

ПРАКТИЧНІ ЗАНЯТТЯ

3-й етап Літньої школи з кібербезпеки 2026

Digital Forensics and Incident Response

Завдання №1. Прихований файл у мережному трафіку

Опис завдання: Вам надано захопленого трафіку *suspicious_file.pcapng*. Користувач переглядав звичайний веб-сайт, але в якийсь момент завантажив підозрілий файл. Ваше завдання – відновити весь ланцюжок подій: від HTTP-запиту до фінального прапора, схованого всередині зображення. Використовуйте Wireshark, інструменти для брутфорсу ZIP-паролів (наприклад, zip2john + john з rockyou.txt) та інструменти для аналізу стеганографії (наприклад, zsteg, Stegsolve, Aperisolve тощо).

Питання для обговорення:

1. Скільки HTTP-запитів (GET) було зроблено клієнтом протягом сесії? Перелічіть усі запитані ресурси. Які з них повернули код 200 OK, а які – 404?
2. Який HTTP-сервер (назва та версія у заголовку Server:) обробляв запити? Що це говорить про те, як саме був розгорнутий цей “веб-сайт”?
3. Серед усіх запитів є один, що явно виділяється на фоні звичайних .html-сторінок – за типом контенту та розміром відповіді. Який це файл і який у нього Content-Type та Content-Length?
4. Витягніть цей файл. Який у нього формат? Чи вдалося відкрити його одразу?
5. Архів захищений паролем. Який метод атаки доцільно застосувати в даному випадку? Підготуйте hash-файл для john (zip2john) і запустіть перебір за словником rockyou.txt. Який пароль було знайдено?
6. Після розпакування архіву з підібраним паролем – що знаходиться всередині?
7. Яка техніка стеганографії найімовірніше застосована для приховування даних у зображенні (LSB, метадані EXIF тощо)? Чому саме LSB є найпоширенішим методом для растрових зображень без втрат (PNG/BMP)?
8. Застосувавши LSB-аналіз до каналів R, G, B зображення, витягніть приховані дані. Який прапор вдалося отримати?

9. (Додатково) Чому передача файлу через HTTP у відкритому вигляді є проблемою з точки зору мережної безпеки, навіть якщо сам файл зашифрований паролем усередині?

10. (Додатково) Яку роль у цьому сценарії відіграв слабкий пароль ZIP-архіву? Що б змінилося, якби пароль був складним і випадковим (наприклад, 20 символів з усіх типів символів)?

Завдання № 2. Аналіз мережної атаки у Wireshark

Опис завдання: Вам надано файл захопленого трафіку *forensics_basic_wireshark.pcapng*. У ньому зафіксована атака одного вузла мережі на інший. Ваше завдання – проаналізувати перехоплений мережний трафік у Wireshark, покроково відтворити хід атаки та відповісти на питання нижче.

Питання для обговорення:

1. Скільки унікальних IP-адрес присутні у трафіку? Яка з них є атакуючою, а яка – жертвою? На основі яких ознак ви це визначили?

2. Який протокол транспортного рівня переважає у трафіку (TCP/UDP)? Чому в захопленому трафіку так багато TCP-запитів з прапорцем SYN без відповідного SYN-ACK / ACK? Що це означає з точки зору мережної безпеки?

3. Визначте 3-4 номери портів на жертві, які атакуючий просканував і які виявились відкритими (тобто отримали у відповідь SYN-ACK). Що це за сервіси (спробуйте зіставити номери портів зі стандартними службами)?

4. Після сканування атакуючий встановлює повноцінне з'єднання з одним конкретним портом і веде текстовий діалог у відкритому вигляді. Який це прикладний протокол? Чому ви змогли прочитати весь діалог у відкритому тексті (plaintext) без розшифрування?

5. Знайдіть у трафіку рядки аутентифікації. Який логін і пароль використав атакуючий для входу на сервер? Оцініть стан безпеки облікового запису.

6. Яку саме команду атакуючий надіслав для перегляду вмісту каталогу на сервері, а яку – для завантаження файлу? Як називається файл, який був викачаний?

7. Використовуючи Wireshark витягніть цей файл із трафіку. Якого він типу? Що знаходиться всередині нього і чи вдалося вам знайти прапор?

8. (Додатково) Яка версія FTP-сервера вказана у банері (220 ...)? Чи відома вам ця версія як історично вразлива? Що атакуючий міг зробити ще, окрім читання файлів, маючи доступ до цього сервісу?

Завдання №3. Аналіз журналу подій безпеки Windows

Опис завдання: Вам надано журналу подій *Security_Event.evtx*, знятий з робочої станції Windows. На системі стався інцидент: хтось намагався увійти в обліковий запис користувача, зрештою досяг успіху, а потім виконав підозрілу команду в PowerShell. Ваше завдання – відкрити журнал подій, знайти ключові події за їхнім Event ID і відновити хронологію атаки.

Корисна інформація:

Event ID 4624 – успішний вхід в обліковий запис.

Event ID 4625 – невдала спроба входу в обліковий запис.

Event ID 4688 – створення нового процесу.

Питання для обговорення:

1. Скільки подій з невдалими спробами входу ви знайшли для облікового запису Jane? У якому часовому проміжку вони відбулись? Про що свідчить дана активність?

2. Подивіться на поле Status / SubStatus у цих подіях (наприклад, 0xC000006A). Чим відрізняється “неправильний пароль” від, наприклад, “обліковий запис заблоковано” чи “обліковий запис не існує”?

3. За значенням поля WorkstationName в невдалих спробах входу визначте звідки саме намагались підключитись. Яка IP-адреса зловмисника? Що може означати ім'я робочої станції, вказане в цьому полі, з точки зору того, хто атакував систему?

4. Знайдіть подію з успішним входом у систему під обліковим записом користувача Jane. Які дата й час цього успішного входу?

5. Яке значення поля LogonType в цій події?

6. Яка подія Windows Security фіксує створення нового процесу в системі? Перегляньте всі такі події від імені Jane – яка команда серед них виглядає найбільш підозріло і чому?

7. У командному рядку підозрілого процесу є параметр `-EncodedCommand` з довгим рядком символів. Що це за формат кодування?

8. Розкодуйте цей рядок. Що містить розкодована команда? Чи вдалося отримати прапор?

Завдання №4. Аналіз логів Linux

Опис завдання: Один із серверів було повністю скомпрометовано. Зловмисник здобув початковий доступ, підвищив привілеї до `root`, встановив руткіт для приховування своїх дій та запустив скрипт із закодованим корисним навантаженням. Проаналізуйте надані артефакти системи (`auth.log` та `.bash_history`), відтворіть хронологію атаки та захопіть прапор.

Питання для обговорення:

Блок 1. Аналіз логів безпеки (`auth.log`):

1. Який саме мережний сервіс піддався атаці?
2. Який обліковий запис став основною мішенню для підбору?
3. Проаналізуйте загальну картину логів (частоту запитів, зміну портів, системні повідомлення). Що це за тип атаки?
4. О котрій годині відбувся перший успішний вхід у звичайний обліковий запис?
5. О котрій годині зловмисник успішно увійшов під обліковим записом `root`?
6. Яку найпершу команду виконав зловмисник у терміналі після отримання прав `root`?
7. Який саме руткіт було завантажено з GitHub та інстальовано в систему?
8. Яке закодоване повідомлення зловмисник передав через `echo` у директорії `/root/magpref_hackdata`?

9. Яке декодоване значення ви отримати?

10. О котрій годині був запущений скрипт `script.sh`?

Блок 2. Аналіз історії команд (`.bash_history`):

1. За допомогою якого інструменту зловмисник шукав вразливості для підвищення привілеїв у системі та в який файл зберіг результат?

2. Версію якого сервісу/бази даних перевіряв зловмисник перед запуском експлойту:
3. Який саме скрипт-експлойт використано для атаки та назву якої бази даних (--dbname) вказано в аргументах?
4. Перегляньте параметр --cmd під час запуску Python-скрипту. Яку саме дію з обліковим записом root виконав цей експлойт?
5. У параметрах запуску експлойту передано пароль у полі --password. Декодуйте другу частину прапора.

Завдання №5 – Аналіз USB-накопичувача у FTK Imager

Опис завдання: Це завдання базується на кімнаті TryHackMe – Advent of Cyber 2023, День 8 (посилання: <https://tryhackme.com/room/adventofcyber2023>).



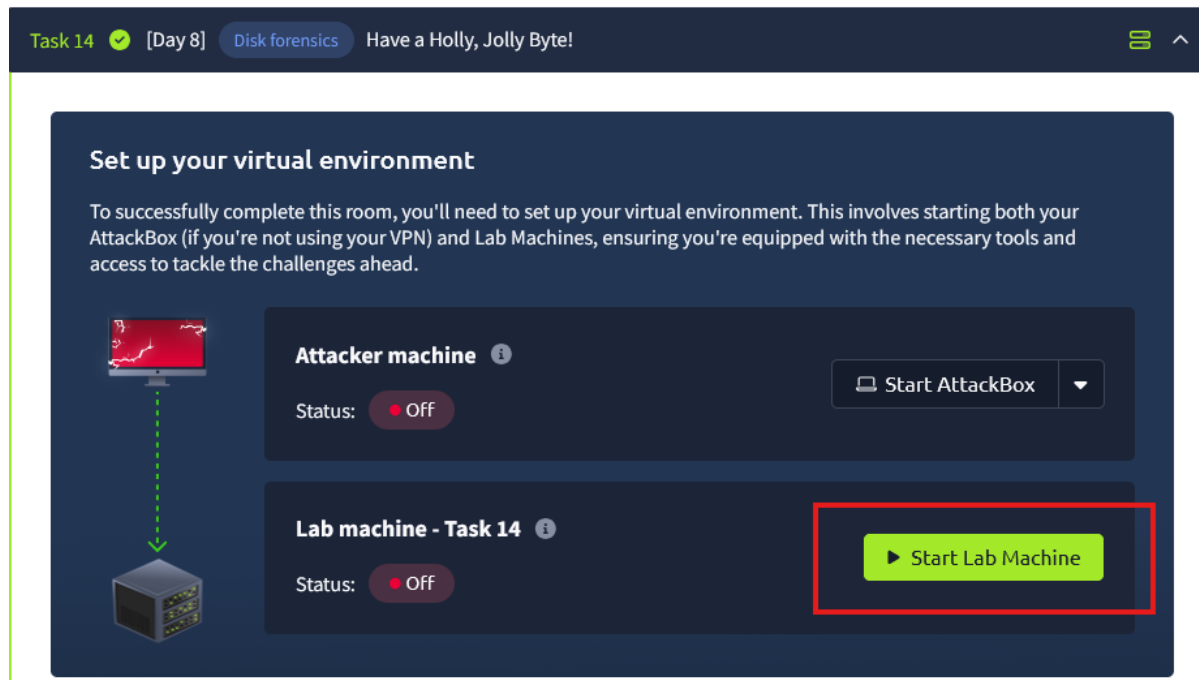
Сценарій навмисно перекликається з відомою атакою Stuxnet: зловмисник залишає заражений USB-накопичувач на парковці підприємства, її знаходять і підключають до робочого комп'ютера – після чого починається розслідування.

Мета – застосувати на практиці такі навички цифрової криміналістики:

1. Аналіз артефактів файлової системи.
2. Відновлення видалених файлів.
3. Перегляд файлів у режимі HEX для пошуку прихованих даних.
4. Перевірка цілісності доказів через обчислення хешів диска/образу.

Для вирішення завдання на платформі TryHackMe розгортається віртуальна машина, доступ до якої ви отримаєте через браузер.

Запуск віртуальної машини:



Питання для обговорення:

1. Після додавання цифрового доказу (Add Evidence Item) ви бачите файлову структуру USB-накопичувача. Як саме FTK Imager візуально позначає видалені файли?
2. Досліджуючи вміст диска, знайдіть підозрілу видалену теку. Що привертає до неї увагу, окрім самої назви? Що знаходиться всередині неї?
3. Один із файлів у цій теці містить фрагмент переписки (чат) між зловмисниками. Уважно прочитайте його вміст. Яка інформація в цьому чаті є критично важливою для розслідування (адреса командного сервера – C2, тобто Command & Control)?
4. У переписці згадується архів (.zip), який також присутній серед видалених файлів. Відкрийте цей архів прямо у FTK Imager (без потреби його розпаковувати назовні). Що знаходиться всередині архіву?
5. Серед видалених файлів є щонайменше два зображення у форматі PNG. Чому для пошуку прихованих даних усередині таких файлів слід використовувати саме режим HEX, а не текстовий перегляд?
6. Прапори у завданнях на платформі TryHackMe мають формат THM{...}. Використовуючи функцію пошуку (Ctrl + F) у режимі перегляду HEX/ASCII,

налаштуйте пошук у режимі Text для потрібного рядка. Перевірте обидва PNG-файли – прапор прихований лише в одному з них.

7. Останній етап – перевірка цілісності доказів через File -> Verify Drive/Image. Який криптографічний алгоритм хешування (окрім SHA1) також зазвичай обчислюється при верифікації? Чому на практиці важливо обчислювати й фіксувати хеш образу диска одразу після його створення, а не пізніше?

8. (Додатково) Якби хеш диска, обчислений на етапі верифікації, не збігався з хешем, зафіксованим на момент створення образу – які наслідки це мало б для допустимості доказів у розслідуванні?