Міністерство освіти і науки України Київський національний університет будівництва і архітектури

Кафедра кібербезпеки та комп'ютерної інженерії

OSINT - сценарії виявлення цифрового сліду організації в умовах навчального кіберполігону

Виконав: здобувач вищої освіти, гр. БІКС-22, Гінзбург Д.Ю.

Керівник: доцент Делембовський М.М.

Київ - 2026

Порівняльна таблиця психологічних чинників

Психологічний чинник	Опис механізму впливу	Наслідок для кібербезпеки
Потреба у визнанні	Публікація досягнень для отримання лайків	Витік фрагментів коду та планів
Ефект оптимізму	Нехтування правилами через віру в безпеку	Відсутність паролів на пристроях
Пріоритет зручності	Використання паперових нотаток з даними	Паролі на фото робочих місць
Ілюзія приватності	Віра в обмежене коло читачів постів	Публікація робочих email адрес
Професійна гордість	Бажання похвалитися написаним скриптом	IP адреси у відкритих репозиторіях

витоку даних

Мета: Розробка інтерактивного навчального сценарію (CTF) для наочної демонстрації ризиків неконтрольованого цифрового сліду.

Підхід: Навчання через симуляцію реальної атаки на основі відкритих джерел (OSINT).

ID	Name	Category	Value	Type	State	Solution
6	Initial Metadata Reconnaissance	Open Source Intelligence	1	standard	visible	
7	Social Media Footprinting	Open Source Intelligence	1	standard	visible	
8	Extracting Artifacts from Imagery	Open Source Intelligence	1	standard	visible	
10	Steganography and Cryptographic Analysis	Open Source Intelligence	1	standard	visible	
11	Network Infrastructure Attribution	Open Source Intelligence	1	standard	visible	

Джеймс Кларксон

- Використання ШІ для генерації вигаданого співробітника (Джеймс Кларксон).
- Відсутність порушення приватності реальних людей.
- Повний контроль над створеними цифровими артефактами.

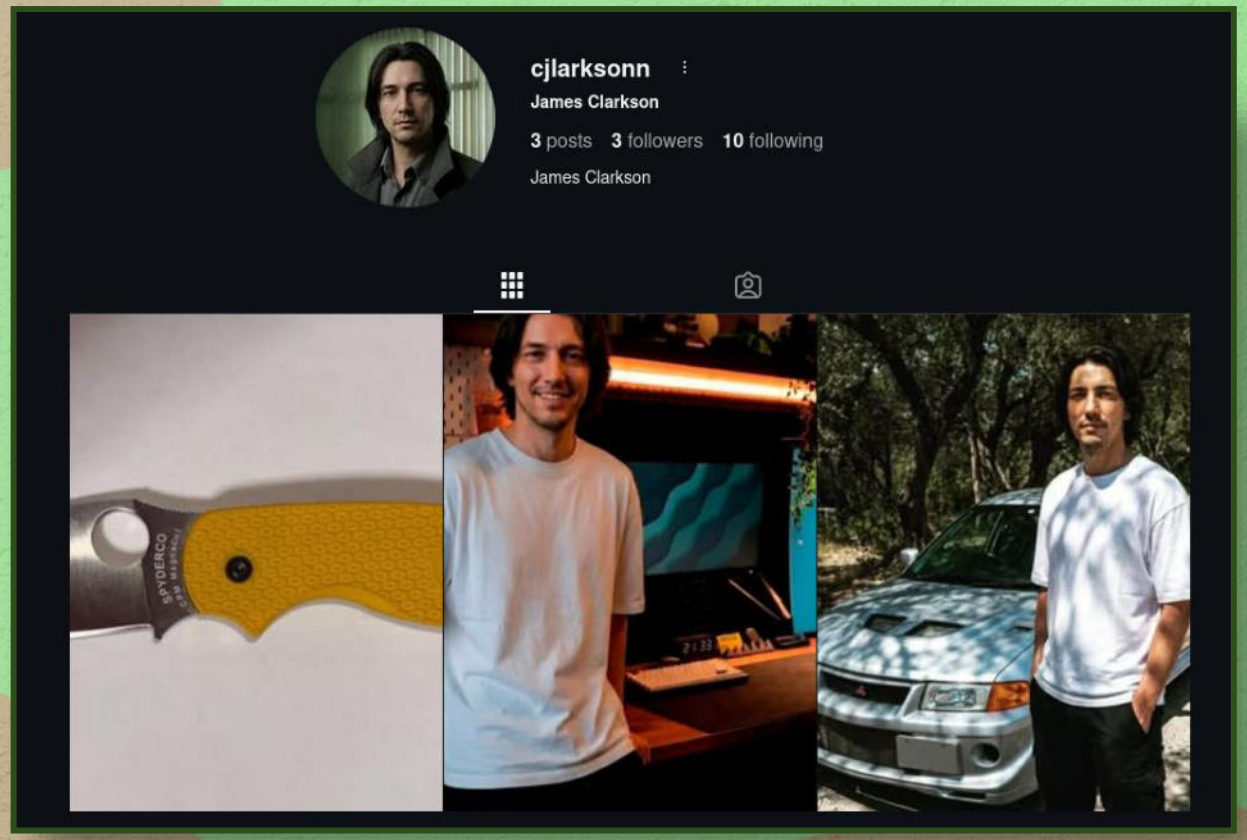
Архітектура кіберполігону

Завдання №1

```
XMP Toolkit                     : Image::ExifTool 13.52
---- XMP-dc ----
Source                          : C:\Users\cjlarksonn\Desktop\J.Clarkson.png
```

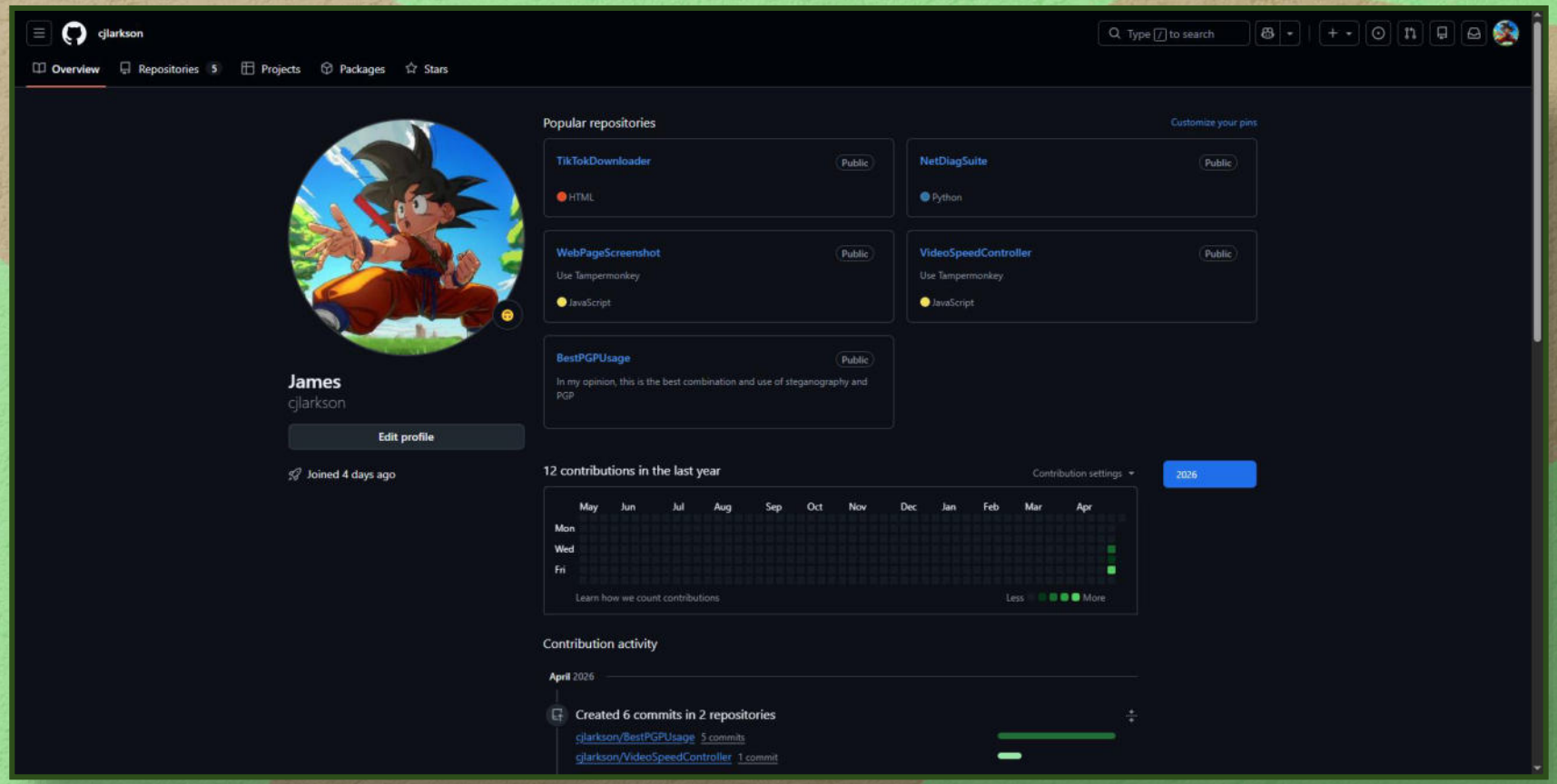
Виявлення унікального нікнейму (cjlarksonn) через технічний тег.

Завдання №2 та №3



Фрагмент фото з Instagram

Завдання №4 та №5



Організаційний рівень	Технічний рівень	Персональний рівень
Політика «чистого столу», заборона паперових носіїв із паролями, навчання цифрової гігієни	Автоматичне очищення метаданих (EXIF) перед публікацією, сканери секретів у CI/CD (GitHub)	Унікальні нікнейми для різних платформ, використання менеджерів паролів

Висновки

Доведено критичну небезпеку накопичення цифрових слідів (від одного фото до компрометації IP)

Розроблено та протестовано алгоритм деанонімізації об'єкта

Створено безпечний інструмент на базі CTFd для тренування фахівців з кібербезпеки та проведення навчання персоналу компанії