КРИПТОЛОГІЯ

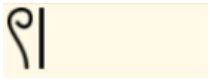
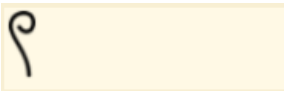
ЛІТНЯ ШКОЛЯ З КІБЕРБЕЗПЕКИ 2026

ПРАКТИЧНЕ ЗАННЯТЯ №1

Завдання 1. Послання стародавнього адміна.

Опис завдання: Під час ремонту серверної університету під старою підлогою знайдено запечатану капсулу часу від перших системних адміністраторів 1990-х років. Усередині – фрагмент “пергаменту” з дивними символами. Попередній аналіз показав, що це система числення, яка використовувалась як прихований спосіб запису пароля до архіву даних.

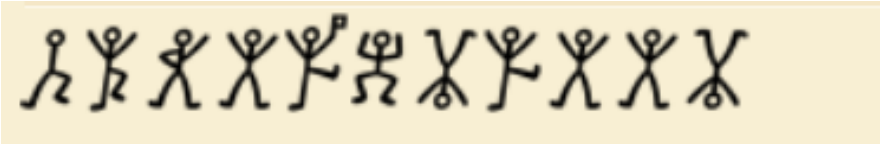
Ваше завдання: Розшифрувати запис та визначити пароль до архіву.

1. 
2. 
3. 
4. 
5. 
6. 
7. 
8. 
9. 
10. 
11. 
12. 
13. 
14. 
15. 
16. 
17. 

Завдання 2. Справа танцюючих чоловічків.

Опис завдання: Під час реставрації архіву старої приватної бібліотеки працівники знайшли копію листування, яке нібито належало самому Шерлоку Голмсу. Серед документів був дивний аркуш із намальованими чоловічками у різних позах. На звороті олівцем написано: “Holmes solved it in a single evening. Can you?”

Ваше завдання: Розшифрувати приховане повідомлення.



Завдання 3. Кам’яна плита з невідомою системою запису.

Опис завдання: Під час археологічної експедиції в Центральній Америці дослідники виявили кам’яну плиту з нанесеними символами, які не відповідають жодній відомій сучасній системі запису чисел. Дослідники припустили, що це може бути позиційна система, де кожне число відповідає певному елементу фіксованого списку.

Ваше завдання: Розшифрувати запис та визначити приховане значення повідомлення.

Завдання 4. Приховані дані у файлі

Опис завдання: Під час аналізу сервера було знайдено текстовий файл із підозрілим вмістом. Частина даних виглядає як звичайний текст, але всередині може бути приховане повідомлення.

Ваше завдання:

1. Знайти підозрілий фрагмент.
2. Визначити тип кодування.
3. Відновити приховане повідомлення.

Вміст файлу:

System check completed
User session restored
Tmp value: 53 65 63 75 72 69 74 79 5F 69 73 5F 63 6F 6F 6C
Connection closed

Завдання 5. Підозрілий стікер

Опис завдання: Під час перевірки комп'ютерного класу лаборант помітив стікер під однією з клавіатур. На ньому був лише дивний набір символів. Викладачі підозрюють, що це пароль до прихованого студентського чату.

Ваше завдання: Декодувати повідомлення та знайти пароль.

Набір символів:

U3R1ZDNudF9DaGF0X1Bhc3M=

Питання для обговорення:

1. Який тип кодування використано в цьому повідомленні?

2. Чому даний тип кодування часто зустрічається в реальних системах та при передачі даних?

3. Чи можна вважати даний тип кодування способом захисту інформації?

Завдання 6. Підозрілий параметр у HTTP-запиті.

Опис завдання: Під час аналізу мережевого трафіку аналітик виявив підозрілий HTTP-запит. Один із параметрів виглядає нетипово.

Ваше завдання:

1. Знайти закодовані дані.
2. Відновити приховане повідомлення.

Фрагмент HTTP-запиту:

GET /login?user=student&token=Q3liZXJTZWN1cml0eV9pc19mdW4= HTTP/1.1

Host: cyber.local

Завдання 7. Шкідливий скрипт.

Опис завдання: До університетської пошти студентам надійшов файл із назвою: "Список студентів на підвищену стипендію.docm". Після відкриття документа система безпеки зафіксувала запуск підозрілого PowerShell-скрипта. Аналітики витягнули фрагмент цього скрипта для подальшого аналізу.

Ваше завдання:

1. Проаналізувати PowerShell-скрипт.

2. Знайти підозрілий фрагмент.

3. Визначити, який тип кодування використовується.

4. Декодувати приховані дані.

5. Встановити адресу сервера, до якого намагається підключитися шкідливий скрипт.

Скрипт:

```
$ErrorActionPreference = "SilentlyContinue"

function Get-SystemInfo {
    $os = (Get-CimInstance Win32_OperatingSystem).Caption
    $user = $env:USERNAME

    return "$user@$os"
}

$temp = "$env:TEMP\sys.log"

$data = Get-SystemInfo
$data | Out-File $temp

Start-Sleep -Seconds 2

$encoded = "aHR0cDovLzE4NS4xOTkuMTA4LjE1Ni9iZWFjb24="

$server = [System.Text.Encoding]::UTF8.GetString(
    [System.Convert]::FromBase64String($encoded)
)

Invoke-WebRequest -Uri $server -UseBasicParsing
```

Завдання 8. Дивна команда в Linux-лозі.

Опис завдання: Адміністратор переглядав історію команд Linux-сервера і знайшов підозрілий запис. Команда не виглядає небезпечною на перший погляд, але містить закодовані дані.

Ваше завдання:

1. Відновити закодований елемент.
2. Пояснити, для чого виконувалась команда.

Команда:

```
/bin/bash -c "$(echo "Y2F0IC9ldGMvcGFzc3dk" | base64 -d)"
```

Завдання 9. Підозрілий токен авторизації.

Опис завдання: Під час аналізу веб-застосунку було перехоплено токен авторизації користувача.

Ваше завдання:

1. Визначити структуру токена.
2. Декодувати дані.
3. Визначити ім’я користувача та його роль.

Токен:

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoic3R1ZGVudCIsInJvbGUiOiJhZG1pbiJ9.

Завдання 10. XOR-повідомлення.

Опис завдання: Було перехоплено повідомлення у HEX-форматі. Відомо, що його зашифрували за допомогою XOR-операції з коротким ключем.

Ваше завдання:

1. Виконати XOR.
2. Відновити початковий текст.

Повідомлення:

0a 45 0a 0e 06 0b 0e 11 59 06 00 0a 18 04 1e 0e

Ключ:

key

Завдання 11. XOR із однобайтовим ключем.

Опис завдання: Було перехоплено повідомлення у HEX-форматі. Відомо, що:

1. Для шифрування використовувався XOR.
2. Ключ складається лише з одного символу.

Ваше завдання:

1. Підібрати ключ.
2. Розшифрувати повідомлення.

Повідомлення:

2d 27 2a 2c 14 28 3f 2d

Завдання 12. XOR “повертає” дані.

Опис завдання: Аналітик стверджує, що XOR має незвичайну властивість: одна й та сама операція може і зашифрувати, і розшифрувати повідомлення. Необхідно перевірити це на практиці.

Ваше завдання:

1. Виконати XOR-операцію для кодування тексту, використовуючи ключ.
2. Повторно виконати XOR-операцію з ідентичним ключем.

Текст:

HELLO_CYBER

Ключ:

hack

Завдання 13. Шифр з журналів.

Опис завдання: Редактор газети закодував сенсаційну новину, щоб запобігти витоку раніше часу. Всі букви зміщені на 13 позицій.

Ваше завдання:

1. Відновити новину, змістивши літери на початкові позиції.

Закодована новина:

Gur pnfuvre fgbyr nyy gur zbarl!

Завдання 14. Темний форум.

Опис завдання: На закритому форумі невідома група залишила повідомлення для нових учасників. Щоб отримати доступ до наступного рівня, потрібно розшифрувати код.

Ваше завдання:

1. Визначити зміщення літер.
2. Розшифрувати повідомлення.
3. Отримати код доступу.

Повідомлення:

t4ha_v0hkc_i3sh3j_f4ii_a3o

Завдання 15. Сигнал із перехопленого каналу

Опис завдання: Під час налаштування старого радіоприймача в лабораторії студенти випадково зафіксували дивний сигнал. Він з'явився лише один раз – короткий, нестабільний і явно штучного походження. Ні голосу, ні музики – лише послідовність даних, ніби хтось передавав повідомлення, не призначене для звичайного прослуховування.

У записі немає жодних пояснень, лише три фрагменти, які виглядають як різні етапи обробки одного й того ж тексту.

Ваше завдання:

1. Виконати 3 етапи декодування повідомлення.

Перехоплений текст:

WE9SIGVuY29kZWQgdGV4dDogcnNzcnJzcnNicnNzc3Nyc3JicnNyc3Nzc3NicnNzcnJzcnJicnNzcnJzcnNicnNzcnJyc3NicnNzcnNzc3NicnNzcnJzcnJicnNzcnJzcnNicnNzcnJzcnNicnNyc3Nzc3NicnNzc3NycnJicnJzc3JycnJicnNzc3Jyc3IKS2V5IGZvciBkZWNvZGU6IDQyIChIRVgp==

Завдання 16. Інцидент на сервері.

Опис завдання: Під час аналізу Linux-сервера спеціаліст з кібербезпеки виявив підозрілий фрагмент журналу подій.

Є підозра, що зловмисник:

1. Передавав приховані дані.
2. Використовував кодування та просте шифрування.
3. Намагався приховати повідомлення від адміністратора.

Ваше завдання:

1. Проаналізувати лог.
2. Знайти приховані дані.
3. Визначити використані перетворення.
4. Відновити фінальне повідомлення.

Лог:

```
Jul 14 21:04:11 srv-web sshd[2241]: Failed password for admin from 192.168.1.15 port 4421 ssh2
Jul 14 21:05:02 srv-web app[3310]: tmp=576d68765a6e4a7761463933636c396d596d566f64585a6f5a6e683162486469
Jul 14 21:05:41 srv-web backup[1881]: archive status completed
```

ПРАКТИЧНЕ ЗАНЯТТЯ №2

Завдання 1. Перехоплене повідомлення.

Опис завдання: Під час аналізу мережевого трафіку аналітик перехопив повідомлення між двома учасниками закритого каналу зв'язку. Є підозра, що зловмисники використовували шифр Віженера замість простого Цезаря, щоб приховати структуру тексту.

Ваше завдання:

1. Розшифрувати повідомлення.
2. Визначити початковий текст.
3. Визначити, чому цей шифр складніше зламати.

Зашифроване повідомлення:

jgehvp bbxr kl eeimlfx

Ключ:

cyber

Завдання 2. Віженер без відомого ключа:

Опис завдання: Аналітик перехопив повідомлення, зашифроване шифром Віженера. Ключ невідомий, але є підозра, що він є коротким англійським словом із тематики кібербезпеки.

Ваше завдання:

1. Проаналізувати шифротекст.
2. Підібрати або визначити ключ.
3. Розшифрувати повідомлення.

Шифротекст:

pcwii tcvwv ycbo bgwt hltgok tazfv ktyjrzpe citcsti gcruiipq iicr yoecaquw stcbo kjc nijuyhi

Завдання 3. Витік повідомлень через повторне використання ключа.

Опис завдання: Аналітик перехопив два повідомлення від зловмисників. Є підозра, що вони використовували один і той самий XOR-ключ для шифрування. Одне з повідомлень вдалося частково відновити.

Ваше завдання:

1. Використати відомий фрагмент.
2. Визначити частину ключа.

3. Відновити друге повідомлення.

Відомий відкритий текст:

ATTACK_AT_NIGHT

Шифротекст №1:

2935372a2b2a3c2a3c3e2d222f2937

Шифротекст №2:

2935372a2b2a3c2a3c3e2d24272f

Завдання 4. AES та неправильний ключ.

Опис завдання: Під час аналізу ноутбука зловмисника SOC-команда знайшла зашифроване повідомлення.

Аналітики змогли визначити:

1. Використано AES.
2. Правильний ключ має відкрити справжній текст.
3. Неправильний ключ дає вибір випадкових символів.

Ваше завдання:

1. Спробувати розшифрувати повідомлення різними ключами.
2. Визначити правильний ключ.
3. Отримати секретне повідомлення.

Шифротекст:

560efd2c8e30ad5a17e6f6f1a2e5a292135aaefb9ba6c584779b2acc21c30d90

Можливі ключі:

Accessaccessacce

matrixmatrixmatr

cybercybercyberc

hackhackhackhack

Завдання 5. Перехоплені повідомлення.

Опис завдання: Під час моніторингу мережевого трафіку SOC-команда перехопила три повідомлення учасників закритого угрупування.

Після первинного аналізу з’ясувалось:

1. Зловмисники використовували різні алгоритми шифрування.
2. Для всіх повідомлень використовувалось одне й те саме ключове слово.

3. Новим учасникам інструкцію щодо ключа та параметрів роботи AES передавали в зашифрованому вигляді.
4. Для передачі цієї службової інформації використали дуже слабкий шифр.

Ваше завдання:

1. Проаналізувати перехоплені повідомлення.
2. Відновити ключове слово.
3. Визначити параметри AES.
4. Розшифрувати всі повідомлення.
5. Встановити місце та час операції зловмисників.

Ключ та параметри AES:

rlfdvyk novza ylwlha rlfdvyk av 16 ifalz mvy hlz tvkl lji

Повідомлення №1:

ylqjxz aifgks chxtz ol fokbazna

Повідомлення №2:

2a2d2a272b263c30273c2237203f30383b2a2122223a

Повідомлення №3:

57c8267c22d50cd9af9e948b9e005bedf10a3da3af5040d5a76e11a45f2e3a18

ПРАКТИЧНЕ ЗАНЯТТЯ №3

Завдання 1. Загублений список паролів.

Опис завдання: Під час аналізу старого сервера було знайдено фрагмент бази користувачів. Паролі у відкритому вигляді відсутні, залишилися лише хеші.

Ваше завдання:

1. Відновити якомога більше паролів.
2. Визначити, який пароль належав адміністратору.

Користувач + хеш:

eagle 5f4dcc3b5aa765d61d8327deb882cf99

shadow e10adc3949ba59abbe56e057f20f883e

falcon 25d55ad283aa400af464c76d713c07ad

ghost 0d107d09f5bbe40cade3de5c71e9e9b7

raven 21232f297a57a5a743894a0e4a801fc3

Завдання 2. Підмінений платіжний документ.

Опис завдання: Після компрометації поштового сервера бухгалтерія отримала два файли платіжного доручення. Співробітник стверджує, що один із документів був змінений зловмисником під час передачі. Відомо, що для оригінального документа раніше було збережено SHA256-хеш.

Ваше завдання:

1. Обчислити SHA256 для отриманих документів.
2. Порівняти результати з еталонним значенням.
3. Визначити, який документ є оригінальним.

Вхідні дані:

task2_document_A.txt

task2_document_B.txt

Еталонний SHA256:

61bcc983ce219bc0e8205efc7758be9ee338fae5fea07b630ac8d8fbae9a5396

Завдання 3. Таємний ключ без передачі ключа.

Опис завдання: Під час моніторингу мережевого трафіку аналітик перехопив увесь обмін даними між двома учасниками закритого каналу зв’язку. Відомо, що для встановлення захищеного з’єднання використовувався алгоритм обміну ключами Діффі–Хеллмана. Аналітик бачить усі передані значення, але не бачить секретний ключ, який сторони отримали в результаті обміну.

Ваше завдання:

1. Обчислити відкриті ключі учасників.
2. Визначити спільний секретний ключ.
3. Переконатися, що обидві сторони отримали однаковий результат.

Вхідні дані:

Публічні параметри:

p = 23

g = 5

Секретне число Alice:

a = 6

Секретне число Bob:

b = 15

Завдання 4. Операція Black Raven.

Опис завдання: Після затримання одного з операторів угрупування SOC-команда отримала набір цифрових артефактів. Під час аналізу встановлено, що всі знайдені дані пов'язані між собою. Для отримання інформації про заплановану операцію необхідно послідовно проаналізувати всі артефакти.

Ваше завдання:

1. Відновити пароль оператора.
2. Використати його для розшифрування службового повідомлення.
3. Визначити справжній документ операції.
4. Встановити місце та час проведення операції.

Артефакт №1. Обліковий запис оператора:

Username: operator

Хеш пароля: 0d107d09f5bbe40cade3de5c71e9e9b7

Артефакт №2. Службове повідомлення.

Аналітикам вдалося встановити, що пароль оператора використовувався як ключове слово для шифрування повідомлення за алгоритмом Віженера.

nlxoo lbnyfqrb ulwa

Артефакт №3. Документи операції:

task4_document_A.txt

task4_document_B.txt

Артефакт №4. Контрольна сума:

Оригінальний документ повинен відповідати SHA256:

02923697501f752a716fb6b78e4ccddf5cf5aa95c9625de691869db0d74773a3

БОНУСНЕ ЗАВДАННЯ. Атака на хеш користувача Linux з використанням словника для перебору з метою зламу пароля.

Завдання на платформі PicoCTF для формування портфоліо з метою долучення до університетської кіберкоманди:

1. https://learn.cylabacademy.org/library/418?page=1&category=2&difficulty=1
2. https://learn.cylabacademy.org/library/144?page=1&category=2&difficulty=1
3. https://learn.cylabacademy.org/library/475?page=1&category=2&difficulty=1