Міністерство освіти і науки України
Національний університет водного господарства та природокористування
Навчально-науковий інститут економіки та менеджменту

Кафедра філософії та кільтурології

06-07-244М

МЕТОДИЧНІ ВКАЗІВКИ
(повторне видання)
до практичних занять з навчальної дисципліни
«Цифрова безпека»
для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Креативна та цифрова культура» спеціальності 034 «Культурологія» денної форми навчання

Рекомендовано
науково-методичною радою
з якості ННІ ЕМ
Протокол № 7 від «28» грудня 2023 р.

Рівне – 2023

Методичні вказівки до практичних занять з навчальної дисципліни «Цифрова безпека» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Креативна та цифрова культура» спеціальності 034 «Культурологія» денної форми навчання. [Електронне видання] / Рейнська В. Б. – Рівне : НУВГП, 2022. – 37 с.

Укладач:
Рейнська В. Б., кандидат економічних наук, доцент кафедри філософії та культурології.

Відповідальний за випуск: Шадюк Т. А., к.філос.н., доцент завідувач кафедри філософії та культурології.

Керівник групи забезпечення
спеціальності «Культурологія» Коберська Т. А. , к.філос.н., доцент, доцент кафедри філософії та культурології.

ЗМІСТ

ВСТУП

Розвиток людського суспільства нерозривно пов'язаний із процесом інформатизації, під яким розуміється безперервно поновлюваний процес створення необхідних умов задоволення інформаційних потреб людини. Протягом усієї історії людської цивілізації і навіть на початковій стадії виникали потреби, пов'язані з отриманням, зберіганням, накопиченням, первинною обробкою, переробкою, пошуком, відображенням, передачею і обміном інформацією.

Сучасний етап інформатизації характеризується створенням інформаційних систем та систем телекомунікації із застосуванням засобів персональної електронної обчислювальної техніки. В результаті накопичення світового практичного досвіду, знань та культурних цінностей кордони національних економік поступово стираються та формується інформаційне суспільство, яке розвивається у відповідному інформаційному просторі.

Під цифровою безпекою розуміється стан захищеності від інформаційних загроз, збереження властивостей об'єкта цифрової безпеки, які зумовлені інформацією, її потоками та інформаційною інфраструктурою.

Програма вибіркової навчальної дисципліни циклу фахової підготовки ВБ 1.1 «Цифрова безпека» складена відповідно до освітньо-професійної програми «Креативна та цифрова культура» підготовки бакалавра спеціальності «Культурологія».

Предметом вивчення навчальної дисципліни «Цифрова безпека» – є класифікація різних видів загроз інформації, виклад політики безпеки, розгляд сучасних методів криптографічного захисту інформації та основ інформаційної безпеки в прогресивних культурних

середовищах. Розглянуті основні поняття є основними при вивченні ряду розділів навчальних курсів спеціалізації «Креативна та цифрова культура».

Метою курсу є формування у майбутніх спеціалістів у області креативної та цифрової культури структури знань про основні поняття та методи захисту інформації та програмного забезпечення (системного, прикладного, інструментального). В контексті даного курсу захист інформації та програмного забезпечення розглядається як комплекс методів забезпечення необхідного рівня фізичної та логічної доступності, цілісності та конфіденційності при існуючих потенційних загрозах.

Курс включає вивчення концептуальних, інформаційних, програмних, фізичних, психологічних, криптографічних, правових, системотехнічних та практичних основ захисту, що разом реалізують парадигму багаторівневої розподіленої системи з урахуванням обмежень кожного методу захисту.

У результаті вивчення навчальної дисципліни студент повинен

знати:

– термінологію, завдання та функції дисципліни;
– топологію цифрової безпеки та підходи до класифікації цифрових загроз;
– основні принципи захисту від несанкціонованого доступу, копіювання, руйнівних програмних засобів, криптографічного захисту, виконання захищених програм та роботи із захищеними програмами.

уміти:

– проводити класифікацію інформації;
– встановити чинники, що впливають на захист інформації;
– ідентифікувати види інформаційних загроз;

– визначати цілі і принципи захисту інформації
– застосовувати методи та форми цифрової безпеки;
– вирішувати стандартні завдання професійної діяльності із застосуванням інформаційно-комунікаційних технологій з урахуванням основних вимог цифрової безпеки;
– вільно орієнтуватися в положеннях сучасної доктрини цифрової безпеки;
– володіти навичками використання комп'ютерної техніки та інформаційних технологій у сфері цифрової безпеки.

1. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва змістових модулів і тем	Кількість годин			
	Лекції	Практ	СРС	Разом
Модуль 1.				
Тема 1. Основи цифрової безпеки та захисту інформації.	2	2	15	19
Тема 2. Програмно-апаратні засоби забезпечення інформаційної безпеки у комп'ютерних системах.	4	4	15	23
Тема 3. Криптографічні системи.	4	4	15	23
Тема 4. Основи побудови комп'ютерних мереж.	4	4	15	23
Модуль 2.				
Тема 5. Введення в аналіз мережевого трафіку.	4	4	15	23
Тема 6. Мережеві атаки: методи злому та захисту.	4	4	15	23
Тема 7. Безпека веб -додатків.	4	4	15	23
Тема 8. Організаційне та правове забезпечення інформаційної безпеки.	4	4	15	23
Усього годин	30	30	120	180

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Теми	Кількість годин
Модуль 1.		
1.	Основи цифрової безпеки та захисту інформації.	2
2.	Програмно-апаратні засоби забезпечення інформаційної безпеки у комп'ютерних системах.	4
3.	Криптографічні системи.	4
4.	Захищені способи передачі даних.	4
Модуль 2.		
5.	Введення в аналіз мережевого трафіку	4
6.	Мережеві атаки: методи злому та захисту.	4
7.	Безпека веб - додатків	4
8.	Організаційне та правове забезпечення інформаційної безпеки.	4

2. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Методичні поради по підготовці до семінарських занять. Практичні завдання є важливою формою роботи студентів по оволодінню змістом дисципліни «Цифрова безпека». Освоївши лекційні матеріали, студент готується до практичного заняття у відповідності до поданого плану. Необхідною умовою якісної підготовки є розуміння принципів роботи механізмів зламу та захисту цифрового об'єкту. При підготовці студент повинен користуватися нижче вказаною літературою. Для самостійної перевірки засвоєних знань до кожного заняття сформульовані

контрольні питання.

3. ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

ТЕМА 1. Основи цифрової безпеки та захисту інформації.

Основні поняття і категорії: шифрування даних в операційній системі Windows; захист портативних носіїв даних; безпека при використанні мереж Wi-Fi; безпечний веб-серфінг; вибір надійних паролів; ознаки фішингової атаки; захист від фішингових атак.

План

1. Захист персональних даних.
2. Надійні паролі та двофакторна авторизація. 3. Безслідне видалення даних.
4. Приватний обмін інформацією. 5. Фішингові атаки.

Контрольні питання:

1. Як відбувається шифрування даних в операційній системі Windows.
2. Опишіть алгоритм захисту даних на портативних носіях.
3. Які загрози виникають під час підключення до відкритої мережі Wi-Fi?
4. Яким чином можна захистити власну мережу Wi-Fi?
5. Що ви розумієте під персональним захистом даних?
6. Що таке приватний режим браузерів?
7. Що таке HTTPS?
8. Що таке HTTPS Everywhere?
9. Яким чином можна очистити історію браузера та що таке cookie-файли?
10. У яких випадках доцільно використовувати файл - ключ?
11. Що таке менеджер паролів?

12. Ознаки фішингової атаки.

Практичні завдання:

1. Встановіть на власний браузер модуль HTTPS Everywhere та продемонструйте його роботу за допомогою знімків екрана.
2. Проведіть очистку історії браузера за певний вибраний період з варіацією опцій очистки та продемонструйте процес за допомогою відео.
3. Створіть нового користувача браузера та наповніть менеджер паролів п'ятьма новими записами, продемонструйте результат за допомогою знімку екрана.
4. Видаліть cookie-файли трьох випадково обраних сайтів, продемонструйте результат за допомогою знімку екрана.

ТЕМА 2. Програмно-апаратні засоби забезпечення інформаційної безпеки у комп'ютерних системах.

Основні поняття і категорії: віруси; троянські програми; антивірусні програми; онлайн-перевірка файлів на віруси; індикатор зламування; введення в «Tails».

План

1. Шкідливі програми та захист від них 2. Кіберзлочинність
3. Захист від шкідливих програм 4. Операційна система «Tails»

Контрольні питання:

1. Що таке ботнети?
2. Розкажіть про платні дзвінки та SMS-повідомлення.
3. Яким чином відбувається крадіжка електронних грошей.
4. Опишіть принцип крадіжок банківських даних.
5. Що таке кібершантаж?
6. Які є види цільових атак?
7. Що таке віруси?

8. Що таке «Network worms»?
9. Які ви знаєте троянські програми?
10. Що потрібно робити при виявленні шкідливої програми?

Практичні завдання:

1. Відкрити антивірусну програму, виконати налаштування параметрів її роботи, запустити перевірку та сформувати звіт за результатами роботи.

ТЕМА 3. Криптографічні системи.

Основні поняття і категорії: закриті та відкриті ключі; сертифікати безпеки; хешування; електронний підпис; Gpg4win; основи шифрування.

План

1. Основи шифрування.
2. Ознайомлення з Gpg4win.
3. Надсилання зашифрованих повідомлень.
4. Читання зашифрованих повідомлень.

Контрольні питання:

1. Що таке електронний підпис?
2. Опишіть основні принцип роботи PGP?
3. Що таке «мережа довіри»?
4. Які є види оповіщення адресатів про використання PGP?
5. Яким чином відбувається завантаження ключів на сервер ключів?
6. Як відбувається пошук інших користувачів PGP?
7. Опишіть алгоритм відкликання PGP-ключа.

Практичні завдання:

1. Зашифруйте будь-який текст за допомогою Gpg4win, та відправте його на пошту викладачу, попередньо обмінявшись з викладачем відкритими ключами через зашифровані електроні листи за допомогою сервісу

ProtonMail.
2. Помістіть будь-який текст у зашифрований контейнер (під виглядом медіа файлу) та відправте його на пошту викладачу, пароль до зашифрованого контейнеру відправте у зашифрованому електронному листі через сервіс ProtonMail.

ТЕМА 4. Захищені способи передачі даних.

Основні поняття і категорії: основи безпечного спілкування; загрози безпеки стільникового зв'язку; приватний обмін миттєвими повідомленнями; використання проксі-серверів; використання анонімайзерів; проксі-сервер; VPN; TOR.

План

1. Приватний обмін інформацією. 2. Використання проксі-серверів. 3. Віртуальні приватні мережі.
4. Анонімні мережі.

Контрольні питання:

1. Які існують загрози безпеки стільникового зв'язку?
2. Розкажіть про приватний голосовий зв'язок.
3. Розкажіть як налаштувати браузер для роботи через проксі-сервери?
4. Як правильно налаштувати мобільний пристрій для роботи через проксі-сервери?
5. Як налаштувати VPN-тунель через протокол SSTP? 6. Як відбувається підміна IP-адрес DNS-серверів?
7. Які існують додаткові способи альтернативної передачі даних?
8. Розкажіть ро децентралізовані анонімні мережі.
9. Розкажіть про принцип роботи Tor.

Практичні завдання:

1. Встановіть на комп’ютер будь-який проксі-сервер (або у вигляді додатка для браузеру) та підтвердіть його справну

роботу за допомогою знімків екранів. Використавши для цього однин із будь-яких онлайн сервісів, що дозволяють відстежити IP користувача.
2. Налаштуйте VPN на домашній операційний системі за допомогою вбудованого інструментарію ОС та зробіть в підтвердження виконаної роботи знімки екрану, що відображають усю послідовність дій даної роботи.
3. Встановіть TOR-браузер та зареєструйте на будь-якому форумі у даркнеті двох користувачів, в подальшому організуйте між ними фіктивну переписку у кількості двох листів з використанням GPG-шифрування. В підтвердження пришліть на пошту викладача послідовність знімків екрану, що підтверджують виконану роботу.

ТЕМА 5. Введення в аналіз мережевого трафіку.

Основні поняття і категорії: OSINT; сканування портів; отримання інформації від DNS-сервера; отримання інформації з використанням SNMP, NetBIOS; пошук вразливостей.

План

1. Отримання інформації з відкритих джерел.
2. Отримання інформації від мережевих сервісів.

Контрольні питання:

1. Що таке OSINT?
2. Розкажіть про методику використання Google для збирання інформації.
3. Як можна визначити активний хост чи ні?
4. Які існують типи записів?
5. Розкажіть про принципи взаємодії із DNS-сервером.
6. Що таке MX-записи?
7. Що таке NS-запити?
8. Як працює процедура перебору імен?
9. В чому полягає принцип передачі зони DNS?

Практичні завдання:

1. Проведіть повний аналіз вибраного вами домену за допомогою OSINT методів та сформуйте із отриманої інформації звіт у вигляді .doc файлу.
2. Проведіть аналіз вразливостей домашньої або іншої мережі за допомогою SPARTA та складіть звіт у вигляді .doc файлу.

ТЕМА 6. Мережеві атаки: методи злому та захисту.

Основні поняття і категорії: пасивне перехоплення трафіку; активне перехоплення трафіку; системи виявлення атак; брандмауери; приманки.

План

1. Перехоплення інформації.
2. Обхід систем безпеки.
3. Захист.

Контрольні питання:

1. Який зв'язок між вразливістю та експлойтом?
2. Вразливості якого класу вважають найбільш небезпечними?
3. Яким є визначення віддаленої вразливості?
4. Який інструмент може виконувати внутрішнє та зовнішнє сканування PCI DSS?
5. Який інструмент створено спеціально для аудиту Linux-систем?
6. Який інструмент інтегрований у SPARTA для сканування сайту?
7. Який зв'язок між вразливістю та експлойтом?
8. Вразливості якого класу вважають найбільш небезпечними?
9. Яким є визначення віддаленої вразливості?

Практичні завдання:

1. Зробіть захоплення пакетів (за певний проміжок часу) за допомогою Wireshark та збережіть захоплені дані у файл

попередньо відфільтрувавши пакети за власним фільтром.

ТЕМА 7. Безпека веб – додатків.

Основні поняття і категорії: збір інформації; карта веб-додатку; мислення хакера; застосування даних, отриманих у процесі розвідки; безпечна архітектура додатків; перевірка безпеки коду; протидія впровадженню; протидія DoS-атакам; захист сторонніх залежностей.

План

1. Введення у розвідку веб-додатків 2. Введення у злом веб-додатків
3. Захист сучасних веб-додатків

Контрольні питання:

1. Проведіть аналіз сучасних та ранніх версій веб-додатків.
2. У чому полягає сутність аналізу API?
3. Які є в браузері інструменти аналізу?
4. Розкажіть які є методи виявлення сторонніх залежностей?
5. Яким чином можна провести пошук слабких місць в архітектурі програми?
6. Що таке XSS? 7. Що таке CSRF?
8. Що таке XXE?
9. Що таке DoS?
10. Які є методи перевірка безпеки коду?
11. Розкажіть про методологію пошуку вразливостей.

Практичні завдання:

1. Виберіть один із типів атак на веб-додатки та опишіть алгоритм протидії даному виду атаки.

ТЕМА 8. Організаційне та правове забезпечення інформаційної безпеки.

Основні поняття і категорії: інформаційні права громадян, інформаційна безпека, механізми забезпечення

інформаційної безпеки.

План

1. Правове забезпечення інформаційних прав громадян
2. Механізми забезпечення інформаційної безпеки

Контрольні питання:

1. Що таке інформаційна безпека?
2. Назвіть об'єкти і суб'єкти інформаційної безпеки.
3. Назвіть основні складові інформаційної безпеки.
4. Перерахуйте основні функції системи забезпечення інформаційної діяльності.

Практичні завдання:

1. Назвіть основні загрози національній безпеці України.
2. Яка державна структура є головною з питань криптографічного та технічного захисту інформації.
3. Основні завдання Держспецзв'язку.

4. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИКОНАННЯ ПРАКТИЧНИХ ЗАВДАНЬ

4.1. Криптографічні системи. Програми сімейства GPG (GNU Privacy Guard) / PGP (Pretty Good Privacy) дозволяють «прозоро» підписувати та зашифровувати всі типи цифрової інформації. За своєю суттю названі інструменти є лише зручною обгорткою, яка спрощує практичне використання відкритих алгоритмів асиметричної криптографії.

Декілька років ведеться полеміка про актуальність використання GPG, в рамках якої висловлюється багато скептицизму про громіздкість та старіння цього криптографічного продукту.

В багатьох UNIX-подібних операційних системах програмний комплекс «Клеопатра» є в репозиторіях за

замовчуванням. Для того щоб встановити дану програму в Debian потрібно в терміналі виконати наступну команду:

```
sudo apt-get install kleopat
```

Для Windows програма поширюється в пакеті GPG4Win, що поєднує кілька корисних інструментів: безпосередньо Kleopatra, GpgEX – зручний плагін для провідника Windows, який додає в контекстне меню пункти «Зашифрувати», «Підписати», «Розшифрувати», «Перевірити контрольні суми» і деякі інші, GPA – ще один більш простий на вигляд і менш функціональний менеджер ключів, GpgOL – плагін для поштового клієнта Outlook).

Перший крок у використанні GPG – створення пари ключів. Публічний ключ надається всім охочим, а секретний зберігається в надійному місці і служить для підписання інформації від імені його власника та розшифровки адресованої йому інформації.

На вибір пропонуються типи ключів X.509 (практично застосовується у корпоративному середовищі) та OpenPGP. Вибираємо OpenPGP. Вводимо контактні дані, які відображатимуться у всіх власників нашого відкритого ключа. Замість цього імені можна вказати псевдонім. Пізніше деяку інформацію ключа можна буде змінити.

За замовчуванням використовується шифрування RSA з довжиною ключа 2048 біт (2048 нулів і одиниць машинного коду). З урахуванням розвитку квантових технологій, це шифрування все менш і менш здається надійним. В даний час добре зарекомендувало використання криптографії на еліптичних кривих. Подібні алгоритми мають неймовірну криптостійкість та хорошу продуктивність завдяки невеликій довжині ключа.

Щоб створити пару ключів на еліптичних кривих, переходимо до додаткових параметрів. Пункт ECDSA/EdDSA – те, що нам потрібно. Додатковий чекбокс

(галочка) +ECDH дасть ключу можливість шифрувати, без неї сертифікат можна буде використовувати тільки для підпису та ідентифікації, оскільки ECDSA/EdDSA – алгоритми підпису, а не шифрування. У списках пропонується вибрати один з алгоритмів: ed25519, brainpool і NIST.

ed25519 (Curve25519)– еталонна та непатентована реалізація криптографії на еліптичній кривій, має 128-бітну довжину. Є ключем EdDSA – найактуальнішим алгоритмом цифрового підпису (вважається, що намістить прихованих «закладок» від силових структур будь-яких країн).

brainpool – алгоритм, розроблений німецькою спільнотою криптографів, до яких входять університети, державні відомства та комерційні організації (наприклад компанія Bosch). Підтримує довжини 256, 384 і 512 біт. При підписі використовує дещо застарілий алгоритм ECDSA.

NIST – американський алгоритм, розроблений Національним Інститутом Стандартів та Технологій. Рекомендований для використання державними органами США. Підтримує довжини 256, 384 і 521 біт. За оцінкою деяких фахівців, NIST краще brainpool за продуктивністю. При підписі використовує дещо застарілий алгоритм ECDSA.

На наступному етапі задається пароль, який є останнім кроком захисту секретного ключа. Не слід передавати комусь секретний ключ, але якщо так все-таки вийшло, буде краще, коли ви задали дуже надійний пароль.

Рекомендується використовувати спеціальні знаки (символи пунктуації тощо) для захисту від брутфорсу. Найкращим варіантом буде довгий пароль, отриманий з генератора випадкових символів, проте не забувайте про

золоту середину між використанням та безпекою. Наприклад, вводити на телефоні дуже довгий і складний пароль із символами з розширеної таблиці ASCII, не маючи можливості його скопіювати з менеджера паролів, буде дуже проблематично.

Клеопатра пропонує зробити резервну копію ключів, що є експортом закритого ключа. Цю операцію надалі можна зробити будь-якої миті. Відкривши експортований ключ у текстовому редакторі, ми побачимо специфічний фрагмент тексту, який починається словами «BEGIN PGP PRIVATE KEY BLOCK». Будьте уважні, не надішліть його комусь помилково! Відкриті ключі, призначені передачі іншим особам, починаються зі слів «BEGIN PGP PUBLIC KEY BLOCK».

Велика перевага GPG перед іншими засобами ідентифікації полягає у легкій переносності ключа.

Експорт та імпорт

Для імпорту ключів (нашого вже існуючого на новому пристрої або отриманого публічного) скористаємося кнопкою «Імпорт». Також можна використовувати подвійний клік за файлом ключа, це автоматично відкриє Клеопатру та імпортує вибраний ключ. GPG-файли зустрічаються з розширеннями *.asc, *.pgp та *.gpg. Це не має великого значення, тому що розширення потрібно більше для зручності користувача і лише небагато додатків. Файл буде коректно прочитаний і у випадку, коли спеціальне розширення змінено або видалено.

Дуже часто ключі розповсюджуються як текстовий блок. У такому разі, скопіювавши ключ, можна імпортувати його через меню операцій із буфером обміну. Програма попросить переконатись у справжності ключа. В даний час найпростішим та ефективнішим способом є порівняння

відбитка, тому його публікують разом із ключем. Якщо відбиток збігається із заявленим, засвідчуємо сертифікат.

Тепер ми можемо перевіряти підпис власника нового ключа та шифрувати для нього інформацію.

Шифрування та підпис

Щоб зашифрувати та підписати файл, скористаємося відповідним пунктом меню на верхній панелі. Після вибору файлу пропонується вибрати потрібні операції. Підпис дозволяє користувачеві переконатися в авторстві файлу.

Ця функція дуже корисна: розшифрувавши зашифрований файл, ми точно знаємо, що файл був зашифрований власником даного ключа, а не кимось іншим, хто просто має в своєму розпорядженні наш публічний ключ.

Найпоширенішим способом безпечного зберігання даних на хмарному сховищі є GPG-шифрування файлів «для себе». У такому разі розшифрувати інформацію можна буде лише нашим ключем. Також можливий підпис без шифрування. Найчастіше застосовується до текстової інформації. Механізм підписання будується на хеш-сумі: дозволяє порівняти актуальний стан інформації про те, якою вона була, коли її підписував відправник. Для прикладу можна відкрити блокнот і написати будь-яке повідомлення.

Призначивши відсутність шифрування для будь-кого, залишаємо тільки підпис і натискаємо кнопку «Підписати». Після введення пароля від ключа, можна побачити, що до розшифрованої фрази буде добавлений додатковий текстовий блок із хеш-сумою SHA512. Якщо перевірити підпис, він буде вірний, але якщо змінити хоча б один символ або додати пробіл, перевірка виявить недійсний для цього тексту підпис.

Усі локальні ключі централізовано зберігаються на пристрої у спеціальній папці. Усі програми, що взаємодіють з GPG, їх бачитимуть. Для спілкування протоколу XMPP (Jabber), захищеного GPG-шифруванням, можна використовувати Gajim, який також є кросплатформним. Для ведення захищеного листування зручно використовувати поштовий клієнт Thunderbird, у який необхідно буде імпортувати секретний ключ, оскільки він має своє ізольоване сховище ключів.

Створення зашифрованого контейнера

VeraCrypt – програмне забезпечення, яке використовується для шифрування «на льоту». VeraCrypt – безкоштовний і відкритий проект. Для створення зашифрованого файлового контейнера потрібно запустити VeraCrypt та натиснути «Створити Том».

У вікні майстра створення томів необхідно вибрати, який тип тома необхідно створити. VeraCrypt може розміщувати зашифрований том у файлі, розділі диска або на диску повністю. У разі ми вибираємо перший пункт. Оскільки він стоїть за замовчуванням, досить просто натиснути кнопку «Далі».

На цьому кроці вам необхідно вибрати тип тому створювати, стандартний або прихований. Виберіть «Звичайний том» VeraCrypt та натисніть «Далі».

В подальшому необхідно вказати ім'я файлу, який буде зашифрованим контейнером для зберігання даних. Для продовження натисніть «Файл» після чого відкриється стандартне діалогове вікно вибору файлів Windows, в якому необхідно вказати шлях та ім'я нового файлу контейнера VeraCrypt. У цьому випадку ми створили файл VeraCrypt Volume у папці «C:\VeraCrypt».

Зверніть увагу, що якщо Ви виберете вже існуючий файл, його буде видалено, а на його місці буде створено

новий файл з таким же ім'ям. Якщо файл з такою назвою у вибраній папці немає, його буде створено. Файли VeraCrypt є звичайними файлами, вони можуть бути видалені, переміщені та скопійовані так само, як будь-які інші файли у Windows. Після того як Ви вибрали шлях та ім'я, натисніть «Зберегти».

У вікні майстра створення томів натисніть «Далі».

В подальшому потрібно вибрати тип алгоритму шифрування та хешування, залишмо значення AES та SHA-512 за умовчанням, як найсильніший варіант. Виберемо розмір тому 1024 МБ, звичайно, можна вказати будь-яке потрібне значення і натиснути кнопку «Далі».

Найважливішим кроком є процедура створення надійного паролю, який буде використовуватися для доступу до зашифрованих даних. В даному процесі варто дуже уважно ознайомитись із рекомендаціями розробників у вікні майстра створення томів про те, як вибрати надійний пароль. На додаток до паролю або окремо можна використовувати ключовий файл, створити або вибрати існуючий.

або пошкодження Ви не зможете отримати доступ до даних у контейнері. Після вибору надійного паролю та/або ключового файлу натисніть кнопку «Далі».

Для зберігання файлів розміром більше 4 Гб у зашифрованому контейнері виберіть Файлову систему NTFS, для невеликих контейнерів краще використовувати FAT або exFAT. Хаотично переміщуйте вказівник миші в рамках вікна майстра створення томів, як мінімум доти, поки індикатор не стане зеленим, чим довше Ви пересуваєте мишу, тим краще. Це дозволяє значно посилити криптостійкість ключа шифрування. Потім натисніть «Розмітити». Розпочнеться створення зашифрованого тому, залежно від його вибраного розміру та швидкодії комп'ютера створення зашифрованого

контейнера може тривати довгий час.

Далі ми будемо монтувати і використовувати щойно створений зашифрований контейнер за прямим призначенням. У головному вікні програми виберіть бажану літеру диска (у нашому випадку це F) та натисніть кнопку «Файл». У діалозі виберіть файл зашифрованого контейнера який ми створили в попередніх кроках. Ви повернетеся до головного вікна програми.

Натисніть кнопку «Змонтувати», після чого з'явиться діалогове вікно введення пароля та/або вибору ключового файлу.

Ми успішно змонтували зашифрований контейнер як диск F. Цей диск повністю зашифрований (включаючи імена файлів, таблицю розділів, вільне місце). Ви можете працювати з цим диском так само, як і з будь-яким іншим диском у вашій системі, копіювати, зберігати, переміщувати файли. Як тільки Ви розміщуєте файл на цьому диску, він відразу зашифровується на льоту.

Після того як Ви розмістите файли в зашифрованому контейнері, важливо безповоротно видалити оригінали за допомогою будь-якої програми для незворотного стирання файлів. Зверніть увагу, VeraCrypt ніколи не зберігає розшифровані дані на диск – коли ви працюєте із зашифрованим контейнером він завжди зашифрований, а файли розшифровуються на льоту і зберігаються в оперативній пам'яті. Це гарантує, що у разі раптового вимкнення живлення або перезавантаження всі файли в контейнері залишаться зашифрованими. Якщо Вам необхідно перезавантажити операційну систему або припинити доступ до контейнера потрібно вибрати відповідну букву диска та натиснути «Розмонтувати».

4.2. Введення в аналіз мережевого трафіку. Аналізатори мережного трафіку або Network traffic analysis (NTA) – це категорія продуктів безпеки, яка використовує мережеві

комунікації як основне джерело даних для виявлення та розслідування загроз безпеки, аномальної або шкідливої поведінки в мережі. Практика збору мережевих даних, їх аналізу та прийняття рішень на основі отриманих результатів існує вже кілька десятиліть.

Системи безпеки Network traffic analysis (NTA) захищають мережу організації та її інфраструктуру шляхом виявлення загроз інформаційної безпеки. Забезпечують оперативне реагування на виявлені загрози, контролюють дотримання всіх політик. Ця категорія продуктів передає всю необхідну інформацію про події, що відбуваються всередині мережі, до центрів моніторингу та реагування (SOC) та SIEM-систем, а також дозволяє виконувати ретроспективний пошук, організувати централізовану протидію кібератакам, сприяє розслідуванню інцидентів.

Для виявлення та ідентифікації просунутих, переважно цільових атак (APT) як ніколи краще підходять системи аналізу мережного трафіку. Вони ж під час своєї роботи перехоплюють великі потоки даних їхнього сканування.

Ключові функції, які так чи інакше включає кожен аналізатор мережевого трафіку:

Аналіз мережевих даних як реального часу. Для забезпечення точного виявлення, розслідування та реагування протягом невизначеного періоду часу, коли загрози можуть бути дійсно небезпечними, кожен продукт NTA повинен проводити дослідження мережі на загрози в режимі реального часу.

Повна видимість операцій. Для того, щоб аналізатор мережного трафіку забезпечував високоточне розуміння поведінки загроз, він повинен мати можливість бачити та аналізувати фактичний зміст мережевих взаємодій. Це означає, що потрібна

повна видимість, починаючи з L2 і закінчуючи рівнем L7. Поряд з цим виконується декодування прикладного протоколу та розшифровка сучасних криптографічних стандартів. *Безпечне, контрольоване розшифрування трафіку.*Наразі понад 70% веб-трафіку зашифровано, і це число швидко зростає. Усередині корпоративних мереж кількість трафіку, що шифрується, також швидко зростає і доходить до 100%. Хоча шифрування є життєво важливим для захисту конфіденційних даних, воно також створює сліпі зони для технологій, що забезпечують безпеку. Однією з основних цілей інструментів NTA є надання повної видимості, що означає, що кожен продукт класу NTA має здатність розшифровувати трафік для аналізу без шкоди.

Нормальна поведінка та виявлення аномалій. Кожен продукт Network traffic analysis повинен мати здатність моделювати базову діяльність пристрою та активність користувача з подальшим порівнянням нових спостережень з поведінкою, яка була прийнята за нормальну. Поведінкова аналітика – це найкращий спосіб отримати дієву інформацію про стан загроз у мережі.

Розвідка з відкритих джерел

Одним із ключових термінів, пов'язаних із збиранням інформації, є розвідка по відкритих джерелах – Open Source Intelligence (OSINT). OSINT – це інформація, отримана із джерел, не захищених засобами контролю безпеки. Ці засоби контролю повинні перешкоджати витоку інформації. Нерідко це відомості з громадських

записів або інформація, якою цільові організації обмінюються при своїй повсякденній діяльності.

Використання спільних ресурсів

В Інтернеті існує кілька загальнодоступних ресурсів, які можна використовувати для збору інформації про цільовий домен. Перевага використання цих ресурсів полягає в тому, що мережевий трафік не надсилається безпосередньо до цільового домену, тому в журнал подій цільового домену такі дії не записуються.

Запит інформації про реєстрацію домену

Після того як ви дізнаєтесь цільове доменне ім'я, вам потрібно запросити базу даних Whois і знайти інформацію про цей домен. База даних Whois надасть інформацію про DNS-сервер та контактну інформацію домену. Whois – це протокол для пошуку реєстрацій в Інтернеті, баз даних зареєстрованих доменних імен, IP-адрес та автономних систем.

Аналіз записів DNS

Метою використання засобів категорії запису DNS є збір інформації про DNS-сервери та відповідні записи цільового домену. Наприклад, при тестуванні на проникнення клієнт може попросити вас дізнатися про всі хости та IP-адреси, доступні для
їхнього домену. Єдина інформація, яку ви маєте, – це доменне ім'я організації.

Deepmagic Information Gathering Tool (DMitry) – інструмент для збирання інформації «все в одному». Його можна використовувати для збору наступної інформації:

- запису протоколу Whois (отримання реєстраційних

даних про власників доменних імен) із застосуванням IP-адреси або доменного імені;

- відомостей про хост від https://www.netcraft.com/;
- даних про піддомени в цільовому домені;
- адрес електронної пошти цільового домену.

Щоб отримати доступ до DMitry введіть у командний рядок таку команду:

```
# dmitry -iwnse hackthissite.c
```

Maltego – програма з відкритим кодом, яка призначена для розвідки та криміналістики. Воно дозволяє видобувати, збирати та систематизувати інформацію. Maltego збирає інформацію із відкритих джерел. Після того як інформація буде зібрана, Maltego допоможе визначити ключові зв'язки між даними та відобразити їх у графічному вигляді. Таке відображення інформації полегшить сприйняття.

Інструмент tcptraceroute у дистрибутивах Linux є доповненням до команди traceroute. Головна перевага використання tcptraceroute полягає в тому, що ми можемо по дорозі від машини тестувальника до цільової машини зустріти брандмауер. Брандмауери часто налаштовуються для фільтрації трафіку ICMP та UDP, пов'язаного з командою traceroute. У цьому випадку інформація про трасування буде спотворена. Використання інструменту tcptraceroute дозволяє встановити TCP-з'єднання на певному порту, через який брандмауер дозволить вам пройти, тим самим показавши шляхи мережевої маршрутизації брандмауер.

Для запуску tcptraceroute у командному рядку слід ввести таку команду:

```
# tcptracerou
```

Metagoofil – це інструмент, який використовує

пошукову систему Google для отримання метаданих із документів, доступних у цільовому домені. В даний час підтримуються такі типи документів: .docx; .doc; .xlsx; .xls; .ods; .pptx; .ppt; .odp; .pdf.

Ідентифікація цільової машини

Інструменти цієї категорії використовуються для визначення цільових машин, до яких випробувач може отримати доступ. Перш ніж розпочати процес ідентифікації, ми повинні знати умови та угоди, які пред'являються нашим клієнтом.

ping – найвідоміший і найчастіше застосовуваний інструмент, який використовується для перевірки доступності конкретного хоста.

```
ping -c 1 172.16.43.1
```

fping – різниця між ping та fping полягає в тому, що інструмент fping може відправляти ping кільком хостам одночасно. У командному рядку можна вказати кілька цільових комп'ютерів або використовувати файл, який містить хости для перевірки зв'язку.

```
# fping 172.16.43.156 172.16.43.150
172.16.43.1
```

Сканування вразливостей – процес виявлення та аналізу критичних недоліків безпеки в цільовому середовищі. Іноді цю операцію називають оцінкою вразливості. Сканування вразливостей – одне з основних завдань програми виявлення та усунення цих недоліків. З його допомогою можна проаналізувати всі елементи керування безпекою IT-інфраструктури. Сканування вразливостей проводиться після того, як було зібрано та перераховано інформацію про інфраструктуру цільової

системи. Інформація, отримана після сканування системи на вразливості, може призвести до компрометації цільової системи, порушення її цілісності та конфіденційності.

Існує три основні категорії вразливостей, які, у свою чергу, можна поділити на локальні та віддалені. Це вразливість, допущена при розробці програмного забезпечення, помилки при реалізації програмного забезпечення та вразливість, що виявляються під час експлуатації системи.

Open Vulnerability Assessment System (відкрита система оцінки вразливостей, OpenVAS) – фреймворк, що складається з кількох сервісів та утиліт. OpenVAS – це сканер із відкритим кодом. Він простий в установці та має зручний інтерфейс, що дозволяє виконувати активний моніторинг (з активними діями у мережі). Відповідно до сайту http://www.openvas.org/about.html під час роботи OpenVAS використовує колекцію вразливостей, що складається з 50 000 тестів (NVTs). OpenVAS є основою лінійки професійних пристроїв Greenbone Secure Manager.

4.3. Мережеві атаки: методи злому та захисту. Wireshark – це потужний мережевий аналізатор, який може використовуватися для аналізу трафіку, що проходить через інтерфейс мережі вашого комп'ютера. Він може знадобитися для виявлення та вирішення проблем із мережею, налагодження ваших веб-додатків, мережевих програм або сайтів. Wireshark дозволяє повністю переглядати вміст пакета на всіх рівнях. Всі пакети перехоплюються в реальному часі та надаються у зручному для читання форматі. Програма підтримує дуже потужну систему фільтрації, підсвічування кольором та інші особливості, які допоможуть знайти потрібні пакети.

Головне вікно програми містить список доступних для аналізу мережевих інтерфейсів.

Після запуску аналізу мережевого інтерфейсу

відкриється вікно вже з потоком пакетів, які проходять через інтерфейс. Це вікно також поділено на кілька частин: Верхня частина – це меню та панелі з кнопками керування; Список пакетів – далі відображається потік мережних пакетів, які ви аналізуватимете; Вміст пакету – трохи нижче розташований вміст вибраного пакета, він розбитий за категоріями в залежності від транспортного рівня; Реальне уявлення – у самому низу відображається вміст пакета у реальному вигляді, і навіть у вигляді HEX.

Перебирати пакети вручну, щоб знайти потрібні дуже незручно, особливо при активному потоці. Тому для такого завдання краще використовувати фільтри. Для введення фільтрів під меню є спеціальний рядок. Ви можете натиснути «Expression», щоб відкрити конструктор фільтрів, але їх дуже багато, тому ми розглянемо лише найголовніші

Фільтри Wireshark :

ip.dst – цільова IP-адреса;

ip.src – IP-адреса відправника;

ip.addr – IP відправника чи одержувача; ip.proto - протокол;

tcp.dstport – порт призначення; tcp.srcport – порт відправника;

ip.ttl – фільтр по TTL, визначає мережну відстань;

http.request_uri– запитувана адреса сайту.

Для вказівки відносин між полем і значенням у фільтрі можна використовувати такі оператори:

= =– рівне; != – не рівне;

<– менше; >– більше;

<=– менше чи одно;

>= – більше чи одно;

matches– регулярне вираження; *contains* – містить.

Для поєднання кількох виразів можна застосовувати:

&&- обидва вирази повинні бути вірними для пакета; ||- може бути вірним один із виразів.

Тепер розглянемо на прикладах кілька фільтрів і спробуємо зрозуміти всі знаки відносин. Спочатку відфільтруємо всі пакети, надіслані на 142.250.180.206 (google.com). Наберіть рядок у полі фільтра та натисніть Apply:

```
ip.dst == 142.250.180.20
```

Для зручності фільтри Wireshark можна зберігати за допомогою кнопки «Save». А щоб отримати не лише відправлені пакети, а й отримані у відповідь від цього вузла, можна поєднати дві умови:

```
ip.dst == 142.250.180.206 || ip.src ==
142.250.180.20
```

Далі можна відібрати пакети з ttl менше 10:

```
ip.ttl < 1
```

Також можна відібрати надіслані великі файли:

```
http.content_length > 500
```

Відфільтрувавши Content-Type, ми можемо вибрати всі зображення, які були завантажені; для цього виконаємо аналіз трафіку Wireshark, пакети якого містять слово image:

```
http.content_type contains ima
```

Аналіз трафіку Wireshark

Для того щоб зрозуміти, що саме завантажували користувачі і які файли вони дивилися, якщо з'єднання не було зашифровано, можна за допомогою Wireshark вилучити контент. Для цього спочатку необхідно зупинити захоплення трафіку за допомогою червоного квадрата на панелі. Потім відкрийте меню File -> Export Objects -> HTTP:

Далі у вікні ви побачите всі доступні перехоплені об'єкти. Вам достатньо експортувати їх до файлової системи. Ви можете зберігати як зображення, так і музику. Далі ви можете виконати аналіз мережного трафіку Wireshark або відразу відкрити отриманий файл іншою програмою, наприклад, плеєром.

Wireshark – це дуже потужна утиліта, яка має багато функцій. Проте всю її функціональність неможливо охопити за один раз, але наведення базової інформації буде цілком достатньо, щоб ви змогли самі освоїти все необхідне.

5. МЕТОДИ ОЦІНЮВАННЯ ЗНАНЬ

Для визначення рівня засвоєння студентами навчального матеріалу використовуються наступні методи оцінювання знань та оціночні бали за їх виконання:

– оцінка за тестові п’ятихвилинки по лекційним матеріалам;

– оцінка за виконання практичних завдань; – модульні контрольні роботи;

– підсумковий екзамен.

Для діагностики знань використовують ЄКТС зі 100-бальною шкалою оцінювання.

№ з/п	Види навчальної діяльності	Бал
1.	Відвідування лекційних занять	0,5 б. за 2 год.
2.	Відвідування семінарських занять	1 б. за 2 год.
3.	Тестова п’ятихвилинка по лекційним матеріалам	2 б.
4.	Виконання практичних завдань	2-5 б. за 1 заняття
5.	Підготовка мультимедійних презентацій	3 б. за 1 тему
6.	Участь у конкурсі студентських наукових робіт	10 б.
7.	Участь у олімпіаді або в засіданні круглого столу	3 б.
8.	Виступ з доповіддю на студентській науковій конференції (в т. ч. в іншому вузі)	5-6 б.
9	Призове місце в олімпіаді чи конференції	5 б.

6. РОЗПОДІЛ БАЛІВ, ЩО ОТРИМУЮТЬ СТУДЕНТИ

Модуль 1– поточне опитування та СРС				Модуль 2 – поточне опитування та СРС				Підсумковий модульний контроль	Сума (іспит
Т.1	**Т.2**	**Т.3**	**Т.4**	**Т.5**	**Т.6**	**Т.7**	**Т.8**	**40**	**100**
5	5	10	10	5	10	10	5		

Шкала оцінювання

Сума балів за всі форми навчальної діяльності	**Оцінка за національною шкалою**	
	для екзамену	**для заліку**
90-100	відмінно	зараховано
82-89	добре	
74-81		
64-73	задовільно	
60-63		
35-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

7. ЛІТЕРАТУРА

1. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
2. Кавун С. В. Інформаційна безпека : навчальний посібник. Харків : Вид. ХНЕУ, 2020. 352 с.
3. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Видавництво: Дакор, Консалтингова компанія Сідкон, 2022. 284 с.
4. Когут Ю. Корпоративна безпека: практичний посібник. Видавництво: Дакор, Консалтингова компанія Сідкон, 2021. 460 с.
5. Методи та засоби захисту інформації : навчальний посібник / В. А. Лахно, Є. В. Василіу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. К. : ЦП «Компринт» О. В., 2020. 444 с.
6. Мистецтво залишатися непоміченим. Хто ще читає ваші мейли / пер. з анг. О. Асташова. К. : Наш Формат, 2019. 280 с.
7. Могильний С. Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник, 2018. К., 2018, 105 с. URL: http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne
8. Андрощук Г. Глобальні стандарти етики штучного інтелекту. *Інтелектуальна власність*. 2021. № 11. С. 34–41.
9. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2021. 554 с.

10. Гупта С. Цифрова стратегія. Посібник для переосмислення бізнесу. Видавництво «КМ-БУКС», 2020. 320 с.
11. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань» : монографія. Київ-Одеса : Фенікс, 2021. 176 с.
12. Зянько В. В. Раціоналізація бізнесової поведінки підприємств України шляхом аналізу переваг танебезпек конкурентної розвідки та промислового шпигунства. *Причорноморські економічні студії*. 2016. Вип. 6. С. 187–191
13. Інтеграція цифрових технологій в освітній процес: виклики та перспективи: монографія / Саєнко Н. С., Голуб Т. П., Лавриш Ю. Е., Лук'яненко В. В., Литовченко І. М. Видавництво: Центр навчальної літератури, 2022. 220 с.
14. Кулініч О. О. Охорона та захист прав інтелектуальної власності: економіко-правові підходи. Видавництво «Ліра-К», 2019. 276 с.
15. Ланде Д. В., Правові питання конкурентної розвідки. *Інформація і право*. 2020. 2(33). С. 51–68. DOI: https://doi.org/10.37750/2616- 6798.2020.2(33).208089
16. Матюшко В. І. Аналітичне дослідження. Широкосмуговий доступ до Інтернету в Україні: стан та перспективи. - Intel, 2012, 146 с.
17. Рейнська В. Б., Кухарчук І. А. Соціальні характеристики медіатехнологій: інформаційно-безпековий підхід. *Сучасні проблеми гуманітаристики: світоглядні і правові підходи, комунікативні та педагогічні стратегії:* Матеріали X Всеукр. наук.-практ. конфер. / Редкол. Бошицький Ю. Л., Вєтров І. В., Українець С. Я. 7 грудня 2023. 295 с.
18. Росс А. Індустрії майбутнього. Видавництво «Наш Формат», 2022. 320 с.

19. Роуз Д. Цифровий брендинг. Видавництво «Фабула», 2020. 256 с.
20. Скіннер К. Людина цифрова. Видавництво «Фабула», 2020. 272 с.