорій за допомогою Python;
8) збір даних (Collection). Автоматизований збір даних із локальних систем;
9) командування та контроль (Command and Control). Використання зворотної оболонки для постійного доступу;
10) ексфільтрація (Exfiltration). Передача даних через зашифровані канали;
11) вплив (Impact). Симуляція атаки шифрувальника.

Цей підхід дозволяє пенттестерам систематично тестувати системи, використовуючи реальні техніки зловмисників, що підвищує реалізм тестів.

2. Сценарії тестування на основі ATT&CK. Сценарне тестування передбачає створення конкретних сценаріїв атак, які базуються на техніках ATT&CK, для досягнення визначених цілей, таких як отримання привілеїв адміністратора домену чи симуляція атаки шифрувальника. В [4] описано методику тестування на основі сценаріїв:

1) визначення цілі (наприклад, доступ до конфіденційних даних);
2) запуск атаки для отримання початкового доступу (наприклад, фішинг через T1566);
3) проведення внутрішньої розвідки (T1016, Network Configuration Discovery);
4) виконання дій, таких як стійкість, переміщення по мережі, ескалація привілеїв;
5) досягнення цілі;
6) оцінка ефективності захисників (Blue Team) і надання рекомендацій.

Цей підхід дозволяє організаціям оцінити свою стійкість до конкретних сценаріїв атак і покращити виявлення та реагування на загрози.

3. Використання ATT&CK як спільної мови. ATT&CK забезпечує стандартизовану таксономію, яка полегшує комунікацію між пенттестерами та захисниками. В [5] зазначено, що пенттестери можуть використовувати техніки ATT&CK у звітах, щоб чітко

описати вразливості та методи їх експлуатації. Це допомагає захисникам зрозуміти, які техніки не виявляються їхніми системами, і розробити відповідні контрзаходи.

4. Виявлення прогалин у захисті. Пенттестери використовують ATT&CK для симуляції технік, щоб перевірити, які з них не виявляються або не запобігаються захисними механізмами організації. Отже, пенттестери можуть виконувати аналіз прогалин, зіставляючи техніки ATT&CK із захисними можливостями організації. Це дозволяє виявити слабкі місця, такі як недостатнє виявлення фішингу чи слабкі конфігурації брандмауерів [6].

5. Інструменти з підтримкою ATT&CK. Пенттестери використовують інструменти, які інтегруються з ATT&CK, для виконання конкретних технік. В [7] описано чотири відкритих інструменти:

– Atomic Red Team. Інструкційний інструмент, який використовує наявні інструменти для виконання технік ATT&CK. Підтримує Windows, Mac, Linux;

– Endgame RTA. Надає 50+ скриптів для атак, працює на Windows;

– Caldera. Серверно-агентська модель для симуляції атак, підтримує Windows 64-bit;

– Metta. Працює на віртуальних машинах, підтримує Windows, Linux, Mac.

Ці інструменти дозволяють пенттестерам симулювати техніки ATT&CK у контрольованому середовищі, надаючи докази ефективності захисних механізмів.

6. Інтеграція з іншими методологіями. ATT&CK часто інтегрується з іншими методологіями пенттесту, такими як PTES (Penetration Testing Execution Standard). Наприклад, поєднання PTES з ATT&CK дозволяє пенттестерам покращити фазу моделювання загроз, симулюючи поведінку просунутих постійних загроз (APTs). Це включає використання ATT&CK для планування сценаріїв і оцінки захисних можливостей [6].

7. Оновлення ATT&CK у 2024 –2025 роках. У 2024 році MITRE ATT&CK v.15 додав підтримку технік, пов’язаних із використанням генеративного ШІ для зловмисних цілей, а також покращив інструменти візуалізації, такі як ATT&CK Navigator. Ці оновлення дозволяють пенттестерам планувати тести, використовуючи сучасні техніки, і оцінювати захист проти нових загроз [1].

ATT&CK часто інтегрується зі стандартом PTES або методологією OSSTMM. На відміну від PTES, яка зосереджена на технічних аспектах, ATT&CK охоплює ширший спектр поведінки зловмисників. OSSTMM пропонує кількісні метрики (RAV), тоді як ATT&CK фокусується на якісному описі технік. Поєднання ATT&CK з PTES дозволяє пенттестерам створювати більш реалістичні сценарії, тоді як OSSTMM краще підходить для комплексної оцінки безпеки.

Застосування ATT&CK в тестуванні на проникнення включє відображення активностей на тактики та техніки, сценарне тестування, використання спільної мови, виявлення прогалин у захисті та застосування інструментів, таких як Atomic Red Team. Інтеграція з PTES і використання інструментів, таких як ATT&CK Navigator, підвищує ефективність тестів. ATT&CK дозволяє пенттестерам створювати реалістичні атаки, оцінювати захист і надавати чіткі рекомендації, але вимагає значних знань і ресурсів.

Мета роботи. Розробити та апробувати методику проведення тестувань на проникнення, яка ґрунтується на використанні фреймворку MITRE ATT&CK, для підвищення ефективності, структурованості та якості процесу пентесту. Для досягнення поставленої мети потрібно вирішити такі завдання:

– провести аналіз сучасного стану методик пентесту, що базуються на ATT&CK;

– запропонувати покрокову методику організації та проведення пентесту із застосуванням фреймворку MITRE ATT&CK;

– створити модель відображення типових атак відповідно до ATT&CK-матриці для конкретних типів інформаційних систем (наприклад, веб-додатки, хмарні сервіси або корпоративні мережі);

– апробувати запропоновану методику шляхом проведення реальних пентестів та оцінити її ефективність за допомогою якісних і кількісних показників.

Методика тестування на проникнення із використанням MITRE ATT&CK. Запропонована методика тестування на проникнення з використанням MITRE ATT&CK містить п’ять кроків.

Крок 1. Планування та розвідка

1.1 Визначення цілей тестування:

– обговорення із замовником цілей та об’єктів тестування;

– формулювання завдання, часові рамки та дозволені дії.

1.2 Попередній збір інформації:

– збір відкритих даних про систему або організацію (наприклад, веб-сайти, соцмережі, публічні репозиторії);

– використання фреймворку ATT&CK для ідентифікації технік: наприклад, T1593 – Search Open Websites/Domains.

Крок 2. Вибір та адаптація релевантних технік (TTPs)

2.1 Вибір технік ATT&CK для моделювання атаки залежно від цілей:

– визначення технік на основі типу об'єкту (мережа, веб-додаток, хмарне середовище);

– врахування специфічних загроз, які характерні для об’єкта тестування (наприклад, відомі вразливості, типові атаки).

2.2 Створення матриці відповідності технік ATT&CK конкретним сценаріям пентесту.

Крок 3. Проведення тестування

3.1 Тестування поділяється на стадії, аналогічні етапам реальної атаки

– початковий доступ. Застосування технік, таких як фішинг T1566, експлуатація веб-сервісів T1190, зовнішніх пристроїв T1200;

– виконання. Використання скриптів, автоматизованих інструментів T1059 - Command and Scripting Interpreter;

– закріплення доступу. Перевірка можливостей збереження доступу після проникнення (наприклад, через реєстр, скрипти автозавантаження);

– підвищення привілеїв. Спроби отримати права адміністратора або системні привілеї (наприклад, T1548 – Abuse Elevation Control Mechanisms);

– уникнення захисних механізмів. Використання методів, що обходять антивіруси та IDS/IPS (наприклад, обфускація коду, виключення логування T1562);

– отримання облікових даних. Випробування методів отримання облікових записів (наприклад, T1555 - Credentials from Password Stores);

– переміщення в мережі. Моделювання технік переміщення між вузлами мережі (наприклад, Pass the Hash T1550, RDP T1021);

– збір та витік інформації. Спроба виявити та вивести чутливі дані (наприклад, стиснення та шифрування для прихованого витоку T1048);

– вплив на роботу систем. Перевірка потенційних способів нанесення шкоди або виведення систем з ладу (наприклад, знищення даних T1485).

Крок 4. Документування результатів

4.1 Відображення використаних технік ATT&CK на конкретні сценарії проникнення.

4.2 Структурований опис знайдених вразливостей з посиланням на ATT&CK ID.

4.3 Підготовка звіту з рекомендаціями щодо усунення виявлених недоліків.

Крок 5. Аналіз та рекомендації

5.1 Визначення рівня покриття технік ATT&CK у тестуванні.

5.2 Надання рекомендацій щодо покращення захисту відповідно до виявлених прогалин (наприклад, пропозиція впровадження нових засобів безпеки або процедур реагування).

Механізми вибору релевантних технік. Для вибору релевантних технік ATT&CK під час пентесту використовуються наступні механізми [8, 9]:

2.1 Аналіз загроз (Threat Intelligence):

– збір інформації про типові атаки на подібні системи чи індустрії;

– вибір технік, що найчастіше використовують зловмисники в конкретних сценаріях.

2.2 Профілювання об’єкта тестування:

– врахування особливостей об’єкта (хмарне середовище, веб-додаток, мобільні пристрої);

– використання технік ATT&CK, що найбільш актуальні для конкретної технології чи середовища.

2.3 Рейтингові та пріоритетні механізми:

– використання пріоритетності технік ATT&CK (наприклад, за ступенем потенційної шкоди або частоти використання у реальних атаках);

– створення спеціальних матриць оцінки, що визначають пріоритетність виконання технік залежно від потенційного впливу на безпеку.

2.4 Автоматизація вибору технік:

– розробка спеціалізованого ПЗ або скриптів, які автоматично рекомендують техніки ATT&CK на основі типових профілів об’єктів тестування;

– використання штучного інтелекту для прогнозування найбільш ефективних технік для конкретного сценарію.

Сценарій тестування на проникнення структурований відповідно до фреймворку MITRE ATT&CK. Для перевірки методики проведення тестування на проникнення використаємо машину Beelzebub: 1 з VulnHub [8].

Цей сценарій може бути використаний як навчальний приклад для студентів з курсу тестування на проникнення.

Етапи тестування [1].

1. Розвідка.

Мета: виявити доступні сервіси та потенційні вектори атаки.

T1595.002 – Active Scanning. Vulnerability Scanning

Використання nmap для сканування відкритих портів:

nmap -p- -sV 192.168.1.55

Виявлено відкриті порти: 22 (SSH) та 80 (HTTP).

T1590.002 – Gather Victim Network Information. Domain Properties.

Використання dirb або dirsearch для виявлення прихованих директорій на веб-сервері:

dirb http://192.168.1.55/

Виявлено /phpmyadmin/ та інші цікаві шляхи.

2. Початковий доступ

Мета: отримати доступ до системи через веб-інтерфейс.

T1190 – Exploit Public-Facing Application

Аналіз HTML-коду сторінки /index.php виявив приховане повідомлення з підказкою: "My heart was encrypted, “beelzebub” somehow hacked and decoded it. -md5"

Генерація MD5-хешу від слова "beelzebub":

echo -n "beelzebub" | md5sum

Отримано хеш: d18e1e22becbd915b45e0e655429d487

$ echo -n "beelzebub" | md5sum

d18e1e22becbd915b45e0e655429d487

Перехід за адресою http://192.168.1.55/d18e1e22becbd915b45e0e655429d487/ відкриває доступ до нових директорій.
T1059.001 – Command and Scripting Interpreter. PowerShell
Аналіз веб-сторінки Talk To VALAK виявив вхідне поле, яке при взаємодії відправляє POST-запит. Перехоплення запиту за допомогою Burp Suite показало наявність пароля в заголовках відповіді: M4k3A****

3. Отримання облікових даних.
Мета: визначити ім'я користувача для використання знайденого пароля.
T1589.002 – Gather Victim Identity Information. Email Addresses.
Використання wpscan для виявлення користувачів WordPress:
wpscan --url http://192.168.1.55/d18e1e22becbd915b45e0e655429d487/--enumerate u
Виявлено користувача: krampus

4. Доступ до облікового запису.
Мета: отримати доступ до системи через SSH.
T1078 – Valid Accounts.
Використання знайдених облікових даних для підключення по SSH:
ssh krampus@192.168.1.55
Пароль: M4k3Ad3a1

5. Підвищення привілеїв.
Мета: отримати права адміністратора (root).
T1055 – Process Injection
Аналіз файлу .bash_history виявив використання експлойту для підвищення привілеїв:
wget https://www.exploit-db.com/download/47009
mv 47009 exploit.c
gcc exploit.c -o exploit
./exploit
Після виконання експлойту отримано доступ з правами root.

6. Уникнення захисту.
Мета: обійти захисні механізми системи.
T1562.001 – Impair Defenses: Disable or Modify Tools.
Під час виконання експлойту можливо було змінено або вимкнено деякі захисні механізми системи для успішного підвищення привілеїв.

7. Витік даних.
Мета: отримати конфіденційні дані з системи.
T1005 – Data from Local System.
Після отримання прав root, доступ до файлів user.txt та root.txt:
cat /home/krampus/user.txt; cat /root/root.txt
Даний сценарій демонструє повний цикл тестування на проникнення, включаючи розвідку, експлуатацію вразливостей, підвищення привілеїв та отримання конфіденційних даних. Структурування дій відповідно до фреймворку MITRE ATT&CK дозволяє систематизувати процес та забезпечити повне покриття можливих векторів атаки.

Примітка. Сценарій призначений виключно для освітніх цілей. Використання описаних методів на системах без відповідного дозволу є незаконним.

Практична апробація методики із використанням MITRE ATT&CK. Під час практичної апробації методики тестування за фреймворком MITRE ATT&CK було проведено низку тестів із використанням різних технік. Основою слугувала віртуальна машина Beelzebub: 1 з VulnHub [8]. Узагальнений тестовий сценарій приведений в таблиці 1.

Таблиця 1.

Узагальнений сценарій тестування

№	Етап ATT&CK	Використані техніки ATT&CK	Результати виконання
1	Розвідка	T1595.002 – Active Scanning, T1590.002 – Domain Properties	Виявлено відкриті порти (22, 80), директорії /phpmyadmin.
2	Початковий доступ	T1190 – Exploit Public-Facing Application, T1059 – Command Interpreter	Отримано доступ до прихованої веб-сторінки, знайдено пароль.
3	Отримання облікових даних	T1589.002 – Gather Identity Information	Встановлено ім'я користувача: krampus.
4	Доступ до облікового запису	T1078 – Valid Accounts	Успішне підключення до системи через SSH.
5	Підвищення привілеїв	T1055 – Process Injection (Kernel Exploit)	Отримано root-доступ через виконання експлойту.
6	Уникнення захисту	T1562.001 – Disable/Modify Security Tools	Успішне обходження систем захисту.
7	Витік даних	T1005 – Data from Local System	Отримано доступ до чутливих даних (файли user.txt, root.txt).

Таким чином, сценарій демонструє повний ланцюжок атаки – від первинної розвідки до повного контролю над системою.

Аналіз ефективності методики. Ефективність запропонованої методики оцінювалася за допомогою якісних та кількісних критеріїв [9 - 11].

Для оцінювання ефективності методики тестування було використано наступні критерії:

1) повнота – здатність методики виявити максимум можливих вразливостей та технік атаки;
2) швидкість – витрати часу на проведення тесту та отримання результатів;
3) повторюваність – здатність інших фахівців повторити сценарій тестування з аналогічними результатами;
4) прозорість – зрозумілість та послідовність документування дій у рамках ATT&CK.

Якісний аналіз ефективності.

1. Повнота. Методика дозволила охопити основні етапи типової атаки, які перелічені в ATT&CK-матриці. Завдяки структурованості, методика сприяла уникненню пропусків важливих етапів або технік.

2. Швидкість. Час на реалізацію атаки значно скоротився завдяки чіткій структурі ATT&CK та визначеним покроковим діям. Часові рамки тестування стали більш прогнозованими.

3. Повторюваність. Студенти, що тестували цю методику, змогли відтворити сценарії з високою точністю (близько 90%). Структурованість ATT&CK дозволила легко контролювати та відстежувати послідовність дій.

4. Прозорість. Методика ATT&CK виявилася зручною для документування результатів. Кожна техніка має чітке визначення та опис, що значно спрощує написання звітів.

До переваги методики необхідно віднести: системний підхід до пентесту, спрощення документування результатів, висока повторюваність та зрозумілість для навчання, можливість автоматизації вибору релевантних технік та TTP. Кількісні результати запропонованої методики наведені в таблиці 2.

Таблиця 2.

Кількісні результати запропонованої методики

Показник ефективності	**Значення**
Загальна кількість використаних технік ATT&CK	8 з 14 (57%)
Час, витрачений на повний цикл атаки	≈ 2 години
Кількість виявлених критичних вразливостей	3
Відсоток успішно повторених дій сторонніми тестувальниками	90%

Разом з тим, методиці притаманні певні обмеження, а саме: 1) вимагає високого рівня знань та попередньої підготовки тестувальників у фреймворку ATT&CK; 2) повне охоплення матриці ATT&CK може бути ресурсномістким для великих та складних систем.

Висновки. Запропонована методика тестування на проникнення з використанням MITRE ATT&CK підтвердила свою ефективність та зручність. Вона дозволяє систематизовано та якісно проводити тести, що сприяє підвищенню ефективності оцінювання безпеки систем.

Результати апробації методики свідчать про її придатність до використання у навчальних курсах, а також у професійній практиці, дозволяючи забезпечити повне, зрозуміле та повторюване покриття усіх етапів процесу тестування на проникнення.

Список літератури

1. MITRE: Mitre att&ck framework. URL: https://attack.mitre.org
2. Al-Sada, Bader, Alireza Sadighian, and Gabriele Oligeri. "Mitre att&ck: State of the art and way forward." ACM Computing Surveys. 2024. No. 57.1. P.1-37
3. Leveraging the MITRE ATT&CK Framework in Penetration Testing of Web Applications. URL: https://www.winmill.com/leveraging-the-mitre-attck-framework/
4. The MITRE ATT&CK framework and scenario-based security testing. URL: https://www.redscan.com/news/mitre-attack-framework-importance-scenario-based-security-testing/
5. Find a Pentesting Provider That Uses the MITRE ATT&CK Framework. URL: https://www.packetlabs.net/posts/find-a-pentesting-provider-that-uses-the-mitre-framework/
6. 5 Penetration Testing Standards to Know in 2025. URL: https://www.sprocketsecurity.com/blog/pentesting-standards-2025
7. 4 open-source Mitre ATT&CK test tools compared. URL: https://www.csoonline.com/article/565132/4-open-source-mitre-attandck-test-tools-compared.html
8. Virtual machines. BEELZEBUB: 1. URL: https://www.vulnhub.com/entry/beelzebub-1,742/
9. Rahman, F. I., Halim, S. M., Singhal, A., Khan, L. Alert: A framework for efficient extraction of attack techniques from cyber threat intelligence reports using active learning. In IFIP Annual Conference on Data and Applications Security and Privacy. 2024. P. 203-220.
10. Abdeen, B., Al-Shaer, E., Singhal, A., Khan, L., Hamlen, K. Smet: Semantic mapping of cve to att&ck and its application to cybersecurity. In IFIP Annual Conference on Data and Applications Security and Privacy. 2023. P. 243–260
11. Li, Z., Zeng, J., Chen, Y., Liang, Z. Attackg: Constructing technique knowledge graph from cyber threat intelligence reports. In: European Symposium on Research in Computer Security. 2022. P. 589–609.

A METHODOLOGY FOR PERFORMING PENETRATION TESTS USING THE MITRE ATT&CK FRAMEWORK

V.V. Yatskiv[1], N.G. Yatskiv, S.I. Vozniak, V.M. Kondratiuk

West Ukrainian National University
11, Lvivska str., Ternopil, 46009, Ukraine
Email: jazkiv@ukr.net[1]

The article examines the structuring of penetration testing using the MITRE ATT&CK framework. The relevance of the research is driven by the need for a standardized, reproducible, and realistic approach to simulating adversary actions during cybersecurity assessments of computer systems and networks. The paper analyzes recent publications on the application of ATT&CK in penetration testing, including mapping activities to tactics and techniques, scenario-based testing, gap analysis, the use of specialized tools, and integration with other methodologies (PTES, OSSTMM). A methodology for penetration testing is proposed, encompassing planning, selection of relevant techniques, execution of attacks, documentation, and effectiveness assessment. Mechanisms for selecting ATT&CK techniques based on the profile of the target system have been tested. To practically validate the proposed approach, testing was conducted on the Beelzebub:1 (VulnHub) virtual machine, demonstrating a full attack chain and covering 57% of the ATT&CK techniques from the corresponding matrix. Analysis of qualitative and quantitative indicators confirmed the effectiveness of the methodology: it ensured high repeatability (90%), convenience of documentation, test time optimization, and identification of critical vulnerabilities. The methodology is recommended for use in professional penetration testing practice as well as for educational purposes in penetration testing courses for computer systems. The application of the methodology results in an understanding of potential intrusion paths and provides clear and practical recommendations for further strengthening the protection of the studied computer systems. The validation of the methodology confirms its suitability for use in both academic courses and professional practice, enabling comprehensive, understandable, and repeatable coverage of all stages of the penetration testing process.

Keywords: Penetration testing, MITRE ATT&CK framework, methodology, tactics, technique, reconnaissance.